NOVA SCHOOL OF SCIENCE & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

RÚBEN ANDRÉ LETRA BARREIRO

Bachelor in Computer Science

SEMI-QUANTUM CONFERENCE KEY AGREEMENT (SQCKA)

A CRYPTOGRAPHIC PROTOCOL OF KEY AGREEMENT FOR MULTIPLE PARTIES, IN SEMI-QUANTUM CONTEXTS

COMPUTER SCIENCE

NOVA University Lisbon
March, 2022

NOVA SCHOOL OF
SCIENCE & TECHNOLOGY

DEPARTMENT OF
COMPUTER SCIENCE

SEMI-QUANTUM CONFERENCE KEY AGREEMENT (SQCKA)

A CRYPTOGRAPHIC PROTOCOL OF KEY AGREEMENT FOR MULTIPLE PARTIES, IN SEMI-QUANTUM CONTEXTS

RÚBEN ANDRÉ LETRA BARREIRO

Bachelor in Computer Science

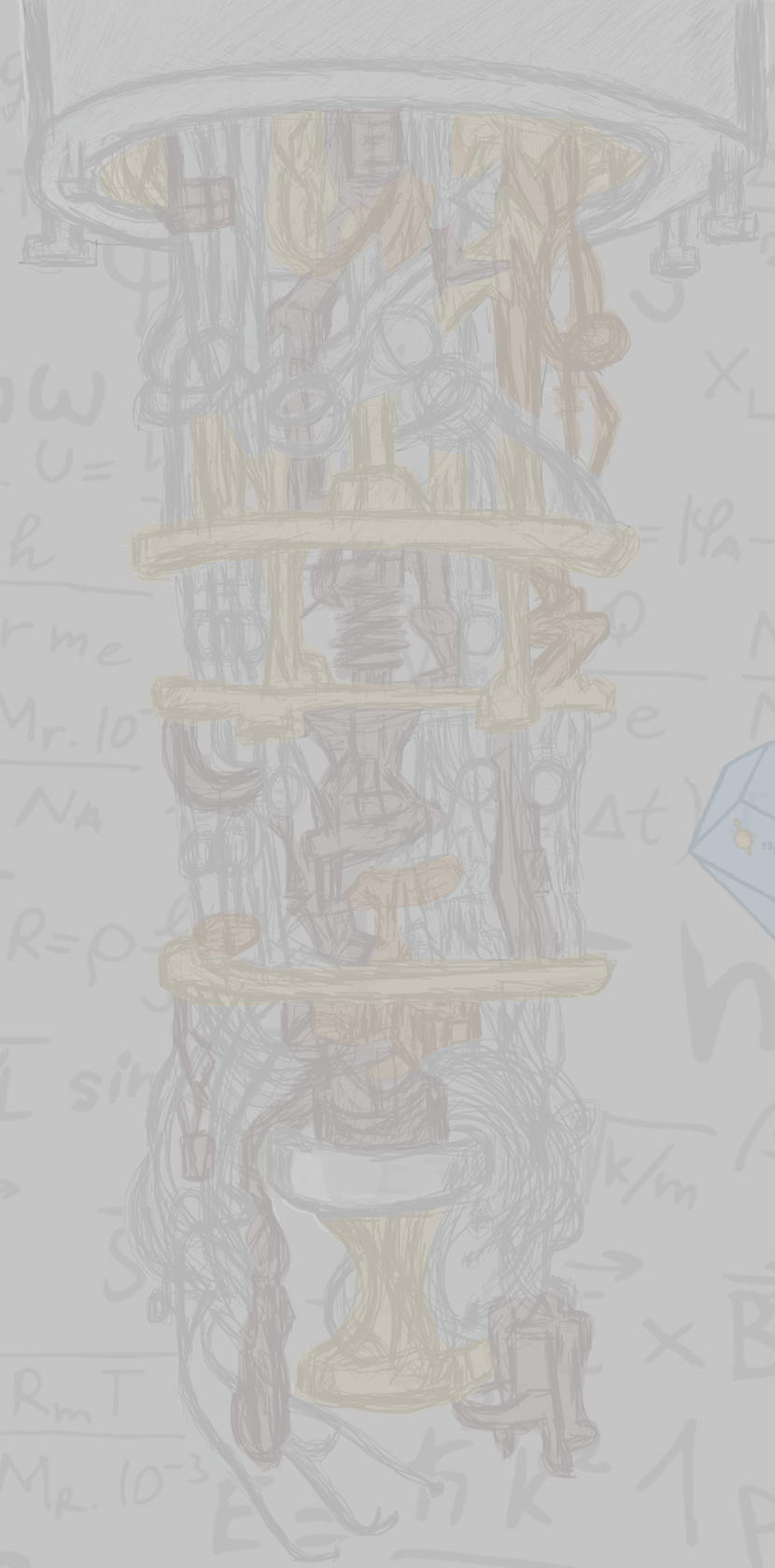
Adviser: André Nuno Carvalho Souto
Assistant Professor, Faculty of Sciences, University of Lisbon

Co-adviser: António Maria Lobo César Alarcão Ravara
Associate Professor, NOVA University Lisbon

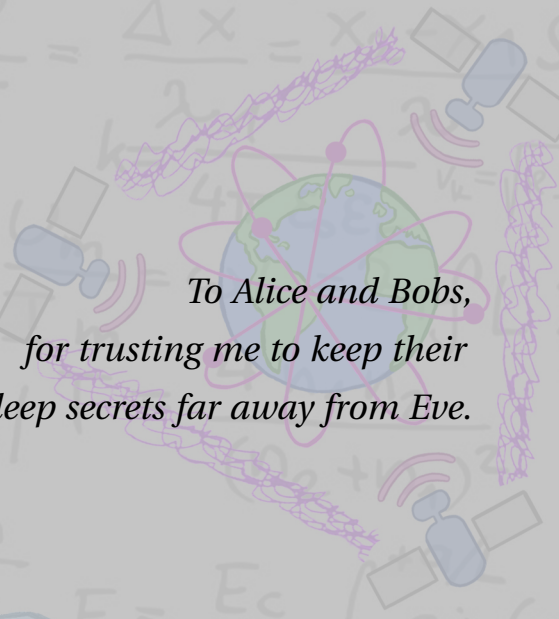
COMPUTER SCIENCE

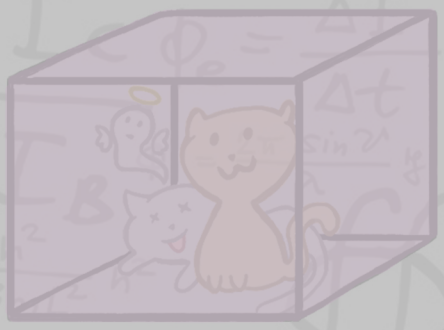
NOVA University Lisbon
March, 2022

Semi-Quantum Conference Key Agreement (SQCKA)



To Alice and Bobs,
for trusting me to keep their
deep secrets far away from Eve.





ACKNOWLEDGEMENTS

Before all, I want to thank my mother for being the woman of my life. I'm grateful for her advice, support, and wisdom in the worse moments of my life. Although initially, she never supported too much the idea of me doing a Master's Thesis in Quantum Computing, thinking that it would be a difficult topic to work on and invest my time in, she never gave up on me.

Similarly, I would also like to thank Catarina for her constant love and patience during this phase of my life. Without her enormous support and care, this task would be much harder.

I also want to thank Pedro, a good friend of mine, for all the good bits of advice over the years and his funny personality, reason why I want to dedicate this Master's Thesis to him.

I couldn't do this Master's Thesis without the collaboration and guidance of some people during this risky, terrifying, and unprecedented Quantum Physically Experience.

First, I need to thank Prof. André Souto. His constant availability to listen to some of my no sense ideas and his infinite patience to deal with my fears and doubts were valuable. He always put me on the correct trail, several times, when sometimes I started to feel my head spinning around, similarly to what happens to the Photons and Electrons in Physics.

Then, I would like to thank also to Prof. Paulo Mateus and Prof. Nikola Paunković for their huge (and unique) sense of humor and graciousness. They made me laugh and always see the funny side in some moments of a wretch. They also introduced me, to the importance of some topics of Quantum Mechanics and Quantum Cryptography, in the current days.

Of course, I also need to thank Prof. Walter Krawec for his collaboration in the work I developed during this Master's Thesis. Additionally, I need to thank Prof. António Ravara for always supporting and encouraging me to work on this scientific area from the beginning.

Other special thanks (for diverse reasons) go to Prof. Hervé Paulino, Prof. Ana Custódio, Prof. Pedro Medeiros, Prof. Isabel Oitavém, Prof. Ruy Costa, Prof. Ludwig Krippahl, Prof. Yasser Omar, Prof. Stephanie Wehner, Prof. Eleni Diamanti, and Prof. Scott Aaronson.

Finally, I would like to thank some institutions and organizations, such as, Instituto Superior Técnico, Universidade de Lisboa, NOVA School of Science and Technology, NOVA University of Lisbon, Security Quantum Information Group, Instituto de Telecomunicações, INESC ID, Fundação Calouste Gulbenkian, Quantum Flagship, TU Delft, University of Connecticut, UT Austin Portugal Program and Carnegie Mellon University Portugal Program.

“God does not play dice with the Universe.” (Albert Einstein)

ABSTRACT

A need in the development of secure quantum communications is the scalable extension of key distribution protocols. The greatest advantage of these protocols is the fact that its security does not rely on mathematical assumptions and can achieve perfect secrecy. In order to make these protocols scalable, has been developed the concept of Conference Key Agreements, among multiple users.

In this thesis we propose a key distribution protocol among several users using a semi-quantum approach. We assume that only one of the users is equipped with quantum devices and generates quantum states, while the other users are classical, i.e., they are only equipped with a device capable of measuring or reflecting the information. This approach has the advantage of simplicity and reduced costs.

We prove our proposal is secure and we present some numerical results on the lower bounds for the key rate. The security proof applies new techniques derived from some already well established work.

From the practical point of view, we developed a toolkit called Qis|krypt⟩ that is able to simulate not only our protocol but also some well-known quantum key distribution protocols. The source-code is available on the following link:
- https://github.com/qiskrypt/qiskrypt/.

Keywords: Quantum, Mechanics, Physics, Optics, Cryptography, Cybersecurity, Communications, Computing, Quantum Mechanics, Quantum Physics, Quantum Cryptography, Quantum Communications, Quantum Computing, Computer Science, Informatics, Key Agreement Protocols

Resumo

Uma das necessidades no desenvolvimento de comunicações quânticas seguras é a extensão escalável de protocolos de distribuição de chaves. A grande vantagem destes protocolos é o facto da sua segurança não depender de suposições matemáticas e poder atingir segurança perfeita. Para tornar estes protocolos escaláveis, desenvolveu-se o conceito de Acordo de Chaves de Conferência, entre múltiplos utilizadores.

Nesta tese propomos um protocolo para distribuição de chaves entre vários utilizadores usando uma abordagem semi-quântica. Assumimos que apenas um dos utilizadores está equipado com dispositivos quânticos e é capaz de gerar estados quânticos, enquanto que os outros utilizadores são clássicos, isto é, estão apenas equipados com dispositivos capazes de efectuar uma medição ou refletir a informação. Esta abordagem tem a vantagem de ser mais simples e de reduzir custos.

Provamos que a nossa proposta é segura e apresentamos alguns resultados numéricos sobre limites inferiores para o rácio de geração de chaves. A prova de segurança aplica novas técnicas derivadas de alguns resultados já bem estabelecidos.

Do ponto de vista prático, desenvolvemos uma ferramenta chamada Qis|krypt⟩ que é capaz de simular não só o nosso protocolo como também outros protocolos distribuição de chaves bem conhecidos. O código fonte encontra-se disponível no seguinte link:
- https://github.com/qiskrypt/qiskrypt/.

Palavras-chave: Quântica, Mecânica, Física, Óptica, Criptografia, Cibersegurança, Comunicações, Computação, Mecânica Quântica, Física Quântica, Criptografia Quântica, Comunicações Quânticas, Computação Quântica, Ciências da Computação, Informática, Protocolos de Acordo de Chaves

Contents

List of Figures

List of Tables

CHAPTER 1

INTRODUCTION

1.1 Historical Review and Context

We often wonder what mankind's invention or achievement was the greatest of them all...

Many will say it was the discovery of fire, while others say it was the invention of the wheel. The building of spaceships and rockets that made it possible for Neil Armstrong to be the first man ever to travel to the moon was also considered an enormous achievement of humanity.

Other younger people will probably say that it was the invention of the Internet and the WWW (World Wide Web). It is easy to see that this magnificent technology allows us to be connected worldwide, regardless of the distance involved, completely changing our lives.

But have we already accomplished the best achievements of our entire history? Have we discovered all that is unknown? Can we better understand the natural world around us? Or can we even fully understand our nature or consciousness? Can we fully comprehend how our brains work? Most of these questions still remain unanswered in the current days...

Perhaps we are about to create a wonderful and magical tool to help us on this exciting journey: the *Quantum Computers*! The Quantum Computing field, despite its hype, is still in its infancy. Yet, we do not know what problems these new devices can solve and how. It is also unknown what new possibilities Quantum Computing will offer us. However, it is reasonable to think that we can also consider this achievement one of the greatest in our history!

1.1.1 The 1^{st} Quantum Revolution: Discovering Quantum Mechanics

Since our beginnings, we have always struggled to understand the principles of nature, time, and reality, as well how the world and universe that surrounds us fundamentally work. And Quantum Mechanics seems to be the best tool we currently have to describe these principles.

Indeed, Quantum Mechanics is perhaps the most successful theory ever formulated!

Throughout the 1800s, most physicists considered Isaac Newton's *Dynamical Laws* [1] as being unquestionable. But it became increasingly clear during the next century that many physical phenomena, especially those related to radiation, absolutely defy Newtonian physics.

Thomas Young revealed the probabilistic nature of Quantum Mechanics and all its strange phenomena, in 1801, with his *Double-Slit Experiment* [2]. In this experiment, he showed that light behaves like both a wave and a particle, at the same time, in their classical definition.

This experiment introduced one of the most important requirements for the development of Quantum Computers: the *Interference*! And this experiment was just the starting point for what we would know as the *Old Quantum Theory*, between the XIX and XX centuries.

Half a century later, in 1860, Gustav Kirchhoff demonstrated that the emissive power of a black-body depends only on its frequency and on its temperature [3]. This claim gave the origin of both radiation and matter branches currently studied in Quantum Mechanics.

By following this claim, both experimentalists and theoreticians were challenged to find such dependencies. In 1893, Wilhelm Wien showed his *Displacement Law* [4], and in 1896, he proposed an exponential meaning to that dependence [5]. However, the black-body radiation problem only met its solution in 1900, when Max Planck modified that dependency with an exceptional success, which still holds nowadays, by introducing his own constant [6].

Also in 1900 and 1901, Max Planck suggested that the radiation, being matter or light, is quantized in discrete values, giving rise to the term *quantum* itself [7]. A *quantum* (or *quanta*, in plural) is the minimum and indivisible amount of any physical entity and property involved in an interaction. However, some entities and properties still take on continuous values.

In 1905, inspired by Planck, Albert Einstein suggested that radiation existed in spatially localized packets, proposing the *quanta* of light for them [8], or photons[1], as we call them today. One year later, he also proposed the well-known *Particle-Wave Duality of Photons* [9].

Some years later, in 1911, Hans Geiger and Ernest Marsden, under the direction of Ernest Rutherford, showed conclusively that a hydrogen atom comprises one electron outside the positively charged nucleus, where almost all the mass is concentrated [10]. This work is known as Rutherford's Model. Namely, electrons were supposed to be just particles but were verified later that they also behave like waves. In 1913, Niels Bohr and Ernest Rutherford improved that model, proposing the Rutherford–Bohr's Model (or just Bohr's Model) [11]. This improvement mainly concerned the new quantum physical interpretation, considering its quantization and describing its discrete energy levels, where electrons can revolve in a definite shell.

Between 1916 and 1917, Albert Einstein made huge contributions to the theory of radiation, combining classical thermodynamics and electromagnetism with Niels Bohr's postulates [12].

Later on, in 1919, during his experiments, Ernest Rutherford found the first evidence ever for a proton, when he found that nitrogen nuclei and other light elements ejected what he suspected was "a hydrogen atom" when he bombarded it with energetic alpha particles [13].

Additionally, in 1924, Louis de Broglie proposed that matter has wave properties [14], while one year later, Wolfgang Pauli formulated the exclusion principle for electrons in an atom [15].

[1] The term "photon" was only coined during the 1920s.

Also in 1925, Niels Bohr, Hans Kramers, Werner Heisenberg, and Wolfgang Pauli addressed the ongoing crisis in Quantum Mechanics, in Copenhagen, starting the transition from the *Old Quantum Theory* to the *Full-Fledged Quantum Mechanics* [16–18]. During this time, Werner Heisenberg successfully formulated the theory only in terms of "observable" quantities, to treat the behavior of electrons, carrying away the concepts of orbits and trajectories. Here, these "observable" quantities are the frequencies of light that atoms absorbed and emitted. This new type of formulation of Quantum Mechanics was mainly based on unitary matrices.

One year later, in 1926, Erwin Schrödinger developed wave mechanics by formulating a wave equation that accurately calculated the energy levels of electrons in atoms, assuming that matter, such as electrons, could be regarded as being both particles and waves [19].

In the same year, Max Born gave a probability interpretation of Quantum Mechanics, when he stated that the probability density of finding a particle at a point, when measured, is proportional to the squared magnitude of the particle's wave-function at that point [20–22].

In 1927, Werner Heisenberg formulated the well-known *Principle of Uncertainty*, by setting the fundamental limits for how accurate physical quantities of a particle, such as position, momentum, and velocity, can be simultaneously predicted, from its initial conditions [23].

Also in 1927, happened what is perhaps the most famous Solvay Conference on Physics, mainly focused on Electrons and Photons. The world's most notable physicists met there to discuss the newly formulated *Quantum Theory*. Some participants of this conference were Erwin Schrödinger, Wolfgang Pauli, Werner Heisenberg, Hans Kramers, Paul Dirac, Louis de Broglie, Max Born, Niels Bohr, Max Planck, Marie Curie, Hendrik Lorentz, and Albert Einstein.

Additionally, Paul Dirac combined both Quantum Mechanics and Albert Einstein's *Special Relativity Theory*, in 1928, to formulate a *Fully Relativistic Quantum Theory*, making Quantum Mechanics to finally become well established [24]. The equation developed by Paul Dirac gave solutions he interpreted as being caused by an unknown particle equivalent to the electron, but with a positive charge. This unknown particle was confirmed to be the positron[2], the first evidence ever of antimatter, through experiments performed by Carl Anderson in 1932 [25].

In the early 1930s, electrons, protons, and photons were demonstrated to be the first-ever identified fundamental particles[3]. However, nowadays, protons are no more considered as being fundamental particles. Since, through Quantum Theory, they were found to contain quarks. And quarks are now considered fundamental particles, in the current *Standard Model*.

More than half a decade later, in 1935, Erwin Schrödinger proposed the famous *Schrödinger's Cat Experiment*, during a discussion with Albert Einstein, to illustrate the paradox of quantum superposition, as well as the *Copenhagen Interpretation* of Quantum Mechanics [26].

We currently address all these events and achievements as the 1^{st} *Quantum Revolution*! And they gave us the rules that govern physical reality, at the atomic and subatomic levels. *De facto*, they helped us to interpret and understand a substantial part of everything in our lives!

[2]Initially, Carl Anderson did not coin the term "positron" but allowed it at the suggestion of the Physical Review journal editor to whom he submitted his discovery paper.

[3]A fundamental particle (or elemental particle) is a subatomic particle that is not composed of other particles.

1.1.2 The rise of Information and Computing

As the world progresses in this never-ending chase for time and wealth, it is undeniable that computer science has made astounding developments. They help us execute complex and complicated tasks much quicker, in an efficient manner. It is almost impossible to imagine modern facilities without the use of computers. And just as computers have become essential in our lives, so is technology. It can be powerful and have an enormous impact on everything.

It influences the way we communicate, learn, and think. It can help society and determine how people interact with each other daily. It can bring people together or drive them away.

Or it can support and transform education, making it easier for teachers and lecturers to create instructional materials, enabling new ways for individuals to learn and work together.

It can even help us in healthcare services by providing the best diagnostic tools, innovative treatments, and minimally invasive procedures, resulting in less pain and quicker healing.

In sciences, it allows scientists to explore nature in different ways and make discoveries. It provides a source of novel and more challenging scientific questions, helping to justify the allocation of resources needed to address them in an efficient and timely manner. It also works as a source of unavailable instruments and techniques desired to address those questions.

For these reasons, it plays a crucial role today, having positive and negative effects on the world. And recently, it became even more important because of the COVID-19 pandemics.

We are living in an era where technological advances are frequent and necessary! But can these technologies become more powerful? Can we develop new technologies different from those we know today? Could they help us make discoveries and solve brand-new problems?

To find the first attempt to represent the information, we must go back some 40, 000 years ago. In prehistoric times, cavemen already used pet paintings to illustrate information about wild animals, symbols, or religious beliefs and practices. It was also painted abstract patterns, or even traces of human hands, as the personal signatures of the "artist" who painted them.

Then, between 2,700 B.C. and 2,300 B.C., the Sumerians created the earliest computational tool known, the *Sumerian Abacus* [27], in Babylon. The *Abacus* (also called *Counting Frame*) is a calculating tool composed of rows of movable beads strung on a wire. These beans represent digits and allow mathematical operations, such as addition, and even a square or cubic root.

But it was necessary to wait until the XIX century to have the first automated machines, slightly similar to what we have today. In 1801, Joseph Jacquard invented a loom based on punched wooden cards which automatically weave fabric designs in France [28]. Following this idea, the early known computational devices would also use that similar punched cards.

Two decades later, in 1822, Charles Babbage conceived a steam-driven calculating machine capable of computing tables of numbers [29]. This machine was part of a project funded by the English Government, but it was a failure. In fact, we needed to wait more than a century to have the world's first digital computer machine built during WWII (World War II) in the 1940s.

Inspired by the first computational devices based on punched cards, Herman Hollerith designed a similar system in 1890 [30, 31], which computed the 1880 census in just three years.

This performance saved the American government $5 million. He also established a company that would ultimately become IBM (International Business Machines) a few years later.

However, if the XIX century presented a considerable technological advance, the XX century even more so! Many current technologies we use started to be thought out during these times...

Between 1935 and 1937, Alonzo Church and Alan Turing presented us with a change of paradigm given by their Church-Turing Thesis [32–35]. Their work introduced a universal machine (or Turing Machine), as any machine capable of computing anything computable through efficient methods. The main concept of the modern computer is based on their ideas.

Also in 1937, John Atanasoff tried to build the first electronic digital computer without gears, cams, belts, or shafts [36]. Four years later, in 1941, he and his graduate student, Clifford Berry, designed a computer that could solve 29 equations simultaneously [37]. This achievement marked the first time a computer was able to store data and information on its main memory.

Then, between 1943 and 1946, John Eckert and John Mauchly built the ENIAC (Electronic Numerical Integrator And Calculator) as the first programmable, electronic, general-purpose digital computer [38]. It was considered the grandfather of digital computers, and it filled a 20-foot by 40-foot room and had 18,000 vacuum tubes. In 1946, they received funding from the American Census Bureau to build the UNIVAC (UNIVersal Automatic Computer) as the first commercial electronic digital computer for business and government applications [39].

Another landmark was the introduction of the Von Neumann Architecture by John von Neumann in 1945 as a model for computer architecture [40]. Namely, this model describes a stored-program computer concept, storing instruction and program data, in the same RW-RAM (Read-Write and Random-Access Memory), still used in most computers produced.

Later, we took an enormous step toward computational growth when William Shockley, John Bardeen, and Walter Brattain of Bell Labs invented the Transistor in 1947 [41–43]. They discovered how to make an electric switch with solid materials and with no need for a vacuum. This notable achievement contributed to their winning Nobel Prize in 1956 for their researches on Semiconductor Devices and their remarkable discovery of the Transistor field effect [44].

In 1948, Frederic Williams, Tom Kilburn, and Geoff Tootill designed and introduced one of the first programmable computers, the Manchester Mark 1 [45–47]. It was used for many purposes, including investigation of the Riemann hypothesis and some calculations in optics.

Extending the earlier idea of William Shockley, John Bardeen, and Walter Brattain, when they invented the Transistor, Jack Kilby and Robert Noyce produced in 1958 the first-ever IC (Integrated Circuit) [48–50]. This component is also known as Computer Chip, Silicon Chip, or just Microchip. It is one of the main components of any computational device we use today. Later, in 2000, Jack Kilby was awarded the Nobel Prize in Physics for his research work [51, 52].

Following the growing manufacturing trend of Transistors and ICs, the newly formed Intel unveiled the Intel 1103, the first DRAM (Dynamic Random Access Memory) chip, and the Intel 4004, the first commercially available microprocessor, in 1970 and 1971, respectively [53].

All of these events and technological advances only prepared us in a way for the beginning of what is probably the most prosperous period in technology: the Digital Information Age!

1.1.3 The birth of the Digital Information Age

In the present, we are all surrounded by data, information, and technology almost everywhere. Computers, smartphones, tablets, or any other similar computational devices have become essential in our quotidian. We can even look at the digital platforms and social networks as being crucial frameworks. Most people nowadays cannot even imagine their lives without them. Everyone now is linked worldwide, practically at a distance of just a single "click".

Over the last years, we entered a new age of technology due to the advances in computing and telecommunications that started in the mid-XX century, mainly because of the beginning of the Internet and WWW. We first started living in the Digital Information Era a few decades ago, or the lovely epoch of IoT (Internet of Things) more recently. Both of these landmarks revolutionized society and industry, changing our lives totally, as never seen before.

In its Annual Internet Report (2018–2023) White Paper, Cisco estimated that existed 3.9 billion total Internet users (51% of the global population) in 2018 [54]. And in this report, Cisco predicts that there will be 5.3 billion total Internet users (66% of the global population) in 2023. This means that nearly two-thirds of the global population will have Internet access soon.

These mentioned technological advances made many research areas emerge over the years, such as Cloud Computing, Ubiquitous Computing, Fog and Edge Computing, or even Smart Cities. And all these new trends demand massive data storage and bandwidth capabilities. This new trend will not only allow us to be connected, but it will allow all smart devices or to communicate among themselves via cloudlets or similar technologies. And, these smart devices could be anything, from a simple coffee machine to an autonomous vehicle.

In the future, smart cities will increase social activities and facilitate living conditions by creating sustainable mechanisms and ensuring the sustainability of cities. The IoT (Internet of Things) has become a prevalent system in which people, processes, data, and things connect to each other through the Internet. Globally, M2M (Machine-to-Machine) connections will grow from 6.1 billion in 2018 to 14.7 billion by 2023, so there will be 1.8 M2M connections for each member of the global population by 2023. And the connected home, car, and city applications via M2M connections will grow from 26% to 48% until 2023 [54]. This phenomenon will affect home security, video surveillance, tracking applications, fleet management, emergency calling, vehicle diagnostics and navigation, showing the pervasiveness of these technologies in our lives. This trend is growing so fast that some experts started to call it IoE (Internet of Everything).

But when and how about all this Internet phenomena started? How can we build efficient and fast communications like the ones we use today? How do we can encode information to transmit them to each other, even if we are physically far away apart? How did we transform these technologies to be pervasive? To answer these questions, we need to go back to the 1790s, when some experts started to think about more efficient ways of connecting people...

In 1792, Claude Chappe built the first-ever Optical Visual Telegraph (or "semaphore") [55] for a communication line between Lille and Paris and later between Paris and Strasbourg. This telegraph used two sets of jointed wooden beams moved by operators through cranks and wires. However, the last commercial lines of Optical Telegraphs were closed in the 1880s.

Almost 50 years later, in 1831, Joseph Henry invented the Electric Telegraph [56], which allowed to send and receive messages over long distances. Then, Samuel Morse invented the Morse Code as a method for the encoding of text characters in standardized sequences of two different signal durations, called dots and dashes (or dits and dahs), in 1835 [57, 58]. Two years later, William Cooke and Charles Wheatstone invented the Electrical Telegraph system [56]. A year later, Samuel Morse developed another type of Electrical Telegraph based on armature systems that use the electric current to activate a telegraph sounder, making the sound of a "click" [56]. However, just in 1844, we had the first-ever communication line of Electrical Telegraph in USA, which was accomplished jointly by Samuel Morse and Alfred Vail [56].

In the next decade, were made the first steps in overseas and continental communications via Electrical Telegraph. First, Cyrus Field succeeded in laying a Telegraph cable across the Atlantic in 1858 [59]. However, it failed after only a month. A few years later, Adelaide and Darwin were linked across the Australian continent by the Overland Telegraph Line in 1870.

One year later, Antonio Meucci filed a patent for the development of a voice-communication apparatus in New York [60]. However, we often credit Alexander Bell as being the inventor of the Telephone [60]. He was awarded the first-ever successful patent for the electromagnetic transmission of vocal sound by undulatory electric current between 1876 and 1877. He made the first practical use of his Telephone patent when called for his assistant from another room. In the same year, he also demonstrated his new invention at the USA's Centennial Exhibition.

In the following 20 years, it is worth mentioning Wireless Communication [61] and Remote Control [62], both created by Nikola Tesla in 1893 and 1898, respectively. Not least important, Guglielmo Marconi, inspired by Heinrich Hertz, invented Radio Signals between 1895 and 1896 for the wireless transmission of Telegraph signals by radio waves communications [63].

Between 1906 and 1907, Lee de Forest developed the Triode Vacuum Tube, called Audion [64], as the first Radio Amplifier, making wireless radio broadcasting practicable. And in 1910, he broadcasted an experimental transmission of a live Metropolitan Opera House performance by several famous opera singers, but with mixed success owing to the poor quality.

Then, in 1913, the USA's navy began transmitting a regular time signal by radio, much used by the nation's watchmakers and menders [65]. And two years later, Alexander Bell called again his assistant as before. But this time, he was in New York, and his assistant was in San Francisco. And, at the same time, radiotelephone messages were transmitted from Arlington in Virginia to the Eiffel Tower in Paris, demonstrating communications across the Atlantic again.

At the beginning of the second half of the XX century, in 1958, the Defence Department of the USA launched the ARPA (Advanced Research Projects Agency), currently known as DARPA (Defense Advanced Research Projects Agency) [66]. Just four years after, ARPA financed the ARPANET (Advanced Research Projects Agency NETwork) [67], between 1962 and 1966, with the idea of being the first-ever wide-area packet-switching network distributed control, enabling remote access to computers. The ARPANET was the experimental computer network that was the forerunner of the Internet we know today. Bob Taylor started this project based on the ideas of Joseph Licklider, who had proposed the Cloud Computing concept in 1963.

During these times, were also launched the first communication satellites. In 1962, NASA

(National Aeronautics and Space Administration), AT&T, and Bell Labs jointly produced and launched the Telstar 1 [68], the first communication satellite, allowing the first live broadcast of television images between the USA and Europe. Then, Hughes Aircraft built the Intelsat I [69] for COMSAT (COMmunications SATellite Corporation) for the first-ever commercial communications via satellite, launched in 1965, in Florida, USA, and deactivated in 1969.

Also between 1963 and 1965, Ted Nelson developed a model for creating and using linked content, coining the terms "hypertext" and "hypermedia" [70]. In 1967, he and Andries van Dam invented the HES (Hypertext Editing System) [71], with links and branching text.

In the following year, in 1968, BBN (Bolt Beranek and Newman Inc.) was selected to build an IMP (Interface Message Processor) [72]. One year later, they started to ship these IMPs to Universities and Research Institutes. In 1969, the first message was sent over the ARPANET, between the first two shipped IMPs. That message was supposed to be the word "LOGIN" transmitted between UCLA (University of California, Los Angeles) and SRI (Stanford Research Institute), both in USA. However, the system crashed right after being typed the "LO" part.

And at the beginning of the 1970s, we started living in what is probably the most remarkable era of technology, which is still ongoing nowadays: the Digital Information Age. This new technological era mainly rose with the introduction of the Internet [73], WWW [74], and PCs (Personal Computers) [75] to the civilization and all the applications they can provide daily.

The 1970s already started to be memorable, when in 1971, Ray Tomlinson invented the networked E-mail [76] as a system capable of send and receive mails between users on different hosts across the ARPANET. These e-mails used the "@" sign to link the username with a destination server, which by the mid-1970s was the form recognized as e-mail. Two years later, Robert Metcalfe and David Boggs developed Ethernet [77] for connecting multiple computers.

In parallel, the Internet as we know took its first steps. First, WHOIS [78] was released as one of the earliest domain search engines. Three years later, the first ".com" domain name was registered, and the Symbolics Computer Company [79] registered the "Symbolics.com", even before the formal beginning of Internet history. Over two years later, only one hundred of ".com"s had been registered. Finally, Tim-Berners Lee invented WWW [74] in 1989, and one year later, he developed the HTML (HyperText Markup Language) [80], leveraging the WWW.

After the creation of the WWW, the first-ever search engines appeared. In 1990, Alan Emtage developed Archie, the first search engine, as a tool for indexing FTP (File Transfer Protocol) [81] archives, allowing users to find specific files easily. In 1996, Sergey Brin and Larry Page started developing the Google search engine [82] as a research project. A year later, the domain name "www.google.com" was registered, and finally, Google [83] became established in 1998.

But should most of these technologies meet any security concerns? Do we need to address some confidentiality and privacy requirements when developing these applications that share data and information among the users? How can we guarantee such demands? How strongly do those demands need to be? Can those secure mechanisms last a considerable amount of time or even forever? Can we design effective or even unbreakable mechanisms? We can answer those questions and analyze such demands from the point of view of *Cryptography*.

1.1.4 A retrospective of Cryptography: From Ancient Egypt to Modern Times

To develop secure technologies and applications in scenarios that an unauthorized person or entity could try to gain access to the data and information involved, we need to ensure a set of assumptions, requirements, and properties. Areas such as Cryptography, Cryptanalysis, Cryptology aims to study these security aspects, being constantly revised and improved.

However, for simplification reasons, all these aspects are commonly just referred to as Cryptography. And it is from the need to exchange data and information in private, that the Cryptography field emerged as the study of secure communication techniques, allowing only a sender and a set of authorized receivers of a message to view its content. We achieve this by performing the processes of encryption and decryption. First, the sender encrypts the message to send to the receiver, by scrambling ordinary text (known as plain-text) into a transformed and unperceivable representation of it (known as cipher-text). Then, the receiver applies the reverse operation, decrypting that scrambled message and recovering its original content.

We define this scrambling process (or encryption) by a mechanism that would transform the content of an original message, usually called a cipher or encryption algorithm. Most specifically, this mechanism receives the original message as input, and possibly, a secret parameter (often denoted as secret key). For instance, this secret key determines the behavior of the cipher, being usually and inherently related to the difficulty of an unauthorized entity undoing the process, following a "try-and-guess" strategy. But if an entity has access to that secret parameter, it can easily undo the applied transformation to the original message.

To speak about Cryptography, we must return around $4,000$ years ago. The first evidence of Cryptography came from Ancient Egyptians, with complex Hieroglyphs [84] and Pictograms [85], written in tombs, chambers and walls. Those Hieroglyphs and Pictograms encoded secret messages often directed to the emperor or other high-ranked people, and only the scribes knew the secret encoding and were capable of unveiling their true meaning. This method of secret encoding (or encryption) is an example of Substitution Cipher, which is any cryptographic mechanism where one character or symbol is replaced by another one. As the Egyptian culture evolved, Substitution Ciphers using Hieroglyph and Pictogram symbols became more common. In fact, this method of encryption was relatively easy to break for those who could read and write. This seems to be very similar to formal and complicated language used in any modern legal document. The Ancient Egyptian Cryptography, at that time, could also have been a manner of a scribe impress others by showing that he could write at a higher level.

Some years later, about 500 B.C., the Spartans developed the Scytale [86], a device used to send and receive secret messages. This device was a cylinder in which they wound a narrow strip of parchment, and they wrote the confidential messages length-wise on that parchment. Once someone unwound the parchment, the secret message became unreadable. To decipher the actual content of that secret message was needed an identical cylinder. Since it was only then that the characters would line up, resulting in the original message. The Scytale is an example of Transposition/Shifting Cipher, where a character or a symbol is shifted and has its order changed in the respective alphabet, rather than being replaced. In the current days, the

Scytale would be very easy to decipher. However, 2,500 years ago, just a few people could read or write, and thus, the Scytale provided the Spartans a secure method of communication.

The earliest military use of Cryptography came from the Roman Empire, around 2,000 years ago. During these times, the emperor Julius Caesar, as the commander of the Roman army, solved the dilemma of making secure communications with his troops. He and his troops developed a Transposition/Shifting Cipher, in which they shifted characters of the alphabet [87]. Only those who knew the fixed number of positions to shift could decipher the secret messages. The messengers delivering those confidential messages did not know that shifting parameter. Thus, if someone caught the messengers, they could not expose the actual content of those secret messages. This gave the Roman army a tremendous advantage during the war.

Later, during the mid-1400s, Leon Alberti invented an encryption system using a cipher disk [88]. This system was a mechanical device with sliding disks that allowed many methods of substitution. This is the base concept of a Poly-Alphabetic Cipher, as an encryption method that switched through several substitution ciphers throughout the encryption process.

In the 1500s, Blaise de Vigenère, taking inspiration from the earlier Alberti's Poly-Alphabetic Cipher, created a cipher that would be later known as the Vigenère Cipher [89]. The Vigenère Cipher worked similarly to the Caesar Cipher, except that it changes with a shifting parameter chosen from a keyword adopted as a secret key throughout the encryption process. This cipher used a grid of characters, giving the shifting parameter and the correspondent character to follow as a replacement. This grid was often called the Vigenère Square, or Vigenère Table.

During the 1700s, Thomas Jefferson came up with a cryptographic system very similar to the Vigenère Cipher, except with higher security [90]. His invention had 26 wheels, with the alphabet randomly scattered on each wheel. The wheels were numbered and ordered in a specific order, and this order worked as the secret key of the encryption algorithm.

The start of WWI (World War I) introduced two essential aspects in Cryptography. First, every time that a cryptographic system is "broken", a stronger one is developed. And second, the reveal of the success in "breaking" a cipher takes time to provide an adversarial advantage from which arise the concept of Cryptanalysis. In 1917, British cryptographers encountered a German encoded Telegram. We refer to this telegram as the Zimmerman Telegram [91]. These cryptographers deciphered this Telegram, and in doing so, they changed Cryptanalysis history. Using this decrypted message, they convinced the USA to join the war. The Zimmerman Telegram was a secret communication method between the Foreign Secretary of the German Empire, Arthur Zimmerman, to the German ambassador in Mexico, Heinrich von Eckardt.

At the end of WWI, Arthur Scherbius invented one of the most ever known cryptographic systems, an electro-mechanical machine called Enigma [92]. The Enigma had several rotors and gears that allowed up to 10,114 possible configurations and it was considered to be unbreakable with "brute-force" approaches, at these times. The first commercial versions were available in the 1920s and the Enigma gained its fame even before WWII. Because of the Enigma's statistical security, Nazi Germany became overconfident about its ability to encrypt secret messages. However, this overconfidence caused the downfall of the Enigma, in a certain sense. Along with several operator errors, the Enigma also had many built-in weaknesses

that Allies' Cryptographers exploited. The major weakness was that its Substitution Cipher mechanism did not allow any character to be mapped to itself. This fault allowed the Allies' Cryptographers to decrypt a huge number of ciphered messages sent by Nazi Germany.

Prior to the beginning of WWII, in 1938, Marian Rejewski designed the Bomba, or Bomba Kryptologiczna ("Bomb" or "Cryptologic Bomb") [93], a special-purpose machine for breaking the Enigma machine ciphers. In 1939, the Poles had been decrypting Enigma messages for over more than 6 years without telling their Allies. Then, they revealed their decryption devices and techniques to the Allies, making it possible for them to decrypt important secret messages of Nazi Germany. For instance, Alan Turing and Gordon Welchman created another version of the "Cryptologic Bomb", and from mid-1940s, German Air Force signals were being read at Bletchley Park and the intelligence gained from them was helping the war effort. However, the success in "breaking" the Enigma machine was only made public more than 20 years later.

While the Allies were focused on "breaking" the Enigma machine during WWII, the Japanese Navy developed a cryptographic system called Purple [94]. In contrast to the Enigma's rotors, the Purple machine was made using stepping switches commonly used for routing telephone signals. During the war, the Japanese were probably the most efficient ones in destroying their cryptographic machines, since nearly no complete Purple system has currently been discovered. Because the Japanese were so good at keeping their encryption methods secret, the American cryptographers had a rough time decrypting their messages. Later on, William Friedman, a renowned cryptographer, and his team built a replica of Purple based only on the encrypted messages recovered, but since they had never seen a Purple system and didn't know how it worked, this proved to be very difficult. Eventually, the team figured out the encryption method used by Purple, and they were able to build a different machine for the decryption of it [95]. This gave an advancement that allowed the USA to access Japanese diplomatic secrets.

However, were other Code-breakers used during WWII, such as the Colossus computers, developed between 1943 and 1945, to help in the Cryptanalysis of the Lorenz Cipher [96]. These Colossus computers[4] were designed by Tommy Flowers, and are also often regarded as the world's first programmable, electronic, digital computers for special purposes, although they were programmed by switches and plugs, not by stored data [97, 98]. A total of 10 Colossus were delivered, each using as many as 2,500 vacuum tubes. More specifically, a series of pulleys transported continuous rolls of punched paper tape, containing some possible solutions to a particular code. The 1^{st} prototype, the Colossus Mark 1, was shown working at the end of 1943. The 2^{nd} prototype, the Colossus Mark 2, had several improvements, such as the use of shift registers to quintuple the processing speed, which was worked for the first time, in mid-1944. The Colossus reduced the time needed to "break" messages encrypted with Lorenz Cipher, from weeks to hours. Thus, it is believed that the use of Colossus machines significantly shortened the time of the war by providing evidence of enemy intentions and beliefs. Once again, the existence of the Colossus computers was not made public until the 1970s.

At the beginning of the XX century, the OTP (One-Time Pad) [99] encryption algorithm was

[4] See more information in: https://www.tnmoc.org/colossus

invented and showed to be unbreakable since then. The OTP algorithm was derived from an early cipher called Vernam Cipher [100], created by Gilbert Vernam in 1917. The Vernam Cipher was an algorithm devised to encrypt TTY (TeleTYpe) messages, combining a message with a key read from a paper tape or pad [101]. We did not consider the Vernam Cipher as unbreakable until Joseph Mauborgne recognized that if the key was completely random, the difficulty of Cryptanalysis would be equal to attempting every possible secret key. Even when trying them, one would still have to review each decryption attempt, verifying if he used the proper key. Thus, the unbreakable property of the OTP came from two assumptions. First, the secret key used needs to be completely random. Second, that same key could not be used more than once since the security of the OTP also relies on keeping the key 100% confidential. The OTP is often implemented with the modular addition (XOR, or eXclusive OR) operation to combine the elements of the plaintext with the respective elements of the secret key. We should also use the same secret key used in the encryption for the decryption process. Then, performing the OTP with the same secret key to the ciphertext would result back in the plaintext.

Until 1972, there was no global standard cipher for encrypting secret or private messages. The NBS (National Bureau of Standards) of the USA, which later became the NIST (National for Standards and Technology), launched an initiative for finding a single secure algorithm for these purposes. The USA's Government had traditionally kept their knowledge of Cryptography to themselves since they considered it crucial to their national security. Because of the NIST initiative, they received several cipher proposals as candidates for the first encryption standard.

When the NIST examined the security of the cipher candidates, they reached out to the NSA (National Security Agency) for help. In 1977, the NIST presented an altered version of a proposal from IBM [102–105], as the new standard with a smaller secret key size, which they called the DES (Data Encryption Standard) [106]. It became the first modern, public, freely-available encryption algorithm. They made all the details regarding DES public, which is always a good practice since it allows researchers to inspect the mathematical formulation. However, the motivation for the design criteria remained secret. The public never learned why the secret key size was reduced, which resulted on some suspicion regarding the involvement of the NSA.

Initially, the DES was meant to be the standard cipher for encryption, from 1977 to 1987. However, no relevant weakness was found, and DES reigned as the standard algorithm for more than two decades, until 1999. During these times, several attempts were made to design and build a machine to attack it, following a Brute-Force approach, what would cost millions of dollars. It was speculated that only government agencies would have the financial resources to build it, and by this time, it was widely believed that the NSA could really "crack" DES.

As the price of hardware fell during the 1990s, the EFF (Electronic Frontier Foundation) built the machine Deep Crack [107, 108]. In 1998, Deep Crack could brute force DES in 56 hours. This event showed us that it was time to select a new standard cipher for encryption.

To prevent this type of attacks in the future, the NIST started an open competition to find a new standard encryption cipher in 1997. The competition had first five finalists: Rijndael [109], MARS [110], RC6 [111], Serpent [112] and TwoFish [113]. This time, the selection process was completely transparent. In 2001, after three competitive rounds and intense Cryptanalysis by

the world's foremost experts, they decided on the winner proposal. The cipher Rijndael [109], designed by Vincent Rijmen and Joan Daemen, was declared as the new encryption standard and was called AES (Advanced Encryption Standard) [114]. This cipher has three possible secret key sizes: 128 bits, 192 bits, and 256 bits. All these secret key sizes were sufficiently large to withstand Brute-Force attacks during these times. For this reason, AES is still widely regarded as the most secure encryption cipher invented and is still the standard in use nowadays.

At the beginning of the XXI century, we felt a significant management problem with the growth of the business industry, powered by the Digital Information Age. Due to the increasing number of secret keys to be distributed between companies and their customers, the direct handling of the secret keys became unbearable. However, Whitfield Diffie, Martin Hellman, and Ralph Merkle anticipated this problem in 1976 [115, 116]. They proposed the idea of key distribution as a workable solution, different from the current public-key cryptosystems. It was based on a pair of asymmetric keys, where one key is public, and the other is kept private.

This procedure, currently known as the Diffie-Hellman Key Exchange, made it possible to establish secret keys, with no need for two participants to share any previous information in advance. It allows an exchange of messages in public while ensuring confidentiality. For instance, it uses modular arithmetic operations and a one-way function, where its security is based essentially on the mathematical properties of the Discrete Logarithm Problem, believed to be computationally hard or an NP-Intermediate Problem, and thus, it is difficult to "break".

Later, in 1977, Ronald Rivest, Adi Shamir, and Leonard Adleman also proposed the RSA cryptosystem, extending the work of Diffie and Hellman [117]. In their cryptosystem, anyone would use the same "public" key to communicate with a user in private. This cryptosystem uses the Factorization Problem, which is a problem also considered as being computationally hard. Its security relies on the mathematical assumption that, if a very large prime number is used in it, it would be extremely difficult to compute the private-key in a reasonable and non-exponential amount of time, considering only the knowledge about the public-key.

Other cryptographic primitives were proposed recently, such as Digital Signatures [116–119], Elliptic-Curve Cryptography [120, 121], Interactive Proofs [122–128], Byzantine Agreements [129, 130], Cryptocurrencies [131, 132], Blockchains [133, 134], or Homomorphic Encryption [135–141].

But can these cryptographic primitives and key exchanges be safe against some future technologies? Can appear even more powerful computing machines in the future? And how can we build more robust cryptographic primitives against these new technologies? Would we still be base these new cryptographic primitives on mathematical assumptions? Or would we follow a novel approach for the future? Can these new cryptographic primitives provide unconditional feasible security? Maybe we will find the answers for these questions very soon...

1.1.5 The 2^{nd} Quantum Revolution: Enabling Quantum Technologies

Over the years, the experts always thought about new ways of developing even more powerful computing machines. But not even the most powerful conventional computers can solve all the computational problems... Could we build new models of computing machines provide

us with technological devices capable of solving those problems never solved before?

During the 1980s, Richard Feynman gave an initial perspective into a different manner of performing computations when he proposed harnessing Quantum Mechanics to build a new, more powerful type of computer distinct from the conventional ones we use nowadays [142].

As conventional computers grew in power, so theoretical physicists started to use them in computations and modeling of physical systems. However, they often struggled to develop ways of representing things that could exist in multiple states simultaneously. But in most cases, many of the systems that the physicist wants to investigate may have many millions of electrons, and the respective number of possibilities becomes unimaginably large. Then, this observation leads us to argue that these physical systems have an enormous complexity, explaining why conventional classical computers cannot simulate them quickly and efficiently.

In fact, Richard Feynman theorized we need to build Quantum Computers to simulate quantum physical systems efficiently. An idea that he postulated in 1982, in a paper entitled "Simulating Physics with Computers" [142], marking the "birth" of Quantum Computing.

Some years earlier, Roman Ingarden already tried to create a Quantum Information Theory in 1976 [143], showing that Claude Shannon's Information Theory does not generalize naturally to the case of Quantum Information. In 1982, Paul Benioff developed his original model of Quantum Turing Machine, when he published a paper that described a Quantum Mechanical Model of a Turing Machine, demonstrating the theoretical possibility of Quantum Computing [144]. A few years later, in 1985, David Deutsch and Roger Penrose gave us the definition of a Universal Quantum Turing Machine [145], extending the earlier work of Church-Turing Thesis.

The first known Quantum Algorithms were proposed in 1992, demonstrating beforehand speedups over their Classical counterparts. First, David Deutsch and Richard Jozsa proposed one of the first examples ever of a Quantum Algorithm, proving that there can be advantages of using a Quantum Computer as a computational tool for a specific problem [146]. Namely, in the respective Deutsch-Jozsa Problem, we have a black-box Quantum Computer known as an Oracle that implements some mapping function. In fact, this Quantum Algorithm showed that a Quantum Computer can solve a black-box problem efficiently with no error. A deterministic Classical Computer would need many queries to the black box to solve the same problem. Later, in 1998, Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca proposed improvements to this algorithm [147]. During these times, Ethan Bernstein and Umesh Vazirani proposed the Bernstein-Vazirani Algorithm [148], as a restrictive extension version of the earlier Deutsch-Jozsa Algorithm. This algorithm is devised to learn a string encoded in a function through a dot product and modular arithmetic. They also designed this Quantum Algorithm to demonstrate an Oracle separation between the complexity classes, BQP (Bounded-error Quantum Polynomial time) and BPP (Bounded-error Probabilistic Polynomial time).

Between 1993 and 1994, Daniel Simon invented an Oracle-based problem known as Simon's Problem [149], for which a Quantum Computer would be exponentially faster than a Classical Computer. We set this problem in the model of a Decision Tree or Query Complexity. This Quantum Algorithm introduced the main ideas used for the Quantum Fourier Transform and the later Quantum Algorithms for Factoring. In particular, it used only a linear number of

queries to solve Simon's Problem. In opposition, any probabilistic (or deterministic) Classical Algorithm would need an exponential number of queries. Similar to what we verified with the Bernstein-Vazirani Algorithm [148], the Simon's Algorithm also held an Oracle separation between the BQP and BPP complexity classes, but nowadays, this separation is exponential.

In 1994, Peter Shor, at AT&T's Bell Labs, during his Ph.D., developed the first-ever Quantum Algorithm for factoring [150, 151], which is exponentially faster than the best currently known algorithm running on a Classical Computer. His algorithm was an important discovery since it allows a Quantum Computer to factor large integer numbers quickly. For this reason, Shor's invention sparked a tremendous interest in Quantum Computing. Additionally, it is probably the most famous Quantum Algorithm because it can seriously affect the modern Cryptography.

Then, in 1996, Lov Grover, also from AT&T's Bell's Labs, invented a Quantum Algorithm for Database Search [152]. This Quantum Algorithm could also affect modern Cryptography soon. Its quadratic speedup is not as dramatic as the speedup from the Shor's algorithm. However, it can be applied and adapted to a much wider variety of problems compared to the other ones. For instance, any problem that has to be solved by random, brute-force search approaches can take advantage of its inherent quadratic speedup in the number of queries required.

Later, in 1997 and 1998, David Cory, Amr Fahmy, and Timothy Havel, as also, at the same time, Neil Gershenfeld and Isaac Chuang, published the first papers performing quantum operations for Quantum Computers based on Nuclear Spin-Resonance, or Thermal Ensembles [153, 154]. The technology used was based on NMR (Nuclear Magnetic Resonance), similar to the well-known medical MRI (Magnetic Resonance Imaging) machines used on healthcare.

Also in 1998, we witnessed the first-ever experimental running demonstration of Quantum Algorithms. More specifically, Jonathan Jones and Michele Mosca, and shortly after, Isaac Chuang, Neil Gershenfeld, and Mark Kubinec used a small NMR Quantum Computer to run Deutsch-Jozsa's and Grover's Algorithms [155, 156], respectively. Additionally, another research group with Isaac Chuang and Seth Lloyd involved, proposed a similar experimental work [157].

In the latter year, Justin Brooke, David Bitko, Thomas Rosenbaum, and Gabriel Aeppli jointly and experimentally demonstrated the basic concepts of Quantum Annealing through a condensed matter system [158]. They argued that using Quantum Tunneling as a mechanism for moving between states could reduce the time scales for Mathematical Optimization.

At the beginning of the century, we witnessed the first execution of Shor's Algorithm on an IBM's Quantum Computer. They executed this Quantum Algorithm at IBM's Almaden Research Center and Stanford University, USA, in 2001. This Quantum Computer factored the number 15 using $1,018$ molecules in a test tube, each one containing 7 active nuclear spins [159].

Also in 2001, Robert Raussendorf and Hans Briegel jointly proposed an innovative scheme of Quantum Computation that consists entirely of single measurements [160]. We know this scheme as Measurement-Based Quantum Computation or One-Way Quantum Computation. They used measurements of quantum states to imprint Quantum Logic Circuits on those same quantum states. This scheme were based on grids of quantum particles, forming a particular case of quantum states, known as the Cluster States. Those Cluster States are thus One-Way Quantum Computers and the measurements are performed to compose the program.

Between 2002 and 2007, the DARPA's Quantum Network was developed as the first-ever Quantum Cryptographic Network in the world, operating 10 optical nodes in Massachusetts, USA [161–163]. The DARPA sponsored it as part of the QuIST Program (Quantum Information Science and Technology Program), being built by BBN Technologies' Labs in collaboration with Harvard University and BUPC (Boston University Photonics Center), both in USA. At last, it eventually became fully operational in 2003 at BBN Technologies' Labs and was fielded through dark fiber[5] under the streets of Cambridge and Boston, Massachusetts, in 2004. This project also introduced the world's first Superconducting Nanowire Single-Photon Detector.

In 2006, we also witnessed some discoveries in Quantum Computing architectures based on QDs (Quantum Dots). Namely, a research team from TU Delft (Technische Universiteit Delft), Netherlands, created a device to manipulate the "up" or "down" states of electrons on QDs [164]. They showed the feasibility of operating single-electron spins in a QD as the fundamental blocks of quantum information for the development of a Quantum Computer.

Following these breakthroughs, a group from Harvard University and Texas A&M University, both in USA, with other researchers from the University of Stuttgart, Germany, developed a Quantum Register based on Diamond in 2007 [165]. The authors used optical and microwave radiation to control an electron spin associated with a novel NV (Nitrogen-Vacancy) center in Diamond. They also demonstrated excellent coherence properties in such quantum registers, arguing that they could be used as a basis for near-term scalable quantum computers.

Also in 2007, Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone, unveiled together a novel QRAM (Quantum Random Access Memory) to address any quantum superposition of numerous memory cells [166]. They presented a more robust architecture that exponentially reduced the requirements for each memory RAM (Random Access Memory) call in contrast to the conventional designs. Their proposal required entanglement among exponentially fewer Quantum Gates, leading to an exponential decrease in the power needed for its addressing.

Two independent R&D Labs also developed the first-ever prototypes of Quantum Bus to connect basic blocks of quantum information on a chip in 2007. First, Mika Sillanpää, Jae Park, and Raymond Simmonds, from NIST, demonstrated how to independently control their two Superconducting units of quantum information [167]. Then, researchers from Yale University, USA, could also transfer quantum states between two units of quantum information, via a superposed state using "virtual" photons, with no energy loss in the Quantum Bus [168].

Over the years, we also witnessed some developments regarding the lifetimes, as also the handing of decoherence in quantum states used in Quantum Computing. First, a research team from NIST extended the life of those quantum states from one millisecond to hundreds of them, using simple operations [169]. Then, another group of physicists from the University of Michigan, Naval Research Laboratory, and University of California San Diego, all in the USA, jointly with collaborators from the University of Hong Kong, China, also extended the lifetime of the basic units of quantum information over $1,000$ times the order of magnitude [170].

Then, Hartmut Neven presented a Quantum Adiabatic Algorithm being developed jointly

[5] A Dark Fibre (or Unlit Fibre) is an unused Optical Fibre, available for use in Fibre-Optic Communications.

by Google, D-Wave Systems, and Purdue University, USA, for training a Binary Classifier, at the NeurIPS (Neural Information Processing Systems) conference [171, 172]. Their algorithm automatically recognized and sorted objects, images, or videos. They tested their algorithm for sorting car images from 20,000 photos faster than anything running in a Google's Data Center.

Additionally, we also witnessed some developments in Quantum Computing processors. First, NIST developed the first-ever chip-scale Quantum Computer with 2 particles [173, 174]. They showed sustained, reliable, scalable Quantum Information Processing operations on internal states of electrically trapped and charged ions, observing no performance loss despite quantum states transport over macroscopic distances. Then, researchers from the University of Waterloo and Université de Sherbrooke, both in Canada, as Yale University, USA, and TU Wien (Technische Universität Wien), Austria, created the first solid-state superconducting Quantum Processor and used it to successfully execute some elementary Quantum Algorithms [175].

In 2011, D-Wave Systems offered the world's first-ever commercially available integrated Quantum Computer based on a Quantum Annealer architecture, called D-Wave One [176]. This Quantum Annealer had a Quantum Processor named "Rainier", which was capable to perform single mathematical discrete optimization operations to solve optimization problems.

At the same time, researchers from the University of California, USA, and the University of Konstanz, Germany, demonstrated a Quantum Memory based on Diamond [177]. They presented us with a room-temperature quantum memory based on the spin of the nitrogen nucleus intrinsic to each NV (Nitrogen-Vacancy) Centre in Diamond. The authors showed that even at room temperature, these defects in a diamond could manipulate quantum information, and these diamonds could become a leading candidate to be a quantum version of a Transistor.

Still in 2011, a group of researchers and scientists from USA, Japan and China, demonstrated a Quantum Integrated Circuit that implemented a quantum version of the Von Neumann architecture [178]. A long-lived QRAM could be programmed in this architecture, exchanging data with a QCPU (Quantum Central Processing Unit), on a single chip, via a Quantum Bus.

Then, NASA, USRA (Universities Space Research Association), and Google jointly launched the initiative Quantum AI Lab (Quantum Artificial Intelligence Lab) in 2013 [179]. The major goal of this initiative was to pioneer research on how Quantum Computing might help with Machine Learning and other computational problems. Initially, this lab was using the most advanced commercially available Quantum Computer, the D-Wave Two, from D-Wave Systems.

Moreover, scientists from TU Delft, Netherlands, collaborating with the British company, Element Six, could transfer data by Quantum Teleportation over more than 3 meters with no error rates in 2014, through a fully deterministic BSM (Bell-State Measurement) combined with a real-time feed-forward [180]. They also got an average quantum state fidelity exceeding the respective classical limit. These results established Diamond Spins as a prime candidate for Quantum Communication Networks, representing a vital step towards a Quantum Internet.

In 2016, a group of physicists from Universität Innsbruck, and ÖAW, both in Austria, jointly with MIT, USA, reported a fully scalable implementation of Shor's Algorithm in an Ion-Trap Quantum Computer [181]. They factored the number 15 by controlling 7 particles for general purposes and 7 particles acting as "cache", together with generalized arithmetic operations.

In the following years, many big players in Information Technology started to put huge efforts into Quantum Computing, in a quest to achieve the so desired Quantum Supremacy.

First, in 2017, IBM announced an industry initiative, called IBM Q, to build commercially available Universal Quantum Computing systems [182]. Then, scientists from IBM successfully broke the barrier for the simulation of 49 quantum particles [183]. Not least, IBM also revealed a working Quantum Computer with 50 fundamental units of quantum information [184]. One of their Quantum Computers managed to maintain quantum states for 90 microseconds [182].

Between 2017 and 2018, IBM, Intel, and Google already each reported preliminary testings on Quantum Processors containing 49, 50, and 72 quantum information units [182–189].

Then, Intel kept pushing significant efforts in developing their first Quantum Processor chips [186]. In 2018, Intel began testing its silicon-based Quantum Computing chip [190]. This Quantum Processor was constructed with isotopically pure silicon wafers and used magnetic resonance to manipulate individual electrons. Then, Intel also confirmed the development of a superconducting chip, with 49 units of quantum information, called "Tangle Lake" [185].

In 2018, Google announced the creation of a superconducting Quantum Processor based on 72 superconducting units of quantum information, called "Bristlecone" [188, 189]. Some experts argued this new Quantum Computer could possess enough power to equalize with any supercomputer in the world, and even overpower it to aim the desirable Quantum Supremacy.

Moreover, the National Quantum Initiative Act was signed into law, establishing the major goals for a 10-year plan to speed up Quantum Information Science in the USA [191, 192].

Finally, IonQ introduced the first commercial Quantum Computer based on trapped ions, hosting 160 units of quantum information [193]. This Quantum Computer was capable of performing simple and full quantum operations on 76 and 11 units of quantum information, respectively. They showed ions could be less error-prone, with error rates lower than 1%.

Then, we witnessed one of the most remarkable events ever in Quantum Computing when, in late 2019, Google finally claimed to reach the Quantum Supremacy, using their Quantum Computer Sycamore, with 53 units of quantum information [194]. Namely, Google's Sycamore could calculate a proof in 3 minutes and 20 seconds, showing the numbers created by an RNG (Random Number Generator) are indeed random. Theoretically, it would take IBM's Summit, the world's most powerful classical supercomputer at that time, about 10,000 years to complete the same task, making the proof practically impossible to be solved by any classical means. At the same time, IBM also revealed its biggest Quantum Computing system until the date, IBM's Q 53 with 53 quantum information units, available online via IBM's Quantum Experience [195].

In 2020, researchers from Harvard and MIT, both in the USA, managed to correct signal losses in a prototype of a quantum node capable of catch, store and entangle units of quantum information [196]. They used a single solid-state spin memory integrated into a nano-photonic diamond resonator to implement an asynchronous BSM. This improved Quantum Memory increased the secret key rate of MDI-QKD (Measurement Device-Independent - Quantum Key Distribution) over the loss-equivalent direct-transmission method while operating MHz (MegaHertz) clock rates. Their concepts could be used in the key components of Quantum Repeaters in Quantum Communication Networks and possibly extend their highest ranges.

Later on, a team of engineers from Google achieved the largest chemical simulation on a Quantum Computer, a Hartree-Fock Approximation [197]. They used Google's Sycamore paired with a Classical Computer which analyzed results to tune new parameters for quantum systems up to 12 hydrogen molecules. Then, they modeled those quantum systems via the binding energies of chains of the hydrogen molecules, as well as the isomerization of diazene. The team also demonstrated error-mitigation strategies, improving the fidelity of their experiments.

At the end of the year, another remarkable event on Quantum Computing took place, when Chinese researchers from USTC (University of Science and Technology of China), China, claimed to have achieved Quantum Supremacy, by using a Photonic Quantum Computer with a maximum of 76 (and an average of 43) detectable photons, known as Jiuzhang [198]. The research team improved their previous Quantum Computing system [199] in performing a GBS (Gaussian Boson Sampling) in about 3 minutes [198]. The same computation would have taken 10,000 years on Fugaku, the world's current most powerful classical supercomputer with 442 PFLOPS (Peta Floating Point Operations per Second), as well as over 2 billion years on Sunway TaihuLight, China's most powerful classical supercomputer with 93 PFLOPS. The researchers also claimed that their Quantum Computer is 10 billion times faster than Google's Sycamore.

In 2021, Frederico Centrone, Niraj Kumar, Ionardis Kerenis, and Eleni Diamanti reported the achievement of Quantum Advantage in an OWC (One-Way Communication) protocol [200]. In their work, they used the Sampling Matching Problem, inspired by the Hidden Matching Problem, featuring an exponential gap between quantum and classical protocols. Then, they showed a Quantum Advantage in the transmitted information over the best-known classical protocol, impossible to be reached for the original Hidden Matching Problem. Namely, their research could have implications in Quantum Verification Proofs and Quantum Cryptography.

Then, researchers from D-Wave Systems also reported a significant near-term Quantum Advantage over classical methods for practical problems, such as designing new materials [201]. For instance, the team showed that their new low-noise Quantum Processor with 1,440 units of quantum information could simulate the behavior of an "untwisting" quantum magnet much faster than a Classical Computer, offering increased speedups for harder simulations.

Later, the same group from USTC, China, whose achieved Quantum Supremacy in 2020, reported again the achievement of Quantum Advantage, introducing a new Photonic Quantum Computer with a maximum of 113 detectable photons, called Jiuzhang 2.0 [202]. A few months later, they also unveiled a super-advanced Quantum Processor, called Zuchongzhi, with 66 units of quantum information in a tunable coupling architecture [203]. They also developed a benchmark on their Quantum Processor by performing a Random Quantum Circuit Sampling, up to a quantum system of 56 quantum particles and 20 cycles, taking around 1 hour and 10 minutes. The authors estimated that the computational cost of this task was 100 to 1,000 times harder than the task performed by Google's Sycamore in 2019, and it would take over 8 years to compute the same calculation using the classical supercomputer Summit from IBM.

In the following months, this team of researchers from USTC, China, kept improving their prototype of a quantum programmable processor, releasing new versions, namely, Zuchongzhi 2.1, with better experimental results for harder problems compared to other prototypes [204].

Then, we witnessed another memorable achievement in Quantum Computing, which could have a vast impact in many areas, when we could create a Time Crystal for the first time. First, a group of Dutch, British, and American researchers built a DTC (Discrete Time Crystal) in a Diamond [205]. One month later, Google in collaboration with Universities and R&D Labs, in the USA and Germany, used Google's Sycamore to show a genuine DTC [206]. Both results could have a huge impact on designing new Materials, Quantum Hardware, and Quantum Processors. They could also boost Quantum Metrology, Quantum Communications, Quantum Simulations, Quantum Optimization, and Quantum Machine Learning applications.

All these events and developments led to an era commonly known as the 2^{nd} Quantum Revolution. The 1^{st} Quantum Revolution, formulated by some notable names, such as Albert Einstein, Max Planck, Werner Heisenberg, Erwin Schrödinger, or Wolfgang Pauli, gave us new rules that govern physical reality, in its fundamental atomic and subatomic levels, during the XX century. The 2^{nd} Quantum Revolution takes these rules and uses them to develop new powerful technologies, where Quantum Computing is one of the most remarkable examples. From this new paradigm in Science and Technology, other novel research topics emerged, such as Quantum Cryptography, Quantum Networks, Quantum Communications, Quantum Artificial Intelligence, Quantum Game Theory, Quantum Machine Learning, Quantum Deep Learning, Quantum Natural Language Processing, Quantum Optimization, Quantum Finance, Quantum Simulation, Quantum Chemistry, Quantum Sensing, or even Quantum Metrology.

It is reasonable to think that Quantum Computing is still living its infancy. However, it already revealed a glimpse of what could be its true potential. The current major drawback of Quantum Computing is its inherent errors and noise, caused by the decoherence of the respective quantum systems used and its information lost during the process, which is always very difficult to overcome. For this reason, we also refer to this era of Quantum Computing as the NISQ (Noisy Intermediate-Scale Quantum) era. The NISQ era was a term coined by John Preskill in 2018 to refer to the state-of-the-art near-term Quantum Processors and Quantum Computers with about 50 to a few hundreds of units of quantum information, but not advanced enough to reach the desired fault-tolerance nor large enough to profit sustainably from Quantum Supremacy and Quantum Advantage [207]. Beyond the NISQ era, we can achieve the FTQC (Fault-Tolerant Quantum Computing). But to reach the FTQC, we need more sophisticated Quantum Hardware capable of support better QEC (Quantum Error-Correction) methods to handle the sensitivity of such systems to the environment, improving the fidelity of the quantum operations while increasing the number of units of quantum information.

But when will we achieve the FTQC? What kind of practical problems will be solvable by the FTQC in the future? Will the FTQC be just about good news for Science and Technology? Could this FTQC represent any threat to other technologies we use nowadays? And could we use it to develop other more powerful technologies capable of protecting us from such threats?

1.2 Motivations for Quantum Computing

There are several motivations for Quantum Computing that we can mention, starting with its almost unlimited applications in science. However, here we will only introduce some simple motivations, which are more directed to the current limitations of Classical Computing.

1.2.1 The end of Moore's Law

The initial massive integration of ICs, with several Transistors, into computational devices led Gordon Moore, from Intel, in 1965, to predict the number of that Transistors in each IC doubles about every year [208–210]. Over the years, this prediction became known as Moore's Law. In fact, this prediction was accurate from 1975 until the current days, mainly due to the constant miniaturization of the Transistors, from μms to nms. For instance, the average size of a single Transistor inside an IC in 2022 is about 3 nms [211]. On the other hand, we estimate that a single IC may include between hundreds and thousands of billions of Transistors inside it [211].

The problem with this process is when we reach scales below the order of nms and pms, where laws of physics start to act differently. Namely, in such small scales, we need to deal with some random quantum effects, such as quantum tunneling [212–214] and Heisenberg's Principle of Uncertainty [23]. In quantum tunneling, an electron does not have a well defined position and behaves like a wave, varying its position within it in a probabilistic sense. As this wave comes close to a barrier, such as a gap between two semiconductors, one end of this wave might overlap that barrier and touch the other semiconductor. That means the electron has the potential to be on the other side of the gap. If the potential is there, it could mean that sometimes the electron is on the other side, like the electron tunneled right through the barrier. This phenomenon follows the probabilistic nature of Quantum Mechanics, inducing randomness and errors in computations, being also predicted by Gordon Moore himself.

For that reason, many scientists and experts agree that Moore's Law will eventually reach its end between 2020 and 2035 [215, 216]. Therefore, it is urgent for us to think of alternatives, such as Quantum Computing [142, 145], Chaos Computing [217–219], DNA Computing [220–224], Membrane Computing [225–227], and Neuromorphic Computing [228–231].

1.2.2 The need for more processing power

In the current state-of-the-art of Computer Science, we know it is impracticable to use Classical Computing to address some problems believed to be computationally hard in a reasonable amount of time. One of the reasons to explain this is that Classical Computing does not scale in terms of parallelism, even when we consider solutions based on GPUs (Graphical Processing Units), Distributed Computing, or other derivatives for HPC (High-Performance Computing). In Classical Computing, the computational devices work with digits as their basic units of information. These classical information digits are often bits, but they can also be trits, quads, or ultimately dits, for $k = 2$, $k = 3$, $k = 4$, and $k = d$ possible configurations, respectively. However, we can only have a single configuration of classical units of information at a time

for every type of these information units, even if we consider n units. Thus, it can lead us to try a single set of inputs in an algorithm for each computational step in an exhaustive search.

On the other hand, the quantum analogous of these classical information digits are often quantum bits, but they can also be quantum trits, quantum quads, or ultimately quantum dits. From the probabilistic and random nature of Quantum Mechanics, we know that an atomic or sub-atomic particle could not have a well-defined position or property. Therefore, a particle can have multiple configurations *simultaneously*, in a probabilistic sense, in a phenomenon called Quantum Superposition. In that case, if we use these particles to employ the previously mentioned quantum units of information, we can take advantage of this phenomenon. Namely, these quantum units of information can have infinite configurations of simultaneous classical digits. In particular, we can have 2^n, 3^n, 4^n, and d^n possible configurations for n classical units of information. For instance, we can try all these k^n possible inputs at once in a single computational step in an exhaustive search strategy. This phenomenon offers us exponential computational power, allowing more powerful and quicker computations when compared to our traditional counterparts. Thus, Quantum Computing could be a better tool to approach some computationally hard problems we know, or even ones never approached before.

In fact, one of the greatest motivations for Quantum Computing is that we cannot perform accurate Quantum Simulations with Classical Computing due to the exponential complexity of quantum systems. The obstacle from the exponential complexity of this problem could be surpassed with Quantum Computing, as Richard Feynman suggested previously [142].

1.3 Proposal and Contributions

In this Master Thesis, we proposed a new cryptographic protocol that achieves a conference key agreement, allowing several users to share a common private key. The novelty of our work relies on the use of entangled quantum states, jointly with a semi-quantum approach for this purpose. In particular, one of the parties, namely Alice, is a fully-quantum entity and can prepare entangled quantum states, namely GHZ State, of arbitrary size. Oppositely, the remaining parties of the protocol, namely multiple Bobs, are only allowed to perform two possible operations: Reflect or Measure in the standard computational basis and Resend the classical outcome. Our protocol has the additional advantages of being accessible and scalable.

We prove that the presented protocol is secure in the standard adversary models. In order to achieve this, we developed reduction techniques specifically for this proposal, which consists of the transformation of our initial protocol to a one-way protocol with the property that if the latter one is secure, so it is the original one. Considering the specific use of GHZ States, we also developed an extensive numerical analysis for the estimation of the key rate based on well-known results using Von Neuman's Entropy. Additionally, we also developed other security proofs against other common attacks, such as IR (Intercept-and-Resend).

From the practical point of view, we developed a custom library called Qis|krypt⟩ based on IBM Qiskit. Our library can simulate not only our protocol but also some other well-known quantum protocols. The source code is available on https://github.com/qiskrypt/qiskrypt/.

1.4 Outline

We organize this document into several chapters, where each of them has a specific purpose. In Chapter 1, we present an initial insight to this Master's Thesis by giving a historical review and context for the several areas of study involved in this work proposal, namely Quantum Mechanics, Computer Science, Communications, Cryptography, and Quantum Computing. Moreover, we also provide some brief motivations for Quantum Computing. Afterward, in Chapter Chapter 2, we review some required preliminaries and other introductory notions of Quantum Mechanics and Quantum Computing. At the end of this chapter, we also review the quantum algorithms that represent a threat to Classical Cryptography, as well as some existing approaches to address this problem in the current state-of-the-art. Then, we introduce the concepts of Quantum Cryptography in Chapter 3 as an ultimate solution for the problem that results from the impact of Quantum Computing in Classical Cryptography, and we describe some quantum cryptographic protocols, mostly in terms of Key Exchanges. In this case, we describe some of the most relevant protocols of Quantum Key Distribution, Semi-Quantum Key Distribution, and Quantum Conference Key Agreement. In addition, we also describe some known attacks on Quantum Cryptography and its security notions in Chapter 3. Next, we introduce the concept of Semi-Quantum Conference Key Agreement protocols, which are the main focus of this work proposal. Namely, we describe our protocol, code-named BKMPS22 Protocol, jointly with its simulation and security analysis (in terms of adversary model we consider, as well as its countermeasures, and its security proof, considering noisy scenarios). Finally, in Chapter 5, we present the conclusions of this work proposal and its future work.

CHAPTER 2

BACKGROUND

We have already seen how Quantum Computing could shake Science and Technology in the near term future. Furthermore, we also saw what type of applications it could have. But what is the science behind these Quantum Computing systems? How can we build and model these units of quantum information mentioned early? How do they behave following the laws of Quantum Mechanics? What kind of interactions can we perform with these same units?

In the following chapter, we will explain some of the science behind these new enthusiastic Quantum Computers. We will also describe some of the fundamental principles which make them get so much attention from scientists and researchers over the last couple of years.

2.1 Preliminaries of Quantum Mechanics

Before introducing what Quantum Computing really is, we first need to enumerate and explain some preliminaries from Quantum Mechanics and its inherent basic algebraic concepts.

2.1.1 Dirac's Notation

Before starting with any topic of Quantum Mechanics and Quantum Computing, we need to introduce Dirac's Notation. The Dirac's Notation (or Bra-Ket Notation) is a specific instance of algebraic notation inherently connected to Quantum Mechanics and Quantum Computing. We use this notation to denote and describe a vector space ψ, mainly through "bras" and "kets". These "bras" and "kets" are basically algebraic vectors with complex numbers as elements.

So, the "ket" representation of a vector space ψ is the following column-vector:

$$|\psi\rangle = \begin{bmatrix} \psi_0 \\ \vdots \\ \psi_{(n-1)} \end{bmatrix} \in \mathbb{C}^n \tag{2.1.1.1}$$

On the other hand, a "bra" is a row-vector composed by the complex conjugates of a given "ket" representation of a vector space ψ. In this case, its "bra" representation is the following:

$$\langle\psi| = \begin{bmatrix} \psi_0^* \dots \psi_{(n-1)}^* \end{bmatrix} \in \mathbb{C}^n \tag{2.1.1.2}$$

As we can see at this point, there is an inherent relationship between the "bra" and "ket" representations of a vector space, since the "bra" vector is nothing more than the conjugate transpose (also known as Hemitian conjugate or adjoint) of the "ket" vector, and vice-versa. Usually, we represent the conjugate transpose of a complex vector space with a "dagger". Thus, from this mathematical definition, we end up having the two following enumerated equalities:

$$\langle\psi|^\dagger = |\psi\rangle \tag{2.1.1.3}$$

$$|\psi\rangle^\dagger = \langle\psi| \tag{2.1.1.4}$$

The reason for this terminology is that an inner product between two vector spaces ϕ and ψ corresponds to the dot product between the "bra" and "ket" ("Bra-Ket") vectors of those vector spaces, respectively. From this mathematical definition, we get the following equality:

$$\langle\phi,\psi\rangle = \langle\phi|\cdot|\psi\rangle = \langle\phi|\psi\rangle, \text{ where } \phi,\psi \in \mathbb{C}^n \tag{2.1.1.5}$$

We can define the inner product (or dot product) of two vector spaces ϕ and ψ as the sum of the multiplication of their corresponding components as demonstrated following:

$$\langle\phi|\psi\rangle = \begin{bmatrix} \phi_0^* \dots \phi_{(n-1)}^* \end{bmatrix} \cdot \begin{bmatrix} \psi_0 \\ \vdots \\ \psi_{(n-1)} \end{bmatrix} = \phi_0^*\psi_0 + \dots + \phi_{(n-1)}^*\psi_{(n-1)}, \text{ where } \phi,\psi \in \mathbb{C}^n \tag{2.1.1.6}$$

Similarly, the inner product of ϕ and ψ can also be represented in terms of trigonometry:

$$\langle\phi|\psi\rangle = |\phi||\psi|\cos\left(\frac{\theta}{2}\right), \text{ where } \phi,\psi \in \mathbb{C}^n \text{ and } \theta \in [0, 2\pi] \tag{2.1.1.7}$$

In this case, θ represents the existing angle between these two vector spaces ϕ and ψ.

Furthermore, the inner product of two vector spaces is commutative. More specifically, the order of the vector spaces in the inner product does not matter, from which we have:

$$\langle\phi|\psi\rangle = \langle\psi|\phi\rangle, \text{ where } \phi,\psi \in \mathbb{C}^n \tag{2.1.1.8}$$

If we multiply a vector space ψ by a constant c, we also need to multiply its dot product with any other vector space ϕ by the same constant c as we demonstrate following:

$$\text{if } \tau = c\psi \implies \langle\phi|\tau\rangle = \langle\phi|c\psi\rangle = c\langle\phi|\psi\rangle, \text{ where } \phi,\psi \in \mathbb{C}^n \text{ and } c \in \mathbb{R} \tag{2.1.1.9}$$

The inner product of a vector space with itself corresponds to the square of its magnitude:

$$\langle\psi|\psi\rangle = |\psi|^2 = \sqrt{|\psi_0|^2 + \dots + |\psi_{(n-1)}|^2}, \text{ where } \psi \in \mathbb{C}^n \tag{2.1.1.10}$$

Obviously, the inner product of a vector space with the zero vector is equal to zero:

$$\langle 0|\psi\rangle = 0, \text{ where } \psi \in \mathbb{C}^n \tag{2.1.1.11}$$

Finally, we consider that some vector spaces ϕ and ψ are perpendicular only if their inner product is zero. In that case, those vector spaces are completely distinguishable:

$$\phi \perp \psi \implies \langle \phi|\psi\rangle = 0, \text{ where } \phi, \psi \in \mathbb{C}^n \tag{2.1.1.12}$$

Therefore, we can also use the inner product to calculate the fidelity of a given vector space ψ compared to another expected vector space ϕ. If the inner product is equal to zero, the two vector spaces ψ and ϕ are completely distinguishable. On the other hand, if the inner product is equal to one, the two vector spaces ψ and ϕ are completely indistinguishable (or equal).

2.1.2 Quantum State

Now, we can define introduce the notion of what a quantum state really is. A quantum state is some physical system that can exist in n different mutually exclusive classical states. Each one of these exclusive classical states is related to a complex number $\alpha_k = (a + bi)_k$, with an amplitude and a phase, where $0 \leq k \leq (n-1)$. More specifically, by a "classical state" we mean a state on which we can find that physical system if we observe it. Additionally, we have two slightly different types of quantum states: *pure* quantum states and *mixed* quantum states.

2.1.2.1 Pure Quantum State

A pure quantum state is the most known type of quantum state. We represent a quantum state by a "ket" (or column-vector) in Dirac's Notation, with the respective complex number elements representing the amplitudes for each one of its possible observable classical states:

$$|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_{(n-1)} \end{bmatrix} = \begin{bmatrix} (a+bi)_0 \\ \vdots \\ (a+bi)_{(n-1)} \end{bmatrix} \in \mathbb{C}^n \tag{2.1.2.1.1}$$

A pure quantum state can have multiple classical states. Generally, we can denote those classical states as $|0\rangle$, ..., $|(n-1)\rangle$. Mathematically, the classical states $|0\rangle$, ..., $|(n-1)\rangle$ form an orthonormal basis of an n-dimensional Hilbert Space $\mathcal{H}$. Therefore, these classical states are also themselves n-dimensional column-vectors equipped with an inner product:

$$|\psi\rangle = \{\ |0\rangle,\ ...,\ |(n-1)\rangle\ \}, \text{ where } |0\rangle, ..., |(n-1)\rangle \in \mathbb{C}^n \tag{2.1.2.1.2}$$

So, the quantum state ψ is in the classical state $|0\rangle$ with amplitude α_0, in the classical state $|1\rangle$ with amplitude α_1, and so on. In the end, the quantum state ψ is in the classical state $|(n-1)\rangle$ with amplitude $\alpha_{(n-1)}$, as well. Additionally, a pure quantum state is a quantum state that we cannot define as a probabilistic mixture of other quantum states. In this case, we can

also represent a pure quantum state ψ by a density matrix (or density operator) $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle\langle\psi|$ is the outer product of this quantum state ψ with itself, demonstrated as follows:

$$\rho = |\psi\rangle\langle\psi| = \begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_{(n-1)} \end{bmatrix} \cdot \begin{bmatrix} \alpha_0^* & \dots & \alpha_{(n-1)}^* \end{bmatrix} = \begin{bmatrix} |\alpha_0|^2 & \dots & \alpha_0\alpha_{(n-1)}^* \\ \vdots & \ddots & \vdots \\ \alpha_{(n-1)}\alpha_0^* & \dots & |\alpha_{(n-1)}|^2 \end{bmatrix} \in \mathbb{C}^{(n\times n)} \quad (2.1.2.1.3)$$

The pure quantum states are also known as wave functions. This term applies particularly when they represent the function of the position or momentum of particles, such as photons.

2.1.2.2 Mixed Quantum State

On the other hand, we can view mixed quantum states as statistical ensembles of other pure quantum states. More specifically, a mixed quantum state *cannot* be described with a single "ket" (or column-vector) as happens with pure quantum states. For this reason, it is more convenient to define this type of quantum state just as density matrices (or density operators).

Therefore, we can represent a mixed quantum state as a probability distribution over n pure quantum states, represented by the density operator $\rho = \sum_{i=1}^{n} p_i|\psi_i\rangle\langle\psi_i|$. In simple terms, a mixed quantum state is in pure quantum states $|\psi_1\rangle$, ..., $|\psi_n\rangle$, with probability p_1, ..., p_n. This density operator ρ is also called a "mixture" of the pure quantum states $|\psi_1\rangle$, ..., $|\psi_n\rangle$.

In particular, these mixed quantum states arise in Quantum Mechanics in two different situations. First, when the preparation of the physical system is not fully known. Here, we must consider a statistical ensemble of possible preparations of that physical system. And second, when we want to describe a physical system entangled with another quantum state which we cannot define as a pure quantum state. These mixed quantum states are quantum states on which we have limited or even no knowledge about the respective physical system.

2.1.2.3 Tensor Product of Multiple Quantum States

Additionally, we can combine different Hilbert Spaces using the mathematical tensor product rule. For example, if $|0\rangle$, ..., $|(m-1)\rangle$ are an orthonormal basis of the Hilbert Space $\mathcal{H}_A$ and $|0\rangle$, ..., $|(n-1)\rangle$ are an orthonormal basis of the Hilbert Space $\mathcal{H}_B$, then the tensor product of those Hilbert Space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ is an mn-dimensional Hilbert Space spanned by the set of spaces $\{\ |\phi\rangle \otimes |\tau\rangle : \phi \in \{0, ..., (m-1)\}, \tau \in \{0, ..., (n-1)\}\ \}$. In this case, we obtain a new arbitrarily quantum state $|\psi\rangle$ in Hilbert Space $\mathcal{H}$ which has the following enumerated form:

$$|\psi\rangle = \sum_{\phi=0}^{(m-1)} \sum_{\tau=0}^{(n-1)} \delta_{(\phi,\tau)}|\phi\rangle \otimes |\tau\rangle \quad (2.1.2.3.1)$$

For example, consider $|\phi\rangle$ and $|\tau\rangle$ are pure quantum states represented as follows:

$$|\phi\rangle = \begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_{(m-1)} \end{bmatrix} \quad \text{and} \quad |\tau\rangle = \begin{bmatrix} \beta_0 \\ \vdots \\ \beta_{(n-1)} \end{bmatrix} \tag{2.1.2.3.2}$$

Then, we define $|\psi\rangle$ as a tensor product of the pure quantum states $|\phi\rangle$ and $|\tau\rangle$ as follows:

$$|\psi\rangle = |\phi\rangle \otimes |\tau\rangle = \begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_{(m-1)} \end{bmatrix} \otimes \begin{bmatrix} \beta_0 \\ \vdots \\ \beta_{(n-1)} \end{bmatrix} = \begin{bmatrix} \alpha_0 \begin{bmatrix} \beta_0 \\ \vdots \\ \beta_{(n-1)} \end{bmatrix} \\ \vdots \\ \alpha_{(m-1)} \begin{bmatrix} \beta_0 \\ \vdots \\ \beta_{(n-1)} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} \alpha_0\beta_0 \\ \vdots \\ \alpha_0\beta_{(n-1)} \\ \vdots \\ \alpha_{(m-1)}\beta_0 \\ \vdots \\ \alpha_{(m-1)}\beta_{(n-1)} \end{bmatrix} \tag{2.1.2.3.3}$$

Generally, we can combine any number of smaller Hilbert Spaces $\mathcal{H}_1$, ..., $\mathcal{H}_k$ using the tensor product $\mathcal{H} = \mathcal{H}_1 \otimes ... \otimes \mathcal{H}_k$. A quantum state in a Hilbert Space resulting from the tensor product of two smaller Hilbert Spaces is called *bipartite*. We can have *tripartite* quantum states in a Hilbert Space that is the tensor product of three smaller Hilbert Spaces, and so on.

2.1.3 Quantum Superposition

The Quantum Superposition is one of the fundamental principles of Quantum Mechanics. This principle says that we can add (or "superpose") two or more classical or quantum states into another valid quantum state. And more generally, we can even represent every quantum state as a sum of two or more other distinct quantum states. But a Quantum Superposition is much more than simply the sum of several possible states describing a physical system.

In a Quantum Superposition, all the possible states of a physical system can simultaneously occur with associated amplitudes. Therefore, we can define a Quantum Superposition as a linear combination of those possible states weighted with the respective complex numbers:

$$|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_{(n-1)} \end{bmatrix} = \begin{bmatrix} \alpha_0 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \begin{bmatrix} 0 \\ \vdots \\ \alpha_{(n-1)} \end{bmatrix} = \alpha_0 \begin{bmatrix} 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \alpha_{(n-1)} \begin{bmatrix} 0 \\ \vdots \\ 1 \end{bmatrix}, \text{ where } |\psi\rangle \in \mathbb{C}^n \tag{2.1.3.1}$$

Thus, we can denote each one of the n possible states of a physical system as a unit vector:

$$|0\rangle = \begin{bmatrix} 1 \\ \vdots \\ 0 \end{bmatrix}, ..., |(n-1)\rangle = \begin{bmatrix} 0 \\ \vdots \\ 1 \end{bmatrix}, \text{ where } |0\rangle, ..., |(n-1)\rangle \in \mathbb{R}^n \tag{2.1.3.2}$$

Through the Quantum Superposition, we can also generally represent a quantum state as:

$$|\psi\rangle = \alpha_0|0\rangle + ... + \alpha_{(n-1)}|(n-1)\rangle, \text{ where } |0\rangle, ..., |(n-1)\rangle \in \mathbb{R}^n \text{ and } \alpha_0, ..., \alpha_{(n-1)} \in \mathbb{C}^n \quad (2.1.3.3)$$

Finally, we can perform unitary operations and quantum interference to the Quantum Superposition of a physical system existing in several states simultaneously until the physical system collapses due to external environment effects or be measured ("observed") by us.

2.1.4 Unitary Operators and Evolution

After learning the Quantum Superposition, we can introduce how we can evolve a physical system of a quantum state by applying some unitary operators to a specific quantum state. Thus, we can generally define the effect of this unitary operation U, demonstrated as follows:

$$U|\psi\rangle \Longrightarrow |\psi'\rangle, \text{ where } |\psi\rangle \text{ and } |\psi'\rangle \in \mathbb{C}^n \quad (2.1.4.1)$$

In particular, Quantum Mechanics only allows linear operations to be applied to quantum states. More specifically, if a quantum state $|\psi\rangle$ is represented by a n-dimensional "ket" (or column-vector) $\begin{bmatrix}\alpha_0, ..., \alpha_{(n-1)}\end{bmatrix}^T$, then applying an operation that changes the quantum state $|\psi\rangle$ to $|\psi'\rangle$ corresponds to multiplying $|\psi\rangle$ by a complex-value unitary matrix $U \in \mathbb{C}^{(n\times n)}$:

$$U\begin{bmatrix}\alpha_0 \\ \vdots \\ \alpha_{(n-1)}\end{bmatrix} = \begin{bmatrix}u_{(0,0)} & \dots & u_{(0,(n-1))} \\ \vdots & \ddots & \vdots \\ u_{((n-1),0)} & \dots & u_{((n-1),(n-1))}\end{bmatrix}\begin{bmatrix}\alpha_0 \\ \vdots \\ \alpha_{(n-1)}\end{bmatrix} = \begin{bmatrix}\beta_0 \\ \vdots \\ \beta_{(n-1)}\end{bmatrix} \quad (2.1.4.2)$$

Note that by linearity we also have $|\psi'\rangle = U|\psi\rangle = U\big(\sum_{i=0}^{(n-1)} \alpha_i|i\rangle\big) = \sum_{i=0}^{(n-1)} \alpha_i U|i\rangle$.

Obviously, this matrix U must always preserve the norm of the "ket" column-vector of the quantum state to which we are applying U. For this reason, the matrix U must represent a unitary operation. More specifically, a matrix U is unitary if its inverse matrix U^{-1} is equal to its conjugate transposed matrix U^*. In mathematical terms, a unitary matrix U always maps a column-vector of norm 1 to another column-vector of norm 1. Since a unitary operation always has an inverse, it follows that any unitary transformation on quantum states must be reversible. In particular, by applying the unitary transformation U^{-1} we can always "undo" the action performed by the unitary transformation U without losing anything in the process.

2.1.5 Measurements

However, in Quantum Mechanics, there is an action that we can apply to a quantum state $|\psi\rangle$, which is clearly non-reversible. This operation is the measurement (or "observation") of a quantum state. This operation leads to a quantum state collapsing to one of the n possible classical states in the Hilbert Space. This operation is non-reversible because we cannot reconstruct the quantum state $|\psi\rangle$ from the "observed" classical state $|i\rangle$, where $0 \leq i \leq (n-1)$.

2.1.5.1 Measurements in Standard Computational Basis

From the action of measuring a quantum state, we can only "observe" classical states, and never a Quantum Superposition itself. More specifically, if we measure a quantum state $|\psi\rangle$ in an n-dimensional Hilbert Space $\mathcal{H}$, we will see only one of the possible classical states $|i\rangle$ of that quantum state, where $0 \leq i \leq (n-1)$. We do not know this in advance, and the only thing we know is that the probability we have to "observe" the classical state $|i\rangle$ is equal to the squared norm of the respective amplitude, i.e., $|\alpha_i|^2$, which is known as the "Born's Rule".

The "Born's Rule" implies that the "ket" vector of amplitudes has Euclidean norm 1:

$$\sum_{i=0}^{(n-1)} |\alpha_i|^2 = |\alpha_0|^2 + ... + |\alpha_{(n-1)}|^2 = 1 \tag{2.1.5.1.1}$$

In this case, if we measure the quantum state $|\psi\rangle$ and get the outcome j as a final result, the wavefunction of the respective quantum state collapse. More specifically, the Quantum Superposition of the quantum state $|\psi\rangle$ itself "disappears", and all that is left is the classical state $|i\rangle$ we "observe" in the n-dimensional Hilbert Space. Additionally, all the "information" previously contained in each one of the other amplitudes α_j also disappears, where $j \neq i$.

Note that the probabilities $|\alpha_i|^2$ of the several possible measurement outcomes are the same when we measure the quantum state $|\psi\rangle$ or when we measure the quantum state $e^{i\theta}|\psi\rangle$. For this reason, we usually say that the "global phase" $e^{i\theta}$ has no physical significance.

Additionally, making the quantum state $|\psi\rangle$ of a physical system evolve to a new quantum state $|\psi'\rangle$ by applying Unitary Operators preserves the constraints of the "Born's Rule" during the whole process. In other words, measuring the resulting new quantum state $|\psi'\rangle$ will make the probability of "observing" the classical state $|i\rangle$ be equal to the squared norm of the new respective amplitude, i.e., $|\beta_i|^2$, where $0 \leq i \leq (n-1)$. More generally, measuring the quantum state $|\psi'\rangle$ should also give a probability distribution, with the constraint $\sum_{i=0}^{(n-1)} |\beta_i|^2 = 1$.

2.1.5.2 Projective Measurements

The Measurements performed in the Standard Computational Basis is the most well-known type of measurement, and for a great range of applications suffices. However, more general and sometimes useful types of measurement are also possible, such as Projective Measurements.

A Projective Measurement with m possible classical outcomes is described by a set of Projectors P_0, ..., $P_{(m-1)}$ that all have the same dimension and that sum to the identity matrix $\left(\sum_{i=0}^{(m-1)} P_i = I\right)$, where $0 \leq i \leq (m-1)$. These Projectors are then pairwise orthogonal, meaning that $P_i P_j = 0$, if $i \neq j$. The Projector P_i projects on some subspace V_i of the total Hilbert Space V, and every quantum state $|\psi\rangle \in V$ can be decomposed as $|\psi\rangle = \sum_{i=0}^{(m-1)} |\psi_i\rangle$, with $|\psi_j\rangle = P_i|\psi\rangle \in V_i$. Since the projectors are orthogonal, the subspaces V_i and the quantum states $|\psi_i\rangle$ are orthogonal as well. When we apply this measurement to the pure quantum state $|\psi\rangle$, then we will obtain the outcome i with probability $||\psi_i||^2 = \text{Tr}(P_i|\psi\rangle\langle\psi|) = \langle\psi|P_i|\psi\rangle$ and the measured quantum state $|\psi\rangle$ will then "collapse" to the new state $\frac{|\psi_i\rangle}{|||\psi_i\rangle||} = \frac{P_i|\psi\rangle}{||P_i|\psi\rangle||}$.

For example, a Measurement in the Standard Computational Basis on an n-dimensional quantum state is the specific Projective Measurement where $m = n$ and $P_i = |i\rangle\langle i|$. In this case, the Projector P_i projects onto the Standard Computational Basis quantum state $|i\rangle$ and the corresponding subspace $V_i \subset V$ is the one-dimensional subspace spanned by $|i\rangle$. Considering the quantum state $|\psi\rangle = \sum_{i=0}^{(n-1)} \alpha_i|i\rangle$, note that $P_i|\psi\rangle = \alpha_i|i\rangle$, so applying our measurement to the quantum state $|\psi\rangle$ will give the outcome j with probability $||\alpha_i|i\rangle||^2 = |\alpha_j|^2$, and in that case the quantum state collapses to the quantum state $\frac{\alpha_i|i\rangle}{||\alpha_i|i\rangle||} = \frac{\alpha_i}{|\alpha_i|}|i\rangle$. The norm factor $\frac{\alpha_i}{|\alpha_i|}$ may be disregarded because it has no physical significance, so we end up with the state $|i\rangle$.

Additionally, instead of the standard orthonormal basis, with the respective basis states $|0\rangle, ..., |(n-1)\rangle$, we may consider any other orthonormal basis B of states $|\phi_0\rangle, ..., |\phi_{(n-1)}\rangle$, and consider the projective measurement defined by the projectors $P_i = |\phi_i\rangle\langle\phi_i|$. This is what we call of "measuring in the basis B". By applying this measurement to the quantum state $|\psi\rangle$, we obtain i with probability $\langle\psi|P_i|\psi\rangle = |\langle\psi|\phi_i\rangle|^2$. Note that if the quantum state $|\psi\rangle$ is equal to one of the basis vectors $|\phi_i\rangle$, then the measurement gives the outcome i with probability 1.

2.1.6 Observables

Furthermore, a Projective Measurement with Projectors $P_0, ..., P_{(m-1)}$ and associated distinct outcomes $\lambda_0, ..., \lambda_{(m-1)} \in \mathbb{R}$, can be written as one single matrix $M = \sum_{i=0}^{(m-1)} \lambda_i P_i$, which we call an Observable. More specifically, an Observable is nothing more than a succinct way to define a Projective Measurement in one matrix with the great advantage that the expected value of the outcome can be easily calculated. Namely, if we measure a quantum state $|\psi\rangle$, then the probability of the outcome λ_i is $||P_i|\psi||^2 = \mathrm{Tr}\big(P_i|\psi\rangle\langle\psi|\big)$, so the expected value of the "observed" outcome is $\sum_{i=0}^{(m-1)} \lambda_i \mathrm{Tr}(P_i|\psi\rangle\langle\psi|) = \mathrm{Tr}\big(\sum_{i=0}^{(m-1)} \lambda_i P_i|\psi\rangle\langle\psi|\big) = \mathrm{Tr}\big(M|\psi\rangle\langle\psi|\big)$. Additionally, note that this unitary matrix M is also Hermitian, such that we have the equality $M = M^*$. Conversely, since every Hermitian matrix M has a spectral decomposition $M = \sum_{i=1}^{m} \lambda_i P_i$, there is a correspondence between Observables and Hermitian matrices.

We can also compose Observables from other smaller Observables, similar to what we can do with the composition of quantum states. For example, if we have two Observables A and I with dimension $n \times n$, we can compose a Joint Observable O using the tensor rule between these smaller Observables A and I, where I is the Identity matrix. This composition results in the Observable $O = A \otimes I$, with dimension $n^2 \times n^2$. This Observable O will act only on the first smaller n-dimensional Hilbert Space part of a bipartite quantum state $|\psi\rangle$. Similarly, an Observable $O = I \otimes B$ defined, in the same way, act only in the second smaller n-dimensional Hilbert Space part of a bipartite quantum state $|\psi\rangle$ defined in a n^2-dimensional Hilbert Space.

Moreover, measuring the Separate Observables A and B on the two parts of a bipartite quantum state is different from measuring the Joint Observable $A \otimes B$. Namely, the Separate Measurements give one outcome for each Separate Observable, while the Joint Measurement will result only in a single outcome. Additionally, the distribution on the post-measurement state may be different. However, the measurement statistics of the product of outcomes are the same as the measurement statistics of the outcome resulting from the Joint Measurement.

2.1.7 Quantum Entanglement

The Quantum Entanglement is a *random* physical phenomenon in which we cannot describe the quantum states or observable physical properties of a physical system composed of two or more particles without referencing each other. This phenomenon leads to "unbreakable" correlations between the quantum states or observable physical properties of a system.

This quantum mechanical phenomenon completely rejects the idea of Local Realism since it implies the principle of Quantum Non-Locality. For this reason, it is valid even some of these individual particles are spatially separated. In simple terms, any action performed in one of these particles will instantaneously influence the others, even if they are too far away from each other. This idea seems to imply FTL (Faster-Than-Light) Communication, which is not necessarily true. Namely, it is always important to remember that this phenomenon has a *random* behavior, and third parties can also intercept some of the involved particles perturbing its global quantum state or observable physical properties, leading to still correlated but wrong outcomes. Then, in order to compare the outcomes composing a transmitted message possibly via Quantum Entanglement, we need to use Classical Communications, which are limited in the best case by the speed of light and Einstein's Special Relativity Theory. In simple terms, we can say that Quantum Entanglement does not physically allow *useful* FTL Communications.

However, the Quantum Entanglement has several applications in some emerging quantum technologies such as Quantum Computing and Quantum Cryptography. Additionally, we can achieve the Quantum Teleportation experimentally by using the Quantum Entanglement.

2.1.8 Quantum Decoherence

The Quantum Decoherence is the loss process of Quantum Coherence of a physical system and some of its properties due to some quantum effects occurring in the physical environment. Most of these quantum effects have a random nature, and we cannot always predict them with certainty. For this reason, we often describe them with a probabilistic interpretation of the respective wavefunction. We say a physical system is coherent as long as there exists a concrete relation between the phases of the different quantum states describing that physical system.

The Quantum Coherence must also be preserved by applying processes described under the laws of Quantum Mechanics. Namely, if a physical system is perfectly isolated, it would maintain its Quantum Coherence indefinitely, but it would be impossible to manipulate such system. On the other hand, if the physical system is not perfectly isolated, such as during the measurement of a physical system, its Quantum Coherence is entangled (or shared) with the physical environment, and we lose the respective information with time. This phenomenon explains why the physical system no longer has its quantum behavior after the performed measurement, just as energy levels appear to be lost by the friction in Classical Mechanics.

Basically, most realistic physical systems are never completely isolated from their physical environment. Then, when a physical system interacts with its physical environment, it will generally become rapidly and strongly entangled with a large number of environmental degrees

of freedom. These entangling interactions dramatically influence what we locally "observe" during the measurement of the physical system and the respective statistics of the system.

2.2 Introduction to Quantum Computing

Now that we introduced the relevant preliminaries of Quantum Mechanics, we can explain how Quantum Computing works and how its fundamental unit blocks of information are modeled and operated. Next, we can finally describe how we can use those unit blocks of information to build routines, algorithms, and protocols more powerful than their classical counterparts.

2.2.1 Quantum Bit

In Classical Computation, the basic unit of information is a classical bit that can be 0 or 1. Differently, in Quantum Computation, the basic information block is a quantum bit (or qubit). In contrast to a bit, a qubit can also be 0 or 1, or even a Quantum Superposition of 0 and 1.

Consider a physical system in a two-dimensional Hilbert Space with two basis states for binary information, denoted as $|0\rangle$ and $|1\rangle$, defined by the following set of orthogonal vectors:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2.2.1.1}$$

As mentioned, a single qubit can also be in any Quantum Superposition with the form:

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \tag{2.2.1.2}$$

The "Born's Rule" is also verified for a single qubit and the respective amplitudes:

$$\sum_{i=0}^{1} |\alpha_i|^2 = |\alpha_0|^2 + |\alpha_1|^2 = 1 \tag{2.2.1.3}$$

For this reason, a single qubit has its amplitudes in the complex-valued vector space $\mathbb{C}^2$.

Similarly, we can think of physical systems of more than one qubit, defined by the tensor product of the Hilbert Spaces of several qubit systems. For example, a 2-qubit system has 4 basis states, such as $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$ and $|1\rangle \otimes |1\rangle$. Here, $|a\rangle \otimes |b\rangle$ means that the first qubit is in its basis state $|a\rangle$ and the second qubit is its basis state $|b\rangle$, where $a \in \{0,1\}$ and $b \in \{0,1\}$. Usually, we abbreviate this 2-qubit system to $|a\rangle|b\rangle$, $|a,b\rangle$, or even $|ab\rangle$.

From a n-qubit system, we can represent a quantum register or a quantum memory using this same tensor product rule. More specifically, we can represent a quantum memory of n qubits $|\psi\rangle_0$, $|\psi\rangle_1$, ..., $|\psi\rangle_{(n-1)}$ as a n-qubit physical system $|\psi\rangle = |\psi\rangle_0 \otimes |\psi\rangle_1 \otimes ... \otimes |\psi\rangle_{(n-1)}$.

Additionally, we can extend these concepts for higher-dimensional Hilbert Spaces, where we must verify $\sum_{i=0}^{1} |\alpha_i|^2 = 1$. We can also have qutrits and qutrats as being the quantum counterparts of trits and trats used in classical computing, respectively. We represent these two units of quantum information in the three-dimensional and four-dimensional Hilbert Spaces, defined as $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle$ and $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \alpha_3|3\rangle$, respectively. In the general case, we have qudits for d-dimensional Hilbert Spaces, $|\psi\rangle = \alpha_0|0\rangle + ... + \alpha_{(n-1)}|(n-1)\rangle$.

2.2.2 Bloch Sphere

The Bloch Sphere is a geometrical representation of the state of a two-level quantum system, through a unit three-dimensional sphere, commonly used to represent a single qubit:

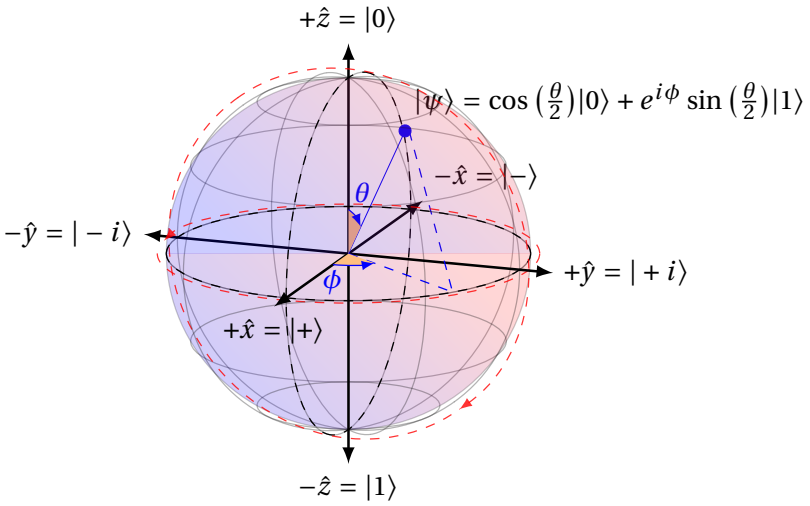


Figure 2.1: Representation of a Qubit in a Bloch Sphere.

Since we can represent a complex number using the exponential form, we can rewrite the coefficients of the two-dimensional Hilbert Space that describes a single qubit system as:

$$\begin{aligned} \alpha_0 &= \rho_0 e^{i\theta_0} = \rho_0\big(\cos(\theta_0) + i\ \sin(\theta_0)\big) \\ \alpha_1 &= \rho_1 e^{i\theta_1} = \rho_1\big(\cos(\theta_1) + i\ \sin(\theta_1)\big) \end{aligned} \tag{2.2.2.1}$$

Here, ρ_0 and ρ_1 are real numbers. Therefore, by following the "Born's Rule", we also have:

$$\begin{aligned} |\alpha_0|^2 + |\alpha_1|^2 &= |\rho_0 e^{i\theta_0}|^2 + |\rho_1 e^{i\theta_1}|^2 \\ &= |\rho_0|^2 |e^{i\theta_0}|^2 + |\rho_1|^2 |e^{i\theta_1}|^2 \\ &= |\rho_0|^2 |\cos(\theta_0) + i\sin(\theta_0)|^2 + |\rho_1|^2 |\cos(\theta_1) + i\sin(\theta_1)|^2 \\ &= |\rho_0|^2 + |\rho_1|^2 \\ &= 1 \end{aligned} \tag{2.2.2.2}$$

From the Fundamental Theorem of Trigonometry, we have the following result:

$$|\rho_0|^2 + |\rho_1|^2 = 1 \Leftrightarrow \left|\cos\left(\frac{\theta}{2}\right)\right|^2 + \left|\sin\left(\frac{\theta}{2}\right)\right|^2 = 1 \tag{2.2.2.3}$$

Then, from the previous equality, we can also derive the following set of parameters:

$$\alpha_0 = \rho_0 = \cos\left(\frac{\theta}{2}\right) \quad \text{and} \quad \alpha_1 = \rho_1 = \sin\left(\frac{\theta}{2}\right) \tag{2.2.2.3}$$

Next, if we multiply the complex number $e^{-i\theta_0}$ by the pure quantum state $|\psi\rangle$ of a single qubit system as defined in Equation (2.2.1.2), we obtain the following set of results:

$$\begin{aligned} e^{-i\theta_0}|\psi\rangle &= e^{-i\theta_0}\alpha_0|0\rangle + e^{-i\theta_0}\alpha_1|1\rangle \\ &= e^{-i\theta_0}\rho_0 e^{i\theta_0}|0\rangle + e^{-i\theta_0}\rho_1 e^{i\theta_1}|1\rangle \\ &= e^{(i\theta_0 - i\theta_0)}\rho_0|0\rangle + e^{(i\theta_1 - i\theta_0)}\rho_1|1\rangle \\ &= \rho_0|0\rangle + e^{i(\theta_1-\theta_0)}\rho_1|1\rangle \\ &= \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i(\theta_1-\theta_0)}\sin\left(\frac{\theta}{2}\right)|1\rangle \end{aligned} \tag{2.2.2.4}$$

If we define $\varphi = (\theta_1 - \theta_0)$, we can simplify the previous results as demonstrated following:

$$e^{-i\theta_0}|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{2.2.2.5}$$

Then, if we multiply $e^{-i\theta_0}$ to the previous result, we obtain the new following result:

$$|\psi\rangle = e^{i\theta_0}\left(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle\right) \tag{2.2.2.6}$$

Finally, we can consider $e^{i\theta} = e^{i\theta_0}$, which is a complex number describing the "global phase" of the quantum state $|\psi\rangle$, which has no physical significance and thus, we obtain:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{2.2.2.7}$$

From this mathematical proof, we can see that we can determine the quantum state of a single qubit with the parameters θ and φ. Additionally, we also know from "Born's Rule" that the probability of "observing" $|0\rangle$ is $\cos^2\left(\frac{\theta}{2}\right)$ and the probability of "observing" $|1\rangle$ is $\sin^2\left(\frac{\theta}{2}\right)$.

Regarding the acceptable ranges for the parameters θ and φ, we can first assume φ is a free parameter valid in $[0, 2\pi]$. On the other hand, we know both cosine and sine are periodic functions, where we obtain the same values for different θ values. More specifically, for the cosine function, we can always rewrite any θ value to be strictly inside the range $[0, \pi]$.

However, if we range the domain of the sine function to be in $[0, \pi]$, we cannot obtain all the values in $[-1, 1]$ as happen in cosine function, which can result in some values missing as the complex number describing the coefficient of $|1\rangle$. But that is what the parameter φ does in this context. Basically, it ensures the missing values for the coefficient of $|1\rangle$ when we have the product $e^{i\varphi}\sin\left(\frac{\theta}{2}\right)$. In particular, the complex number $e^{i\varphi}$ represents the "relative phase" of the quantum state $|\psi\rangle$. For this reason, we say the "relative phase" has a physical significance when describing a qubit, in opposition to the "global phase" that we may ignore.

2.2.3 Circuit-Based Model for Quantum Computing

The Circuit-Based Model for Quantum Computing is a model of quantum computation, where we mainly build what is called a quantum circuit. Basically, this quantum circuit describes a set of quantum and classical operations we will apply to some quantum and classical data, respectively. A quantum circuit is composed of quantum and classical registers (or memories).

These registers have several "wires" carrying information of its kind. Namely, a quantum register comprises some "quantum wires" carrying quantum information, while a classical register comprises some "classical wires" carrying classical information. More specifically, the quantum information operated in these quantum "wires" is usually through qubits. In a similar fashion, the classical information manipulated in the "classical wires" is usually through bits.

Additionally, other quantum circuits operating on quantum states in higher dimensions are also valid. However, they are not so popular in Quantum Computing compared to the others acting on two-dimensional Hilbert Spaces. In particular, we can build different quantum circuits that manipulate quantum states in three-dimensional Hilbert Spaces. In this case, we operate the quantum information in qutrits and classical information in trits. Generally, we can even have quantum circuits acting on quantum states in d-dimensional Hilbert Spaces, where we manipulate the quantum information in qudits and classical information in dits.

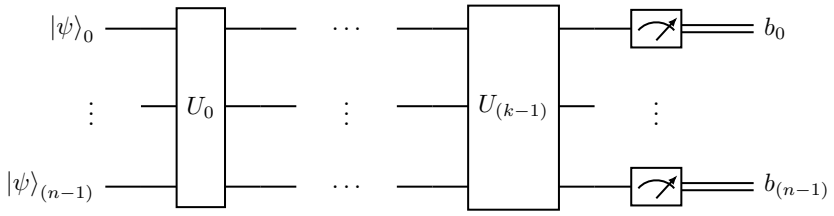


Figure 2.2: Circuit-Based Model for Quantum Computing, considering qubits.

Other relatively popular models for Quantum Computing are OWQC (One-Way Quantum Computing), AQC (Adiabatic Quantum Computing), and Topological Quantum Computing.

2.2.3.1 Elementary Gates for a Single Quantum Bit

The elementary gates for a single quantum bit are the ones that act on only one quantum bit at an operation time, such as the ones we will describe in the following set of paragraphs.

Pauli Gates

There are a total of four Pauli Gates. Three of these Pauli Gates act on three axes of the Bloch Sphere, which describes a qubit system. The following operators define these Pauli Gates:

$$\begin{aligned} \sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ \sigma_1 = X = NOT = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ \sigma_2 = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},\ \text{and } \sigma_3 = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \end{aligned} \tag{2.2.3.1.1}$$

In the Circuit-Based Model for Quantum Computing, we represent Pauli Gates as follows:

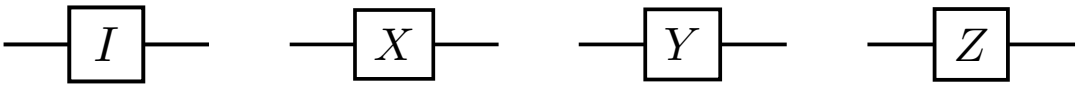


Figure 2.3: The Pauli Gates used in Circuit-Based model for Quantum Computing.

The I Gate does not result in any change to the qubit. The X Gate is equivalent to a bit flip, and performs the mappings $|0\rangle \mapsto |1\rangle$, and $|1\rangle \mapsto |0\rangle$. The Y Gate performs the mappings $|0\rangle \mapsto i|1\rangle$, and $|1\rangle \mapsto -i|0\rangle$. The Z Gate, which is also known as phase flip, performs the mappings $|0\rangle \mapsto |0\rangle$, and $|1\rangle \mapsto -|1\rangle$. In geometrical terms, the X, Y, and Z Gates corresponds to counter clockwise rotations of 180° (π radians), around the $\hat{X}$, $\hat{Y}$ and $\hat{Z}$ axis of the Bloch Sphere, respectively. The Pauli Gates are involutory, i.e., $I^2 = X^2 = Y^2 = Z^2 = -i \cdot X \cdot Y \cdot Z = I$, and thus, their own inverses, i.e., $I^{-1} \cdot I = I^2 = X^{-1} \cdot X = X^2 = Y^{-1} \cdot Y = Y^2 = Z^{-1} \cdot Z = Z^2 = I$.

Hadamard Gate

The H (Hadamard) Gate is one of the most important unitary operators, defined as follows:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \tag{2.2.3.1.2}$$

In the Circuit-Based Model for Quantum Computing, we represent this gate as follows:

Figure 2.4: Hadamard Gate in Circuit-Based Model for Quantum Computing.

The H (Hadamard) Gate creates an equally distributed quantum superposition of states when applied to the basis states $|0\rangle$ and $|1\rangle$. This gate performs the mappings $|0\rangle \mapsto |+\rangle$ and $|1\rangle \mapsto |-\rangle$. From these mappings, we have 50% of chance of "observing" $|0\rangle$ and $|1\rangle$, from the resulted quantum state $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. This unitary operator is involutory and its own inverse, since $H^2 = I$ and $H^{-1} \cdot H = H^2 = I$. In geometric terms, this operator corresponds to counter clockwise rotations of 180° (π radians) around the $\frac{(\hat{X}+\hat{Z})}{\sqrt{2}}$ axis of the Bloch Sphere.

Phase Shift Gates

The Ph (Phase Shift) Gates are the set of quantum gates performing shiftings on the phase of a qubit. These gates correspond to counter-clockwise rotations of π radians around the $\hat{Z}$ axis of the Bloch Sphere. Therefore, they are defined by the general unitary operator $R_z(\varphi)$:

$$Ph(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}, \text{ where } \varphi \in [0, 2\pi] \tag{2.2.3.1.3}$$

In the Circuit-Based Model for Quantum Computing, we represent this gate as follows:

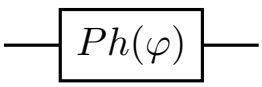


Figure 2.5: $Ph(\varphi)$ Gate in Circuit-Based Model for Quantum Computing.

The Z (Pauli-Z) Gate (see Section 2.2.3.1) can also be considered a Ph (Phase Shift) Gate.

S Gate

The S Gate is a special case of a Ph (Phase Shift) Gate, with $\varphi = \frac{\pi}{2}$. In geometric terms, this unitary operator performs a counter-clockwise rotation of 90° $\left(\frac{\pi}{2} \text{ radians}\right)$ around the $\hat{Z}$ axis of the Bloch Sphere. More specifically, the S Gate is defined by the following unitary matrix:

$$S = \sqrt{Z} = Ph\left(\frac{\pi}{2}\right) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \tag{2.2.3.1.4}$$

In the Circuit-Based Model for Quantum Computing, we represent this gate as follows:

Figure 2.6: S Gate in Circuit-Based Model for Quantum Computing.

The S Gate is hermitian, and thus, its inverse is its conjugate transpose, $S^\dagger$. In geometric terms, this unitary operator performs a clockwise rotation of 90° $\left(\frac{\pi}{2} \text{ radians}\right)$ around the $\hat{Z}$ axis of the Bloch Sphere. Namely, the $S^\dagger$ Gate is defined by the following unitary matrix:

$$S^\dagger = \sqrt{Z}^\dagger = Ph\left(-\frac{\pi}{2}\right) = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix} \tag{2.2.3.1.5}$$

In the Circuit-Based Model for Quantum Computing, we represent this gate as follows:

Figure 2.7: $S^\dagger$ Gate in Circuit-Based Model for Quantum Computing.

T Gate

The T Gate is a special case of a Ph (Phase Shift) Gate, with $\varphi = \frac{\pi}{4}$. In geometric terms, this unitary operator performs a counter-clockwise rotation of 45° $\left(\frac{\pi}{4} \text{ radians}\right)$ around the $\hat{Z}$ axis of the Bloch Sphere. More specifically, the T Gate is defined by the following unitary matrix:

$$T = \sqrt{S} = \sqrt[4]{Z} = Ph\left(\frac{\pi}{4}\right) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} \cdot (1+i) \end{bmatrix} \tag{2.2.3.1.6}$$

In the Circuit-Based Model for Quantum Computing, we represent this gate as follows:

Figure 2.8: T Gate in Circuit-Based Model for Quantum Computing.

The T Gate is hermitian, and thus, its inverse is its conjugate transpose, $T^\dagger$. In geometric terms, this unitary operator performs a clockwise rotation of 45° $\left(\frac{\pi}{4} \text{ radians}\right)$ around the $\hat{Z}$ axis of the Bloch Sphere. Namely, the $T^\dagger$ Gate is defined by the following unitary matrix:

$$T^\dagger = \sqrt{S}^\dagger = \sqrt[4]{Z}^\dagger = Ph\Big(-\frac{\pi}{4}\Big) = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} \cdot (1-i) \end{bmatrix} \tag{2.2.3.1.7}$$

In the Circuit-Based Model for Quantum Computing, we represent this gate as follows:

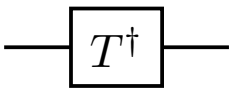


Figure 2.9: $T^\dagger$ Gate in Circuit-Based Model for Quantum Computing.

Squared Root Gates

The Squared Root Gates are the set of quantum gates represented by the unitary operators $\sqrt{U}$, from which, we can verify the equality $\sqrt{U} \cdot \sqrt{U} = \left(\sqrt{U}\right)^2 = U$, where $\left(\sqrt{U}\right)^2, \sqrt{U}, U \in \mathbb{C}^{(n\times n)}$.

Some notable examples of Squared Root Gates are the following unitary operators:

$$\begin{gathered} \sqrt{I} = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ \sqrt{X} = \frac{1}{2}\begin{bmatrix} (1+i) & (1-i) \\ (1-i) & (1+i) \end{bmatrix} = \begin{bmatrix} \left(\frac{1}{2}+\frac{1}{2}i\right) & \left(\frac{1}{2}-\frac{1}{2}i\right) \\ \left(\frac{1}{2}-\frac{1}{2}i\right) & \left(\frac{1}{2}+\frac{1}{2}i\right) \end{bmatrix}, \\ \sqrt{Y} = \frac{1}{2}\begin{bmatrix} (1+i) & -(1+i) \\ (1+i) & (1+i) \end{bmatrix} = \begin{bmatrix} \left(\frac{1}{2}+\frac{1}{2}i\right) & -\left(\frac{1}{2}+\frac{1}{2}i\right) \\ \left(\frac{1}{2}+\frac{1}{2}i\right) & \left(\frac{1}{2}+\frac{1}{2}i\right) \end{bmatrix}, \text{ and } \sqrt{Z} = S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \end{gathered} \tag{2.2.3.1.8}$$

$$\begin{gathered} \sqrt{H} = \begin{bmatrix} \left(\frac{\left(2+\sqrt{2}\right)}{4} + \frac{\left(2-\sqrt{2}\right)}{4}i\right) & \frac{(1-i)}{2\sqrt{2}} \\ \frac{(1-i)}{2\sqrt{2}} & \left(\frac{\left(2-\sqrt{2}\right)}{4} + \frac{\left(2+\sqrt{2}\right)}{4}i\right) \end{bmatrix}, \ \sqrt{S} = T = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}} \cdot (1+i) \end{bmatrix}, \\ \text{and } \sqrt{T} = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{\frac{1}{\sqrt{2}} \cdot (1+i)} \end{bmatrix} \end{gathered} \tag{2.2.3.1.9}$$

In the Circuit-Based Model for Quantum Computing, we represent these gates as follows:

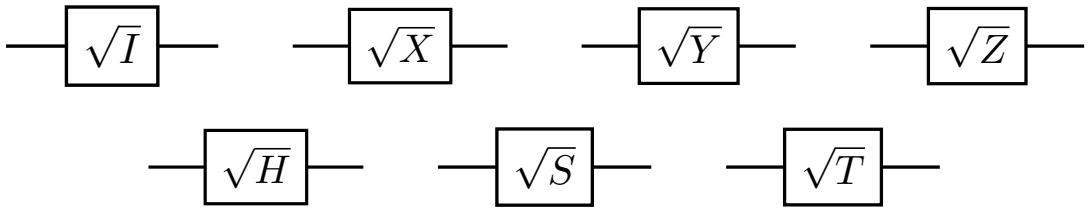


Figure 2.10: Some Squared Root Gates in Circuit-Based Model for Quantum Computing.

R_X, R_Y and R_Z Gates

Additionally, we can also manipulate the quantum state of a single qubit by applying to it the R_X, R_Y and R_Z Gates. More specifically, these gates correspond to rotations of θ radians around the $\hat{X}$, $\hat{Y}$ and $\hat{Z}$ axis of the Bloch Sphere, defined by the following set of unitary operators:

$$
\begin{aligned}
R_X(\theta) &= \cos\left(\frac{\theta}{2}\right)\cdot I - \sin\left(\frac{\theta}{2}\right)\cdot i\cdot X = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right)i \\ -\sin\left(\frac{\theta}{2}\right)i & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}, \\
R_Y(\theta) &= \cos\left(\frac{\theta}{2}\right)\cdot I - \sin\left(\frac{\theta}{2}\right)\cdot i\cdot Y = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}, \text{ and} \\
R_Z(\theta) &= \cos\left(\frac{\theta}{2}\right)\cdot I - \sin\left(\frac{\theta}{2}\right)\cdot i\cdot Z = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) - \sin\left(\frac{\theta}{2}\right)i & 0 \\ 0 & \cos\left(\frac{\theta}{2}\right) + \sin\left(\frac{\theta}{2}\right)i \end{bmatrix} = \\
&= \begin{bmatrix} e^{-\left(\frac{\theta}{2}\right)i} & 0 \\ 0 & e^{\left(\frac{\theta}{2}\right)i} \end{bmatrix}
\end{aligned}
\tag{2.2.3.1.10}
$$

In the Circuit-Based Model for Quantum Computing, we represent these gates as follows:

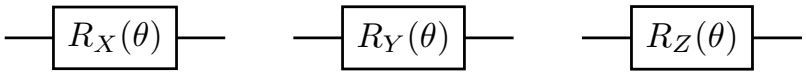


Figure 2.11: R_X, R_Y, and R_Z Gates in Circuit-Based Model for Quantum Computing.

Measurement Gate

Finally, we also have the Measurement Gate, which is responsible to measure the current quantum state of a qubit in the $\mathbb{Z}$-basis (Standard Computational basis) by default, collapsing its wavefunction. In the Circuit-Based Model for Quantum Computing, we represent it as:

Figure 2.12: Measurement Gate in Circuit-Based Model for Quantum Computing.

2.2.3.2 Measurement Bases of a Single Quantum Bit

Now that we reviewed the elementary gates for a single qubit, we can use them to prepare an arbitrary qubit on any measurement basis. In particular, there are three measurement bases we use for single-qubit systems. These measurement bases are the $\mathbb{Z}$-basis (Standard Computational basis), the $\mathbb{X}$-basis (Diagonal Hadamard basis), and the $\mathbb{Y}$-basis (Diagonal Imaginary basis), corresponding to the axes of the Bloch Sphere. By default, when we measure a qubit, the measurement is performed in the $\mathbb{Z}$-basis (Standard Computational basis) since it corresponds to the equivalent classical computational states $|0\rangle$ and $|1\rangle$. However, if we apply some unitary operations, we can prepare and measure a qubit in one of the other bases.

$\mathbb{Z}$-basis (Standard Computational basis)

First, we start by the $\mathbb{Z}$-basis (Standard Computational basis), which is the default one. For this reason, we can prepare a qubit on such a measurement basis by applying the Pauli-I Gate (or even no elementary gate at all to the qubit since the Pauli-I Gate does not change its quantum state). Note that by default, we often start a qubit configured in the $|0\rangle$ (ground state), which corresponds to one of the states comprised in the Z-axis of the Bloch Sphere. In this case, we can denote the $\mathbb{Z}$-basis (Standard Computational basis) as $\tilde{Z} = \{+\tilde{z}, -\tilde{z}\} = \{|0\rangle, |1\rangle\}$.

In the Bloch Sphere representation for a qubit, we represent this basis as follows:

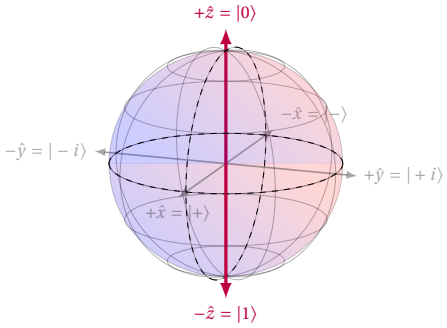


Figure 2.13: Representation of the $\mathbb{Z}$-basis (Standard Computational basis) in a Bloch Sphere.

In the Circuit-Based Model for Quantum Computing, we represent this basis as follows:

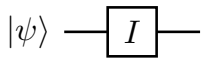


Figure 2.14: Measuring in the $\mathbb{Z}$-basis (Standard Computational basis) in Circuit-Based Model for Quantum Computing.

$\mathbb{X}$-basis (Hadamard Diagonal basis)

Another well-known measurement basis is the $\mathbb{X}$-basis (Hadamard Diagonal basis). We can prepare a qubit on this measurement basis by simply applying the Hadamard Gate. Note that if we start a qubit configured in the $|0\rangle$ (ground state) and then, apply the Hadamard Gate, the qubit will be in the quantum state $|+\rangle$. This quantum state corresponds to one of the states comprised in the X-axis of the Bloch Sphere. In particular, we can denote the $\mathbb{X}$-basis (Hadamard Diagonal basis) as $\tilde{X} = \{+\tilde{x}, -\tilde{x}\} = \{|+\rangle, |-\rangle\}$, shown in the Bloch Sphere as follows:

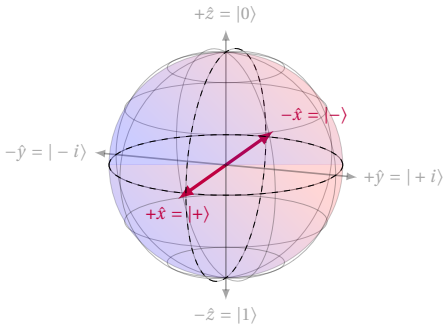


Figure 2.15: Representation of the $\mathbb{X}$-basis (Hadamard Diagonal basis) in a Bloch Sphere.

In the Circuit-Based Model for Quantum Computing, we represent this basis as follows:

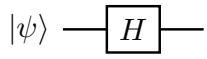


Figure 2.16: Measuring in the $\mathbb{X}$-basis (Hadamard Diagonal basis) in Circuit-Based Model for Quantum Computing.

$\mathbb{Y}$-basis (Imaginary Diagonal basis)

Finally, we also have the $\mathbb{Y}$-basis (Imaginary Diagonal basis). Namely, we can prepare a qubit on this measurement basis by applying the Hadamard and S Gates. Note that if we start a qubit configured in the $|0\rangle$ (ground state) and apply the Hadamard Gate, followed by the S Gate, the qubit will be configured in the quantum state $|+i\rangle$. In geometric terms, this quantum state corresponds to one of the states comprised in the $\hat{Y}$-axis of the Bloch Sphere. In particular, we can denote the $\mathbb{Y}$-basis (Imaginary Diagonal basis) as $\tilde{Y} = \{+\tilde{y}, -\tilde{y}\} = \{|+i\rangle, |-i\rangle\}$.

In the Bloch Sphere representation for a qubit, we represent this basis as follows:

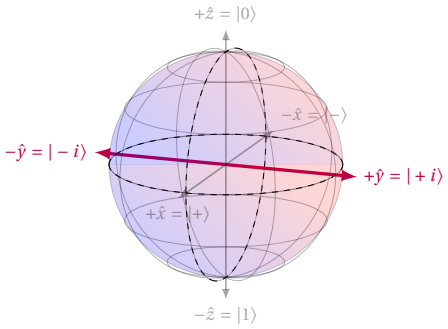


Figure 2.17: Representation of the $\mathbb{Y}$-basis (Imaginary Diagonal basis) in a Bloch Sphere.

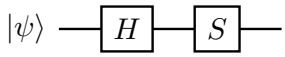


Figure 2.18: Measuring in the $\mathbb{Y}$-basis (Imaginary Diagonal basis) in Circuit-Based Model for Quantum Computing.

2.2.3.3 Elementary Gates for Multiple Quantum Bits

The elementary gates for multiple quantum bits are the ones that act on only more than a quantum bit at an operation time, such as the ones described in the following set of paragraphs.

SWAP Gate

The SWAP Gate swaps the current state of two qubits in a physical system. More specifically, it performs the mapping $|\psi_0\rangle|\psi_1\rangle \mapsto |\psi_1\rangle|\psi_0\rangle$ and is defined by the following unitary operator:

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{2.2.3.3.1}$$

In the Circuit-Based Model for Quantum Computing, we represent this gate as follows:

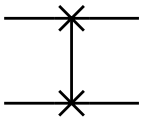


Figure 2.19: SWAP Gate in Circuit-Based Model for Quantum Computing.

Controlled Gates

The Controlled Gates (or Controlled-U Gates) act on two or more qubits, where one or more qubits behave as a control for some quantum operation U on another one or more target qubits. The quantum operation U to be applied to the target qubit(s) can be any quantum gate, such as a Pauli Gate, a Hadamard Gate, a Phase Shift Gate, an Inverse Gate, a Square Root Gate, a SWAP Gate, a generic R_X, R_Y, or R_Z Gate, or even, another valid unitary operator.

If *all* the control qubit(s) is/are in the state $|1\rangle$, this quantum gate applies the unitary operator U to the respective target qubit(s). Otherwise, the target qubit(s) remains unchanged.

The Controlled Gates $C^{\otimes m}(U)$, given U as an input parameter, are generally defined as:

$$C^{\otimes m}(U) = \begin{bmatrix} 1 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & u_{(0,0)} & \dots & u_{(0,(n-k-1))} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & u_{((n-k-1),0)} & \dots & u_{((n-k-1),(n-k-1))} \end{bmatrix}, \tag{2.2.3.3.2}$$

$$\text{where } m \geq 1 \text{ and } U = \begin{bmatrix} u_{(0,0)} & \dots & u_{(0,(n-k-1))} \\ \vdots & \ddots & \vdots \\ u_{((n-k-1),0)} & \dots & u_{((n-k-1),(n-k-1))} \end{bmatrix}.$$

Additionally, in the Circuit-Based Model for Quantum Computing, we can generally represent these Controlled Gates $C^{\otimes m}(U)$. For the simplest case, with only one control qubit (with $m = 1$), we can represent the Controlled Gates $C(U)$. Some notable examples of Controlled Gates $C^{\otimes m}(U)$ with different number of controlled qubits are the following ones:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \text{ and } Toffoli = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \tag{2.2.3.3.3}$$

In the Circuit-Based Model for Quantum Computing, we represent these gates as follows:

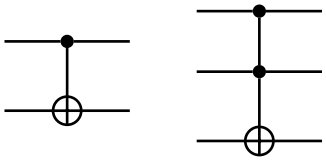


Figure 2.20: *CNOT* and *Toffoli* Gates in Circuit-Based Model for Quantum Computing.

The *CNOT* Gate is often applied after a Hadamard Gate to create quantum entangled states, such as the well-known Bell and GHZ states. In particular, this quantum gate is, in a certain sense, related to the XOR operation since, when applied to a two qubit-system, it performs the mapping $|\psi_{1_{control}}, \psi_{2_{target}}\rangle \mapsto |\psi_{1_{control}}, (\psi_{1_{control}} \otimes \psi_{2_{target}})\rangle$. Similarly, we can think about the Toffoli (or *CCNOT*) Gate as being the generalization of the *CNOT* Gate for three qubits with two control qubits and one target qubit, where it is performed the mapping $|\psi_{1_{control}}, \psi_{2_{control}}, \psi_{3_{target}}\rangle \mapsto |\psi_{1_{control}}, \psi_{2_{control}}, ((\psi_{1_{control}} \wedge \psi_{2_{control}}) \otimes \psi_{3_{target}})\rangle$.

2.2.4 Configurations of Quantum Entanglements

After learning the most known elementary gates for both single and multiple qubits, we can use them to create some specific configurations of Quantum Entanglements mentioned before (see Section 2.1.7). We can apply these particular Quantum Entanglements in the context of Quantum Computing, namely for Quantum Communications and Quantum Cryptography, among many other applications. One observation we can make on such quantum entangled states is that we cannot build them as a mathematical tensor product of other quantum states.

2.2.4.1 Bell States

The Bell states [232, 233] [1] are bipartite quantum states of two qubits which are maximally entangled. In particular, these quantum entangled states compose an orthonormal basis in a four-dimensional Hilbert Space, $\mathcal{H}_1 \otimes \mathcal{H}_2$. They have a total of four possible configurations:

$$\begin{aligned} |\phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle^{\otimes 2} \pm |1\rangle^{\otimes 2}) = \frac{(|00\rangle \pm |11\rangle)}{\sqrt{2}} \\ |\psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle \pm |1\rangle \otimes |0\rangle) = \frac{(|01\rangle \pm |10\rangle)}{\sqrt{2}} \end{aligned} \tag{2.2.4.1.1}$$

In the Circuit-Based Model for Quantum Computing, we can prepare them as follows:

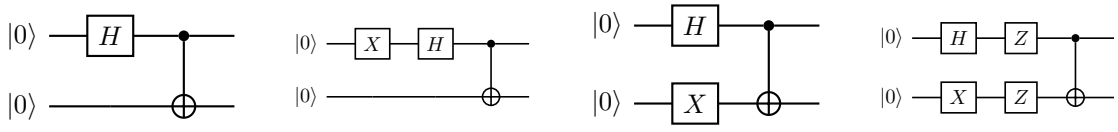


Figure 2.21: Preparing the Bell states in Circuit-Based Model for Quantum Computing.

[1] The Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,)$ is also known as the EPR pair.

The notion of the Bell state refers to the quantum superposition of all linear combinations of two pure quantum states $|0\rangle$ and $|1\rangle$. The measurement of one qubit of this entangled state will make the other qubit collapse immediately, resulting in two groups of correlated outcomes. Here, these correlated outcomes happen randomly with equal probability after the measurements of those qubits. In normal conditions, the group of these correlated outcomes depends on the configuration of the Bell state we used initially to prepare the two qubits.

On the other hand, we can also measure a certain quantum state on the Bell state basis. These types of measurements are often called BSMs (Bell State Measurements). Namely, in the Circuit-Based Model for Quantum Computing, we can prepare these BSMs as follows:

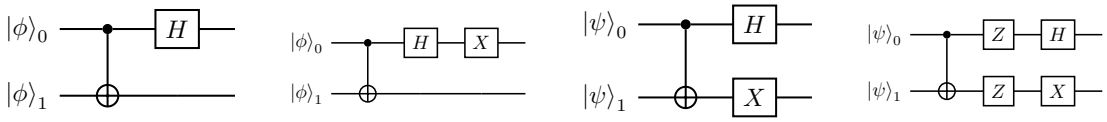


Figure 2.22: Measuring in the Bell state bases in Circuit-Based Model for Quantum Computing.

2.2.4.2 GHZ States

The GHZ states [234] are multipartite quantum states of three or more qubits which are maximally entangled. More specifically, these quantum entanglements have extremely non-classical properties. The notion of GHZ state refers to the quantum superposition of all possible pure quantum states with the exact same quantum state, being all either $|0\rangle$ or $|1\rangle$. They compose an orthonormal basis in n-dimensional Hilbert Space, $\mathcal{H}_1 \otimes ... \otimes \mathcal{H}_n$, with $n \geq 3$:

$$|GHZ_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}) = \frac{(|0...00\rangle + |1...11\rangle)}{\sqrt{2}} \tag{2.2.4.2.1}$$

In the simplest case, we can define the GHZ state concerning only 3 qubits as follows:

$$|GHZ_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes 3} + |1\rangle^{\otimes 3}) = \frac{(|000\rangle + |111\rangle)}{\sqrt{2}} \tag{2.2.4.2.2}$$

We can consider the GHZ state as the generalization of the EPR pair for the case $n \geq 3$, also exhibiting a strong correlation. Namely, under normal conditions, if there is no decoherence, we will obtain the same outcome for all the involved qubits after measuring one of them.

In the Circuit-Based Model for Quantum Computing, we can prepare GHZ states as:

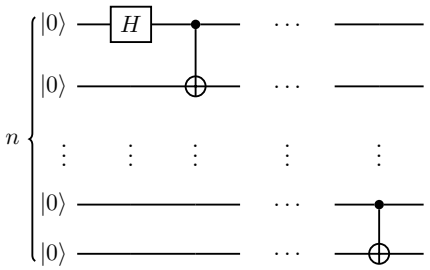


Figure 2.23: Preparing the GHZ state in Circuit-Based Model for Quantum Computing.

Once again, we can measure a given quantum state on the GHZ state basis. Namely, in the Circuit-Based Model for Quantum Computing, we can prepare these measurements as follows:

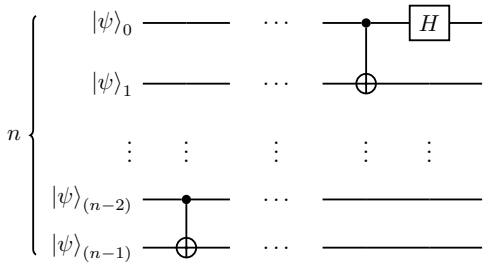


Figure 2.24: Measuring in the GHZ state basis in Circuit-Based Model for Quantum Computing.

2.2.4.3 W States

The W states [235] are multipartite quantum entangled states of three or more qubits. The notion of W state refers to the quantum superposition with equal expansion coefficients of all possible pure quantum states, in which only one of the qubits has the quantum state $|1\rangle$ while all the remaining ones have the quantum state $|0\rangle$. These quantum entangled states also compose an orthonormal basis in a n-dimensional Hilbert Space, $\mathcal{H}_1 \otimes ... \otimes \mathcal{H}_n$, with $n \geq 3$:

$$|W_n\rangle = \frac{(|0...01\rangle + |0...10\rangle + |1...00\rangle)}{\sqrt{n}} \tag{2.2.4.3.1}$$

In the simplest case, we can define the W state concerning only 3 qubits as follows:

$$|W_n\rangle = \frac{(|001\rangle + |010\rangle + |100\rangle)}{\sqrt{3}} \tag{2.2.4.3.2}$$

Additionally, we can also negate the W state, having the notation of $|\overline{W}\rangle$, defined as follows:

$$|\overline{W}_n\rangle = \frac{(|0...11\rangle + |1...01\rangle + |1...10\rangle)}{\sqrt{n}} \tag{2.2.4.3.3}$$

Similarly, in the simplest case, the negated W state for only 3 qubits is defined as follows:

$$|\overline{W}_3\rangle = \frac{(|011\rangle + |101\rangle + |110\rangle)}{\sqrt{3}} \tag{2.2.4.3.4}$$

In the Circuit-Based Model for Quantum Computing, we can prepare W states as:

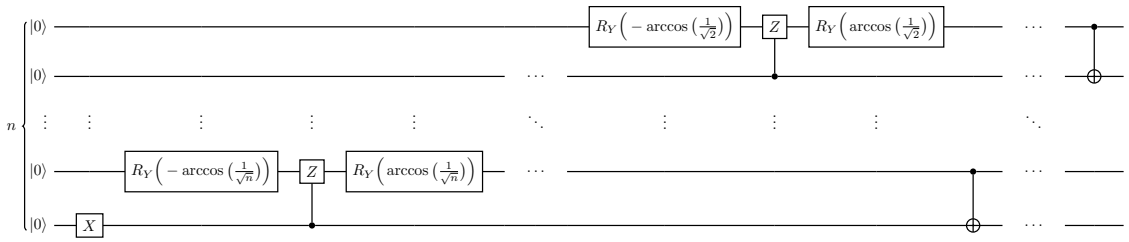


Figure 2.25: Preparing the W state in Circuit-Based Model for Quantum Computing.

Once again, we can measure a given quantum state on the W state basis. Namely, in the Circuit-Based Model for Quantum Computing, we can prepare these measurements as follows:

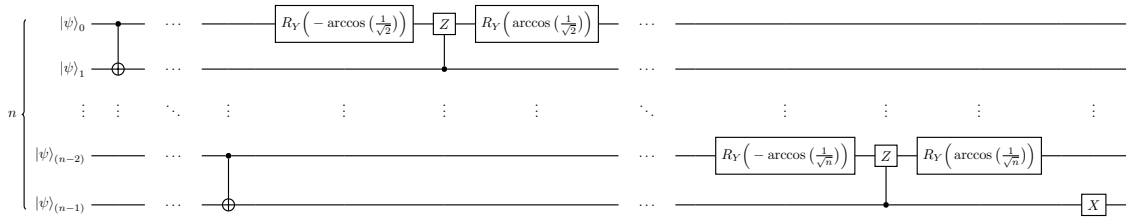


Figure 2.26: Measuring in the W state basis in Circuit-Based Model for Quantum Computing.

In particular, this quantum entanglement is more robust against losses or measurements of a single qubit compared to GHZ states. For a W state with n qubits, an entangled quantum state of $(n-1)$ qubits remains after a loss or measurement of a single qubit. For this reason, we often say that a W state is "less entangled" than a GHZ state. Both GHZ and W states are non-biseparable and cannot be transformed into each other by local quantum operations.

2.2.4.4 Resource States

The Resource states [236–240] are multipartite quantum states of multiple qubits being highly entangled. These quantum states compose an orthonormal basis in an n-dimensional Hilbert Space, $\mathcal{H}_1 \otimes ... \otimes \mathcal{H}_n$, with $n \geq 2$. Basically, we use Resource states to establish undirected "graphs" of qubits, and we can classify them as either a Graph state or a Cluster state. Here, the main difference is that a Graph state acts as a representation of a graph of qubits acting as nodes concerning a given set of edges between them. Differently, a Cluster state is a graph of qubits representing a fully (or almost fully) connected lattice structure. For this reason, the Cluster state does not need to consider any given set of edges between the qubits as input.

These quantum entangled states are useful to some topics and applications in Quantum Computing, such as Quantum Error-Correction Codes, Quantum Entanglement Measurements, Quantum Entanglement Purifications, One-Way Quantum Computing, or even large Quantum Communication Networks. Additionally, these quantum states can also be very suitable to establish quantum communication links, and we can see these Resource states as appropriate for the configuration between several components of a possible global Quantum Internet.

Both Graph and Cluster states are different from the GHZ and W states, in such a way that it is much harder to eliminate the Quantum Entanglement by Projective Measurements.

The Graph states are multipartite quantum states which we can define in two equivalent ways. Namely, we can introduce these multipartite quantum entangled states through the notion of the Circuit-Based Model for Quantum Computing or formalism of Stabilizer Codes.

In particular, since Graph states represent "graphs" of qubits, we can use them to define n-vertex paths or n-vertex polygons of qubits, denoted as $|P_n\rangle$ and $|K_n\rangle$, respectively.

Given a graph (also called a resource in this context) $G = (V, E)$, with the set of vertices V and another set of undirected edges E, the corresponding Resource State, is defined as follows:

$$|G\rangle = \prod_{(a,b)\in E} CZ^{\{a,b\}} \otimes |+\rangle^{\otimes |V|} \tag{2.2.4.4.1}$$

More in detail, a multipartite Resource State is created, by performing the following steps:

1. Apply the Quantum Hadamard Transform (see Section 2.2.5.2) to the $|V|$ qubits that represents all the vertices of the resource (or graph) to obtain $H^{\otimes |V|} \otimes |0\rangle^{\otimes |V|} = |+\rangle^{\otimes |V|}$.
2. For each edge (a, b)[2] $\in E$, apply the CZ gate (see Section 2.2.3.3) to the qubits that represents all the vertices of the resource (or graph) to obtain $CZ^{\{a,b\}} \otimes |+\rangle^{|V|}$.

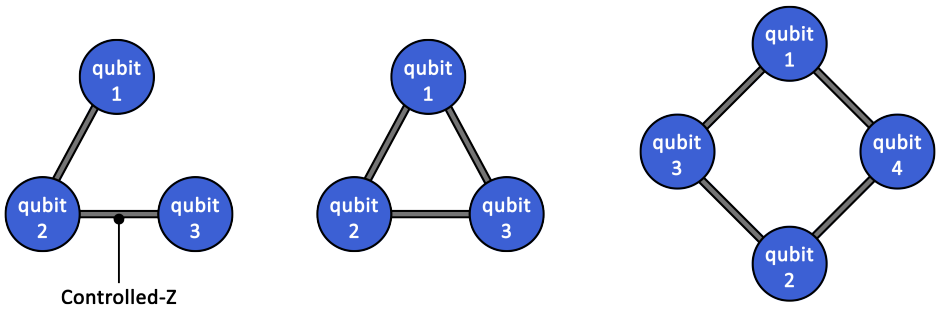
For example, a Graph state can have some of the following configurations:

a) $|P_3\rangle = \frac{1}{\sqrt{8}}$ ($|000\rangle$ + $|001\rangle$ + $|010\rangle$ - $|011\rangle$ + $|100\rangle$ + $|101\rangle$ - $|110\rangle$ + $|111\rangle$)

b) $|K_3\rangle = \frac{1}{\sqrt{8}}$ ($|000\rangle$ + $|001\rangle$ + $|010\rangle$ - $|011\rangle$ + $|100\rangle$ - $|101\rangle$ - $|110\rangle$ - $|111\rangle$)

c) $|K_4\rangle = \frac{1}{4}$ ($|0000\rangle$ + $|0001\rangle$ + $|0010\rangle$ + $|0011\rangle$ + $|0100\rangle$ - $|0101\rangle$ - $|0110\rangle$ + $|0111\rangle$
+ $|1000\rangle$ - $|1001\rangle$ - $|1010\rangle$ + $|1011\rangle$ + $|1100\rangle$ + $|1101\rangle$ + $|1110\rangle$ + $|1111\rangle$)

Namely, we can represent the previous examples of Graph states as follows:



a Three-vertex path. b Triangle on three vertices. c Diamond on four vertices.

Figure 2.27: Some examples of Graph states.

Any connected Graph state with $m = |V|$ vertices is a maximally entangled m-particle state and violates some Bell Inequality. On the other hand, the Cluster State is a particular instance of Graph state, where the underlying graph is a connected subset of a d-dimensional lattice.

[2]The pair of vertices forming an edge on a Resource State is commutative, $(a, b) = (b, a)$. Therefore, the order of qubits of this pair used as control-qubit or target-qubit for the CZ gate is irrelevant.

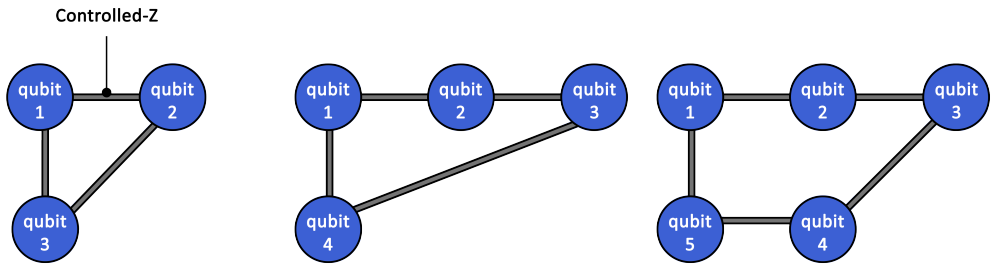
For example, a Cluster State can have some of the following configurations:

a) $|CL_3\rangle = \frac{1}{\sqrt{8}} (|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle - |110\rangle - |111\rangle)$

b) $|CL_4\rangle = \frac{1}{4} (|0000\rangle + |0001\rangle + |0010\rangle - |0011\rangle + |0100\rangle + |0101\rangle - |0110\rangle + |0111\rangle$
$+ |1000\rangle - |1001\rangle + |1010\rangle + |1011\rangle - |1100\rangle + |1101\rangle + |1110\rangle + |1111\rangle)$

c) $|CL_5\rangle = \frac{1}{\sqrt{32}} (|00000\rangle + |00001\rangle + |00010\rangle - |00011\rangle + |00100\rangle + |00101\rangle - |00110\rangle + |00111\rangle$
$+ |01000\rangle + |01001\rangle + |01010\rangle - |01011\rangle - |01100\rangle - |01101\rangle + |01110\rangle - |01111\rangle$
$+ |10000\rangle - |10001\rangle + |10010\rangle + |10011\rangle + |10100\rangle - |10101\rangle - |10110\rangle - |10111\rangle$
$- |11000\rangle + |11001\rangle - |11010\rangle - |11011\rangle + |11100\rangle - |11101\rangle - |11110\rangle - |11111\rangle)$

Once again, we can represent the previous examples of Graph states as follows:



a 2D Cluster State with 3 qubits. b 2D Cluster State with 4 qubits. c 2D Cluster State with 5 qubits.

Figure 2.28: Some examples of 2D Cluster States.

2.2.5 Common Quantum Routines

After learning the most known elementary gates for both single and multiple qubits, we can use them to create some common Quantum Routines. We can apply these routines in several configurations of Quantum Entanglements and Quantum Algorithms commonly studied.

2.2.5.1 Quantum Fourier Transform

The DFT (Discrete Fourier Transform) [241, 242] is a unitary transform used for numerical computation in digital signal processing related to the respective times and frequencies. Namely, we often use the DFT for spectrum analysis, data compression, partial differential equations, or mathematical operations such as convolutions and multiplication of large integer numbers.

The DFT transforms a sequence of n discrete-time samples $\{x_j\} = \{x_0, x_1, ..., x_{(n-1)}\}$ into another sequence of n discrete-frequency samples $\{y_k\} = \{y_0, y_1, ..., y_{(n-1)}\}$, where the both sequences are, in fact, composed by n complex numbers, being mathematically defined as:

$$y_k = \sum_{j=0}^{(n-1)} x_j \cdot e^{-\left(i \cdot \frac{2\pi}{n} kj\right)} = \sum_{j=0}^{(n-1)} x_j \cdot \left[\cos\left(\frac{2\pi}{n} kj\right) - i \cdot \sin\left(\frac{2\pi}{n} kj\right) \right] \tag{2.2.5.1.1}$$

Oppositely to the DFT, the IDFT (Inverse Discrete Fourier Transform) basically transforms a sequence of n discrete-frequency samples $\{y_k = \{y_0, y_1, ..., y_{(n-1)}\}$ into another sequence of n discrete-time samples $\{x_j\} = \{x_0, x_1, ..., x_{(n-1)}\}$, being mathematically defined as following:

$$x_j = \frac{1}{n} \sum_{k=0}^{(n-1)} y_k \cdot e^{\left(i \cdot \frac{2\pi}{n} kj\right)} = \frac{1}{n} \sum_{k=0}^{(n-1)} y_k \cdot \left[\cos\left(\frac{2\pi}{n} kj\right) + i \cdot \sin\left(\frac{2\pi}{n} kj\right) \right] \tag{2.2.5.1.2}$$

The QFT (Quantum Fourier Transform) [243] is the quantum analog of the DFT, being computed originally in n^2 operations, which can be efficiently improved, in order to take only $n \cdot \log(n)$ operations, with a time complexity of $O(n)$. For this reason, this unitary quantum operator is exponential faster than its best counterpart in the classical regime, the FFT (Fast Fourier Transform), which is computed in $n \cdot 2^n$ operations, with a time complexity of $O(2^n)$.

More specifically, the QFT is an operator acting on a quantum state $|x\rangle = \sum_{i=0}^{(2^n-1)} x_i |i\rangle$ and maps it to a quantum state $|y\rangle = \sum_{i=0}^{(2^n-1)} y_i |i\rangle$, according to the following formula:

$$y_k = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{(2^n-1)} x_j \omega_{2^n}^{-jk} = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{(2^n-1)} x_j e^{-\left(i \cdot \frac{\pi}{2^{(n-1)}} kj\right)}, \text{ where } k = 0, 1, ..., (2^n - 1) \tag{2.2.5.1.3}$$

Oppositely, the IQFT (Inverse Quantum Fourier Transform) acts similarly to the QFT but with the sign of the phase factor inverted. Namely, it acts on a quantum state $|y\rangle = \sum_{i=0}^{(2^n-1)} y_i |i\rangle$ and maps it to a quantum state $|x\rangle = \sum_{i=0}^{(2^n-1)} x_i |i\rangle$, according to the following formula:

$$x_j = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{(2^n-1)} y_k \omega_{2^n}^{jk} = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{(2^n-1)} y_k e^{\left(i \cdot \frac{\pi}{2^{(n-1)}} kj\right)}, \text{ where } j = 0, 1, ..., (2^n - 1) \tag{2.2.5.1.4}$$

In this mathematical formulation, if we set the equality $N = 2^n$, we also have the equality $\omega_N = \omega_{2^n} = e^{\left(i \cdot \frac{2\pi}{N}\right)} = e^{\left(i \cdot \frac{\pi}{2^{(n-1)}}\right)}$ and we have the equality $\omega_N^m = \omega_{2^n}^m = e^{\left(i \cdot \frac{2\pi}{N} m\right)} = e^{\left(i \cdot \frac{\pi}{2^{(n-1)}} m\right)}$ as the m^{th} root of unity. Then, we can define the unitary operator F_N for the QFT as follows:

$$F_N = \frac{1}{\sqrt{N}} = \frac{1}{\sqrt{2^n}} = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \dots & \omega^{(N-1)} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \dots & \omega^{2\times(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \dots & \omega^{3\times(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{(N-1)} & \omega^{2\times(N-1)} & \omega^{3\times(N-1)} & \dots & \omega^{(N-1)\times(N-1)} \end{bmatrix} \tag{2.2.5.1.5}$$

The QFT is a very well-known and popular routine in Quantum Computing, namely because it is strongly related to Shor's Algorithm and its exponential speedup. More specifically, we apply the QFT in Shor's [150, 151] and Phase Estimation Algorithms [244]. In Shor's Algorithm, we can use this routine for Factoring and computing the Discrete Logarithm. In the Phase Estimation Algorithm, we use it for estimating the eigenvalues of a unitary operator.

2.2.5.2 Quantum Hadamard Transform

The Hadamard Transform [245, 246] is a generalized class of multidimensional DFTs of size 2^n, which performs an orthogonal, symmetric, and linear operation on 2^n complex numbers.

We can represent this DFT as a family of operators, recursively, starting with its base case:

$$H_0 = 1 \tag{2.2.5.2.1}$$

Then, we can generalize from the base case to the remaining cases as follows:

$$H_n = H^{\otimes n} = \frac{1}{\sqrt{2}} \begin{bmatrix} H_{(n-1)} & H_{(n-1)} \\ H_{(n-1)} & -H_{(n-1)} \end{bmatrix} \tag{2.2.5.2.2}$$

Here, $\frac{1}{\sqrt{2}}$ works as the normalization factor to keep the linearity of Quantum Mechanics.

Since H_1 is equivalent to the Hadamard Gate for a single qubit (see Section 2.2.3.1), then, we have that for $n \geq 2$, the general operator H_n can be additionally defined as follows:

$$H_n = H^{\otimes n} = H_1 \otimes H_{(n-1)} \tag{2.2.5.2.3}$$

The Quantum Hadamard Transform is nothing more than the Hadamard Transform performed by any quantum computational device. In the domain of Quantum Computing, due to its inherent quantum parallelism, we can execute the Quantum Hadamard Transform with $\log(n)$ operations, with a time complexity of $O(1)$. In terms of comparison, its best classical counterpart is the Fast Walsh–Hadamard Transform, computed in $n\log(n)$ operations, with a time complexity of $O(n)$. For this reason, the Quantum Hadamard Transform is always much faster than the classical Fast Walsh–Hadamard Transform [247]. We use this transform in most Quantum Algorithms known, such as Grover's [152] and Shor's [150, 151] Algorithms. In addition, the Quantum Hadamard Transform is often used in random processes, such as some current proofs of Quantum Advantage, since it is a way of exploring all the possible solutions simultaneously for a given problem due to the resulting Quantum Superpositions.

2.2.5.3 Quantum Teleportation

The Quantum Teleportation is a technique to transfer quantum information via a qubit [248–252]. In this technique, the sender knows neither the location of the receiver nor the quantum state that will be transferred to the receiver. Namely, this procedure is of great importance for Quantum Communications and Quantum Cryptography, being one pillar for Quantum Internet. For the procedure of Quantum Teleportation, we need to consider:

- A source S, which is mainly responsible for generating and distributing pairs of bipartite quantum entangled states, such as EPR pairs (see Section 2.2.4.1).
- Two parties, A and B, which are able to handle (or store) quantum information.
- A classical communication channel between the two parties A and B.

Then, the procedure of quantum teleportation proceeds as described following:

1. Let $|\psi\rangle$ be the quantum state to be transferred (or "teleported") from A to B.
2. The source S generates an EPR pair $|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$, sending one qubit of it, $|\phi^+\rangle_A$, to the location of A and the other qubit of it, $|\phi^+\rangle_B$ to the location of B.
3. Then, the party A performs a BSM (see Section 2.2.4.1) on both qubits in its possession, the qubit, $|\psi\rangle$, to be transferred to the location of B, and its part of the EPR pair, $|\phi^+\rangle_A$.
4. Next, the party A stores one of the four possible classical outcomes resulting from the BSM, encoding them in two classical bits b_0 and b_1, discarding its both qubits.
5. The party A sends these two classical bits b_0 and b_1 to the location of B through the classical communication channel between their respective locations.
6. Finally, the party B will operate its part of the EPR pair, $|\phi^+\rangle_B$, with respect to the received classical bits b_0 and b_1, according to the specification given in the following Table 2.1:

b_0	b_1	$\|\phi^+\rangle_B$	B's Operation
0	0	$\alpha\|0\rangle_B + \beta\|1\rangle_B$	I Gate
0	1	$\alpha\|1\rangle_B + \beta\|0\rangle_B$	X Gate
1	0	$\alpha\|0\rangle_B - \beta\|1\rangle_B$	Z Gate
1	1	$\alpha\|1\rangle_B - \beta\|0\rangle_B$	X Gate and Z Gate

Table 2.1: Set of quantum operations to be performed by the party B on its qubit $|\phi^+\rangle_B$ according to the received classical bits b_0 and b_1.

Now, we illustrate an example of Quantum Teleportation in the following Figure 2.29:

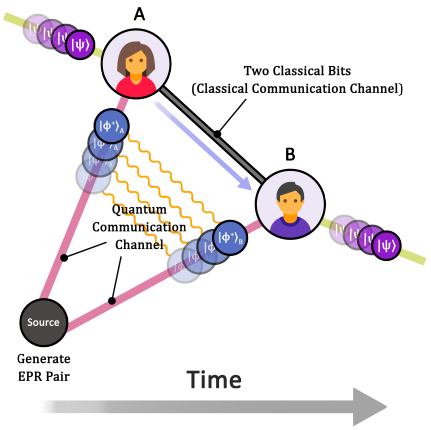


Figure 2.29: Quantum Teleportation for the parties A and B.

The step 5 is the only potentially time-consuming step since the transfer of classical information is always limited by the speed of light. Namely, Quantum Teleportation can offer another point of view on why we cannot use Quantum Entanglement to transfer *useful* information in an eventual FTL Communication. Note the party A always need to classically

communicate to the party B what operation the latter needs to perform in order to "recreate" the quantum state being "teleported" initially at the location of A. In simple terms, we always need to transfer two classical bits to achieve a transfer of one single qubit between locations.

2.2.5.4 Quantum Entanglement Swapping

As seen before, Quantum Teleportation enables the transmission of arbitrary pure quantum states between two parties. However, it is also possible to "teleport" mixed quantum states which we can see as the quantum state of a single quantum physical subsystem of a quantum entangled pair. Imagine that two parties A and B share an entangled quantum state, such as an EPR pair, and the party B "teleports" its qubit to a third-party C, then the qubit of the party A is now entangled with the one that the party C possesses. We often refer to this quantum routine as Quantum Entanglement Swapping [253–255]. It allows the Quantum Teleportation across 3 parties for huge distances (usually above 100 kms), where the probability of having missing photons became high due to some physical phenomena inevitably occurring in the mediums, such as Photoelectric Effect, Compton Effect or Birefringence, among many others.

More specifically, we can generalize this quantum routine for a sequence of an arbitrary number n of parties P_0, P_1, ..., $P_{(n-1)}$, with $n \geq 3$, allowing Quantum Communications over arbitrarily large distances. Here, note that the "middle parties" P_k need to always perform a BSM on their parts of the pairs of entangled quantum states shared with the previous and next parties on the sequence of parties, namely $P_{(k-1)}$ and $P_{(k+1)}$, where $0 < k < (n-1)$.

Namely, for the case of $n = 3$, considering the sequence of parties A, B, and C, the routine of Quantum Entanglement Swapping needs to consider the existence of the following elements:

- Two sources, S_0 and S_1, generating and distributing entangled pairs, such as EPR pairs.
- Three parties, A, B, and C, capable of handle (or store) quantum information.
- A classical communication channel between the two parties B and C.

Then, the routine of Quantum Entanglement Swapping for $n = 3$ proceeds as follows:

1. The sources, S_0 and S_1, generate two EPR pairs, $|\phi^{+\prime}\rangle_{AB'} = \frac{1}{\sqrt{2}}(|00\rangle_{AB'} + |11\rangle_{AB'})$ and $|\phi^{+\prime\prime}\rangle_{B''C} = \frac{1}{\sqrt{2}}(|00\rangle_{B''C} + |11\rangle_{B''C})$, distributing each qubit of each pair, in such a way that A and C hold $|\phi^{+\prime}\rangle_A$ and $|\phi^{+\prime\prime}\rangle_C$, respectively, while B hold $|\phi^{+\prime}\rangle_{B'}$ and $|\phi^{+\prime\prime}\rangle_{B''}$.
2. Then, the party B performs a BSM on both qubits in its possession, $|\phi^{+\prime}\rangle_{B'}$ and $|\phi^{+\prime\prime}\rangle_{B''}$.
3. Next, the party B stores one of the four possible classical outcomes resulting from the BSM, encoding them in two classical bits b_0 and b_1, discarding its both qubits.
4. The party B sends these two classical bits b_0 and b_1 to the location of C through the classical communication channel between their respective locations.
5. Finally, the party C will operate its part of the EPR pair, $|\phi^{+\prime\prime}\rangle_C$, with respect to the received classical bits b_0 and b_1, similarly to Quantum Teleportation (see Table 2.1).

In the previous description, note that although the parties A and C never interact directly with each other, they share now a entangled pair of qubits. In the general case, with n parties, this is also valid. Therefore, the parties P_0 and $P_{(n-1)}$ can share an entangled quantum state over large distances ($\geq$ 100 kms) without never interacting directly with each other.

We illustrate the routine of Quantum Entanglement Swapping for $n = 3$ in Figure 2.30:

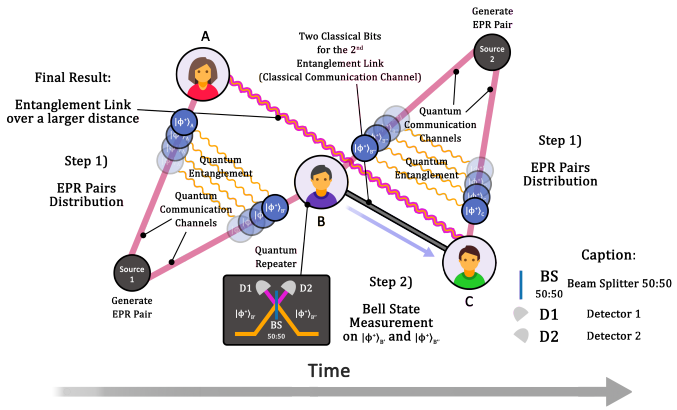


Figure 2.30: Quantum Entanglement Swapping for the parties A, B and C.

Notice that in the general case of the Quantum Entanglement Swapping for n parties, it is required $(n-2)$ classical communication channels and $(n-2)$ BSMs. In fact, these classical communications are, once again, the only potentially time-consuming steps being limited by the speed of light, in the best case. Additionally, we can also call this routine Quantum Teleportation of Entanglement since we perform Quantum Teleportation on an entanglement link rather than merely a single quantum state. Namely, this procedure represents one of the main components of a Quantum Repeater [256–258] for the Quantum Internet [259–264] to overcome the inherent Quantum Decoherence, and other physical phenomena, such as Photoelectric Effect, Compton Effect, and Birefringence over large distances ($\geq$ 100 kms).

2.2.5.5 Quantum Entanglement Distillation

The Quantum Entanglement Distillation (or Quantum Entanglement Purification) [265–268] is a routine for overcoming the inherent Quantum Decoherence and other phenomena, such as Photoelectric Effect, Compton Effect, and Birefringence in noisy quantum communication channels. In simple terms, this routine distills an initial set of less (or "degraded") qubits to a smaller subset of pure entangled (or "purified") qubits, enhancing their purity and correlations through some local operations. Thus, this routine increases the quality of noisy quantum communication channels since their fidelity decreases exponentially with their distance.

The fidelity F of a quantum entangled pair is a measure that expresses the similarity (or "closeness") between their qubits, which from their density operators ρ and σ is defined as:

$$F(\rho,\sigma) = \left[\mathrm{Tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)\right]^2 \tag{2.2.5.5.1}$$

If the qubit represented by the density operator ρ corresponds to a pure quantum state, then we have $\rho = |\rho\rangle\langle\rho|$ and $F(\rho,\sigma) = \langle\rho|\sigma|\rho\rangle = \mathrm{Tr}(\sigma\rho)$. Conversely, it the qubit represented by the density operator σ corresponds to a pure quantum state, then we have $\sigma = |\sigma\rangle\langle\sigma|$ and $F(\rho,\sigma) = \langle\sigma|\rho|\sigma\rangle = \mathrm{Tr}(\rho\sigma)$. Additionally, if both the qubits represented by the density operators ρ and σ correspond to pure quantum states, we have $\rho = |\rho\rangle\langle\rho|$ and $\sigma = |\sigma\rangle\langle\sigma|$. From this result, we have $F(\rho,\sigma) = |\langle\rho|\sigma\rangle|^2$ and $F(\sigma,\rho) = |\langle\sigma|\rho\rangle|^2$. Finally, we also have the property of symmetry of this metric, from which we have $F(\sigma,\rho) = F(\rho,\sigma)$. Note that this metric is given in terms of probability, so we also must verify $0 \leq F(\sigma,\rho) = F(\rho,\sigma) \leq 1$.

We can use Bell states (see Section 2.2.4.1) to quantify an entanglement link. Namely, let m be the number of high-fidelity copies of a Bell state. From this number m of Bell states, we can quantify the efficiency Y (also known as the "yield") of a protocol P of Quantum Entanglement Distillation. Namely, for a protocol P, where n copies of a mixed quantum state ρ, i.e., $\rho^{\otimes n}$, are used to obtain m exact copies of a maximally entangled state, have its "yield" defined as:

$$Y_{\rho,P} = \frac{m}{n}, \text{ where } m \leq n \tag{2.2.5.5.2}$$

Basically, this metric is the ratio of the number of maximally entangled states obtained by the protocol over the total number of initial copies of the quantum state ρ, where often the limit $n \mapsto \infty$ is considered. As obvious, a protocol P aims to saturate this limiting ratio.

The maximum number n of copies of the noisy quantum entangled state ρ, which we can convert into a maximally entangled quantum state $|\phi^+\rangle$ is equal to its Quantum Entropy $S(\rho)$:

$$S(\rho) = -\mathrm{Tr}\big(\rho\log(\rho)\big) \tag{2.2.5.5.3}$$

Finally, we can quantify an entanglement link as the Quantum Entropy of either ρ_A or ρ_B which are the quantum states of the parts of the entangled pair for party A and B, respectively:

$$E(\rho) = S(\rho_A) = S(\rho_B) = -\mathrm{Tr}\big(\rho_A\log(\rho_A)\big) = -\mathrm{Tr}\big(\rho_B\log(\rho_B)\big) \tag{2.2.5.5.4}$$

In this context, the "quantity" measure $E(\rho)$ of an entanglement link ρ ranges from 0 to 1, for a product quantum state and maximally quantum entangled state, respectively.

There are several different protocols of Quantum Entanglement Distillation, which differ in the set of quantum states they can purify, as well as on their efficiency (or "yield"), and the number of copies of the noisy quantum states they operate. Namely, these protocols can be classified as Filtering Protocols [269–271], Recurrence Protocols [266, 267, 272, 273], Hashing and Breeding Protocols [267, 274, 275], or $n \mapsto m$ Protocols [276–278]. A Filtering Protocol operates on a single copy of a noisy quantum entangled state. A Recurrence Protocol operates simultaneously on two copies of a noisy entangled state at each step. A Hashing and Breeding Protocols operates simultaneously on a large number n of copies of a noisy quantum entangled state, where $n \mapsto \infty$. Finally, a $n \mapsto m$ Protocol operates on n input copies of a noisy quantum entangled state and produces m output copies of a maximally quantum entangled state, being also eligible to be executed recursively, similar to what happens in the Recurrence Protocols.

One of the possible protocols for Quantum Entanglement Distillation is the well-known BBPSSW (Bennett-Brassard-Popescu-Schumacher-Smolin-Wooters) Protocol [266], which can be seen as a Recurrence Protocol. This protocol for n noisy entangled pairs is described as:

1. Initially, two parties A and B have n noisy entangled quantum states $|\phi^+\rangle_{AB}^{j}$ shared among them, also denoted as $|\phi^+\rangle_{i}^{j}$, where $0 \leq j \leq (n-1)$ and $i = \{A, B\}$.

2. Then, the parties A and B apply recurrent and individual pairwise bilocal *CNOT* (see Section 2.2.3.3) on the quantum entanglement links $|\phi^+\rangle_{i}^{k}$ and $|\phi^+\rangle_{i}^{\ell}$, acting as control and target qubits, respectively, where $0 \leq k, \ell \leq (n-1)$ and $k \neq \ell$, followed by a $\mathbb{Z}$-Basis measurement (see Section 2.2.3.2) on that same target qubit manipulated previously.

3. Next, both parties A and B exchange the classical outcomes obtained from the $\mathbb{Z}$-Basis measurement of their target qubits via a classical communication channel.

4. If both parties A and B agree in the outcomes b_A and b_B of each of their pairwise $\mathbb{Z}$-Basis measurements (namely, $b_{A,B} = 00$ or $b_{A,B} = 11$), they keep the control qubit. Otherwise, they discard that unmeasured control qubit, claiming that the Quantum Entanglement Distillation process for this entangled pair failed (namely, when $b_{A,B} = 00$ or $b_{A,B} = 11$).

When the parties obtain the same outcomes from the measurements of the target qubits, the process Quantum Entanglement Distillation was successful. This claim holds since the unmeasured control qubit will have higher fidelity, so long as the initial fidelity of both qubits of the entangled pair was greater than 50% and the local operations were accurate enough.

By repeating the BBPSSW Protocol recursively, it is possible to distill m purified entangled quantum states from a subset of n noisy entangled pairs of fidelity $F_{in} > \frac{1}{2}$. Then, the obtained m purified entangled pairs will have a fidelity arbitrarily high, namely $F_{out} < 1$. However, this distillation protocol is not scalable and has a "yield" that goes to 0 in the limit, when $F_{out} \mapsto 1$.

Each individual step of the BBPSSW Protocol is illustrated in the following Figure 2.31:

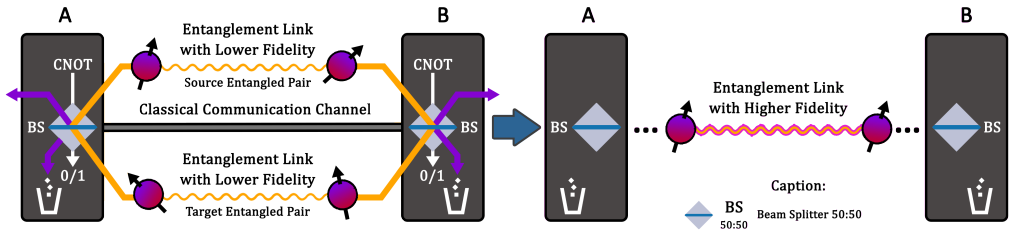


Figure 2.31: Individual step of the BBPSSW Protocol for the parties A and B.

Basically, for each step, the BBPSSW Protocol distills two identical quantum states ρ_{in} into a single final quantum state ρ_{out} with a higher fidelity F, closer to the Bell state $|\phi^+\rangle$. Originally, the BBPSSW Protocol was mainly designed to purify isotropic states (also known as Werner States), which are composed by a parametrized family of mixed quantum states consisting of $|\phi^+\rangle$ and the completely mixed quantum state $I/4$ (which is also known as white noise).

Other known protocols for Quantum Entanglement Distillation are EPL (Extreme Photon Loss) [279, 280] and DEJMPS (Deutsch-Ekert-Jozsa-Macchiavello-Popescu-Sanpera) [272].

2.2.6 No-Go Theorems

The No-Go Theorems are understood to be any theorem, showing that a particular situation is not physically possible. They are strongly related to some principles of Quantum Mechanics.

2.2.6.1 No-Cloning Theorem

The No-Cloning Theorem [281–283] says it is impossible to create an independent and identical copy of an arbitrary unknown quantum state. More specifically, given two quantum states $|\psi\rangle$ and $|\tau\rangle$, there is no unitary operation U, such that $U(|\psi\rangle\otimes|\tau\rangle) = U(|\psi\tau\rangle) = |\psi\psi\rangle = |\psi\rangle\otimes|\psi\rangle$.

In order to verify this No-Go Theorem, we can consider the supposed copying procedure for two given pure quantum states $|\psi\rangle$ and $|\phi\rangle$, and a target quantum state $|\tau\rangle = |0\rangle$ as:

$$\begin{cases} U(|\psi\otimes 0\rangle) = U(|\psi 0\rangle) = |\psi\psi\rangle = |\psi\rangle\otimes|\psi\rangle \\ U(|\phi\otimes 0\rangle) = U(|\phi 0\rangle) = |\phi\phi\rangle = |\phi\rangle\otimes|\phi\rangle \end{cases}$$

Then, one possible mathematical proof for this theorem is the following one:

1. Consider $|\sigma\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle)$ and $\tau = 0$. Then, by applying U, we obtain the result:

$$U(|\sigma 0\rangle) = \frac{1}{\sqrt{2}}\big[U(|\psi 0\rangle) + U(|\phi 0\rangle)\big] = \frac{1}{\sqrt{2}}\big(|\psi\psi\rangle + |\phi\phi\rangle\big) \tag{2.2.6.1.1}$$

2. But if U is a copying procedure, then, we can also obtain the following result:

$$\begin{aligned} U(|\sigma 0\rangle) = |\sigma\sigma\rangle = |\sigma\rangle\otimes|\sigma\rangle = \left[\frac{1}{\sqrt{2}}\big(|\psi\rangle + |\phi\rangle\big)\right]\otimes\left[\frac{1}{\sqrt{2}}\big(|\psi\rangle + |\phi\rangle\big)\right] = \\ = \frac{1}{2}\Big(|\psi\psi\rangle + |\psi\phi\rangle + |\phi\psi\rangle + |\phi\phi\rangle\Big) \end{aligned} \tag{2.2.6.1.2}$$

   This last result is different than the one obtained in step 1, even by applying the same procedure. Thus, we see the supposed copying procedure is not physically possible.

Additionally, we can consider the inner product of the two quantum states $|\psi\rangle$ and $\phi\rangle$ as being equal to its square, in order to check the fidelity of one of these quantum states against the other one. Then, we see that the only two cases in which that may be possible it is when they are completely orthogonal (i.e., corresponding to different measurement bases) or when they are the exact same quantum state. In the first case, the copying procedure may fail because the quantum states are orthogonal. On the other hand, the copying procedure is only possible when the fidelity is equal to one, which means we need to already know one of the quantum states beforehand or we already "observed" the quantum state at the moment of the supposed copying procedure, which corresponds to the classical copying procedure:

$$\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2 \Leftrightarrow x = x^2 \Leftrightarrow \begin{cases} x = 0 \\ x = 1 \end{cases} \tag{2.2.6.1.3}$$

Basically, the No-Cloning Theorem says that it is physically impossible to copy an arbitrarily unknown and unmeasured quantum state which is not equivalent to a classical state.

Additionally, the No-Deleting Theorem [284] is a time-reversed dual to the No-Cloning Theorem explained before. More specifically, this No-Go Theorem that says that, in general, given two copies of some arbitrary quantum state, it is impossible to delete one of the copies.

2.2.6.2 No-Communication Theorem

The No-Communication Theorem (or No-Signaling Principle) [285, 286] is a No-Go Theorem that argues that it is physically impossible for one "observer" to communicate any *useful* information to another "observer" by measuring a physical subsystem of a global entangled quantum physical system. The theorem is important because contradicts the intuition that some events can be strongly correlated even if they are at very far distances through Quantum Entanglement, what seems to suggest the theoretical possibility of FTL Communication.

We can apply the results from this No-Go Theorem to understand the so-called paradoxes in Quantum Mechanics, such as the EPR (Einstein-Podolski-Rosen) paradox or violations of Local Realism obtained in tests of Bell's Theorem. In these experiments, the No-Communication Theorem shows that the failure of Local Realism does not lead to what we could refer to as the famous so-called "Spooky Action at a Distance" that Albert Einstein pointed initially in 1935.

A possible mathematical proof for the No-Communication Theorem is the following one:

1. Let A and B be two parties that share an entangled Bell state $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

2. Then, let the parties A and B perform the measurement of the quantum physical subsystems at their disposal by using the detectors D_A and D_B, respectively.

3. Following the Bell's Experiment, assume that the detectors are initially oriented along the z-axis and rotated independently at the end of the parties A and B in such a way that the difference between the angles of the detectors D_A and D_B is denoted as θ_{AB}.

4. Then, we compute the conditional probabilities of measurement outcomes:

$$\begin{aligned} P_{00} &= |\langle 0|_A \langle 0|_B |\psi^+\rangle|^2 = \frac{1}{2}\sin^2\left(\frac{\theta_{AB}}{2}\right) \\ P_{01} &= |\langle 0|_A \langle 1|_B |\psi^+\rangle|^2 = \frac{1}{2}\cos^2\left(\frac{\theta_{AB}}{2}\right) \\ P_{10} &= |\langle 1|_A \langle 0|_B |\psi^+\rangle|^2 = \frac{1}{2}\cos^2\left(\frac{\theta_{AB}}{2}\right) \\ P_{11} &= |\langle 1|_A \langle 1|_B |\psi^+\rangle|^2 = \frac{1}{2}\sin^2\left(\frac{\theta_{AB}}{2}\right) \end{aligned} \tag{2.2.6.2.1}$$

   Here, as expected, we can verify the normalization condition $P_{00} + P_{01} + P_{10} + P_{11} = 1$.

5. We compute the probabilities of the measuring $|0\rangle$ and $|1\rangle$ at the end of A:

$$\begin{aligned} P_0^A &= P_{00} + P_{01} = \frac{1}{2} \\ P_1^A &= P_{10} + P_{11} = \frac{1}{2} \end{aligned} \tag{2.2.6.2.2}$$

6. Similarly, we compute the probabilities of the measuring $|0\rangle$ and $|1\rangle$ at the end of B:

$$\begin{aligned} P_0^B &= P_{00} + P_{10} = \frac{1}{2} \\ P_1^B &= P_{01} + P_{11} = \frac{1}{2} \end{aligned} \tag{2.2.6.2.3}$$

Thus, we see that the measurement outcomes are totally independent on the angle θ_{AB} and the actions performed by measurements at either the end of the party A or B are not detected at another end (and vice-versa). Namely, this independence of the difference between the angles of the detectors and actions of both parties is the essence of the No-Communication Theorem. Additionally, none of the parties can tell the difference between what the other party did and the effect of an eventual random measurement.

2.2.7 Quantum Algorithms as a Threat for Classical Cryptography

From the emergence of Quantum Computing over the years, there are a lot of Quantum Algorithms already developed for several applications. In general, these algorithms have huge computational advantages compared to their classical counterparts in terms of accuracy and speedup. Some of them will have a huge impact on the Classical Cryptography used nowadays. We will review these algorithms and the threats they represent in the following paragraphs.

2.2.7.1 Grover's Algorithm

The Grover's Algorithm [152, 287–289] is a quantum algorithm for a probabilistic search that finds some solution(s) from a set of n possible ones with a high probability in a black-box function (or "Oracle"). In particular, this algorithm was originally proposed for searching item(s) in an unsorted database. However, we can adapt it for any unstructured search.

In the classical regime, for an unsorted search problem where we want to find some item(s) in an unstructured list, the best strategy is literally to iterate that list and check its items one by one. This search strategy is linear and has a complexity time of $O(n)$. Generally, in the worst case, this approach takes, on average, n steps. In the best case, this approach could take $\frac{n}{2}$ steps if we take a more efficient strategy of randomly sorting the current item we are checking.

On the other hand, in the quantum regime, Grover's Algorithm solves the same unsorted search problem in only $\sqrt{n}$ steps, providing a quadratic speedup in comparison to the existing strategies in the classical regime. This quantum algorithm has a complexity time of $O(\log(n)$ quantum operations for each step. Thus, this quantum algorithm provides a huge advantage for this type of computational problems and is considered asymptotically optimal [290].

In the domain of the Classical Cryptography currently used, the Grovers's Algorithm can perform quantum attacks, by brute-force, in order to possibly "break" cryptographic keys and allow the decrypting of the respective cipher, in a polynomial time and threatening then, some classical symmetric encryptions, such as the well-known AES [291–294]. This algorithm could "brute-force" a symmetric cryptographic key of n bits in $2^{\frac{n}{2}}$ iterations. Thus, this quantum algorithm can "brute-force" symmetric keys of 128, 192, and 256 bits in roughly 2^{64},

2^{96}, and 2^{128} iterations. For this reason, Grover's Algorithm will make the AES-128 and AES-192 ciphers obsolete. However, we currently consider AES-256 cipher as quantum-resistant since it has a security level of 128 even against "brute-force" attacks made by this quantum algorithm.

Additionally, we can also use Grover's Algorithm to perform collision attacks and pre-image attacks for Hash Functions, such as SHA (Secure-Hash Algorithm). However, this quantum algorithm may not necessarily be the most efficient one since, for example, the parallel Pollard's Rho Algorithm can find a collision in SHA more efficiently than Grover's Algorithm [295].

2.2.7.2 Simon's Algorithm

The Simon's Algorithm [149] is a probabilistic quantum algorithm that implements a black-box function (or "Oracle") to solve Simon's Problem. The Simon's Problem is a computationally hard problem in the model of Decision Tree or Query Complexity. It provides an exponential separation between the complexity classes BPP (Bounded-error Probabilistic Polynomial time) and BQP (Bounded-error Quantum Polynomial time). This problem is defined as follows:

- Given a function $f : \{0,1\}^n \mapsto \{0,1\}^n$ with the promise that for some $s \in \{0,1\}^n$, it holds that $[f(x) = f(y)] \Leftrightarrow [x \otimes y \in \{0^n, s\}]$, find the binary string s of n bits.

This quantum algorithm was the first one offering an exponential speedup compared to its best classical counterparts in the bounded-error setting. Namely, any classical algorithm requires $O(2^{\frac{n}{2}})$ to find the binary string s, while the Simon's Algorithm succeeds using only $O(n)$ queries to the black-box function f. More specifically, executing the quantum part of the Simon's Algorithm $O(n)$ of times results in a full-rank system of linear equations, which we can classically solve efficiently to obtain the binary string s as a classical post-processing.

Intuitively, the hardness of this problem in the classical regime is that we need to find two different inputs x and y for which we have $f(x) = f(y)$. Moreover, there is not necessarily any structure in the function f that would help us to find two such inputs. In the best case, we can only learn something about the function f when, for two different inputs, we obtain the same output. In the classical setting, we would need to guess around $\sqrt{2^n}$ different inputs before being likely to find a pair on which the f takes the same output, as happens in the Birthday Problem. Therefore, we consider this problem computationally hard in the classical regime, even if we use pseudo-random processes and accept a small error probability for the solution.

Due to its natural relation with the Birthday Problem, we can also adapt and extend this quantum algorithm to perform collision attacks and pre-image attacks for Hash Functions. Additionally, we can develop a few modified versions of Simon's Algorithm to attack MACs (Message Authentication Codes) and block ciphers based on the Feistel Cipher Structure, such as DES and AES [293, 296–298], with some speedups comparable to Grover's Algorithm.

2.2.7.3 BHT Algorithm

The BHT (Brassard-Høyer-Tapp) Algorithm is a quantum (or "hybrid") algorithm that solves the Collision Problem [299]. In this problem, is given an integer parameter n and an r-to-1

function $f : \{1, ..., n\} \mapsto \{1, ..., n\}$. Then, the main goal is to find two inputs x and y, such we verify $f(x) = f(y)$. This algorithm combines the square root speedup from the Birthday Paradox using classical randomness with the square root speedup from Grover's Algorithm.

The best-known classical solution for the Collision Problem is exploring the Birthday Paradox allowing pseudo-randomness. Here, we choose distinct queries at random, from which we find a collision in any fixed 2-to-1 function with high probability after $O(\sqrt{n})$ queries.

In the quantum setting, the BHT Algorithm solves this problem optimally by taking only $O(\sqrt[3]{(n)})$ queries to the r-to-1 function f. First, $\sqrt[3]{n}$ inputs to the function f are selected at random and used as queries. If there is a collision among these inputs, the BHT Algorithm returns the pair of inputs queried. Otherwise, all these inputs map to distinct values in the function f. Then, the BHT Algorithm uses the Grover's Algorithm to find new inputs to the function f that give a collision. Since there are n input values to f initially, and $\sqrt[3]{n}$ of them would form a collision with the already queried values, Grover's Algorithm can find a collision with $O\left(\sqrt{\frac{n}{\sqrt[3]{n}}}\right) = O(\sqrt[3]{n})$ extra queries to the function f in the black-box (or "Oracle") model.

Since this algorithm combines the Birthday Paradox with Grover's Algorithm, we also know it known as Quantum Birthday Attack. This "hybrid" algorithm provides advantage compared to its best classical counterparts for collision attacks and pre-image attacks on Hash Functions, weakening their security levels by a factor $\frac{n}{3}$. Thus, we expect this algorithm will make some cryptographic hashes obsolete, such as SHA-224 and SHA-256 [300, 301]. Other Hash Functions with larger output lengths, such as SHA-384 and SHA-512, are considered quantum-resistant.

2.2.7.4 Shor's Algorithm

The Shor's Algorithm [150, 151] is an algorithm that solves the Integer Number Factorization Problem. The main goal of this problem is simple and is defined as follows. Given an integer prime number n, find its prime factors (or divisors) u and v, such that $n = u \cdot v$. Namely, this computational problem is considered easy for a relatively small prime integer number n. However, when the prime number n is extremely large, this problem becomes computationally hard in the classical setting, taking an exponential (and unbearable) complexity time.

The most efficient classical algorithm to solve this problem is the GNFS (General Number Field Sieve) Algorithm [302]. More specifically, this algorithm can factor prime numbers larger than 10^{100}. Empirically, the GNFS Algorithm have a sub-exponential complexity time of $O\left(e^{1.9\times\sqrt[3]{n}\times\sqrt[3]{(\log(\log(n)))^2}}\right)$. The GNFS Algorithm consists in finding a pair of small smooth numbers polynomials with prime factors sharing a common root modulo n. Finding such small smooth numbers has a sub-exponential complexity time in the size of the initial n.

In the quantum setting, the Shor's Algorithm can find the smallest even order period from which it is possible to obtain a factor that solves the Integer Number Factorization Problem. In particular, this quantum algorithm takes only $\log(n)$ steps and have a polynomial complexity $O((\log(N))^2 \times (\log(\log(N))) \times (\log(\log(\log(N)))))$. For this reason, the Shor's Algorithm is exponentially faster than the most efficient known classical counterparts, such as the GNFS Algorithm. This computational advance is due to the efficiency of the QFT (see Section 2.2.5.1)

and its mathematical method for fast Modular Exponentiation by repeated squaring.

On the other hand, this quantum algorithm can also solve the Discrete Logarithm Problem. The Discrete Logarithm Problem is related to the Integer Number Factorization Problem. The classical asymmetric cryptography and public-key cryptosystems currently used are all based on three mathematical problems, the Integer Number Factorization Problem (e.g., RSA [117]), the Discrete Logarithm Problem (e.g., DSA [303] and ElGamal [304]), and the Elliptic-Curve Discrete Logarithm (e.g., ECDSA [305] and ECDH [306]). For this reason, they can be all easily "broken" by Shor's Algorithm in a very short amount of time. Oppositely to Grover's, Simon's, and BHT Algorithms, extending the size of their parameters will not mitigate the main threat. For this reason, we do not consider all these cryptographic primitives secure anymore for the Post-Quantum Era. It was also shown that a modified version of the Shor's Algorithm running in a quantum computer with considerable power may also "break" the ECC primitives [121].

2.2.8 Possible Cryptographic Approaches for the Post-Quantum Era

Due to the emergence of Quantum Computing and its future impact on Cryptography, from the threats of Grover's [152, 287–289], Simon's [149], BHT [299], and Shor's [150, 151] Algorithms, several new quantum-resistant cryptographic primitives and protocols are being studied.

In particular, these new alternatives of Cryptography are mainly focused on Public-Key Cryptography since the expected impact of Grover's, Simon's, and BHT Algorithms on Hash Functions and Symmetric Cryptography is minor. On the other hand, Shor's Algorithm will have an enormous impact on Asymmetric Cryptography and Public-Key Cryptosystems.

From these eminent threats, two additional main families of Cryptography arose, such as Post-Quantum Cryptography [291, 307] and Quantum Cryptography [308–310]. There are other less popular families of Cryptography that are being studied for the Post-Quantum Era. Some examples are Chaos-Based Cryptography [311, 312] and DNA-Based Cryptography [313, 314]. However, it is not completely clear the quantum resistance of these groups of cryptography.

Namely, the Post-Quantum is based on mathematical problems and assumptions, similar to what happens in Classical Cryptography. But, differently from Classical Cryptography, these primitives are *believed* to be hard to be solved even by a considerably powerful Quantum Computer. From this family of Cryptography, we can enumerate Lattice-Based Cryptography [315–330], Code-Based Cryptography [331–338], Hash-Based Cryptography [118, 339–348], Isogeny-Based Cryptography [349–351], Multivariate Cryptography [352–363], Group-Based (Non-Commutative) Cryptography [364–367], and ZKPs (Zero-Knowledge Proofs) [368–371].

Moreover, we can also consider some of the previous cryptographic primitives used in Classical Cryptography being quantum-resistant under specific security parameters as being primitives of Post-Quantum Cryptography. These cryptographic primitives may include AES for symmetric keys of 256 bits and SHA for cryptographic hashes with sizes of 384 and 512 bits.

The Quantum Cryptography follows a different approach, which is mainly based on quantum mechanical properties and phenomena, such as the Heisenberg's Uncertainty Principle, Quantum Superposition and Quantum Entanglement (see Sections 2.1.3 and 2.1.7),

rather than mathematical assumptions. We can use such phenomena to develop new *unhackable* cryptographic primitives, once and forever. The biggest advantage of Quantum Cryptography is that it can ensure *unconditional security* and it is impossible to be "broken".

Considering the possible impact of Quantum Computing in Cryptography, the NIST is already preparing solutions for the Post-Quantum Era, with the still running Post-Quantum Cryptography Standardization Competition[3]. The main reason for NIST opted first by choosing Post-Quantum Cryptography, instead of Quantum Cryptography, for his current standard is that Quantum Cryptography could not still be accessible and implemented, at a large scale:

Post-Quantum Cryptography	**Quantum Cryptography**
Accessible at large scale (low cost)	Not accessible at large scale (high-cost)
Based on Mathematics	Based on Quantum Mechanics
Believed to be secure against Classical and Quantum Attacks (and have yet to be developed)	***Known*** to be secure against Classical and Quantum Attacks (provide *unconditional security*)

Table 2.2: Post-Quantum Cryptography vs. Quantum Cryptography.

At an initial phase, the Post-Quantum Cryptography will dominate the high volume consumer and the global mobile communications. Oppositely, the Quantum Cryptography will be directed for systems requiring high levels of security, such as governments, military, and financial services or critical infrastructures. But, in the long term, Quantum Cryptography may be a safer and lasting solution because it will offer unconditional security [372, 373]. Namely, it replaces those mathematical assumptions with facts derived from the laws of physics.

[3]See more information in: https://csrc.nist.gov/Projects/post-quantum-cryptography/

CHAPTER 3

QUANTUM CRYPTOGRAPHY

In this chapter, we introduce the concept of Quantum Cryptography. This novel cryptographic approach for the Post-Quantum Era is mainly based on Quantum Mechanics and Laws of Physics, rather than on mathematical and computational hardness assumptions as happens with the Classical Cryptography and Post-Quantum Cryptography. Here, we will explain some of the developed protocols and primitives of Quantum Cryptography from the 1980s until the present. We describe the main procedures of such cryptographic protocols, as well as their inherent security properties and guarantees. For a reader with no background in Mathematics, Quantum Mechanics, and Quantum Information Science, we strongly recommend the reading of Chapter 2, because their notions are at the core of the topic of Quantum Cryptography.

3.1 Bringing the Laws of Physics to Cryptography

In the same way that we can perform novel powerful Quantum Computations and Quantum Communications with these particles in atomic and subatomic scales, we can also use them in order to exchange secrets on the fly. And when we think about those secrets as being secret keys, we end up having what we call Quantum Cryptography. Once again, as usual, since in such configurations we are dealing with atomic and subatomic scales, we have to consider the weird quantum mechanical phenomena. And from these strange phenomena, Quantum Cryptography can give rise to an unbreakable and unprecedented level of privacy. In general, attackers and hackers usually tend to have several difficulties in dealing with randomness. And Quantum Mechanics can be a great candidate (if not the best one) to provide a source of true randomness that Cryptography usually needs. Following this claim, we can use some of the well-known principles and concepts of Quantum Mechanics, jointly with the laws of physics, to achieve a whole new level of security, never seen before. Some of those principles and

concepts may include Heisenberg's Uncertainty Principle, Quantum Superposition, Quantum Entanglement, No-Go Theorems (see Sections 2.1.3, 2.1.7 and 2.2.6), among many others.

Similar to Quantum Communications, we often perform Quantum Cryptography using light particles, (or more specifically, photons). Thus, we also need to consider the principles of the Wave-Particle Duality and Theory of Light. In order to develop such physical cryptographic systems, we need to use the same proper optical elements used in Quantum Communications, or commercial solutions already available in the market, from specialized companies, such as IDQ (ID Quantique), Quintessence Labs, Toshiba, Qrypt, QNu Labs and MagiQ Technologies[1].

3.2 Introduction to Quantum Cryptography

As seen before, Quantum Cryptography is the science of exploiting and applying quantum mechanical properties to perform cryptographic tasks. We usually attribute this invention to Stephen Wiesner in the 1970s, when he originally conceived it in an unpublished written manuscript [308]. However, it was only between the 1980s and 1990s that this scientific topic gained its final form, as we know nowadays. Since then, were proposed dozen of protocols of this kind, mainly focused on key exchanges, including QKDs (Quantum Key Distributions) [309, 374–386], SQKDs (Semi-Quantum Key Distributions) [387–394], QCKAs (Quantum Conference Key Agreements) [395–407], among others. But Quantum Cryptography may also include other further cryptographic tasks not focused on secret key exchanges, such as QRNGs [408–412], Quantum Cryptocurrencies [308, 413–417], Quantum Multiparty Computations [418–420], Mistrustful Quantum Cryptography [421–426], QMACs (Quantum Message Authentication Codes) [427, 428], Quantum Hashes [429, 430], QDSAs (Quantum Digital Signature Algorithms) [431–433], or even QPKEs (Quantum Public-Key Encryptions) [434].

Since we end up having rules, facts, and laws derived from Physics and nature, at the core of Quantum Cryptography, it may turn out to be a better solution for the long-term in the Post-Quantum Era. However, in the current state-of-the-art, Quantum Cryptography has two major drawbacks that need to be considered when developing solutions of this kind.

First, it is necessary to note that our conventional Classical Computers are not suitable for these tasks by default, since here we are dealing with quantum information instead of classical information. And usually, specialized hardware to operate quantum information, namely in the domains of Quantum Communications and Quantum Cryptography, can have high costs in the current state-of-the-art, compared to the conventional devices we use in the quotidian. The accessibility aspect represents a disadvantage when compared to the known protocols of Post-Quantum Cryptography, which are always implementable in our current conventional classical technologies. However, in the last years, a new family of quantum cryptographic protocols for semi-quantum contexts were proposed, trying to relieve the cost and accessibility

[1] See the following links: https://www.idquantique.com/ (Switzerland), https://quantumxc.com/ (USA), https://www.quintessencelabs.com/ (Australia), https://www.toshiba.co.jp/qkd/en/index.htm (Japan), https://www.qrypt.com/ (USA), https://www.qnulabs.com/ (India), https://www.magiqtech.com/ (USA).

issues. One of the most known proposals of such protocols was the introduction of SQKDs (see Section 3.4), and their main idea is also on the origin of our proposal (see Chapter 4).

Second, these quantum cryptographic protocols require specialized hardware and optical elements that still have imperfections. The theoretical ideology for these protocols assumes single-photon sources, but perfect single-photon sources are challenging to build. Most of the currently available quantum cryptographic solutions use nearly perfect laser sources for a quantum communication medium, such as faint laser sources. Despite such laser sources being almost perfect, they may end up not producing always single-photons by each pulse of light as pretended in theory. Such physical imperfections can allow an attacker to exploit this physical attack surface by performing the well-known PNS (Photon-Number Splitting) attack [435–437], for example. These quantum cryptographic protocols also require multiple SPDs (Single-Photon Detectors) that, in real-world implementations, are tuned to detect an incoming photon during a short time window or pulse of only a few nanoseconds. Because of manufacturing differences between these detectors, their respective detection windows will be shifted by a finite time. An attacker can take advantage of this inefficiency in the detection of the incoming photons by performing Faked-State [438] and Time-Shift [439] attacks.

One of the motivations of Wiesner during the 1980s when he published his paper was the development of Quantum Money that cannot be counterfeit by inserting photons polarized in four possible quantum states (later known as BB84 States) in each banknote [308]. In his idea, Wiesner claimed that nobody can copy the photons present in the banknotes, and thus, he provided a currency impossible to be forged. He made this observation due to what became later known as the No-Cloning Theorem (see Section 2.2.6.1), which, in simple terms, states that any attempt at copying a particle will change its state. The ideas behind Quantum Money, namely the use of polarized photons and conjugate quantum states to detect cheating attempts from dishonest entities, worked as a starting point for Quantum Cryptography some years later.

As expected, at the top of primary tools from Cryptography is the secret key exchange (or key distribution). In 1984, Charles Bennett and Gilles Brassard developed the first-ever QKD, known as the BB84 protocol (see Section 3.3.1.1) [309]. Here, they guaranteed a safe exchange of a secret key between two parties, configuring single-photons in four possible polarizations.

Inspired by the work of these two proposals, some scientists and researchers focused their effort on the study and development of several new quantum cryptographic protocols.

3.3 Quantum Key Distributions (QKDs)

As we already saw, a QKD is a secure communication method devised for the distribution of symmetric encryption keys using the phenomena of Quantum Mechanics. For QKDs, we are usually interested in bipartite scenarios, considering only two parties (e.g., Alice and Bob). Additionally, this family of protocols has a fully-quantum nature, and thus, we assume that the two parties have access to quantum resources, such as quantum devices and optical elements (see Section 3.2). It simply works by encoding those secret keys in quantum particles, usually

single-photons, and sharing those quantum particles between the two parties, rather than using classical light pulses with multiple photons as in conventional communications.

In the first place, these cryptographic protocols should take advantage of the Observer's Effect, which says that any attempt by an eavesdropper (e.g., Eve) to observe the transmitted photons will indeed perturb the quantum communication transmission. Such a perturbation in the stream of transmitted photons leads to transmission errors (also referred to as noise), detectable by the two parties. Usually, we achieve such detection by "sacrificing" random samples of the single-photons where we can verify the existence of those errors. However, in the current state-of-the-art, we cannot isolate properly the medium through which the photons are traveling. For this reason, the photons can also suffer undesirable influences from the external environment as being absorbed by an electron that may be present in the medium. As evident, we can easily see that such external random phenomena also lead to transmission errors since a receiver can expect to receive a photon that will never arrive. And that is why we need to consider the noise introduced not only by the eavesdropper but also by the external environment, in most cases. We use these same samples of photons to verify the security of the distributed secret key and estimate lower-bounds in terms of transmission errors. Finally, from such a lower-bound, we can infer a threshold in which we should consider the presence of an eavesdropper in the quantum transmission medium and retry or abort the protocol. The estimations of the rates of transmission errors are called QBERs (Quantum Bit Error Rates).

In order to communicate the random samples chosen from the photons transmitted, the parties need to announce them publicly. Usually, the parties perform this post-processing step by using public communications through a medium of classical nature that needs to be authenticated to ensure their legitimacy, that can be achieved by the traditional classical (or novel quantum) techniques. In the end, we can expect that both parties will have an equal final symmetric key that can be used in the typical symmetric encryption methods.

The final result is that QKD can use an authenticated communication result and transform it into a secure communication channel. In theory, we should combine the QKDs with OTP [100] encryption to achieve provable security. However, an OTP encryption requires symmetric keys, which are as long as the size of the data to be encrypted, and we can use it only once. This feature of OTP encryption would impose direct limitations on the available bandwidth because, in the current state-of-the-art, the key distribution rate of QKDs is typically $1,000$ to $10,000$ times lower than traditional classical optical communications. Therefore, in practice, QKDs are often combined with conventional classical symmetric encryption, such as AES, and we use it frequently to refresh short encryption keys. In this case, we often use AES-256 since we know that AES with symmetric keys smaller than 256 bits turns out to be insecure against Grover's Algorithm. Another solution may be to combine the arbitrary secret key resulted from QKDs with QOTP (Quantum One-Time Pad) encryption [440], but in this case, we will have the same previously mentioned limitations of bandwidth again. In particular, QOTP requires two secret keys with the size equal to the size of the message. Either way, this is a challenging problem that remains open, which also depends on future improvements to the hardware and optical elements for quantum communications, along with the study of new quantum attacks.

However, because of these limitations in bandwidth caused by the defects still existing in quantum cryptography, most real-world QKDs are combined with AES-256 and classical public authentication methods. And here, we will follow this setup to describe these systems in detail.

First, at a high-level, the main components required for a traditional QKD are two endpoint modules (sender and receiver), a quantum communication medium, and an authenticated communication medium. If we consider Alice to be the sender and Bob to be the receiver of the symmetric key exchanged, we can illustrate a QKD as shown in the following Figure 3.1:

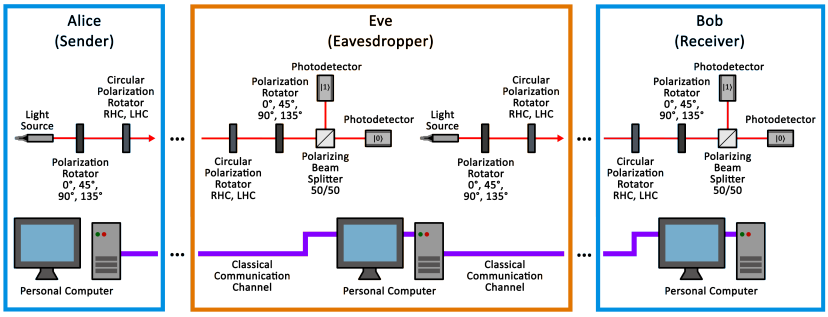
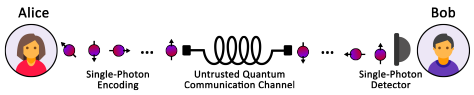
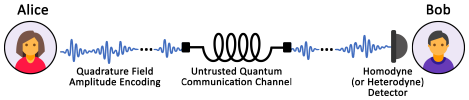


Figure 3.1: Example of a setup schematic of a QKD (Quantum Key Distribution).

Regarding the detection of the incoming particles, we can divide the QKDs into three main groups, known as DV-QKDs (Discrete Variable QKDs) [309, 374–376, 378], DPR-QKDs (Distributed Phase Reference QKDs) [441, 442], and CV-QKDs (Continuous Variable QKDs) [377, 443–447]. The early two use single-photon detectors, while the latter uses heterodyne or homodyne detectors. For the DV-QKDs and DPR-QKDs, we encode the information of the secret key in very weak optical signals, ideally single-photons. In this case, we use some of their properties, such as polarization and phase, and their resulting outcomes are discrete (i.e., $|0\rangle$ for vacuum or $|1\rangle$ for photon "clicks"). On the other hand, for the CV-QKDs, the information is encoded through the quadrature axes of randomly selected coherent states of light. Here, we encode the information through projections of the amplitude and phase of their electric fields, using shot-noise limited coherent detection, resulting in continuous values (i.e., in the interval $[0, 1]$ for each light pulse). The difference between these two methods is given in Figure 3.2:



a DV-QKDs and DPR-QKDs with single-photon encoding and single-photon detectors.



b CV-QKDs with quadrature field amplitude encoding and homodyne/heterodyne detectors.

Figure 3.2: Examples of the types of QKDs (Quantum Key Distributions), regarding their signal encoding and detection.

The technology for the single-photon detectors used in DV-QKDs and DPR-QKDs requires cryogenic refrigerated devices, having higher distance reaches, higher costs, and lower system complexities, while the CV-QKDs require devices that are already developed for classical optical communications, however, they have lower distance reaches but higher system complexities.

For the case of CV-QKDs, the basic difference existing between heterodyne and homodyne detectors is in the frequencies of their signal carriers (ω_s) and local oscillators (ω_{LO}) [448–450]. For the case of homodyne detection, we directly convert the optical signals of light to the baseband. In this case, the frequency of a local oscillator matches the one from the transmitted signal carrier and whose phase we lock to the incoming signal (i.e., $\omega_s = \omega_{LO}$). It is difficult to build such receivers because local oscillators must have excellent spectral purity and no power fluctuations. In this configuration, we mix the field of the incoming optical signals of light waves with the local oscillator, whose frequency and phase we lock with the ones of the light waves of the signal carriers, via a PLL (Phase-Locked Loop), also making the whole circuit complex. The resultant electrical signal is then filtered, and the light pulse sequence is then recovered back to the original data by a decision subsystem. However, this detection method allows us to obtain the information from the electrical signal directly, at a single frequency and is extremely sensitive. Then, we can transmit this information through amplitude, phase, or frequency modulation. In opposite, for heterodyne detection, we do not need to match the frequency of the local oscillator and the transmitted signal carrier. Here, we do not need either the locking of the phase of the incoming optical signals (i.e., $\omega_s \neq \omega_{LO}$). In other words, we choose the local oscillator to differ from the signal carrier, such that the intermediate frequency is in the microwave region for reference. In this configuration, the sensitivity of this detector is a little degraded, despite the circuit being easier to implement. Here, a further demodulator is required to convert the optical signals of light to the baseband since we cannot convert them directly. In particular, the intermediate frequency carries the optical signal, and the optical signal is demodulated again to the baseband. We illustrate a possible high-level configuration for homodyne and heterodyne detection in Figures 3.3 and 3.4:

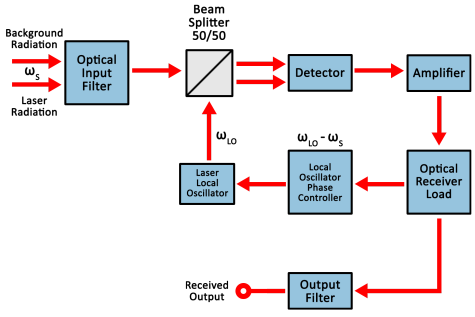


Figure 3.3: Schematic setup for Homodyne Detection.

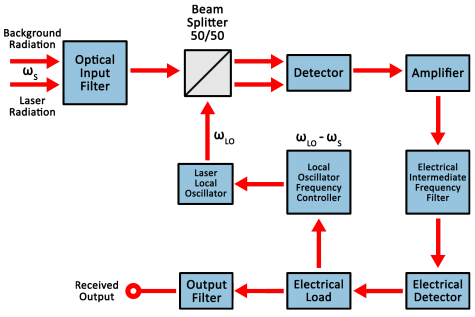


Figure 3.4: Schematic setup for Heterodyne Detection.

The CV-QKDs use two different modulation types for the optical signal modes, known as GM (Gaussian Modulation) and DM (Discrete Modulation). Therefore, we commonly referred to these two distinct configurations as GM-CV-QKDs (Gaussian Modulation CV-QKDs) and DM-CV-QKDs (Discrete Modulation CV-QKDs). As the name suggests, the first uses optical signal pulse modes which are randomly selected from a complex-valued Gaussian Probability Distribution, with a given variance, while the latter uses optical signal pulse modes which are randomly selected from a complex-valued Discrete Probability Distribution. The GM-CV-QKDs have obvious drawbacks, such as the extreme burden on the transmitter's RNG (or QRNG) source, since the number of optical signal modes is much larger compared to DM-CV-QKDs. Additionally, DM-CV-QKDs require error-correction techniques that may be inefficient and computationally demanding. On the other hand, the DV-CV-QKDs can leverage an efficient modulation and the use of error correction codes, as also a low-overhead RNG source while keeping the same ease aspects of implementing homodyne and heterodyne detectors.

In the end, a possible way to classify all the existing approaches for QKDs in the current state-of-the-art, regarding the detection of the incoming photons, is shown in Figure 3.5:

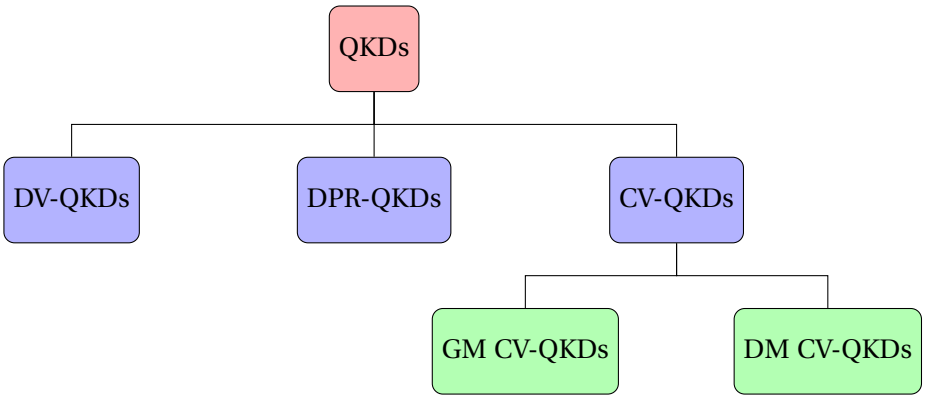


Figure 3.5: Classification of the several types of QKDs, in the current state-of-the-art, regarding the detection of the incoming photons.

Additionally, we can also classify QKDs as MDD-QKDs (Measurement Device Dependent QKDs) and MDI-QKDs (Measurement Device Independent QKDs), regarding the feature of they be able to ensure their security properties considering or not the correct functionality of the hardware. Here, the hardware we often deal with is namely their measurement devices (e.g., photodetectors). In particular, MDD-QKDs are QKDs that need their security to be ensured by trusted measurement devices, while, as the opposite, MDI-QKDs are QKDs that can have their security established by untrusted ones. For instance, we consider an MDI-QKD to be a QKD allowing the two parties to exchange a secret key with perfect security, even if the measurement devices they are using have been tampered with by an eavesdropper and thus are not trusted.

In the end, we can classify all the DV-QKDs, DPR-QKDs, and CV-QKDs, as PM-QKDs (Prepare-and-Measure QKDs) or EB-QKDs (Entanglement-Based QKDs) regarding the way the secret keys are transmitted and extracted of the secret keys. The earlier approach usually uses the preparation and measurement of photons, ideally single-photons, while the latter is

based on bipartite quantum entanglements. The BB84 protocol (see Section 3.3.1.1) is a good example of a MDD-QKD and the E91 protocol (see Section 3.3.2.1) is an example of a MDI-QKD.

We refer to the ideal conditions for QKDs, considering single-photon sources, isolated quantum communication medium, and perfect measurement devices with no noise from the external environment, as Noiseless Scenarios. On the opposite, we call Noisy Scenarios to the non-ideal conditions for QKDs and a quantum communication medium not perfectly isolated where the transmission errors are not introduced only by the eavesdropper but also by the external environment. For the reasons mentioned before, in the current state-of-the-art, we do not all the conditions required for Noiseless Scenarios. However, we often start with the Noiseless Scenarios when developing these protocols since they require fewer assumptions.

However, notice that in both Noiseless and Noisy Scenarios, we may not detect a possible occurrence of eavesdropping. For example, imagine that by chance, none of the photons that were tampered with by an eavesdropper are present in the random samples chosen. Here, even if we do not detect a real eavesdropping, it may also be necessary to correct possible errors in both the secret keys that the sender and receiver have. This further step is achievable through an Information Reconciliation, where it is applied some error correction code. The most known example of error correction code used in QKDs is the Cascade protocol [451, 452], but other variants were proposed, such as Turbo codes [453, 454], LDPC codes [455, 456], and Polar codes [457]. This step is usually interactive and requires interactions between the two users that are performed on a public authenticated communication channel. The eavesdropper still may have partial information about both secret keys that were leaked during the transmission of the secret key through the quantum communication medium or even during the step of Information Reconciliation and the respective exchange of information regarding the error correction codes used. In this case, it is often also performed a last operation called Privacy Amplification [272, 458], where both parties produce a final new, shorter secret key, in such a way that the eavesdropper has none or only negligible information about the new secret key. In most cases, we can eliminate this residual information by applying a Universal Hash Function [459], selected at random and agreed publicly. Once again, it may involve some interaction rounds between the parties involved on a public authenticated communication channel.

Usually, in the steps of classical nature, we use the classical authentication methods, but it is not mandatory to build a QKD in that way. If we could overcome the drawback of the current limitations of bandwidth in quantum communications, we may employ quantum methods instead of classical ones. In fact, we can apply such methods not only for the authentication of the public communication channel but also for Privacy Amplification. Such quantum methods may namely include the previously mentioned QMACs [428], QDSAs [431, 432], QKEs [434] for the authentication of the public communication channel, or even Quantum Hashes [430] for the further step of Privacy Amplification. However, such methods are being studied and improved over the years, and it is still uncertain how they will impact Cryptography.

Some very extensive and comprehensive surveys of the current state-of-the-art of Quantum Cryptography, including several protocols and QKDs, security notions and concepts, practical implementations, attacks, and future perspectives, are given in the refs. [443, 447, 460–464].

We can summarize the complete procedure of a QKD on the following enumerated steps:

1) *Quantum Transmission*:

a) *Preparation of Quantum States*:

- The sender creates a random binary string, encoding each bit on a photon prepared on a randomly chosen basis or on a configured bipartite quantum entanglement, such as an EPR Pair or a Bell State (see 2.2.4.1).

b) *Transmission of Quantum States*:

- The sender sends the photon he prepared to the receiver through an untrusted quantum communication medium that can be noisy. This quantum communication medium can be eavesdropped on as well.

c) *Measurement of Quantum States*:

- The receiver measures every received photon, often on a randomly chosen basis. Then, both sender and receiver have what we call raw keys, that may be different. These differences are due to noise present on the quantum communication medium, which may be not perfectly isolated, or even from potential eavesdropping.

2) *Classical Post-Processing*:

a) *Secret Key Sifting*:

- Both parties announce to each other the polarizations and measurement bases used. They discard the bits of their raw keys corresponding to different polarizations and measurement bases used.

2) *Classical Post-Processing* (*cont.*):

a) *Secret Key Sifting* (*cont.*):

- These discarded bits should correspond to conjugate states. The result is what we call sifted keys that are not still error-free.

b) *Parameter Estimation*:

- Both parties announce to each other a random sample of bits from their sifted keys, jointly with the polarizations and bases used for such rounds, on which they should be able to estimate the QBERs of Quantum Transmission. Then, depending on QBERs, they can decide to continue or abort the protocol due to the additional noise introduced by an eventual eavesdropper. If they agree not to abort protocol, they should discard the bits used in the random sample from their sifted keys.

c) *Information Reconciliation*:

- Both parties apply a classical error correction code to their sifted keys, in which they agree on the final result with high probability. The result is an error-free reconciled key.

d) *Privacy Amplification*:

- Both parties eliminate leakage of information or knowledge of an eavesdropper about their reconciled key, by applying a Two-Universal Hash Function, resulting in the final secret key.

Therefore, we can illustrate the usual steps for QKDs in Noiseless Scenarios as follows:

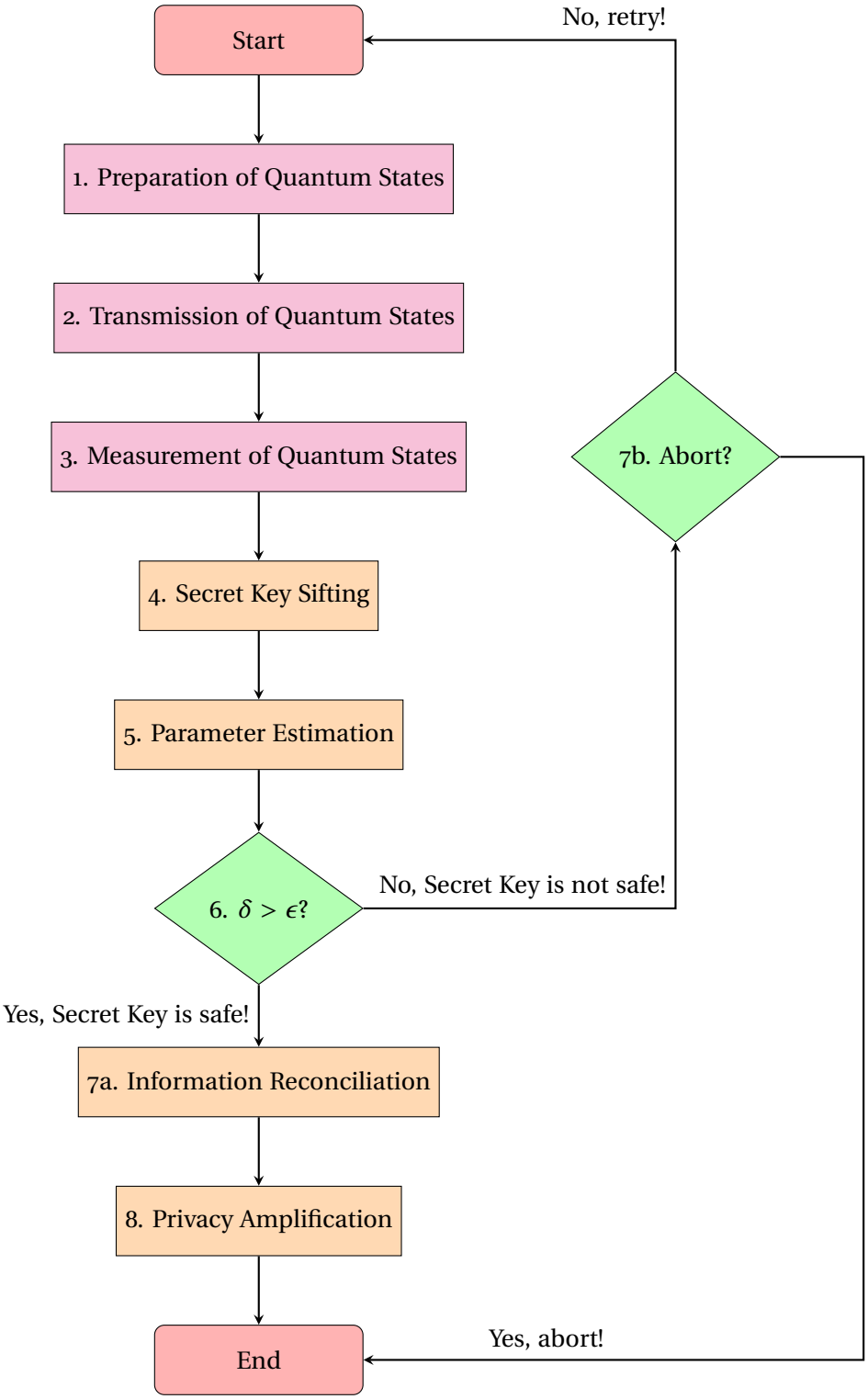


Figure 3.6: Steps for QKDs in Noiseless Scenarios. Here, we represent the steps of classical nature in purple labels, while we represent the steps of classical nature in orange labels. Note that in Parameter Estimation, we only abort the protocol if the transmission errors δ are above a threshold acceptable, considering only noise ϵ introduced by an eavesdropper.

Similarly, we can illustrate the usual steps for QKDs in Noisy Scenarios as follows:

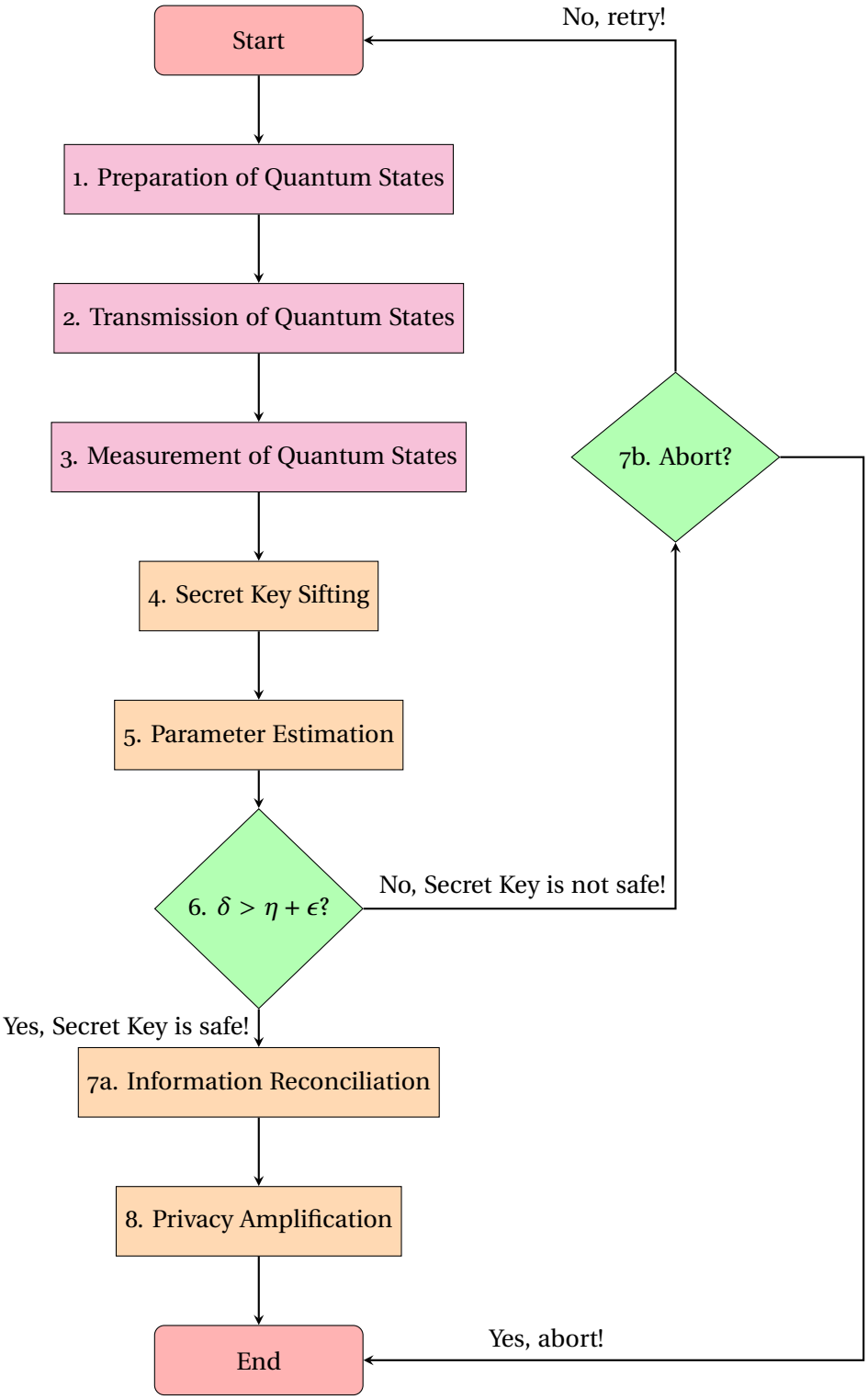


Figure 3.7: Steps for QKDs in Noisy Scenarios. Again, we represent the steps of classical nature in purple labels and the steps of classical nature in orange labels. Note that now in Parameter Estimation, we need to consider the transmission errors δ introduced by both the not perfectly isolated quantum communication medium η and a possible eavesdropper ϵ.

During the description of the following QKD protocols, we will use the standard notation and denote the sender as Alice, the receiver as Bob, and a possible eavesdropper as Eve.

3.3.1 Prepare-and-Measure Quantum Key Distributions (PM-QKDs)

As we already mentioned, a QKD can be a PM-QKD, where the sender simply prepares each photon (ideally, a single-photon) on some randomly chosen polarization before sending it to the receiver. Then, the receiver measures the incoming photons also on some randomly chosen basis. Here, we expect the photons prepared and measured on the same associated polarizations and bases should always give the correct outcomes under ideal conditions. We can claim this observation since we represent the observables of those polarizations and bases by unitary operators. Therefore, if we apply two consecutive equal operators to some quantum state, we will get the same initial quantum state. The same does not happen when we apply two successive different operators. This core idea is what mainly defines PM-QKDs.

3.3.1.1 BB84 Protocol

The BB84 protocol [309] is the most known PM-QKD and the first-ever proposal of a QKD. This protocol makes use of photons prepared in four possible different quantum states, two in each of two mutually conjugate bases. Additionally, the quantum states on the same basis are orthogonal to each other. More specifically, the photons are prepared and measured on the $\mathbb{X}$-Basis (Hadamard Basis) and $\mathbb{Z}$-Basis (Standard Computational Basis). The sender often performs the preparation of each photon on such bases through Laser Sources and Polarizers for the polarization of photons, while the receiver can measure each photon using Photodetectors.

In particular, we can represent the outcomes resulting from Alice preparing the photons in quantum states, through horizontal ($\leftrightarrow$), diagonal ($\nearrow$), vertical ($\updownarrow$) or anti-diagonal ($\nwarrow$) spins, which correspond to 0°, 45°, 90° and 135° polarizations, respectively. On the other side, we can also represent the bases Z and X through which Bob performs the measurements of the incoming photons as rectilinear ($\leftrightarrow\!\!\updownarrow$) and anti-rectilinear ($\nearrow\!\!\nwarrow$) spins, respectively. As obvious, we can also represent these four polarizations through the previously mentioned ket notation for Jones Vectors. In both situations, Alice and Bob randomly choose the polarizations used to prepare and measure each photon, respectively. In the following Table 3.1 we show the four polarizations used in this protocol, as well as their several corresponding notations:

Polarization	Bit	Quantum State	Basis	Jones Ket	Prep. Spin	Meas. Spin
0°	0	$\|0\rangle$	$\mathbb{Z}$	$\|H\rangle$	$\leftrightarrow$	$\leftrightarrow\!\!\updownarrow$
45°		$\|+\rangle$	$\mathbb{X}$	$\|D\rangle$	$\nearrow$	$\nearrow\!\!\nwarrow$
90°	1	$\|1\rangle$	$\mathbb{Z}$	$\|V\rangle$	$\updownarrow$	$\leftrightarrow\!\!\updownarrow$
135°		$\|-\rangle$	$\mathbb{X}$	$\|A\rangle$	$\nwarrow$	$\nearrow\!\!\nwarrow$

Table 3.1: Possible configurations of Quantum States for BB84 protocol. Here, we also show the corresponding Polarizations, Bases and Spins for each possible Quantum State.

Here, if Bob measures the photon on a basis corresponding to one of the polarizations that composes that basis, they can be sure about the expected final secret bit. For example, if Alice uses a polarization of 90° for a photon and Bob measures that photon in the $\mathbb{Z}$-Basis, they both can be sure that the corresponding secret bit should be 1. However, if Bob measures that photon in the $\mathbb{X}$-Basis, he will obtain the quantum state $|-\rangle$, which after the measurement can be equally either 0 or 1. For this reason, this photon should be discarded and not be used to compose the final secret key, and because of that, they should sift this bit. But this is also valid for Eve once she does not know what basis Alice used to prepare the random bit, and the only choice Eve has is trying to guess it at random. In the previous example, imagine that Bob has chosen the correct basis (i.e., the $\mathbb{Z}$-Basis) for that photon. In this case, Alice and Bob should both obtain the secret bit 1, but Eve has a 50% chance of guessing it correctly without being noticed. If she measures that photon in the $\mathbb{Z}$-Basis, she can intercept that secret bit 1 without being noticed by both Alice and Bob. However, if she measures that photon in the $\mathbb{X}$-Basis, she will obtain the quantum state $|-\rangle$ that can be again either 0 or 1. With Eve measuring that bit as 0, Bob will also obtain the bit as 0, which is different from the secret bit as 1 generated initially by Alice. In this case, both Alice and Bob are sure about that bit corresponding to an error either introduced by an eavesdropping attempt from Eve or by noise present in the quantum communication medium used. Otherwise, if Eve obtains the bit 1 after measuring the photon in the $\mathbb{X}$-Basis, she will intercept that secret bit without being noticed. Since here, we are repeatedly dealing with random events, any "good luck" from Eve in guessing precisely the bases used for each photon will not last forever, and they will detect her sooner or later.

Here, we illustrate the four possible polarizations for this protocol Figure 3.8, and the respective two measurement bases in Figure 3.9 in a bi-dimensional trigonometric space:

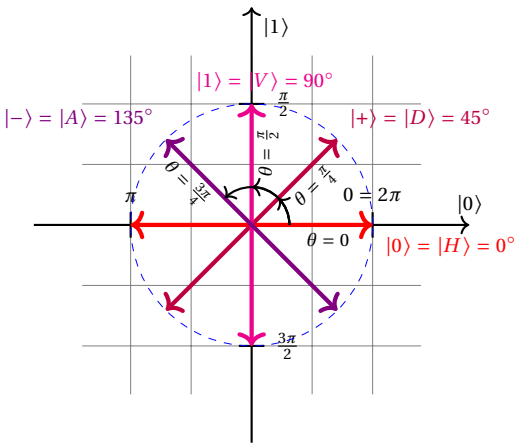


Figure 3.8: Polarizations of Photons in BB84 protocol.

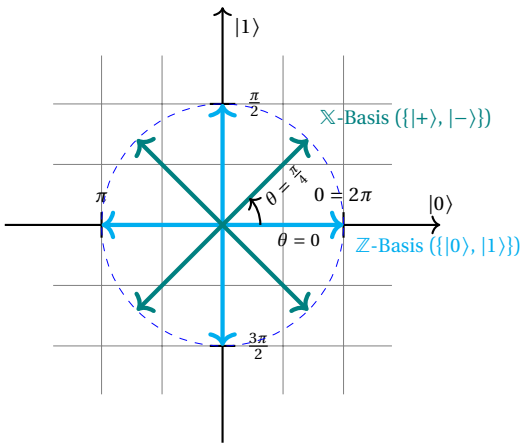


Figure 3.9: Measurement Bases for Incoming Photons in BB84 protocol.

After the quantum transmission, Alice and Bob have their raw keys that might have errors. Then, they publicly announce to each other the bases used, usually through an authenticated classical communication channel. They discard the bits corresponding to measurements of photons in which Bob does not choose the basis corresponding to the respective polarizations

of those photons by Alice. As we already saw before, we cannot use these bits for the final secret key since they result from the observation of quantum states in mutually orthogonal bases. These bits might be random and not perfectly correlated between them. When Alice and Bob do this shortening of their raw keys, it halves their lengths, resulting in their sifted keys. Despite resulting from correlated polarizations and bases, their sifted keys might still have errors. These errors can happen due to noise present in the quantum communication medium used during the transmission or a possible attempt to eavesdrop from Eve.

On the remaining bits of their sifted keys, Alice and Bob perform the Parameter Estimation step. They start by choosing a random sample of their sifted keys with half of their length. For the Noiseless Scenarios, both Alice and Bob can expect no transmission errors with no eavesdropping from Eve. Otherwise, for the Noisy Scenarios, if both Alice and Bob know the quantity of noise present in the quantum communication medium, they can also estimate how much information they potentially leaked to Eve. More specifically, they can determine the QBERs of the quantum communication medium that they pretend to use a priori through a pre-analysis free of eavesdropping. From this pre-analysis, they can establish a maximal upper bound from those QBERs, above which they should abort or retry the protocol again.

In the state-of-the-art, the estimated QBERs with no eavesdropping for the BB84 protocol are always below 17%[443, 461, 465, 466] (on average are around 11%[467, 468]), usually used as the maximal upper bound of noise naturally present in the quantum communication medium. With a QBER value above such a maximal upper bound, both Alice and Bob should consider an eavesdropping attempt from Eve. How more rounds Alice and Bob use in the Quantum Transmission, the greater will be their chance of detecting Eve in the Parameter Estimation.

Then, after the Parameter Estimation step, Alice and Bob perform the further Information Reconciliation and Privacy Amplification steps, in that order. In the end, both Alice and Bob should have a final, secure, and secret symmetric key with a shorter length, from which Eve has practically no knowledge about it (for reference, much less than one bit of information).

We give an illustration of the execution of this protocol in the following Figure 3.10:

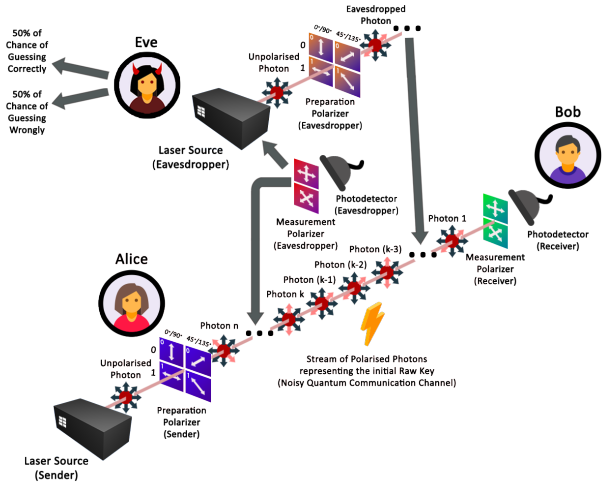


Figure 3.10: Example schematic of the BB84 Protocol.

An example of this protocol, considering the previous illustration, is given in Table 3.2:

Example of execution of the BB84 protocol									
Quantum Transmission	Photon no.	1	2	3	4	5	6	⋮	n
	Alice's Bit	0	1	1	0	0	0		1
	Alices' Polarization	↗	↘	↕	↗	↗	↔		↘
	Eve's Meas. Basis	-	✢	-	⤫	⤫	⤫		✢
	Bob's Meas. Basis	✢	⤫	✢	✢	⤫	✢		⤫
	Bob's Bit	0	0	1	1	0	0		0
Classical Post-Processing	Alice's Sifted Key	-	1	1	-	0	0		1
	Bob's Sifted Key	-	0	1	-	0	0		0
	Parameter Estimation	-	✗		-	✓			
	QBER	$\frac{1+\epsilon}{k-2}$, where $k \approx \frac{n}{4}$ and $\epsilon < k-2$							
	Alice's Remaining Bits	-	-	1	-	-	0	⋮	1
	Bob's Remaining Bits	-	-	1	-	-	0		0
	Information Rec.	-	-	0	-	-	0		1
	Privacy Amp.	-	-	1	-	-	0		-

Table 3.2: Example of execution of the BB84 protocol.

We can think about the probability of both Alice and Bob detecting Eve as the probability of the opposite event (i.e., Eve not being detected). Here, Eve does not need to consider the rounds in which Bob has chosen a measurement basis different from the polarization used by Alice. So, for each not sifted round of the protocol, Eve is not detected in two situations. One is when she guesses the measurement basis used by Bob correctly, and the other is if she wrongly guesses the measurement basis used by Bob and the random conjugated quantum state collapses to the same bit initially generated by Alice. The first situation happens with a probability of 50%, while the second occurs with a chance of 25% since it happens half the time but is also conditioned by an equal possibility of the conjugate quantum state collapse to the same bit that Alice has prepared (i.e., $50\% \times 50\% = 25\%$). Thus, for each round, the probability of Eve intercepts a photon without being noticed is given by $50\% + 25\% = 75\% = \frac{3}{4}$. But Eve needs to have the same "good luck" for each round of the entire protocol. For a protocol with n rounds, we have a probability of $\left(\frac{3}{4}\right)^n$ for never detecting Eve during the execution of the protocol. If we take the probability of the opposite event, the expression $P_D(n) = 1 - \left(\frac{3}{4}\right)^n$ gives us the probability of detecting Eve during the execution of the protocol. If we consider an infinite n, we have $\lim_{n\to+\infty} P_D(n) = 1$. However, we do not need an infinite number of rounds, but only a sufficiently large one. For example, with only $n = 20$, we have the probability $P_D(20) = 1 - \left(\frac{3}{4}\right)^{20} \approx 0.997 = 99.7\%$. We can see the behaviour of this function in Figure 3.11.

This protocol ensures that Alice and Bob can produce a random secret symmetric key. It is random due to the initial random generation of a raw key and a collection of polarization of photons from Alice. Additionally, the secret symmetric key is also random because of the measurement bases which are randomly chosen by Bob for those photons. For these purposes, we should also ensure such randomness with a perfect true random source, such as QRNGs. The protocol has another further random component since Alice prepares some photons in a quantum superposition that, if Eve intercepts them, will lead also to random interferences in

the stream of photons that Eve cannot control. By comparing randomly selected small pieces of information resulting from the measurements of the streaming of photons, Eve can easily be detected, even in Noisy Scenarios, admitting a maximal QBER for the protocol.

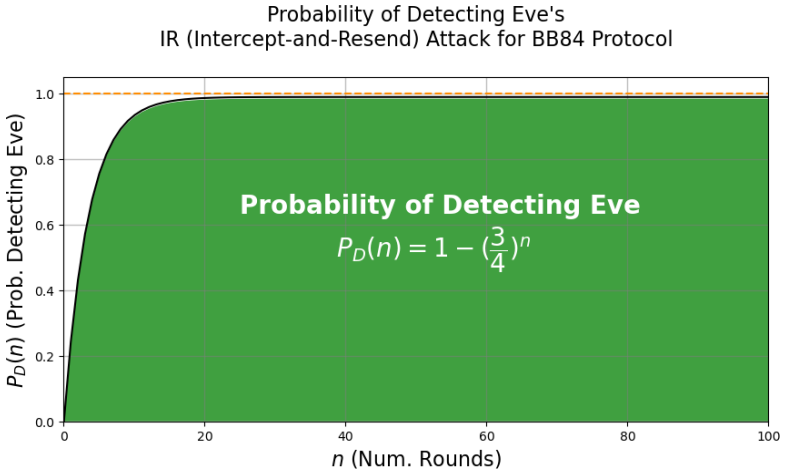


Figure 3.11: Probability of detecting IR (Intercept-and-Resend) attack for the BB84 Protocol.

Therefore, the BB84 protocol does not allow Eve to measure successive photons before Bob receives them without being noticed. So, Eve cannot perform an Intercept-and-Resend attack since it will introduce detectable noise. Eve cannot either copy any of those photons neither perform a Replay attack due to the No-Cloning Theorem (see 2.2.6.1). For those reasons, we consider this protocol unconditionally secure provable if ideally single-photons are used.

3.3.1.2 Other variants of PM-QKDs

Since the proposal of the BB84 protocol, other variants of PM-QKDs were proposed over the years. One of them was the B92 protocol, proposed by Charles Bennett in 1992 [375]. Basically, he made a slight modification to his earlier BB84 protocol, considering now only two different possible non-orthogonal quantum states, instead of four. In this protocol, Alice can prepare the photons through horizontal ($\leftrightarrow$) or diagonal ($\nearrow$) spins, which correspond once again to 0° and 45° polarizations, respectively. On the other side, we can also represent the bases $\mathbb{Z}$ and $\mathbb{X}$ through which Bob performs the measurements of the incoming photons as rectilinear ($\updownarrow$) and anti-rectilinear ($\nwarrow\!\!\!\!\searrow$) spins, respectively. Once again, in both situations, either Alice and Bob randomly choose the polarizations used to prepare and measure each photon.

In the following Table 3.3 we show the possible configurations for the preparation of the photons for the B92 protocol on Alice's side, as well as their corresponding notations:

Polarization	Alice's Bit	Prep. Quantum State	Basis	Jones Ket	Prep. Spin
0°	0	$\|0\rangle$	$\mathbb{Z}$	$\|H\rangle$	$\leftrightarrow$
45°	1	$\|+\rangle$	$\mathbb{X}$	$\|D\rangle$	$\nearrow$

Table 3.3: Possible configurations of Quantum States prepared by Alice for B92 protocol. We also show the corresponding Polarizations, Bases and Spins for each possible Quantum State.

In contrast to the BB84 protocol [309], instead of Alice and Bob comparing the polarizations and measurement bases they used, they will compare classical bits. More specifically, Alice never sends her polarizations neither her random bits generated. Bob sends the bits resulting from his random measurements to Alice over an authenticated public communication channel. He announces these bits because what he will use to compose the final secret key will be his coin flips jointly with the random bits initially generated by Alice. For obvious reasons, Bob never reveals to anybody his random coin flips. We can also imagine the measurement bases randomly chosen by Bob from his coin flip c as two observable operators O_c defined as follows:

- If $c = 0$, $O_c = O_0 = I$, where I is the Pauli-I operator.
- If $c = 1$, $O_c = O_1 = HZ$, where H and Z are the Hadamard and Pauli-Z operators, respectively.

Now, in the following Table 3.4 we show the possible choices for the measurement of the incoming photons for the B92 protocol on Bob's side, according to his random coin flips:

Alice's Bit	Prep. Quantum State	Bob's Coin (c)	Meas. Spin	Meas. Quantum State	Bob's Bit
0	$\|0\rangle$	0	↕	$O_0\|0\rangle = I\|0\rangle = \|0\rangle$	0
		1	⤫	$O_1\|0\rangle = HZ\|0\rangle = \|-\rangle$	0 or 1
1	$\|+\rangle$	0	↕	$O_0\|+\rangle = I\|+\rangle = \|+\rangle$	0 or 1
		1	⤫	$O_1\|+\rangle = HZ\|+\rangle = \|0\rangle$	0

Table 3.4: Possible configurations of Quantum States measured by Bob for B92 protocol. We also show the several corresponding notations for each possible Quantum State.

Additionally, we can also illustrate all the four possible cases of the final classical outcomes for the B92 protocol as a probability tree, as demonstrated in the following Fig. 3.12:

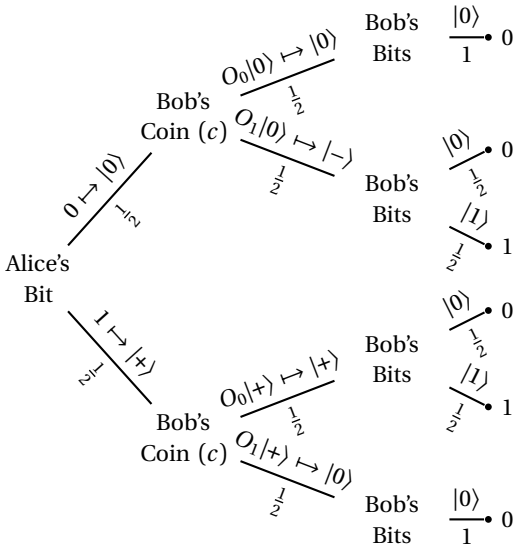


Figure 3.12: Representation of all possible cases of the final outcomes for the B92 protocol as a probability tree for each round, regarding the Alice's Bit, as well as Bob's Coin and Bit.

As mentioned before, after the quantum transmission of states, Alice and Bob have their raw keys composed by the initial random binary string generated by her and by the random binary string composed by Bob's coin flips. Then, Bob sends to Alice every bit resulting from the measurements he performed on photons, from which she will discard some bits of her raw key and communicate to Bob every bit he needs to discard from his coin flips. More specifically, Alice and Bob sift their raw keys according to the following enumerated four possible cases:

- If $c = 0$, Bob used the operator O_0 ($\updownarrow$ measurement spin), we have two cases:
    1. If Bob obtained the bit 0 after his measurement, he cannot be sure if Alice prepared the photon with a 0° polarization and he guessed the correct basis, or whether if Alice prepared the photon with a 45° polarization, and by guessing wrongly the measurement basis, he made that photon collapse to the bit 0 just by chance. This round should not be considered, as well as both Alice's bit and Bob's coin flip.

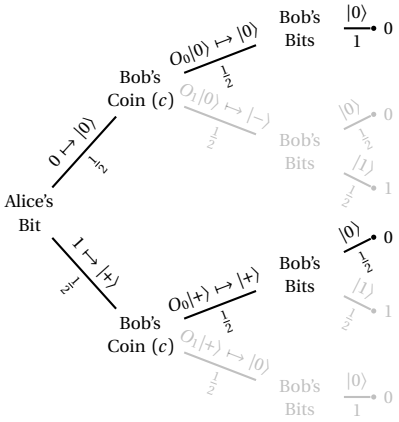


Figure 3.13: Representation of the 1^{st} case of the final outcomes for the B92 protocol.

    2. If Bob obtained the bit 1 after his measurement, he can be sure that Alice prepared the photon with a 45° polarization, since is the only case on which Bob can obtain the bit 1, considering he used the operator O_0, measuring the quantum state $|+\rangle$. This round should be considered, as well as both Alice's bit and Bob's coin flip.

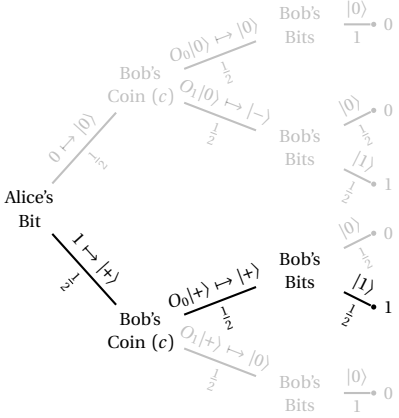


Figure 3.14: Representation of the 2^{nd} case of the final outcomes for the B92 protocol.

- If $c = 1$, Bob will use the operator O_1, from which can result two possible cases:

    1. If Bob obtained the bit 0 after his measurement, he cannot be sure if Alice prepared the photon with a 0° polarization, and by guessing wrongly the basis, he made that photon collapse to the bit 0 just by chance, or whether if Alice prepared the photon with a 45° polarization, and he guessed the correct measurement basis. This round should not be considered, as well as both Alice's bit and Bob's coin flip.

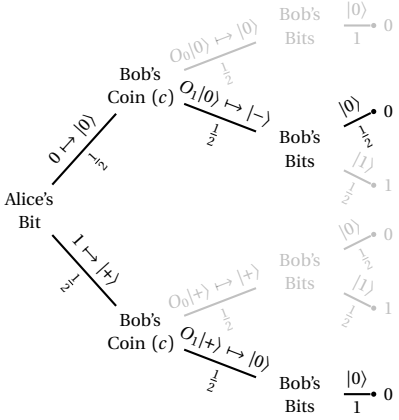


Figure 3.15: Representation of the 3^{rd} case of the final outcomes for the B92 protocol.

    2. If Bob obtained the bit 1 after his measurement, he can be sure that Alice prepared the photon with a 0° polarization, since is the only case on which Bob can obtain the bit 1, considering he used the operator O_1, measuring the quantum state $|-\rangle$. This round should be considered, as well as both Alice's bit and Bob's coin flip.

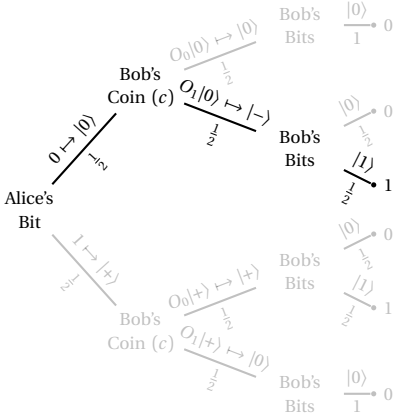


Figure 3.16: Representation of the 4^{th} case of the final outcomes for the B92 protocol.

In simple terms, they discard the rounds of the protocol where Bob correctly guessed the measurement basis and where Bob wrongly guessed the measurement basis and obtained the bit 0. They kept the remaining rounds of the protocol for the construction of the sifted key.

However, if for the remaining rounds, we consider the pairs of Alice's bits and Bob's coin flips that compose the sifted key, we see that they always have the form of {0,1} or {1,0}. For

this reason, Alice should keep her bits as they are, and Bob needs to flip his coin flips to get the same bits of Alice's sifted key. But, as usual, these sifted keys can have some errors due to inherent noise present in the quantum communication medium or due to an eventual eavesdropping interference from Eve. For this reason, Alice and Bob choose a random sample of their bits (e.g., with the size of half of their sifted keys) and announce them to estimate the QBER by comparing each pair of bits, checking if they are equal or not. Then, they perform the usual further steps of Information Reconciliation and Privacy Amplification. The remaining errors are corrected, and they eliminate practically all the information possibly leaked to Eve.

Following the current state-of-the-art, the estimated QBERs with no eavesdropping for the B92 protocol are usually around 25% (or more precisely 25.3%), which is usually used as the maximal upper bound of noise naturally present in the quantum communication medium.

In this protocol, we have that the probability of Eve being noticed in each round is equal to 12.5% (i.e., $50\% \times 50\% \times 50\% = 12.5\% = \frac{1}{8}$), for which we can claim that the probability of Eve not being noticed during all the protocol, considering n rounds, is equal to $\left(\frac{7}{8}\right)^n$. By computing the probability of the opposite event, the probability of detecting Eve during the execution of the B92 protocol is given by $P_D(n) = 1-\left(\frac{7}{8}\right)^n$, where, as usual, we also have $\lim_{n\to+\infty} P_D(n) = 1$. For example, if we consider again only $n = 20$, we have $P_D(20) = 1-\left(\frac{7}{8}\right)^{20} \approx 0.931 = 93.1\%$. In the following Figure 3.17, we illustrate the behaviour of this probability function, as n grows:

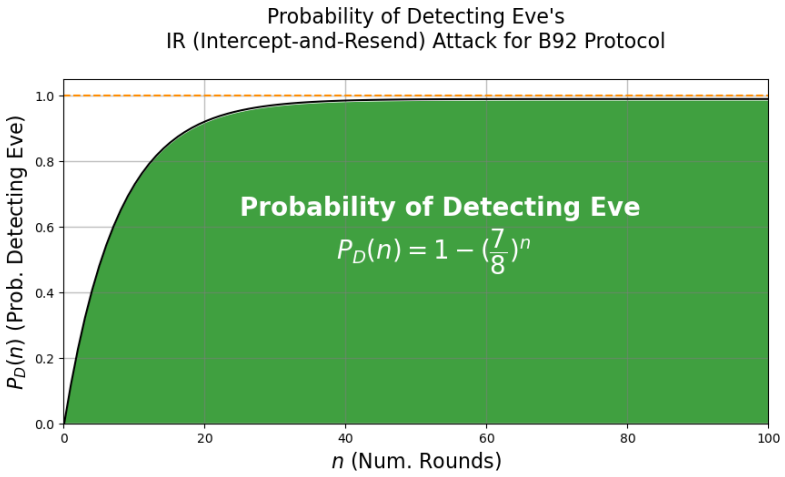


Figure 3.17: Probability of detecting IR (Intercept-and-Resend) attack for the B92 Protocol.

Some years later, namely in 1999, Helle Bechmann-Pasquinucci and Nicolas Gisin proposed another PM-QKD, which was later known as SSP (Six-State Protocol) [378]. This protocol is very similar to the BB84 protocol but uses six possible polarizations for the photons, two in each of three orthogonal bases. Here, the photons are prepared and measured on the $\mathbb{X}$-Basis (Hadamard Basis), $\mathbb{Y}$-Basis (Imaginary Basis), and $\mathbb{Z}$-Basis (Standard Computational Basis).

In SSP, the transmitted photons are prepared in quantum states, through horizontal ($\leftrightarrow$), diagonal ($\nearrow$), vertical ($\updownarrow$) or anti-diagonal ($\nwarrow$), right-hand ($\circlearrowright$) and left-hand ($\circlearrowleft$) spins, which correspond to the following 0°, 45°, 90°, 135°, RHC (Right-Hand Circular), and LHC (Left-Hand Circular) polarizations, respectively. We can also represent the bases $\mathbb{Z}$, $\mathbb{X}$ and $\mathbb{Y}$

through which Bob can perform the measurements of the incoming photons as rectilinear ($\updownarrow\!\!\!\!\leftrightarrow$), anti-rectilinear ($\nearrow\!\!\!\!\searrow$) and circular ($\circlearrowright$) spins, respectively, as demonstrated in Table 3.5:

Polarization	Bit	Quantum State	Basis	Jones Ket	Prep. Spin	Meas. Spin
0°	0	$\|0\rangle$	$\mathbb{Z}$	$\|H\rangle$	$\leftrightarrow$	$\updownarrow\!\!\!\!\leftrightarrow$
45°		$\|+\rangle$	$\mathbb{X}$	$\|D\rangle$	$\nearrow$	$\nearrow\!\!\!\!\searrow$
RHC		$\|+i\rangle$	$\mathbb{Y}$	$\|R\rangle$	$\circlearrowright$	$\circlearrowright$
90°	1	$\|1\rangle$	$\mathbb{Z}$	$\|V\rangle$	$\updownarrow$	$\updownarrow\!\!\!\!\leftrightarrow$
135°		$\|-\rangle$	$\mathbb{X}$	$\|A\rangle$	$\nwarrow$	$\nearrow\!\!\!\!\searrow$
LHC		$\|-i\rangle$	$\mathbb{Y}$	$\|L\rangle$	$\circlearrowright$	$\circlearrowright$

Table 3.5: Possible configurations of Quantum States for SSP. We also show the corresponding Polarizations, Bases and Spins for each possible Quantum State.

Similar to the BB84 protocol, if Bob measures the photon on a basis corresponding to one of the polarizations that composes that basis, they can be sure about the expected final secret bit. For example, if Alice uses a polarization of RHC for a photon and Bob measures that photon in the $\mathbb{Y}$-Basis, they can be sure the corresponding secret bit should be 0. However, if Bob measures that photon in the $\mathbb{Z}$-Basis, he will obtain the quantum state $|+i\rangle$, which after the measurement can be equally either 0 or 1. For this reason, we should not consider this photon to compose the final secret key, and we can sift it. But once again, this is also valid for Eve once she does not know what basis Alice used to prepare the random bit, and the only choice Eve has is trying to guess it at random, as usual. In the previous example, imagine that Bob has chosen the correct basis (i.e., the $\mathbb{Y}$-Basis) for that photon. Here, Alice and Bob should both obtain the secret bit 0, but now Eve has a 33.33% chance of guessing it correctly without being noticed since now, in this protocol, we have three measurement bases instead of two. If she measures that photon in the $\mathbb{Y}$-Basis, she can intercept that secret bit 0 without being noticed by both Alice and Bob. However, if she measures that photon in the $\mathbb{Z}$-Basis or $\mathbb{X}$-Basis, she will obtain the quantum states $|+i\rangle$ or $0.5\big[(1+i)|0\rangle+(1-i)|1\rangle\big]$ that can be either 0 or 1, in both cases. With Eve measuring that bit as 1 and resending it, Bob can also obtain the bit 1, which is different from the secret bit 0 generated initially by Alice. In this case, both Alice and Bob are sure about that bit corresponding to an error either introduced by an eavesdropping attempt from Eve or by noise present in the quantum communication medium. Otherwise, if Eve obtains the bit 0 after measuring the photon in the $\mathbb{Z}$-Basis or $\mathbb{X}$-Basis, resends it, and Bob also obtains 0, she will be able to intercept that secret bit without being noticed.

As usual, after the quantum transmission, Alice and Bob have their raw keys that might have errors. Then, they perform the Secret Key Sifting, where publicly announce to each other the bases used, discarding the bits corresponding to measurements of photons in which Bob does not choose the basis corresponding to the respective polarizations of those photons by Alice. After the Secret Key Sifting, the remaining bits might still have errors. On the remaining bits of their sifted keys, Alice and Bob perform the usual Parameter Estimation, estimating the QBERs, deciding if they continue or abort the current execution of the protocol. In the current state-of-the-art, the estimated QBERs with no eavesdropping for the SSP are around 12.6%,

frequently used as a threshold above which Alice and Bob should abort the protocol.

Finally, after the Parameter Estimation step, Alice and Bob perform the standard steps of Information Reconciliation and Privacy Amplification, in that order. In the end, both Alice and Bob should have a shorter secret symmetric key, where Eve has negligible knowledge about it.

In SSP, we have that the probability of Eve not being noticed in each round is equal to 66.66% (i.e., $33.33\% + 2 \times 33.33\% \times 50\% = 33.33\% + 33.33\% = 66.66\% = \frac{2}{3}$), for which we can claim that the probability of Eve not being noticed during all the protocol, considering n rounds, is equal to $\left(\frac{2}{3}\right)^n$. By computing the probability of the opposite event, the probability of detecting Eve during the execution of the SSP is given by $P_D(n) = 1 - \left(\frac{2}{3}\right)^n$, where, as usual, we also have $\lim_{n \to +\infty} P_D(n) = 1$. For example, if we consider again only $n = 20$, we have $P_D(20) = 1 - \left(\frac{2}{3}\right)^{20} \approx 0.999 = 99.9\%$, and we can see that it is even easier to detect Eve in SSP when compared to BB84 protocol. We can see the behaviour of this function in Figure 3.18:

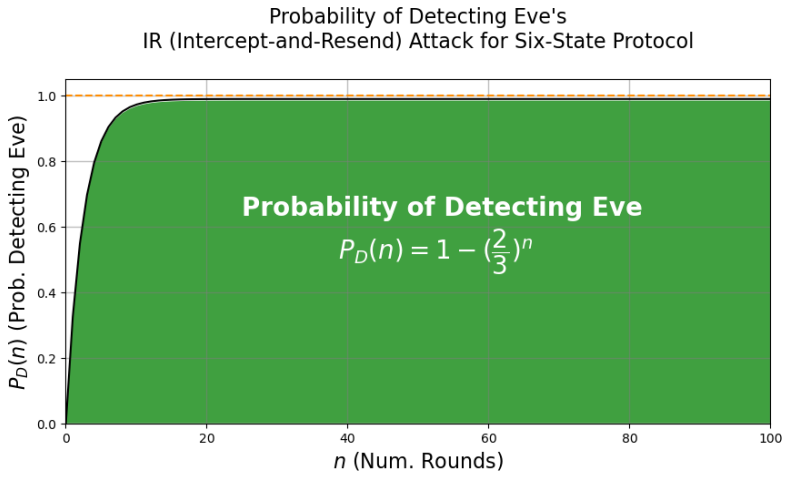


Figure 3.18: Probability of detecting IR (Intercept-and-Resend) attack for the Six-State Protocol.

Other well-known PM-QKDs are the MSZ96 Protocol [377], Decoy State Protocol [379], SARG04 Protocol [382], and T12 [386] Protocol. In particular, the SRG04 Protocol was a proposal designed as a modification of the BB84 Protocol [309] to countermeasure PNS attacks.

3.3.2 Entanglement-Based Quantum Key Distributions (EB-QKDs)

On the other hand, a QKD can be an EB-QKD, where we extract the secret bits from pairs of entangled photons (ideally, single-photons). In these protocols, such pairs of entangled photons can be either prepared by a sender or even by a third-party (e.g., a server), which never keeps any photon to itself. Then, the receiver (or receivers, when we have a third-party) measures the incoming photons on some randomly chosen basis. Using the inherent perfect correlation of quantum entanglements with some of its principles (such as its randomness and monogamy), we can ensure the exchange of a symmetric secret key that should be perfectly correlated, random, and private. These principles are what essentially defines EB-QKDs.

3.3.2.1 E91 Protocol

The E91 protocol is the first-ever proposed EB-QKD, developed by Artur Ekert in 1991 [374]. In this protocol, we consider a single source that transmits pairs of entangled photons, described by a Bell State, namely with the form $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. This source can be owned by Alice or even by another untrusted third-party. If Alice owns that source, she needs to keep a photon of the pair to itself. Otherwise, if the source is owned by an untrusted third-party, then that party gains nothing to keep a photon of the pair to itself. These photons can be polarized, entangled, separated, and then distributed to Alice and Bob, each one getting half of each entangled pair. Recall that we need to have the photons close to each other and make them interact in some way to create a quantum entanglement. Then, Alice and Bob measure the received photons by choosing a random measurement basis out of three possible choices. They adopt these measurement bases according to a CHSH (Clauser-Horne- Shimony-Holt) test [469] to be applied after the transmission of the stream of pairs of entangled photons.

More specifically, Alice and Bob choose randomly the azimuthal angles a_i, b_j, respectively, to perform the measurements, considering a bi-dimensional xy plane that is perpendicular to the trajectory z of the photons. We define the pairs of azimuthal angles (a_i, b_j) chosen by Alice and Bob for their measurement bases as demonstrated following, where $i, j = \{1, 2, 3\}$:

$$a_i = \begin{cases} \theta_1^a = 0, & i = 1 \\ \theta_2^a = \frac{\pi}{4}, & i = 2 \\ \theta_3^a = \frac{\pi}{2}, & i = 3 \end{cases} \quad \text{and} \quad b_j = \begin{cases} \theta_1^b = \frac{\pi}{4}, & j = 1 \\ \theta_2^b = \frac{\pi}{2}, & j = 2 \\ \theta_3^b = \frac{3\pi}{4}, & j = 3 \end{cases}$$

The azimuthal angles θ_1^a, θ_2^a, and θ_3^a chosen by Alice correspond to the measurement bases $\mathbb{Z}$ (Standard Computational Basis), $\frac{(\mathbb{X}+\mathbb{Z})}{\sqrt{2}}$ and $\mathbb{X}$ (Hadamard Basis), respectively. On the other hand, the azimuthal angles θ_1^b, θ_2^b, and θ_3^b chosen by Bob correspond to the measurement bases $\frac{(\mathbb{X}+\mathbb{Z})}{\sqrt{2}}$, $\mathbb{X}$ (Hadamard Basis) and $\frac{(\mathbb{X}-\mathbb{Z})}{\sqrt{2}}$, respectively. Additionally, the measurement bases $\frac{(\mathbb{X}+\mathbb{Z})}{\sqrt{2}}$ and $\frac{(\mathbb{X}-\mathbb{Z})}{\sqrt{2}}$ correspond to the two following enumerated unitary quantum operators:

$$\frac{(\mathbb{X}+\mathbb{Z})}{\sqrt{2}} = \begin{bmatrix} \frac{\sqrt{2+\sqrt{2}}}{2} & \frac{\sqrt{2-\sqrt{2}}}{2} \\ \frac{\sqrt{2-\sqrt{2}}}{2} & -\frac{\sqrt{2+\sqrt{2}}}{2} \end{bmatrix} \quad \text{and} \quad \frac{(\mathbb{X}-\mathbb{Z})}{\sqrt{2}} = \begin{bmatrix} \frac{\sqrt{2-\sqrt{2}}}{2} & \frac{\sqrt{2+\sqrt{2}}}{2} \\ \frac{\sqrt{2+\sqrt{2}}}{2} & -\frac{\sqrt{2-\sqrt{2}}}{2} \end{bmatrix}$$

In terms of circuit-based quantum computing models, we can define the measurement bases $\frac{(\mathbb{X}+\mathbb{Z})}{\sqrt{2}}$ and $\frac{(\mathbb{X}-\mathbb{Z})}{\sqrt{2}}$, as the sequences of quantum gates, $R_Y(\frac{\pi}{4})Z$ and $R_Y(\frac{3\pi}{4})Z$, respectively, where $R_Y(\theta)$ is the Rotation-Y gate and Z is the Pauli-Z gate. Additionally, we can also note that $R_Y(0)Z = Z$ and $R_Y(\frac{\pi}{2})Z = H$, which correspond to the $\mathbb{Z}$-Basis and $\mathbb{X}$-Basis, respectively. Here, the azimuthal angles start from the quantum state $|0\rangle$, and the Pauli-Z gate can be used to prepare a quantum state in the $\mathbb{Z}$-Basis since it does not affect the quantum state $|0\rangle$.

We can also represent these azimuthal angles a_i and b_j by vectors $a_i^{\rightarrow}$ and $b_j^{\rightarrow}$. In particular, for a bi-dimensional Cartesian plane, we can convert an angle θ in a vector $u^{\rightarrow}$ with x and y coordinates, with the mathematical rules $u_x{}^{\rightarrow}(\theta) = ||x|| \cos(\theta)$ and $u_y{}^{\rightarrow}(\theta) = ||y|| \sin(\theta)$. Note that in Quantum Mechanics we usually deal with unit vectors (i.e., their norms are mostly equal to 1), and thus, we have that $||x|| = ||y|| = 1$. So, we can simplify these mathematical

rules to simply $u_x^{\rightarrow}(\theta) = \cos(\theta)$ and $u_y^{\rightarrow}(\theta) = \sin(\theta)$, in a bi-dimensional trigonometric plane. Finally, by converting these azimuthal angles a_i and b_i to the respective vectors $a_i^{\rightarrow}$ and $b_j^{\rightarrow}$, we end up with the following set of correspondences, where $i, j = \{1, 2, 3\}$:

$$a_i^{\rightarrow} = \begin{cases} a_1^{\rightarrow}(\theta_1^a) = a_1^{\rightarrow}(0) = \big(\cos(0), \sin(0), 0\big) = (1, 0, 0), & i = 1 \\ a_2^{\rightarrow}(\theta_2^a) = a_2^{\rightarrow}(\frac{\pi}{4}) = \big(\cos(\frac{\pi}{4}), \sin(\frac{\pi}{4}), 0\big) = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0), & i = 2 \\ a_3^{\rightarrow}(\theta_3^a) = a_3^{\rightarrow}(\frac{\pi}{2}) = \big(\cos(\frac{\pi}{2}), \sin(\frac{\pi}{2}), 0\big) = (0, 1, 0), & i = 3 \end{cases}$$

$$b_j^{\rightarrow} = \begin{cases} b_1^{\rightarrow}(\theta_1^b) = b_1^{\rightarrow}(\frac{\pi}{4}) = \big(\cos(\frac{\pi}{4}), \sin(\frac{\pi}{4}), 0\big) = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0), & j = 1 \\ b_2^{\rightarrow}(\theta_2^b) = b_2^{\rightarrow}(\frac{\pi}{2}) = \big(\cos(\frac{\pi}{2}), \sin(\frac{\pi}{2}), 0\big) = (0, 1, 0), & j = 2 \\ b_3^{\rightarrow}(\theta_3^b) = b_3^{\rightarrow}(\frac{3\pi}{4}) = \big(\cos(\frac{3\pi}{4}), \sin(\frac{3\pi}{4}), 0\big) = (-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0), & j = 3 \end{cases}$$

In Fig. 3.19 and Fig. 3.20, we show these measurement angles in the bi-dimensional plane:

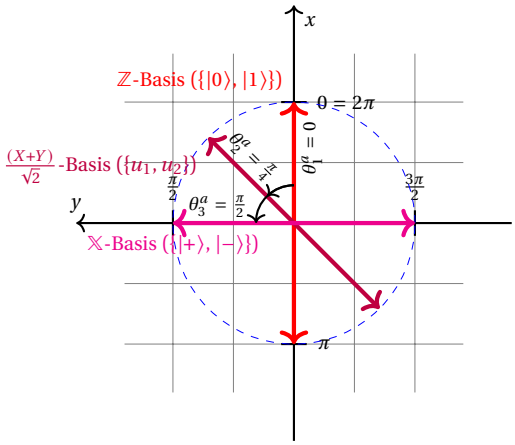


Figure 3.19: Measurement Bases of Photons for Alice in E91 protocol, considering the azimuthal angles $a_i = \theta_i^a$, with $i = \{1, 2, 3\}$. Here, we have $u_1 = \begin{bmatrix} \frac{\sqrt{2+\sqrt{2}}}{2} & \frac{\sqrt{2-\sqrt{2}}}{2} \end{bmatrix}^T$ and $u_2 = \begin{bmatrix} \frac{\sqrt{2-\sqrt{2}}}{2} & -\frac{\sqrt{2+\sqrt{2}}}{2} \end{bmatrix}^T$.

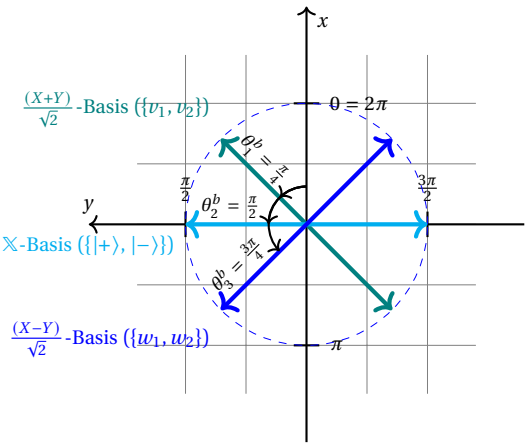


Figure 3.20: Measurement Bases of Photons for Bob in E91 protocol, considering the azimuthal angles $b_j = \theta_j^b$, with $j = \{1, 2, 3\}$. Here, we have $v_1 = \begin{bmatrix} \frac{\sqrt{2+\sqrt{2}}}{2} & \frac{\sqrt{2-\sqrt{2}}}{2} \end{bmatrix}^T$, $v_2 = \begin{bmatrix} \frac{\sqrt{2-\sqrt{2}}}{2} & -\frac{\sqrt{2+\sqrt{2}}}{2} \end{bmatrix}^T$, $w_1 = \begin{bmatrix} \frac{\sqrt{2-\sqrt{2}}}{2} & \frac{\sqrt{2+\sqrt{2}}}{2} \end{bmatrix}^T$ and $w_2 = \begin{bmatrix} \frac{\sqrt{2+\sqrt{2}}}{2} & -\frac{\sqrt{2-\sqrt{2}}}{2} \end{bmatrix}^T$.

Additionally, we can also define the probability of obtaining the possible classical outcomes along with the azimuthal angles a_i and b_j, using the following enumerated notations:

- $P_{|00\rangle}(a_i, b_j)$: The probability of Alice and Bob obtain both 0.
- $P_{|01\rangle}(a_i, b_j)$: The probability of Alice and Bob obtain 0 and 1, respectively.
- $P_{|10\rangle}(a_i, b_j)$: The probability of Alice and Bob obtain 1 and 0, respectively.
- $P_{|11\rangle}(a_i, b_j)$: The probability of Alice and Bob obtain both 1.

Then, we can define the correlation coefficient of the measurements performed by Alice and Bob, along with a_i and b_j, respectively, as the following mathematical expression:

- $E(a_i, b_j) = P_{|00\rangle}(a_i, b_j) + P_{|11\rangle}(a_i, b_j) - P_{|01\rangle}(a_i, b_j) - P_{|10\rangle}(a_i, b_j)$.

From the definition of these correlation coefficients, we are able to obtain the following values for all possible azimuthal angles a_i and b_j randomly chosen by Alice and Bob:

- $E(a_1, b_1) = P_{|00\rangle}(a_1, b_1) + P_{|11\rangle}(a_1, b_1) - P_{|01\rangle}(a_1, b_1) - P_{|10\rangle}(a_1, b_1) =$
  $= 0.0732226025 + 0.0732226025 - 0.4267726025 - 0.4267726025 = -0.7071 \approx -\frac{1}{\sqrt{2}}$.
- $E(a_1, b_2) = P_{|00\rangle}(a_1, b_2) + P_{|11\rangle}(a_1, b_2) - P_{|01\rangle}(a_1, b_2) - P_{|10\rangle}(a_1, b_2) =$
  $= 0.25 + 0.25 - 0.25 - 0.25 = 0$.
- $E(a_1, b_3) = P_{|00\rangle}(a_1, b_3) + P_{|11\rangle}(a_1, b_3) - P_{|01\rangle}(a_1, b_3) - P_{|10\rangle}(a_1, b_3) =$
  $= 0.4267726025 + 0.4267726025 - 0.0732226025 - 0.0732226025 = 0.7071 \approx \frac{1}{\sqrt{2}}$.
- $E(a_2, b_1) = P_{|00\rangle}(a_2, b_1) + P_{|11\rangle}(a_2, b_1) - P_{|01\rangle}(a_2, b_1) - P_{|10\rangle}(a_2, b_1) =$
  $= 0 + 0 - 0.5 - 0.5 = -1$.
- $E(a_2, b_2) = P_{|00\rangle}(a_2, b_2) + P_{|11\rangle}(a_2, b_2) - P_{|01\rangle}(a_2, b_2) - P_{|10\rangle}(a_2, b_2) =$
  $= 0.0732226025 + 0.0732226025 - 0.4267726025 - 0.4267726025 = -0.7071 \approx -\frac{1}{\sqrt{2}}$.
- $E(a_2, b_3) = P_{|00\rangle}(a_2, b_3) + P_{|11\rangle}(a_2, b_3) - P_{|01\rangle}(a_2, b_3) - P_{|10\rangle}(a_2, b_3) =$
  $= 0.25 + 0.25 - 0.25 - 0.25 = 0$.
- $E(a_3, b_1) = P_{|00\rangle}(a_3, b_1) + P_{|11\rangle}(a_3, b_1) - P_{|01\rangle}(a_3, b_1) - P_{|10\rangle}(a_3, b_1) =$
  $= 0.0732226025 + 0.0732226025 - 0.4267726025 - 0.4267726025 = -0.7071 \approx -\frac{1}{\sqrt{2}}$.
- $E(a_3, b_2) = P_{|00\rangle}(a_3, b_2) + P_{|11\rangle}(a_3, b_2) - P_{|01\rangle}(a_3, b_2) - P_{|10\rangle}(a_3, b_2) =$
  $= 0 + 0 - 0.5 - 0.5 = -1$.
- $E(a_3, b_3) = P_{|00\rangle}(a_3, b_3) + P_{|11\rangle}(a_3, b_3) - P_{|01\rangle}(a_3, b_3) - P_{|10\rangle}(a_3, b_3) =$
  $= 0.0732226025 + 0.0732226025 - 0.4267726025 - 0.4267726025 = -0.7071 \approx -\frac{1}{\sqrt{2}}$.

Additionally, we can see that the previous correlation coefficients of the measurements performed by Alice and Bob, along with a_i and b_j, can be equally written as follows:

- $E(a_i, b_j) = -a_i \cdot b_j$.

For the pairs of measurement bases of the same orientation (or with the same azimuthal angle), Alice and Bob should get a total anti-correlation in their resulting outcomes:

- $E(a_2, b_1) = E(a_3, b_2) = -1$.

After the quantum transmission of states, Alice and Bob announce publicly which bases they used for their measurements, as happens in PM-QKDs. Afterward, they divide the pairs of measurement bases (a_i, b_j) used for each round into two separate groups. The first group

(G_1) is composed of the rounds on which their pairs of measurement bases have different orientations, while the second group (G_2) is composed by the rounds on which their pairs of measurement bases have equal orientations. Then, they will use the rounds of G_1 to perform a statistical test for the CHSH Inequality. For such a statistical test, they can exclude the pairs of measurement bases with a correlation coefficient of 0, as well as those on which either or both of them failed to detect a photon at all. Therefore, we can define this statistical test S based on CHSH Inequality as the mathematical equation demonstrated as follows:

- $S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3)$.

By doing the calculations according to the statistical test S based on the CHSH Inequality, we can claim that the result Alice and Bob should obtain under ideal conditions is the following:

- $S = -2\sqrt{2}$.

After Alice and Bob perform the statistical test S, they can check a possible eavesdropping attempt from Eve. More specifically, if the $-2 \leq S \leq 2$ holds, it would indicate either that the received photons are not truly entangled. The fact of the photons not being truly entangled could be because of noise present in the quantum communication medium or an attempt to eavesdrop, or even because of some problem with the measurement device. By contrast, if everything works perfectly and there is no eavesdropper, the expected value of the statistical test S will be the maximal violation $-2\sqrt{2}$. This verification assures that Alice and Bob can use the rounds in G_2 to build the secret key since, with no eavesdropping, the bits resulting from those rounds should be completely anti-correlated. As obvious, Alice and Bob must discard the bits from the rounds of G_1, since the measurement bases they used do not match with each other. In particular, Alice can keep her secret bits, while Bob can flip his secret bits to match those from Alice. This protocol should not require the step of Information Reconciliation since the bits of G_2 are completely anti-correlated. But can be combined with a Universal Hash Function at the end, similar to what happens with PM-QKDs, during Privacy Amplification.

Here, Eve cannot get any information from the photons while they are being transmitted through the quantum communication medium used, simply because there is no information encoded there. The information is only extracted from the photons after Alice and Bob perform measurements on them and communicate in public the measurement bases they used for it then. Additionally, Eve may even try to substitute her own prepared photons for Alice and Bob to misguide them. However, as she does not know which orientation of the measurement angles Alice and Bob will choose for a given pair of photons, there is no good strategy for Eve to escape from being detected. Her intervention will be equivalent to introducing elements of our physical reality to the measurements that affect the non-locality of Quantum Mechanics.

Other popular EB-QKDs are the BBM92 Protocol [376] and Twin Field - QKD [470].

3.4 Semi-Quantum Key Distributions (SQKDs)

However, not all bipartite quantum cryptographic protocols known for the exchange of secret symmetric keys require that both Alice and Bob have access to Quantum Resources. These Quantum Resources may include some optical elements, such as Laser Sources, Polarizers, Beam Splitters, or Phase Shifters, as well as other common Quantum Devices, such as Quantum Computers or Quantum Memories. More specifically, we can equip only one of the parties (Alice or Bob) with Classical Resources which are equivalent to Optical Elements with classical properties, such as Polarizers, Mirrors, or Photodetectors. We often refer to these protocols as SQKDs (Semi-Quantum Key Distributions) and configure the receiver of the secret symmetric key in these protocols to be the party with Classical Resources. Here, we assume Bob has access only to Classical Resources while keeping practically the same security properties of QKDs. These protocols operate basically with the same steps as QKDs, with some slight differences.

In this semi-quantum cryptographic model, we referred to Alice as a quantum entity and Bob as a classical or semi-quantum entity. Here, Alice has access to a quantum communication medium starting at her endpoint, traveling outside, and returning to her endpoint again. On the other side, Bob can access a portion of this quantum communication medium. Thus, SQKDs operate over a two-way quantum communication medium where photons, or other quantum particles, travel first from the quantum entity, Alice, to the classical entity, Bob, then return to the quantum entity, Alice. This cryptographic model is shown in Figure 3.21:

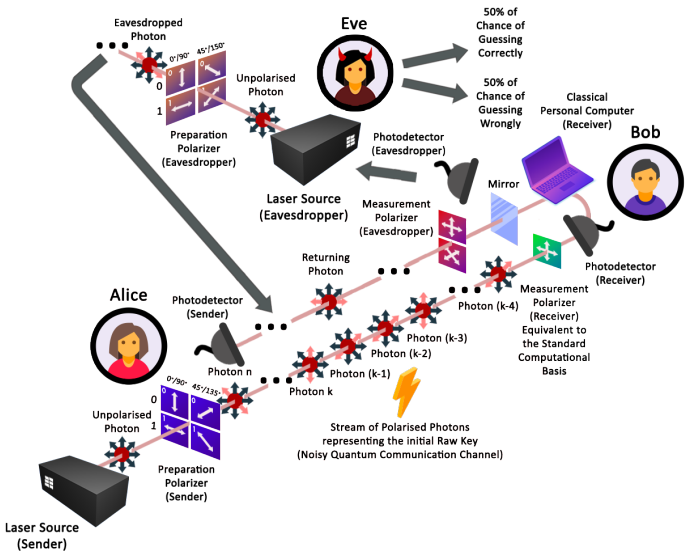


Figure 3.21: Semi-Quantum Cryptographic Model.

Besides the requirement of a two-way quantum communication medium, SQKDs also put a further restriction on Bob's side. More specifically, this model only allows him to interact with the quantum communication medium by performing measurements on the $\mathbb{Z}$-Basis or sending photons (or any quantum particle) prepared in the $\mathbb{Z}$-Basis. Here, it is important to enhance the classical nature of Bob, since preparing a photon in the $\mathbb{Z}$-Basis (Standard Computational Basis) will result in the quantum states $|0\rangle$ and $|1\rangle$, which are equivalent to

the classical bits 0 and 1, respectively. Alternatively, Bob can also simply ignore the quantum communication medium, disconnecting from it for a brief period, equivalent to a time window of a light pulse. In this case, Alice will be basically like "communicating with herself". Thus, for these protocols, there are five operations that we need to consider to Bob's endpoint:

1. *Measure*:
    - Bob measures the incoming photon in the $\mathbb{Z}$-Basis, observing its quantum state, via Optical Elements such as Polarizers and Photodetectors.
2. *Prepare*:
    - Bob prepares a photon in the $\mathbb{Z}$-Basis and sends it to Alice on the reverse quantum communication medium, using Optical Elements such as Polarizers.
3. *Measure-and-Resend*:
    - Basically, it is the combination of both two previous operations. Bob measures the incoming photon in the $\mathbb{Z}$-Basis and then resends the resulting classical outcome as the equivalent photon prepared in the $\mathbb{Z}$-Basis. We impose that Bob must always send the quantum state equivalent to the observed classical state (i.e., $|0\rangle$ or $|1\rangle$).
4. *Reflect*:
    - Bob simply reflects back the incoming photon to Alice, letting its quantum state undisturbed, with the help of Mirrors. This operation is equivalent to purely disconnecting from the quantum communication medium and forwarding everything back to Alice. Since Bob does not measure the incoming photon, he does not learn anything about its quantum state. Thus, Alice should get the photon in the same quantum state she sends initially to Bob, when he uses this operation.
5. *Permute*:
    - Bob reorders the photons received (or a subset of that photons) without disturbing them. Once again, Bob does not learn anything about the respective quantum states of those photons, permuting only their order. In particular, Bob can achieve this operation with the aid of Optical Elements such as Delay Lines.

Some advantages of such protocols are their low-cost and accessibility since most of the Quantum Resources in the state-of-the-art are still expensive and not globally accessible.

3.4.1 BGKM07 and BGKM09 Protocols

The most known SQKDs are the BKM07 [387] and BGKM09 [388] protocols, the earlier proposed by Michel Boyer, Dan Kenigsberg, and Tal Mor in 2007, while the latter was proposed by the same authors jointly working with Ran Gelles in 2009. The first protocol is an MR-SQKD (Measure-Resend SQKD), while the second is an RB-SQKD (Randomization-Based SQKD).

In the BKM07 protocol, Alice starts by preparing a photon with the same configuration as the BB84 protocol (see 3.3.1.1). More specifically, for each round of the protocol, she prepares a single-photon in a randomly chosen spin orientation, such as horizontal ($\leftrightarrow$), diagonal ($\swarrow\!\!\nearrow$), vertical ($\updownarrow$) or anti-diagonal ($\nwarrow\!\!\searrow$) spins, corresponding to 0°, 45°, 90° and 135° polarizations, respectively. In Table 3.1, we show all the possible configurations of quantum states for each photon in this protocol. For the incoming photons, Bob will randomly choose between the Measure-and-Resend and Reflect operations. Then, Alice will measure the returning photon on the same basis she initially used to prepare it ($\mathbb{Z}$-Basis or $\mathbb{X}$-Basis). After the quantum transmission of states, Alice reveals to Bob the basis she used to prepare the photons sent in each round, while Bob reveals the operation he used for each round. As expected, Alice keeps her quantum states initially generated in secret, while Bob also keeps in private the classical bits obtained from the rounds he has chosen to measure the incoming photon. Finally, they use the rounds where she chose to send a photon prepared in the $\mathbb{Z}$-Basis and he chose the Measure-and-Resend operation to build their raw key. In the Measure-and-Resend operation, Bob also uses the $\mathbb{Z}$-Basis, and they should expect the resulting secret bits to be completely correlated if Alice prepared the respective photon in the $\mathbb{Z}$-Basis. These rounds are used to build their initial sifted keys, which are not error-free. For the rounds on which Alice prepared the photons on the $\mathbb{X}$-Basis and Bob chosen the Measure-and-Resend operation, Bob should expect a uniform distribution for the resulting observed classical outcomes (i.e., $|0\rangle$ in 50% of times and $|1\rangle$ in 50% of times). For the remaining rounds on which Bob has chosen the Reflect operation, Alice performs a first Parameter Estimation, estimating the QBERs on the quantum communication medium. These QBERs are based on her possible choices of bases to prepare photons (i.e., $\mathbb{Z}$-Basis and $\mathbb{X}$-Basis). Then, Alice and Bob also choose a random sample of bits from their sifted keys, on which they perform a second Parameter Estimation. For both groups of bits used in the two Parameter Estimations, if at least one of the estimated QBERs is above some predefined maximal upper bound, they should abort the protocol. Otherwise, Alice and Bob should discard these two groups of bits, and they should expect to have completely correlated bits on their shortened sifted key. The protocol should also include the standard steps of Information Reconciliation and Privacy Amplification to correct some remaining errors in the sifted keys and enhance the security of the reconciled key, respectively. Finally, from these last two steps, Alice and Bob should agree on the resulting final secret symmetric key.

Differently, in the BGKM09 protocol, Bob uses the Permute operation as opposed to the Measure-and-Resend operation. In this protocol, Alice starts again by preparing a photon with the same configuration as the BKM07 protocol. In each round of the protocol, she prepares a single-photon in a random spin orientation, such as horizontal ($\leftrightarrow$), diagonal ($\swarrow\!\!\nearrow$), vertical ($\updownarrow$) or anti-diagonal ($\nwarrow\!\!\searrow$) spins, corresponding again to 0°, 45°, 90° and 135° polarizations, respectively. Then, for the incoming photons, Bob will randomly choose between the Measure and Reflect operations. For the rounds in which Bob has chosen the Reflect operation, he also performs the Permute operation before returning back the photons to Alice. In particular, Bob does not perform any measurement on the photons nor disturb them in this operation. However, he reorders them before resending them back to Alice. Oppositely, Bob does not

resend back the photons in the round on which he has chosen the Measure operation. Then, Alice stores all the returning photons from Bob in a Quantum Memory until the end of the quantum transmission of states. After the quantum transmission of states ends, Bob publicly announces the photons of the rounds on which he had chosen the Reflect operation and the order he reflected them back to Alice from the Permute operation. Then, Alice undoes the random order of those photons on which Bob used the Permute operation, measuring them on the same basis she used to prepare them initially. Afterward, Alice publicly announces to Bob the rounds on which she prepared the photons in the $\mathbb{Z}$-Basis. If Bob had chosen the Measure operation in those rounds, he and Alice should have correlated secret bits to compose their sifted key. However, since Eve may have eavesdropped on some of those rounds at random, this sifted key can still contain some errors. On the rounds on which Bob had chosen the Reflect and Permute operations, Alice performs an initial Parameter Estimation. Furthermore, Alice and Bob also take a random sample of bits from their sifted keys to perform a further Parameter Estimation. If at least one of these estimated QBERs is higher than a predefined threshold, they should abort the protocol immediately. Otherwise, the bits from the rounds not used to compose their sifted key should be discarded, together with the bits composing the random sample from their sifted keys. Then, Alice and Bob should have a shorter sifted key, which is still not error-free. As usual, Alice and Bob should perform the Information Reconciliation step to correct the remaining errors of their shortened sifted key. Additionally, they can also perform the Privacy Amplification step, from which they agree on a final symmetric key.

In these protocols, we refer to the rounds on which Bob chooses the Measure-and-Resend (or just Measure) operation as SIFT rounds, while we refer to the rounds on which Bob takes the Reflect operation as CTRL rounds. Still, in these protocols, the bits chosen from the initial sifted key to perform a Parameter Estimation are often called TEST bits, while the remaining ones are called INFO bits. In the following Table 3.6, we describe these rounds (see ref. [388]):

Alice's Preparation Basis	Bob's Operation	Type of Round	Usage and Observations
$\mathbb{Z}$-Basis	Measure-and-Resend (or Measure)	SIFT	A pool for INFO and TEST bits from sifted keys
$\mathbb{X}$-Basis			Bob expects a uniform distribution
$\mathbb{Z}$-Basis	Reflect	CTRL	Alice expects that the bits resulting from the returning photons are unchanged
$\mathbb{X}$-Basis			Alice expects that the bits resulting from the returning photons are unchanged

Table 3.6: Bit usage in the BKM07 and BGKM09 protocols.

However, when developing the BGKM09 protocol, the authors discovered that this protocol is not robust. More specifically, right after the step of the two Parameter Estimations, Eve can count the number of 0s and 1s measured by Bob without being detected and get about 30%

of the INFO bits. In order to be sure that Eve cannot use statistics of occurrence of 0s and 1s, computing the Hamming Weight (see ref. [388]) of those bits, the authors propose the use of a binary string generated from a function, jointly with a new parameter given a priori. More specifically, Alice chooses a subset of bits from the shortened sifted key, with a precisely equal number of 0s and 1s, if it is possible. Otherwise, Alice and Bob should abort the protocol immediately. Then, Alice generates a binary string from the mentioned function and randomly chooses a substring from the subset of bits previously taken from the shortened sifted key such that these two binary strings match. After that, Alice publically announces to Bob the indices of her reduced sifted key, from which she has chosen the bits that match the previous requirement. Subsequently, they can finally perform the remaining steps of Information Reconciliation and Privacy Amplification to agree both on the final secret symmetric key with high probability.

Note that in these protocols, if Bob does not resend the measured photons, then he must permute the remaining ones. Otherwise, these protocols become susceptible to the so-called double CNOT attack [388]. Indeed, in this case, Eve can apply the equivalent of a CNOT gate to the qubits modeling all photons traveling in the forward direction with some ancilla qubits she prepared a priori. If Bob measures, but does not resend those photons, Eve will notice a vacuum, with no photon, leaving Bob's endpoint, in which case, a measurement of her ancilla qubit provides full information of the missing photon to her. If Bob reflects the photon, Eve can simply apply a CNOT gate in the reverse quantum communication medium, undoing the initial state of her action. In particular, Bob's operation is the identity operation in this type of round, and the CNOT gate is an involutory unitary operator. And therefore, if Eve applies two CNOT gates in the quantum communication medium, the first in the forward direction and the second in the reverse direction, she will avoid being detected. Therefore, any SQKD needs to have the classical entity to perform the Resend operation or the Permute operation.

3.4.2 Other variants of SQKDs

Since then, some scientists and researchers investigated many other variants of SQKDs over the years. These protocols gained interest attempts to reduce the requirements of quantum resources needed. From these research works, we learn to classify SQKDs as n-state SQKDs, where n is the number of states the quantum entity may choose to prepare. If $n = 1$, we call the protocol a single-state SQKD, while otherwise, we call the protocol a multi-state SQKD, when $n > 1$. For example, the BKM07 and BGKM09 protocols are considered four-state SQKDs.

One of these variants is the Single-State SQKD, proposed by Xiangflu Zou, Daowen Qiu, Lvzhou Li, Wu Lihua, and Lvjun Li in 2009 [389]. In this protocol, Alice prepares a single-photon always in the state $|+\rangle$ and sends it to Bob via a forward quantum communication medium. Then, for the incoming photon, Bob chooses randomly between the Measure-and-Resend and Reflect operations, recording his choice. If Bob chooses the Measure-and-Resend operation, he also records the bit resulting from his measurement outcome, resending a photon prepared in a classical state (i.e., $|0\rangle$ and $|1\rangle$) equivalent to the observed outcome. For the returning photons on the reverse quantum communication medium, Alice measures them randomly in

the $\mathbb{Z}$-Basis or $\mathbb{X}$-Basis. Afterward, Alice and Bob publicly disclose their choices. If Bob has chosen the Measure-and-Resend operation and Alice has chosen to measure the photon in the $\mathbb{Z}$-Basis, they should share a correlated bit that can be used to build their raw key. If Bob has chosen the Reflect operation and if Alice has chosen to measure the photon in the $\mathbb{X}$-Basis, she should observe the quantum state $|+\rangle$. In these rounds of the protocol, Alice might get a uniform distribution of their measured outcomes. Therefore, if Alice observes something different from that expected distribution, she can consider that as a potential eavesdropping attempt from Eve, and Alice and Bob should abort the protocol in that case. In their work, the authors also proposed other variants of SQKDs using two and three quantum states.

Another popular variant is the Reflection-Based SQKD proposed by Walter Krawec in 2014 [471]. Here, Alice and Bob must have access to private coin flips and internal registers for each round of the protocol. In particular, we denote the coin flip and internal register of Alice as c_A and $accept_A$, respectively. Similarly, Bob also has a coin flip and an internal register, which are denoted as c_B and $accept_B$, respectively. So, for each round, Alice prepares a single-photon in the quantum state $|+\rangle$ and sends it to Bob via the forward quantum communication medium. In each round of the protocol, Bob will flip his random coin c_B. If $c_B = 0$, Bob will choose the Reflect operation, and he sets $accept_B$ to true with 50% of probability, otherwise, he will set $accept_B$ to false. If $c_B = 1$, he will choose the Measure-and-Resend operation, setting $accept_B$ to true only if he measures the incoming photon and observes the bit equivalent to the quantum state $|0\rangle$. Otherwise, if the observes the bit equivalent to the quantum state $|1\rangle$, he should set $accept_B$ to false. As usual, when Bob chooses the Measure-and-Resend operation, he should also resend back a photon to Alice in the quantum state equivalent to the bit he obtained. Then, for each returning photon in the reverse quantum communication medium, Alice should randomly choose to measure it in the $\mathbb{Z}$-Basis and $\mathbb{X}$-Basis. If Alice chooses the $\mathbb{Z}$-Basis and observes the bit equivalent to the quantum state $|1\rangle$, she sets $c_A = 0$ and $accept_A$ to true. If she chooses the $\mathbb{X}$-Basis and observes the quantum state $|-\rangle$, she will set $c_A = 1$ and $accept_A$ to true. For all other remaining measurement outcome possibilities, she will set $accept_A$ to false, setting also c_A as 0 or 1, arbitrarily. After the quantum transmission of states ends, both Alice and Bob publicly announce to each other the values of their internal registers, $accept_A$ and $accept_B$ for each round. If both registers $accept_A$ and $accept_B$ are true in a specific round, they will keep the respective coin flips, c_A and c_B, to compose their sifted keys. Otherwise, Alice and Bob use this round of protocol for Parameter Estimation and discard it then. In the Parameter Estimation step, if one or both the registers have the value false for a specific round of the protocol, Bob should also publicly disclose to Alice the value of his coin flip c_B in that round. Additionally, for the cases of rounds of the protocol in which $c_B = 1$, Bob should also inform Alice of the resulting bit from his measurement outcome. If Bob has chosen the Reflect operation ($c_B = 0$) and Alice measured the photon of that respective round in the $\mathbb{X}$-Basis, she should have received the quantum state $|+\rangle$. In these rounds, Alice should expect a uniform distribution of 0s and 1s. Otherwise, they can suspect *a priori* a possible eavesdropping attempt from Eve and abort the protocol in the last case. If Bob has chosen the Measure-and-Resend operation ($c_B = 1$) and Alice measured the photon in the $\mathbb{Z}$-Basis,

she should have obtained the same bit resulting from the measurement performed by Bob. Therefore, if the number of errors, in this case, exceeds a predefined threshold, they should abort the protocol immediately. In the end, Alice and Bob should also perform the further well-known steps of Information Reconciliation and Privacy Amplification, in order to agree on a common error-free reconciled key and final secret symmetric key, respectively.

Over the years, many authors also presented other variants of SQKDs different from the ones presented here (see refs. [390–394] for more information about these protocols).

3.5 Quantum Conference Key Agreements (QCKAs)

However, it is reasonable to say that both QKDs and SQKDs are not suitable for multiparty scenarios, where we may pretend that more than two parties agree on a common symmetric key. We can make such an observation since QKDs and SQKDs are not scalable for more than two parties. In particular, by performing individual PM-QKDs, we need all the parties to agree on the same basis to extract usable rounds (i.e., rounds of the protocol they will use to build their sifted keys). For example, suppose a PM-QKD with M possible measurement bases between Alice and multiple $(p-1)$ Bobs. Note the number of usable rounds where all the $(p-1)$ Bobs chosen the same measurement basis, equivalent to the basis initially used by Alice to prepare the quantum state used in that round, is $P_M(p) = \frac{1}{M^{(p-1)}}$, which decreases exponentially with the number p of parties. We illustrate this observation in Figure 3.22:

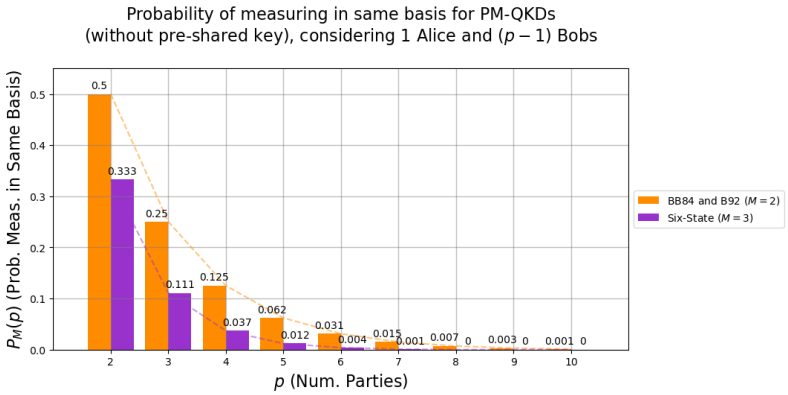


Figure 3.22: Probability of measuring in same basis for PM-QKDs (without pre-shared key), considering 1 Alice and $(p-1)$ Bobs.

On the other hand, EB-QKDs uses bipartite entangled states, such as Bell States (or EPR Pairs), not suitable for more than two parties. Following this approach with bipartite entangled photons for each pair composed by Alice and each one of the multiple Bobs will result in pairs of photons that are only correlated pairwise. It is easy to see that SQKDs are also not suitable for multiparty scenarios since they behave similar to BB84 Protocol due to its operations.

Nevertheless, we may consider other configurations of multipartite entangled states for these situations, such as the well-known GHZ States, W States, Cluster States, Graph States (see Sections 2.2.4.2 to 2.2.4.4), among many others. With such multipartite entanglements, the

multiple parties involved are able to achieve the same perfect correlation from the bipartite ones on the classical outcomes resulting from their measurements. And thus, as obvious, these different configurations end up being a solution more suitable for these multiparty scenarios. From this idea of using multipartite entangled states to achieve the secure establishment of a common secret symmetric key (here, also known as a conference key) among two or more parties, we gave rise to what is currently known as QCKAs [405] in the state-of-the-art.

Nevertheless, the use of multipartite entangled states is enough to ensure that the multiple parties successfully extract a conference key? What kind of further requirements should this family of new protocols have? Do these new protocols scale for any number of parties? These are all reasonable questions we may want to cover when we are developing such protocols...

3.5.1 How to extend Quantum Key Agreements for Multiparty Scenarios?

In fact, multipartite entangled states seem to be the key for not only key exchanges in quantum regimes but for multiparty Quantum Cryptography, in general. It is common to see protocols for Quantum Cryptocurrencies and Quantum Multiparty Computations, such as Quantum Blockchains, Quantum Byzantine Agreements, and Quantum Secret Sharing, using some of the multipartite entanglements mentioned before. As we can expect, the same approach can be used for Quantum Key Agreements for multiparty scenarios. But how we can do that?

The simple approach to developing a QCKA as an extension of QKD among several parties is not practical as it does not scale properly, as we already saw. In particular, we could also think about naturally using GHZ States as a possible generalization of the six most-known non-orthogonal quantum states from $\mathbb{Z}$-Basis, $\mathbb{X}$-Basis, $\mathbb{Y}$-Basis (i.e., $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, $|+i\rangle$, and $|-i\rangle$). However, if we let the parties choose randomly on different measurement bases, the probability of establishing a common secret bit will vanish exponentially for both cases (see Figure 3.22). Additionally, note also we always need to sacrifice a certain amount of rounds for the Parameter Estimation step in order to detect a possible eavesdropping attempt from Eve.

Alternatively, using pairwise instances of QKDs between Alice and each Bob to distribute initial pre-shared keys to be used by Alice to wrap a final conference key generated on the fly, to be shared among them, scales linearly with the number of participants. This approach requires the several pairwise steps of Information Reconciliation and Privacy Amplification to be much more accurate. On the other hand, it also increases the burden of Alice be constantly establishing several bipartite symmetric keys with Bobs to wrap the conference key and then distribute it to all of them using AES [109], OTP [100], or QOTP [440] encryptions. However, Alice and Bobs may use this initial exchanged conference key as a pre-shared key used as a parameter for the following conference key agreements between them. More specifically, they can use this same pre-shared key to choose jointly which type of operation they will perform in each round of the protocol. This pre-shared key must be refreshed at each execution of QCKA and can be compressed to a length of $\ell \cdot h(p_{PE})$ bits. Here, ℓ is the number of rounds of the protocol and p_{PE} is the probability of occurring a $\mathbb{X}^{\otimes p}$-measurement round (i.e., a round of the protocol on which all the parties choose the same measurement basis, without a pre-shared

key). For example, the compressed pre-shared key could be a small secret seed that could be expanded with a Hash Function, such as SHA-256, SHA-384, or SHA-512, in private.

Here, this short pre-shared key marks rounds that parties will use to build their raw key and the rounds used for the usual Parameter Estimation step. Essentially, following this direction, the scientific community took a fresh look at QCKA over the last few years, presenting several proposals of this kind. In particular, Dagmar Bruß, Frederico Grasselli, Hermann Kampermann, and Gláucia Murta presented a complete review survey of QCKAs in 2020 [405]. In this survey, the authors showed the current state-of-the-art for QCKAs and reinforced the need to use a short pre-shared key to overcome the natural limitation of all the parties agreeing on the same basis for each round. Therefore, according to this pre-shared key, there are two types of rounds:

- 1^{st} type: All the parties jointly measure the photons in the $\mathbb{Z}$-Basis.
  - This event happens with a probability of $1 - p_{PE}$.
  - These rounds of the protocol are marked with the bit 0 in the pre-shared key.
  - These rounds of the protocol are also called Key Generation rounds.
- 2^{nd} type: All the parties jointly measure the photons in one of the remaining bases.
  - This event happens with a probability of p_{PE}.
  - These rounds of the protocol are marked with the bit 1 in the pre-shared key.
  - These rounds of the protocol are also called Parameter Estimation rounds.

The first Multiparty N-QKDs and QCKAs proposed which are known dated between the 2000s and the 2010s [472–474]. However, these novel protocols just gained more popularity in the last couple of years with the recent scientific advances and developments in Quantum Communications and Quantum Networks for what might be the future Quantum Internet.

3.5.2 Multiparty N-Six-State Protocol (N-SSP)

The Multiparty N-SSP protocol [399] is one of the most recent and well-known QCKAs in the state-of-the-art. It was proposed by Dagmar Bruß, Michael Epping, Hermann Kampermann, and Chiara Macchiavello in 2017. The Multiparty N-SSP protocol starts with Alice preparing p photons in a GHZ State, keeping one to herself. Then, she distributes the remaining photons to Bobs, each photon to each one of $(p-1)$ Bobs, via a designated quantum communication medium. Afterward, all Bobs measure the incoming photons at their endpoints, while Alice also measures her photon in her endpoint. They will jointly measure the photons according to the bit of the pre-shared key corresponding to the current round. If the bit is 0, they all will measure their respective photons in the $\mathbb{Z}$-Basis, otherwise, if the bit is 1, they will jointly measure their respective photons randomly in the $\mathbb{X}$-Basis or $\mathbb{Y}$-Basis. After the distribution of all the l entangled states, Alice and Bobs perform the Parameter Estimation step to estimate the global and individual pairwise QBERs. First, Alice and Bobs announce to each other the bits resulting from the measurements performed on the 2^{nd} type rounds together with the

measurement bases chosen. Here, for each 2^{nd} type round, Alice flips her bit if the number of parties who measured in the $\mathbb{Y}$-Basis is not a multiple of four due to the cyclic pattern of the power of imaginary numbers. Still, in the 2^{nd} type rounds, if an even number of parties measured in $\mathbb{Y}$-Basis (including zero), Alice and Bobs calculate the QBER Q_X. Then, Alice also announces a randomly chosen sample of size $\ell \cdot p_{PE}$ from the 1^{st} type rounds, denoted as Test rounds, for which all Bobs should announce their obtained bits on them. From those bits, they compute the global QBER Q_Z and the individual pairwise QBERs Q_{AB_i}. After the step of Parameter Estimation, Alice flips a coin for each 1^{st} type round to decide if all Bobs should flip the respective bits corresponding to that $\mathbb{Z}^{\otimes p}$-measurement round, to implement effectively the depolarization channel $\mathbb{X}^{\otimes p}$ to prevent possible existing noise in the quantum communication medium. Finally, Alice and Bobs perform the Information Reconciliation step, on which Alice sends an Error Correction Code (for $\max_i Q_{AB_i}$) to all Bobs, which they apply to their sifted keys. Then, they also perform the Privacy Amplification to obtain the final common conference key by applying a Two-Universal Hash Function [459], randomly chosen by Alice.

Another well-known QCKA is the Multiparty N-BB84 Protocol [401], which extends the bipartite BB84 Protocol (see Section 3.3.1.1) for multiparty scenarios, using GHZ States (see Section 2.2.4.2). This Multiparty N-BB84 Protocol is similar to the Multiparty N-SSP Protocol, with the obvious main difference of using just measurements in the $\mathbb{Z}$-Basis and $\mathbb{X}$-Basis.

In these protocols, note that the initial raw key always ends up being shortened from ℓ bits to $\ell - 2 \cdot p_{PE} \cdot \ell$ bits. First, Alice and Bobs discard around $p_{PE} \cdot \ell$ rounds of 2^{nd} type to perform the Parameter Estimation step, which happens with probability p_{PE}. Then, Alice and Bobs also discard a sample of $p_{PE} \cdot \ell$ rounds of 1^{st} type to estimate QBER Q_Z. For this reason, we need to choose p_{PE}, verifying $0 < p_{PE} < 0.5$. Notice that if $p_{PE} = 0.5$, we may not be able to extract a sifted key after the Parameter Estimation step. The Figure 3.23 illustrate this observation:

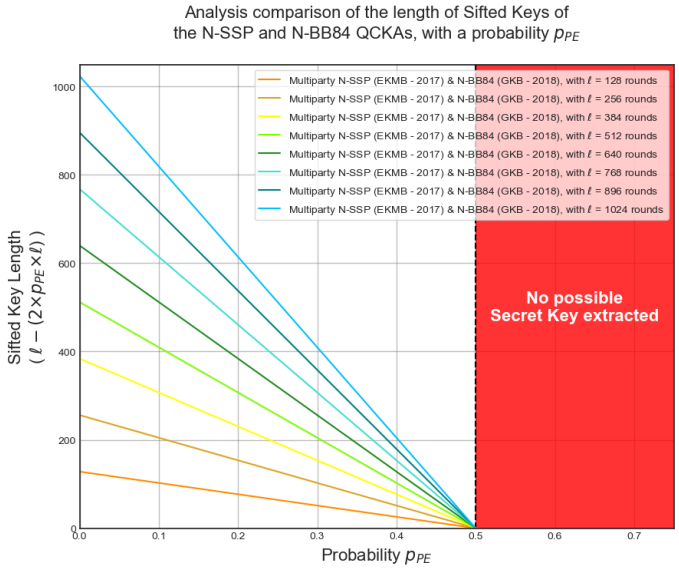


Figure 3.23: Analysis comparison of the length of Sifted Keys of the N-SSP and N-BB84 QCKAs, with a probability p_{PE}.

3.5.3 W State Protocol

In 2019, another interesting QCKA was jointly presented by Dagmar Bruß, Federico Grasselli, and Hermann Kampermann [403]. This protocol is an extension of the bipartite TF-QKD [470] for multiparty scenarios, and for certain configurations can be seen as a W State Protocol. In this protocol, Alice and all $(p-1)$ Bobs start by preparing an optical pulse E_i entangled with a single-photon e_i, having a configuration similar to an EPR Pair (see Section 2.2.4.1) with the form $|\phi\rangle_{E_i e_i} = \sqrt{q}|0\rangle_{E_i}|0\rangle_{e_i} + \sqrt{1-q}|1\rangle_{E_i}|1\rangle_{e_i}$, $\forall i \in \{1,2,...,p\}$, where $0 \leq q \leq 1$, $|0\rangle_{e_i}$ is the vacuum state, $|1\rangle_{e_i}$ is the single-photon state, and $\{|0\rangle_{E_i}, |1\rangle_{E_i}\}$. Then, Alice and Bobs send their optical pulses e_i to an untrusted central node via a lossy quantum communication medium, in a synchronized manner, keeping the photon to themselves. The central node then applies a Bell-Multiport Beam Splitter with m input and output ports to the incoming optical pulses and features a threshold detector D_j at each port, for $j = 1,2,...,m$, where $m \geq p$, for the measurement of those optical pulses. Afterward, the central node publicly announces to Alice and Bobs the bits b_i resulting from the measurements it performed for every detector D_j, with $b_i = 0$ and $b_i = 1$ corresponding to a no-click and click events on the associated detectors, respectively. A round of the protocol gets discarded if $\sum_{i=1}^{m} b_i \neq 1$ (i.e., whenever single-photon interference did not occur in the central node). The probability of only a detector D_j being clicked is given by p_j. In Figure 3.24, we give an illustration of the W State Protocol for $p = 3$ parties and in Table 3.7, we summarize all the possible number of clicks for detectors D_j:

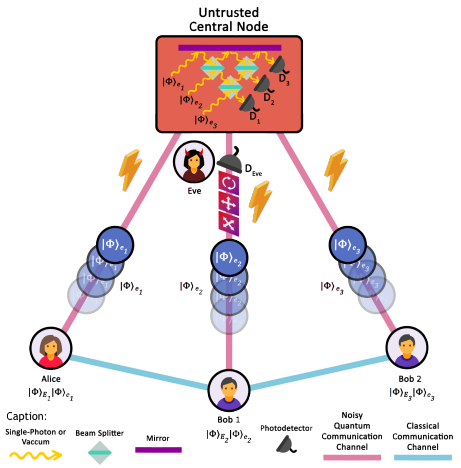


Figure 3.24: W State Protocol for $m = p = 3$.

m_3	m_2	m_1	$\sum_{i=1}^{m} b_i$
b_3	b_2	b_1	
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	2
1	0	0	1
1	0	1	2
1	1	0	2
1	1	1	3

Table 3.7: Possible number of clicks for the detectors D_j for $m = p = 3$.

Notice that when the round is valid, the quantum state resulting from the Bell-Multiport Beam Splitter will be equivalent to a W State (see the highlighted cells in Table 3.7 and see Section 2.2.4.3). In that case, and according to the bit of the pre-shared key corresponding to the current round of the protocol, Alice and Bob will consider that round as a Key Generation round or a Parameter Estimation round. If it is the first case, Alice and Bobs will measure their local photons on the basis of the operator $O_{XY}(\theta_i) = \cos(\theta_i)X + \sin(\theta_i)Y$, with $\theta_i = arg(U_{ij})$ for that Key Generation round, where $U_{ij} = \frac{1}{\sqrt{m}} e^{i\frac{2\pi}{m}(i-1)(j-1)}$. Here, X and Y are the Pauli operators (see Section 2.2.3.1). Namely, Alice and Bobs obtain the bits on the Key Generation

rounds by measuring their local photon in a specific direction in the XY plane of the Bloch Sphere (see Section 2.2.2) modeling that photon. The direction is the one that minimizes the bipartite QBER and depends on which detector D_j has a single-photon click. If it is the second case, Alice and Bobs will measure their local single-photons in the $\mathbb{Z}$-Basis for that Parameter Estimation round. There are on average $k_{PE} = m \cdot p_j \cdot \ell \cdot p_{PE}$ Parameter Estimation rounds which are not discarded, while are on average $k_{KG} = m \cdot p_j \cdot \ell \cdot (1 - p_{PE})$ Key Generation rounds which are not discarded. Note the number of rounds not discarded also depends on the probability of occurring a single-photon interference due to the click event on a single detector (i.e., $m \cdot p_j$). After the transmission of quantum states, Alice and Bobs should have a raw key with $m \cdot p_j \cdot \ell$ bits. They should publicly announce to each other the bits resulting from their measurements in the valid Parameter Estimation rounds, on which they will compute the QBER Q_z. Additionally, from the Key Generation rounds, Alice and Bobs will randomly choose a sample of the resulting bits with the size $m \cdot p_j \cdot \ell \cdot p_{PE}$ to estimate the pairwise bipartite QBERs $Q_{p_1 p_r}$, with $2 \leq r \leq p$. Then, their sifted keys result from the remaining $m \cdot p_j \cdot \ell - 2 \cdot k_{KG}$ bits from the initial raw key, considering only the Key Generation rounds. After that, Alice and Bobs perform the Information Reconciliation step, on which Alice sends an Error Correction Code to all Bobs, to allow them to match her sifted key. Finally, they can also perform the Privacy Amplification step to obtain the final conference key by applying a Two-Universal Hash Function [459].

Other recent QCKAs may include protocols with single particles [395], dynamic groups [402], multipartite entanglements [396, 397, 404], photon loss [406], or phase-matching [475].

3.6 Attacks on Quantum Cryptography

There are several attacks on Quantum Cryptography existing on the current state-of-the-art. However, most of these attacks exploit aspects and issues of their physical implementation on real devices rather than the design of the protocols themselves. Some of these attacks are extensively described in refs. [447, 464]. Recall the Quantum Cryptography offer us the promise of unconditional security, when we are dealing with ideal real and physical implementations.

3.6.1 Intercept-and-Resend (IR) Attack

The simplest type of attack strategy for an eavesdropper is the IR (Intercept-and-Resend) Attack [447]. In this attack, the eavesdropper simply measures the traveling qubit in the quantum communication medium with a measurement basis of its choice and resends replacement qubits in the state equivalent to the classical outcome found. As the eavesdropper does not know which basis was used by the sender to prepare the qubit, it can only guess the measurement basis in the same way as the sender does. Usually, the eavesdropper randomly chooses these measurement bases according to the same possible choices the receiver has. If the eavesdropper takes the measurement basis correctly, it also measures the qubit with the correct basis that the sender used to prepare it and resends a new qubit in the correct quantum state to the receiver. However, if it chooses the measurement basis incorrectly, the quantum

state the eavesdropper measures is random. Here, the quantum state of the qubit sent to the receiver by the eavesdropper could not be the same as the one initially sent by the receiver. If the receiver then measures this quantum state on the same measurement basis as the receiver chose before sending the respective qubit, the receiver will get a random classical outcome. In other words, as the eavesdropper sent a quantum state on the opposite orthogonal basis to the receiver, it will result in an erroneous result with a chance of 50%. Basically, in half of these situations, the sender and receiver will have incorrect classical outcomes instead of the correct classical outcome that the receiver would get without the presence of an eavesdropper. For example, for the BB84, B92, and Six-State protocols (see Sections 3.3.1.1 and 3.3.1.2), the eavesdropper will introduce errors of 25%, 12.5%, and 33.3%, respectively, for each qubit.

3.6.2 Denial-of-Service (DoS) Attack

Since the quantum cryptographic protocols require quantum communication mediums, such as dedicated fiber optical links or line-of-sight free-space links between the legitimate parties involved, an eavesdropper can perform DoS (Denial-of-Service) Attacks [476]. These attacks can be mounted by simply cutting or blocking one of the links of quantum communication mediums used during the execution of these protocols. This attack is one of the greatest motivations for the development of QKD networks, as well as sufficiently large metropolitan Quantum Communication Networks in general (or, ultimately, the Quantum Internet), which would manage the routing of the quantum communications via other alternate links.

Another possible way for an eavesdropper to perform such an attack is by continuously performing IR Attacks (see Section 3.6.1) on purpose to be detected and forcing the protocol to abort immediately. If the eavesdropper does this attack several times in a row, it will not allow a successful exchange of secret keys. Here, the legitimate parties need to find which quantum communication mediums are being intercepted and replace them with alternative ones, similar to what happens in conventional Classical Communication Networks.

However, note this attack strategy does not compromise the security strength of the secret key in any form, despite not allowing the successful complete execution of the protocol.

3.6.3 Attacks for Discrete-Variables (DV) Protocols

As mentioned previously, most quantum cryptographic protocols should, in ideal conditions, encode quantum states in single-photons (i.e., discrete variables). However, they do it in attenuated light pulses due to the practical limitations of physical implementations existing in the current state-of-the-art. In this case, some inefficiency and issues of the respective practical implementations can allow an attacker to exploit some resulting weaknesses.

3.6.3.1 Faked-States Attack and Detector Efficiency Mismatches (DEMs)

We can see the Faked-States Attack [438, 447, 477, 478] on quantum cryptographic protocols as a variant of an IR Attack (see section 3.6.1). In this attack, an eavesdropper does not try to

reconstruct the original quantum states but generates instead light pulses that get detected by the legitimate parties in a way controlled by itself while not setting off alarms. We know that an IR Attack which considers single-photons ends mostly by failing if an eavesdropper tries to regenerate the quantum states as close to the original as possible after detection. However, an eavesdropper may sometimes fool the legitimate parties when they use imperfections of their quantum hardware into thinking they are detecting original quantum states, while they are, in fact, detecting light pulses generated by the eavesdropper. Namely, these light pulses are called Faked-States, and we call these attacks of Faked-States Attacks, which are specifically designed to each cryptographic scheme or even a particular sample of quantum hardware equipment.

When this attack is successful, it provides the eavesdropper with complete knowledge about the secret key. On the other hand, when this attack is partially successful, it gives the eavesdropper partial insight into the final secret key. We can direct these attacks at PM-QKDs and EB-QKDs, targeting the optical equipment at the receiver's endpoint, namely when it uses both active and passive choice of measurement bases. These attacks mainly point to DEMs (Detector Efficiency Mismatches) [438, 439, 478–490], taking advantage of inaccuracies at the Photodetectors used. Several characteristics of the incident light pulses can exploit these inaccuracies, such as their intensity, phase shift modulation, reflection, polarization, and frequency. Some Faked-States Attacks may include Backflash [491–493], Time-Shift [439, 464, 480, 481], or Detector Blinding [478, 485, 486, 494–497] Attacks (see Sections 3.6.3.3 to 3.6.3.5).

3.6.3.2 Photon Number Splitting (PNS) Attack

The PNS Attack [435, 436, 447, 464, 498] targets the possible real-world optical implementations of QKDs that use individual photons as quantum information carriers. For example, the BB84 Protocol is theoretically perfectly secure when considering laser sources that emit a single-photon encoding a qubit in four possible polarization degrees of freedom of individual photons for each round of the protocol. However, it may happen that, in most of the physical implementations in the current state-of-the-art, the laser source sometimes accidentally emits two or more photons at once, which then carry the same polarization. More specifically, the quantum states emitted by this laser source will have the configuration $|0\rangle^{\otimes n}$, $|+\rangle^{\otimes n}$, $|1\rangle^{\otimes n}$, or $|-\rangle^{\otimes n}$, where n is the number of photons emitted in a specific round of the protocol.

First, note that one single-photon carries no information about the choice of the basis used to prepare it. Indeed, for either the choice of the basis used in the BB84 protocol (i.e., $\mathbb{Z}$-Basis or $\mathbb{X}$-Basis), the density operator describing the photon is maximally mixed, namely:

- $\frac{1}{2}(|0\rangle\langle 0|) + \frac{1}{2}(|1\rangle\langle 1|) = \frac{1}{2}(|+\rangle\langle +|) + \frac{1}{2}(|-\rangle\langle -|) = \frac{1}{2}\sigma_I = \frac{1}{2}I$,
  where $\sigma_I = I$ is the Pauli-I operator.

However, it is no longer the case for a pulse of light comprising n photons, namely:

- $\frac{1}{2}(|0\rangle\langle 0|)^{\otimes n} + \frac{1}{2}(|1\rangle\langle 1|)^{\otimes n} \neq \frac{1}{2}(|+\rangle\langle +|)^{\otimes n} + \frac{1}{2}(|-\rangle\langle -|)^{\otimes n} \neq \frac{1}{2}{\sigma_I}^{\otimes n} = \frac{1}{2}I^{\otimes n}$,
  where $\sigma_I = I$ is the Pauli-I operator.

Therefore, if the laser source accidentally emits more than one photon equally polarized instead of just one, it reveals information about the basis used by the sender to prepare them, what should not happen. For this reason, it is not surprising an eavesdropper can exploit that such n-photon pulses to attack the protocol. More specifically, the eavesdropper, who intercepts the quantum communication medium, may split the n-photon pulse into two groups, keeping $(n-1)$ photons to itself and sending the remaining one to the receiver. Then, the receiver receives the photons exactly according to the theoretical description of the protocol without noticing the mentioned interception. Meanwhile, the eavesdropper may measure the photons captured during the Quantum Transmission stage. In principle, if the eavesdropper has access to a quantum memory, it could even wait to choose its measurement choices until the sender and the receiver publicly exchange the bases they used for each round of the protocol. This imperfection in a real-world practical implementation may totally compromise the security of the protocol. In the worst case, the eavesdropper can get full information about the polarizations used to prepare each one of the supposed single-photons.

3.6.3.3 Backflash Attack

Another different type of attack, considering imperfections on the hardware used in real-world practical implementations, is the Backflash Attack [447, 491–493]. Some photodetectors based on Avalanche Photodiodes sometimes emit or reflect light (referred to as backflash light) upon detecting a light pulse. This backflash light can give information to an eavesdropper about the classical outcomes that the receiver got in several ways. The polarization of the backflash light can provide an insight into which components at the receiver's endpoint it has passed through. This imperfection could tell the eavesdropper which photodetector originated the backflash light. Alternatively, the time of traveling of the photons of the backflash light after entering the receiver's photodetector, or the path-dependent alterations to the profile of the outgoing backflash light, can also give this information to the eavesdropper. This imperfection could tell which measurement basis was chosen by the receiver to the eavesdropper. While for some setups of photodetectors, it could even reveal the classical outcomes got by the receiver.

3.6.3.4 Time-Shift Attack

The Time-Shift Attack [439, 464, 480, 481] exploits the imperfections on the hardware at the receiver's endpoint, namely through inaccuracies on the Photodetectors. More specifically, in order to avoid dark counts[2], we commonly install Photodetectors in such a way that they only count photons that arrive within a small time window around the time we expect a light pulse to reach the receiver's endpoint. Usually, the device system at the receiver's endpoint consists of more than one Photodetector (e.g., one for each possible polarization). However, the problem with this approach is that most times, the time windows of the different Photodetectors used are not perfectly synchronized. This inaccuracy means that there may be times that the receiver is more sensitive to light pulses regarding one polarization configuration

[2]The dark count is the registered counts without any incident light pulse on the considered Photodetector.

than others. Here, the eavesdropper may delay the respective light pulses traveling in the quantum communication medium. By doing that, the eavesdropper can bias the detected light pulses towards one or the other polarization and thus gain information about what measurement choices the receiver made. Despite this information may be partial, it can, together with the Error Correction Information in the posterior Classical Post-Processing stage that can be available to an Eavesdropper, be sufficient to infer the final symmetric secret key.

3.6.3.5 Detector Blinding Attack

Another attack that aims towards the receiver's endpoint is the Detector Blinding Attack [447, 464, 478, 485, 486, 494–497]. In this attack, the eavesdropper tries to gain control over the existing Photodetectors by illuminating them with brighter light pulses. In particular, when we consider a theoretical perfect implementation, the quantum cryptographic protocols use the encoding of information into the polarization of single-photons. In this case, we usually should configure the photodetectors in such a way that they can optimally detect light pulses containing individual single-photons. In particular, they should "click" whenever the incoming light pulse consists of a photon, and "not click" if the light pulse is empty (i.e., is nothing more than a vacuum). However, the behavior of such photodetectors may be different in scenarios where the incoming light pulses contain many photons. For example, when we expose these photodetectors to bright light pulses with a particular intensity, they may "click". On the other hand, they may never "click" for another intensity of light pulses. An eavesdropper may control immediately the "clicks" of the photodetectors existing at the receiver's endpoint. Here, the eavesdropper can send light pulses with appropriately chosen polarizations and intensities to such photodetectors. In order to exploit this inaccuracy for an attack, an eavesdropper may mimic the receiver's actions by intercepting the photons sent from the sender and measuring them on a randomly chosen basis, as the receiver would do. Basically, the eavesdropper can send bright light pulses to the photodetectors at the receiver's endpoint to ensure that the receiver obtains the same "clicks" of the photodetectors at the receiver's endpoint as if the receiver had directly obtained the photons from the sender's endpoint. This attack works particularly well for practical implementations that use a passive choice of measurement basis. For these scenarios, the measurement basis chosen by the receiver is not provided as an input parameter but by the photodetectors themselves. In this case, an eavesdropper can essentially remotely control the receiver's endpoint and thus, get hold of the entire final secret key.

3.6.3.6 Phase-Remapping Attack

In some real-world optical practical implementations of quantum cryptographic protocols (e.g., plug-and-play [499] and circular systems [500]), the sender does not have a laser source that emits single-photons. But instead, it encodes information by modulating an incoming light pulse from the receiver before resending it back to the sender again. Therefore, the light pulse travels twice in opposite directions through the same optical links, which helps to reduce possible fluctuations because of birefringence and noise present in the environment

of the quantum communication medium of that optical link. However, the two-fold use of the possibly insecure quantum communication medium opens additional opportunities for attacks that an eavesdropper can exploit. An example of an attack directly aimed at real-world implementations in the state-of-the-art is the Phase-Remapping Attack [464, 501, 502].

The Phase-Remapping Attack exploits the fact that the modulator used by the sender to encode information into the light pulses coming from the receiver's actions on that light pulse during a particular time interval. In this specific attack, the eavesdropper slightly advances or delays the light pulses in its direction from the receiver to the sender in a way that no longer lies entirely within that time interval. The modulation performed by the sender will then be incomplete, which means that the encoding of the information in the light pulse differs from what the protocol predicted before the hand. Afterward, the eavesdropper can exploit the incomplete phase shift modulation of the light pulses returning back from the sender's endpoint to the receiver's endpoint through an IR Attack (see Section 3.6.1).

3.6.3.7 Trojan-Horse Attack (THA) for Discrete-Variables (DVs)

Another possible attack for quantum cryptographic protocols with DVs (Discrete Variables) is the THAs (Trojan-Horse Attacks) [489, 503–508]. In this attack, the idea is to send a bright laser light pulse via the optical link into a component at the endpoint of one of the legitimate parties to extract information about its internal settings. Depending on the hardware they are using, measuring the reflection of the light pulse can allow the eavesdropper, for instance, to determine the choices made by the sender and the receiver, to prepare and measure the photons, respectively. For example, an eavesdropper may consider using large light pulses of photons to gain information about these choices of bases. This eavesdropper can get this information by sending a light pulse into the trusted devices via the quantum communication medium and performing measurements on its back-reflection, analyzing the resulting samples.

Consider the case on which the sender encodes its photon to send through a Phase-Shifter. Additionally, suppose an eavesdropper can also pass its own light pulse through that phase modulator and measure the resulting light pulse. Then, it may also get some information about the quantum state of the sender's photon. This inaccuracy happens because the phase modulator on the sender's endpoint operates for a finite amount of time. In a correct practical setup, this phase modulator should only be operational for exactly long enough to modulate the quantum state of the outgoing photon. Therefore, this imperfection may open a time window in which an eavesdropper can send a light pulse through the phase modulator, to be modulated similarly to the photon leaving the sender's endpoint. Here, the information that the eavesdropper obtains, in this case, can be partial, giving only the basis used by the sender, or may even directly give the secret bit. Even in the case that the eavesdropper only obtains the bases used to prepare the photons for each round of the protocol, the security of the same is still compromised. In particular, the eavesdropper can now always choose the measurement bases equivalent to the bases used by the sender to prepare the photons. Then, if the eavesdropper performs an IR Attack (see Section 3.6.1) on that outgoing photon, it can

gain full information about the symmetric secret key without introducing errors on the same.

Alternatively, an eavesdropper may be able to target these THAs to the Photodetectors at the receiver's endpoint. Considering the B92 or SARG04 protocols (see section 3.3.1.2), it is sufficient for the eavesdropper to know the measurement bases chosen by the receiver to gain complete information about the secret key. In the BB84 protocol (see section 3.3.1.1), if the eavesdropper can discover the measurement basis that the receiver will use before the light pulse arrives at the receiver's endpoint, it can carry out an undetectable IR Attack by choosing the same measurement basis as the receiver. Even if the eavesdropper only gains information about the measurement basis chosen by the receiver after the light pulse is measured, this vulnerability can help it with a practical PNS Attack since it reduces the need for quantum memory. Namely, the eavesdropper can measure the photons it receives immediately, rather than wait after all the Classical Post-Processing stage ends. This vulnerability does not help too much an eavesdropper who is limited only by the laws of physics, but it could help one who is using the currently available technology which does not meet the ideal conditions yet.

3.7 Security Notions for Quantum Cryptography

Additionally, there are some security notions we should consider when we are developing a quantum cryptographic protocol. These notions are more directed toward protocols for the exchange of keys. However, we can easily extend them to other types of quantum cryptographic protocols. We will briefly describe the most important ones in the following paragraphs.

3.7.1 Security Definitions

In order to prove the security of a quantum cryptographic protocol designed to exchange keys, we should always demonstrate some security definitions (see refs. [405, 461, 464, 509, 510]).

3.7.1.1 Soundness

A protocol is *sound* and ε_s*-correct-and-secret* if, it is both, ε_{corr}*-correct* and ε_{sec}*-secret*.

Definition 3.7.1.1.1 (Correctness):
A protocol is *correct* and ε_{corr}*-correct* if, $p(K_A = K_{B_1} = ... = K_{B_{(N-1)}}) \geq (1 - \varepsilon_{corr})$, where $p(K_A = K_{B_1} = ... = K_{B_{(N-1)}})$ is the probability for all the keys $K_A, K_{B_1}, ..., K_{B_{(N-1)}}$ be *identical*.

Definition 3.7.1.1.2 (Secrecy):
A protocol is *secret* and ε_{sec}*-secret* if, for an event Ω where the protocol does *not* abort, is verified that, $p(\Omega)\frac{1}{2}||\rho_{K_AE|\Omega} - \tau_{K_A} \otimes \rho_{E|\Omega}|| \leq \varepsilon_{sec}$, where $p(\Omega)$ is the probability of Ω, $\rho_{K_AE|\Omega}$ is the state shared by Alice and Eve, given Ω, $\tau_{K_A} = \frac{1}{|S|}\sum_{s_i \in S} |s_i\rangle\langle s_i|$ is the maximally mixed state over all possible values for key K_A, and $S = \{0,1\}^{\times \ell}$, where ℓ is the length of the key K_A.

3.7.1.2 Completeness

A protocol is *complete* and ε_c*-complete*, if has a *honest* implementation, i.e., $p(\Omega) \geq (1 - \varepsilon_c)$.

3.7.2 Security Model

As a standard which can be adopted to design an acceptable security model, the security of quantum cryptographic protocols usually relies on the following enumerated assumptions:

1. All quantum devices used by Alice and Bob(s), and quantum communication channel(s) connecting them, are correctly and completely described by Quantum Mechanics.

2. The classical communication channel(s) that Alice and Bob(s) use to exchange classical messages are authenticated, i.e., Eve cannot modify those messages or insert new ones.

3. The quantum devices that Alice and Bob(s) use locally to execute the steps of the quantum cryptographic protocol, such as preparing and measuring quantum physical systems, should do exactly the same that they are instructed to do a priori.

Other well-known assumptions that we can consider for a security model of a quantum cryptographic protocol is the i.i.d. (identical and independently distributed) assumption regarding the attack strategy of Eve or even her access to quantum computational devices.

The description of these security models are available in refs. [405, 443, 460, 498, 511–515].

3.7.3 Collective Attacks

In Collective Attacks, we consider the security model under the previously mentioned i.i.d. assumption on Eve's side. This assumption demands that a sequence of i.i.d. maps describe the quantum communication channel(s) connecting Alice and Bob(s). In physical terms, it means that Eve's intercept strategy is such that each signal sent from Alice to Bob(s) is always modified in the same exact way and independently of the other remaining light pulses.

Basically, Eve performs the same attack for each round of the protocol, by attaching independent quantum probes to each light pulse or even entangling it to another one she prepared initially a priori. In this case, we assume Eve has access to a quantum memory, allowing her to store quantum information from every round on her side. Since she can keep her quantum probes in a quantum memory, she can perform a global operation on the quantum information on her side at the end of the execution of the protocol, from which she can measure those several quantum probes coherently and collectively for her own benefit.

3.7.4 Individual (Incoherent) Attacks

The Individual (Incoherent) Attacks are a more restricted version of Collective Attacks, in a sense that, Eve has no access to a quantum memory, and she can only store classical data. In this security model, the best attack strategy for Eve is to perform a measurement on the quantum information on her side at each round that she gained from each light pulse sent from Alice to Bob(s) or even entangling it to another one she prepared initially a priori. Oppositely to Collective Attacks, Eve cannot perform an attack correlated to previous rounds or a global operation at the end of the protocol. Usually, it is difficult to argue why we should restrict Eve in that way, and we consider the corresponding security guarantee from this model as weak.

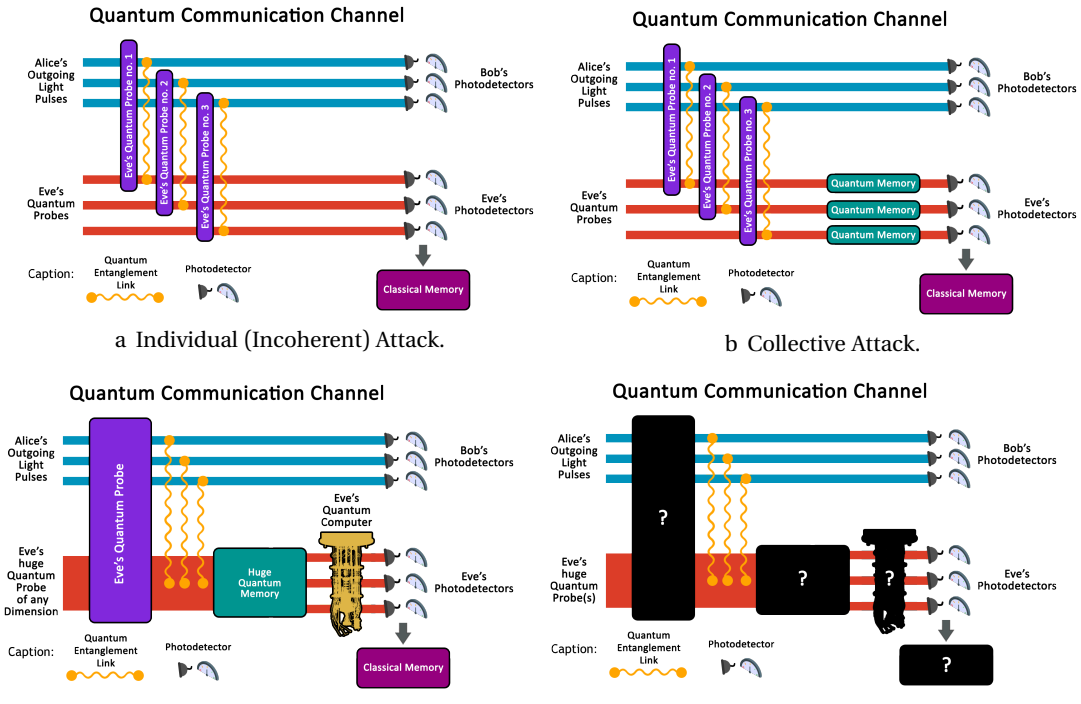
3.7.5 Coherent Attacks

The Coherent Attacks are another more general version of Collective Attacks, where Eve has access to a Quantum Computer and a quantum memory of huge capacity capable of storing quantum information of a physical quantum system of any dimension of Hilbert Space. Here, Eve can treat the entire quantum transmission as one quantum physical system, which she can also entangle with a large quantum probe that she can keep in her quantum memory. For this reason, Eve can apply any quantum operation and obtain arbitrary correlations with previous and future rounds of the execution of the quantum cryptographic protocol.

3.7.6 Joint Attacks

Finally, the Joint Attacks are the most general attacks to consider against a security model. In particular, we make no assumptions about Eve's capabilities in these attacks. More specifically, we do not impose any limitations on her resources to process and store quantum information. Additionally, the quantum communication channel connecting the quantum devices of Alice and Bob(s) can be arbitrary and may even be entirely in control of Eve. Basically, we can say that Eve is limited only by the laws of Physics and Quantum Mechanics in these attacks.

Since the Joint Attacks are the most general ones and Eve has several degrees of freedom in her actions, it is extremely difficult and challenging to perform an exhaustive analysis of it and prove the security properties of any quantum cryptographic protocol against these attacks.



a Individual (Incoherent) Attack.

b Collective Attack.

c Coherent Attack.

d Joint Attack.

Figure 3.25: Examples of Attacks for Security Models in Quantum Cryptography.

Chapter 4

Semi-Quantum Conference Key Agreements (SQCKAs)

At this point, we learned how the cryptographic protocols using the properties of Quantum Mechanics work. We also understood the possible different perspectives and points of view they offer. In this context, we can highlight the fully-quantum and semi-quantum contexts, by mention the advantages of the latter one. Or point out the differences between bipartite and multipartite scenarios, not forgetting the use cases where the second is more suitable.

But here, one important argument we can reason about is: "Can we have the best of those two worlds?" More specifically, can we design and develop quantum cryptographic protocols that consider semi-quantum contexts taking into account their inherent advantages, making them also scalable for multipartite scenarios? These questions will also be of great importance for the future Quantum Internet, with its use cases and applications. In this chapter, we focus on answering these questions, which also results in the main work of this Master's Thesis: "A Cryptographic Protocol of Key Agreement for Multiple Parties, in Semi-Quantum Contexts".

4.1 Work Proposal

In this Master Thesis, we propose a protocol that follows the idea of the combination of both SQKDs and QCKAs as the development of a multiparty QKD for semi-quantum contexts. We can refer to these protocols as SQCKAs (Semi-Quantum Conference Key Agreements) or even as MSQKDs (Multiparty Semi-Quantum Key Distributions). To the best of our knowledge, this proposal differs from others presented in the literature [516–519]. In fact, our protocol is directed to semi-quantum contexts and uses multipartite entanglements instead of multiple bipartite QKDs (see Section 3.5 and ref. [405]). On the other hand, our proposal does not

require a trusted third-party (e.g., a trusted quantum server), as happens in the protocol of ref. [518]. We give this role directly to one of the parties of the protocol and make all the parties use a compressible pre-shared key, which also works as an authentication factor to participate in our protocol. Note that a party needs this pre-shared key to choose the correct operation together with the other parties in every round of the protocol. Otherwise, it will lead to not correlated operations, introducing noise during the execution of the protocol. In the end, if an eavesdropper tries to guess the correct operation for every round of the protocol by chance, it will eventually denounce its presence. This feature represents an additional security advantage in the real-world scenario. As a consequence, we do not have to handle the cases of a third-party being impersonated by a curious agent or even by an eavesdropper (we suggest the reading of ref. [520] for a more comprehensive discussion about it). This protocol has the advantage of having lower costs for practical implementation, keeping the accessibility from SQKDs since we impose that at least only one of the parties needs to have quantum resources while maintaining the scalability of the usual QCKAs. We designed a prototype of a possible implementation for this protocol in Python, using mainly IBM's Qiskit[1] library, among others. Namely, we are implementing our customized Qis|krypt⟩[2] library for the simulation of several protocols of cryptography and communications in the Post-Quantum Era. Regarding our protocol, we consider some possible attacks presented in our adversary model (see Section 4.3.1) and their possible security countermeasures (see Sections 4.3.1.1 and 4.3.1.2). Additionally, we address the implementation of our protocol for Noiseless Scenarios (see Section 4.2), and we also provide its security analysis and proof even for the Noisy Scenarios (see Section 4.3).

4.1.1 BKMPS22 Protocol

Here, we propose an SQCKA protocol, which we can also refer to as the BKMPS22 protocol[3]. Suppose there are P parties who want to agree on a common conference key, namely an Alice and $(P-1)$ Bobs denoted as Bob_i, where $1 \leq i \leq (P-1)$. In our protocol, we only impose that at least one of the parties needs to be a quantum entity, while the remaining ones are classical entities. For simplicity, we will assume that Alice is the quantum entity, while all Bob_i are classical ones for the description of our protocol. Additionally, all the parties have an equal short pre-shared key PSK, with size $\left(R \cdot h(p_{PE})\right)$, where p_{PE} is an adjustable parameter given for the protocol a *priori*. Since each party has this pre-shared key PSK, we can denote them as $\left(PSK_{Alice} = PSK_{Bob_1} = ... = PSK_{Bob_{(P-1)}}\right)$. Namely, we need to assume the existence of this pre-shared key among all the parties to guarantee that all the parties perform the correct operation, otherwise the key rate does not scale with the number of parties involved. The size of this pre-shared key, when compared to the expected size of the new common conference key, which the parties want to agree on, has to be small. As mentioned before, there are standard

[1] See more information about IBM's Qiskit open-source library on the link: https://qiskit.org/

[2] See more information about our Qis|krypt⟩ open-source library on the link: https://qiskrypt.github.io/

[3] This protocol is code-named with the first capital letter of the last name of the authors and co-authors, in alphabetic order, and the last two digits of the year of the development of this work proposal. This procedure of naming protocols is a usual standard in quantum cryptographic protocols. Following this naming procedure, we have the code-name BKMPS22 (Barreiro-Krawec-Mateus-Paunković-Souto-2022) for our cryptographic protocol.

techniques to achieve this goal, such as, for R rounds, one can choose $\sqrt{R}$ rounds to be used for the CTRL rounds, costing $\log_2(R \cdot \sqrt{R})$ bits of the pre-shared key to establish $(R - \sqrt{R})$ secure sifted bits of that conference key. Another alternative is to use quantum-resilient Hash Functions, such as SHA-384, or SHA-512, on a small secret shared among the parties a *priori* (see Section 3.5.1 for a better comprehension about this requirement). Our protocol could be configurable with many multipartite entangled states, such as GHZ states, W states, or Cluster states (see Sections 2.2.4.2 to 2.2.4.4), among others with the respective adjustments. In the scope of this Master's Thesis, we will only focus on the protocol variant using GHZ states. However, we leave open the possibility of a future implementation of other variants of the protocol with different multipartite entanglements, such as W states and Cluster states.

We demonstrate a high-level illustrative schematic of our protocol in Figure 4.1:

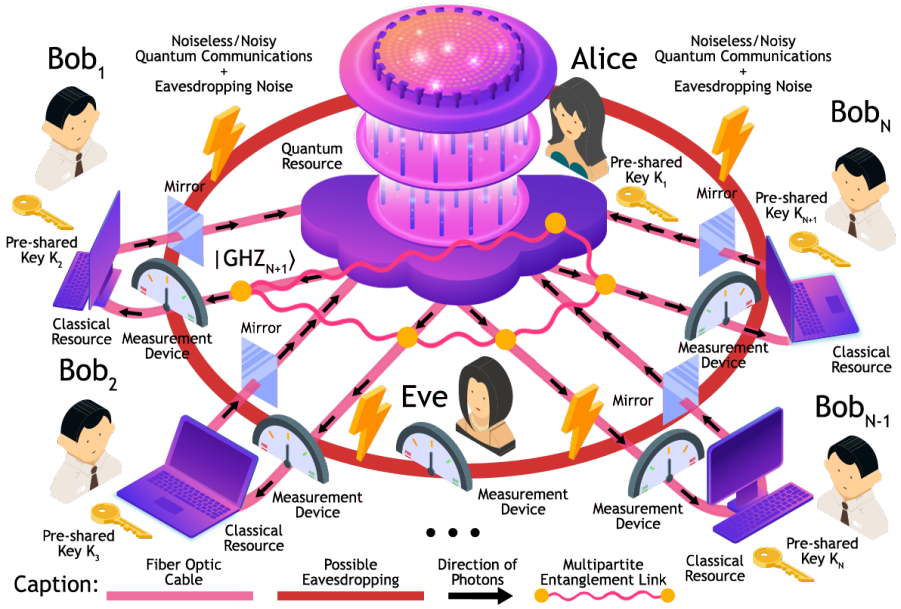


Figure 4.1: Schematic illustration for our SQCKA proposal.

4.1.1.1 BKMPS22 Protocol with GHZ States (BKMPS22-GHZ^P)

The high-level description of the BKMPS22 protocol with GHZ states (BKMPS22-GHZ^P) is:

1) **Quantum Transmission**:

   i. *Preparation of Quantum States:*

   - Alice prepares a GHZ state $|GHZ_P\rangle$ with P entangled photons, keeping one of these photons (e.g., the first one) to herself in her private quantum register.

   ii. *Transmission of Quantum States:*

   - Alice sends the other $(P-1)$ photons to each Bob$_i$, through the respective quantum communication medium qcm_i, until each photon reaches the associated Bob$_i$'s endpoint, and his corresponding private quantum register.

iii. *Measure-and-Resend or Reflect of Quantum States:*

- Each Bob_i, according to the pre-shared key PSK_{Bob_i}, will either choose to measure the incoming photon in the $\mathbb{Z}$-Basis and send back to Alice the measurement outcome encoded as an equivalent quantum state prepared in the same classical bit found (i.e., $|0\rangle$ or $|1\rangle$) Bob_i (Measure-and-Resend operation) or to simply reflect the incoming photon back to Alice, letting it undisturbed (Reflect operation), with the following described purposes:
  - The rounds on which Bob_i chooses the Measure-and-Resend operation which happens with higher frequency $\big($i.e., with probability of $(1 - p_{PE})\big)$, are denoted as SIFT rounds and are used to establish the secret bits that will compose the final conference key among all the involved parties.
  - The rounds on which Bob_i chooses the Reflect operation happen with lower frequency (i.e., with probability of p_{PE}), are denoted as CTRL rounds and are used for spotting an eventual eavesdropping attempt from Eve.

iv. *Secret Bit Generation or Eavesdropping Checking from Quantum States:*

- For the returning photons from Bob_i, according to the pre-shared key PSK_{Alice}, Alice either choose to measure them all individually in the $\mathbb{Z}$-Basis (Secret Bit Generation operation) or to follow an eavesdropping checking strategy chosen a *priori* (Eavesdropping Checking operation), with the following purposes:
  - The rounds on which Alice chooses the Secret Bit Generation operation are correlated with the Measure-and-Resend operations from Bob_i. Here, after Alice measures the photon in her internal private quantum register in the $\mathbb{Z}$-Basis, she expects to obtain the same classical bit as Bob_i got in his side.
  - The rounds on which Alice ends up choosing the Eavesdropping Checking operation, she will follow the strategy agreed a *priori*, to check if the returning entangled GHZ state is the same she prepared initially and was not intercepted by Eve. Basically, the main idea of this strategy is to verify the fidelity of the quantum state collected be the original GHZ state.

2) **Classical Post-Processing:**

i. *Secret Key Sifting and Parameter Estimation:*

- Alice checks a possible eavesdropping attempt from Eve on every CTRL rounds by computing the individual pairwise QBERs $Q_{CTRL_{(Alice,Bob_i)}}$ and the global Q_{CTRL}. If some of these QBERs exceeds a predefined threshold $\big(\varepsilon$ for Noiseless Scenarios and $(\eta + \varepsilon)$ for Noisy Scenarios$\big)$, Alice notify all Bob_i to retry or abort the protocol. Otherwise, they discard all the CTRL rounds and continue the protocol. Additionally, Alice also announces the classical bits she observed from a randomly chosen sample of the SIFT rounds to each Bob_i, computing the individual pairwise QBERs $Q_{\mathbb{Z}_{(Alice,Bob_i)}}$, and if some Bob_i

obtains a QBER exceeding a predefined threshold (once again, ε for Noiseless Scenarios and $\eta + \varepsilon$ for Noisy Scenarios), he notify Alice and all the other Bob_j to retry and abort the protocol, where $j \neq i$ and $1 \leq j \leq (P-1)$. Otherwise, they should continue the execution of the protocol. After this step, Alice and each Bob_i will have their sifted keys which may still contain some errors.

ii. *Information Reconciliation:*

- Alice sends an Error Correction Code (for $\max_i Q_{\mathbb{Z}_{(Alice,Bob_i)}}$) to each Bob_i, that should be applied individually by each Bob_i to its respective sifted key, to match the Alice's secret bits and agree on a common error-free reconciled key.

iii. *Privacy Amplification:*

- Alice and each Bob_i randomly choose a Two-Universal Hash Function to apply to their reconciled key, to eliminate any remaining leakage of information during the Transmission of Quantum States or Information Reconciliation steps, and partial knowledge Eve may have about that reconciled key, resulting in their final conference key $\big($i.e., $(CK_{Alice} = CK_{Bob_1} = ... = CK_{Bob_{(P-1)}})\big)$.

4.2 Experimental Methodology

For the simulation of the Quantum Transmission stage, we followed an approach based on quantum circuits. We developed this simulation in our custom Qis|krypt⟩ library in Python, using IBM's Qiskit library, to build the quantum circuits required (see Section 2.2.3). We needed to develop one different quantum circuit for each type of round (i.e., SIFT and CTRL rounds, based on the pairs of Measure-and-Resend/Secret Bit Generation and Reflect/Eavesdropping Checking operations). However, in our protocol, we developed two different strategies for the Eavesdropping Checking. The first strategy goes on by Alice measuring the returning undisturbed photons along with her photon on the GHZ-Basis (see Section 2.2.4.2), denoted as GHZ_{MEAS} strategy. While the second strategy works by Alice performing the well-known SWAP Test with those undisturbed photons with another equal GHZ state, prepared a *priori*, denoted as $SWAP_{TEST}$ strategy. We also note the $SWAP_{TEST}$ strategy imposes Alice to have more quantum resources (i.e., larger quantum registers) compared to the GHZ_{MEAS} strategy. Namely, Alice must have a quantum register with $(2P+1)$ qubits in CTRL rounds since she needs to create another GHZ state in the earlier strategy to perform the SWAP Test between that additional GHZ state and the one returning from Bob. On the other hand, Alice only needs a quantum register with P qubits for the latter strategy since she simply measures the returning supposed GHZ state in the GHZ-Basis. Thus, we initially follow the given explanation of these rounds for the simulation of our protocol for the Noiseless Scenario in the next sub-section.

4.2.1 Simulation of Noiseless Scenarios

The simulation of our BKMPS22 protocol with GHZ states, for Noiseless Scenarios is given as:

Simulation of Protocol 1 BKMPS22 protocol with GHZ states (Noiseless Scenarios)

***Inputs*:**

(i) The number of parties P.

(ii) An eavesdropping checking strategy $S \in \{SWAP_{TEST}, GHZ_{MEAS}\}$.

***Setup*:**

(i) p_i are the P parties of the protocol, with $P \geq 2$ and $i = 1, ..., P$, where p_1 is the `sender` and the remaining p_i are the `receivers`.

(ii) qcm_k are quantum communication mediums between p_1 and p_i, with $k = 1, ..., (P-1)$ and $i = (k+1)$.

(iii) R is the number of rounds of the protocol, with $R \geq 1$.

(iv) e is a possible `eavesdropper`, who can perform attacks on the quantum communication mediums qcm_k, during the different r rounds. If e is `NULL`, there is no `eavesdropper`.

(v) PSK_{p_i} is the pre-shared key among all p_i, with $i = 1, ..., P$ and $(PSK_{p_1} = ... = PSK_{p_P})$.

***Steps*:**

a) For each round r of the protocol, with $1 \leq r \leq R$:

1) According to the chosen Eavesdropping Checking strategy S:

(i) If $S = SWAP_{TEST}$, p_1 prepares a $|GHZ_P\rangle$ state and a $|GHZ_P\rangle_{SWAP}$ state, in its respective private quantum registers.

(ii) If $S = GHZ_{MEAS}$, p_1 prepares a $|GHZ_P\rangle$ state on its private quantum register.

2) p_1 sends each qubit q_i of the $|GHZ_P\rangle$ state to the other p_i through the respective quantum communication medium qcm_k, keeping the first qubit to itself, with $2 \leq i \leq P$ and $k = (i-1)$.

3) If $e \neq$ `NULL`, it can perform some attack on one or more of the forwarding quantum communication medium qcm_k, with $k = 1 \leq i \leq (P-1)$ (see Section 4.3.1).

4) Each p_i (with $i \geq 2$) will perform one of the following operations, according to the bit r of its pre-shared key PSK_{p_i}:

(i) If $PSK_{p_i,r} = 0$ (`SIFT` round), p_i performs the Measure-and-Resend operation:

- p_i measures the qubit q_i in the $\mathbb{Z}$-Basis.
- p_i keeps the resulting bit to itself and resend a quantum state equivalent to that bit (i.e., $|0\rangle$ or $|1\rangle$) to p_1.

(ii) Otherwise, if $PSK_{p_i,r} = 1$ (`CTRL` round), p_i performs the Reflect operation:

- p_i simply reflects the qubit q_i back to p_1.

Steps (cont.) ***:***

a) For each round r of the protocol, with $1 \leq r \leq R$ (cont.):

5) Each qubit q_i travels back to p_1 via the quantum communication medium qcm_k.

6) Again, if $e \neq$ NULL, it can perform an attack on one or more of the reverse quantum communication medium qcm_k, with $k = 1 \leq i \leq (P-1)$ (see Section 4.3.1).

7) Regarding the type of the round r, known from the bit r of the pre-shared key PSK_{p_i}, p_1 will perform one of the following operations:

(i) If $PSK_{p_1,r} = 0$ (SIFT round), p_i performs the Secret Bit Generation operation:

- p_1 measures its qubit q_1 jointly with remaining returning qubits q_i in the $\mathbb{Z}$-Basis, with $2 \leq i \leq P$.
- The bit resulting from the measurement of the qubit q_1 made by p_1 is added to its sifted key.

(ii) Otherwise, if $PSK_{p_1,r} = 1$ (CTRL round), p_i performs the Eavesdropping Checking operation:

- p_1 performs the eavesdropping checking strategy S to detect an eventual eavesdropper, estimating QBER $Q_{CTRL_{(p_1,p_i)}}$, with $2 \leq i \leq P$:
  - If $S = SWAP_{TEST}$, p_1 performs the SWAP Test routine (see ref. [521]) between the $|GHZ_P\rangle$ state and $|GHZ_P\rangle_{SWAP}$ state.
  - If $S = GHZ_{MEAS}$, p_1 measures the $|GHZ_P\rangle$ state in the GHZ-Basis (see Section 2.2.4.2).
- If $Q_{CTRL_{(p_1,p_i)}} \geq \epsilon$, p_1 aborts the protocol and notifies the other p_i (with $2 \leq i \leq P$). Otherwise, p_1 discard these rounds and corresponding bits.

b) After all the rounds of the protocol being completed, p_1 publicly announces to all the other p_i (with $2 \geq i \leq P$) a random sample of $p_{PE} \cdot R$ bits obtained in the SIFT rounds, on which they should estimate the QBERs $Q_{\mathbb{Z}_{(p_1,p_i)}}$. If a QBER $Q_{\mathbb{Z}_{(p_1,p_i)}} \leq \varepsilon$, the parties p_1 and p_i should abort the protocol, notifying all the other p_j (with $2 \leq i,j \leq P \wedge i \neq j$). Otherwise, they discard these rounds and the corresponding bits, keeping the remaining bits to compose their sifted keys sk_{p_i}, which may still contain some errors among them.

c) p_1 chooses a random Error Correction Code and announces it to the other p_i to apply it to the bits of their sifted keys sk_{p_i} to agree on a common reconciled key rk_{p_i}.

d) p_1 chooses a random Two-Universal Hash Function and announces it to the other p_i to be applied to the bits of their reconciled keys rk_{p_i}, extracting the conference key ck_{p_i}.

We show the quantum circuit for SIFT rounds, with no eavesdropper, in Figure 4.2:

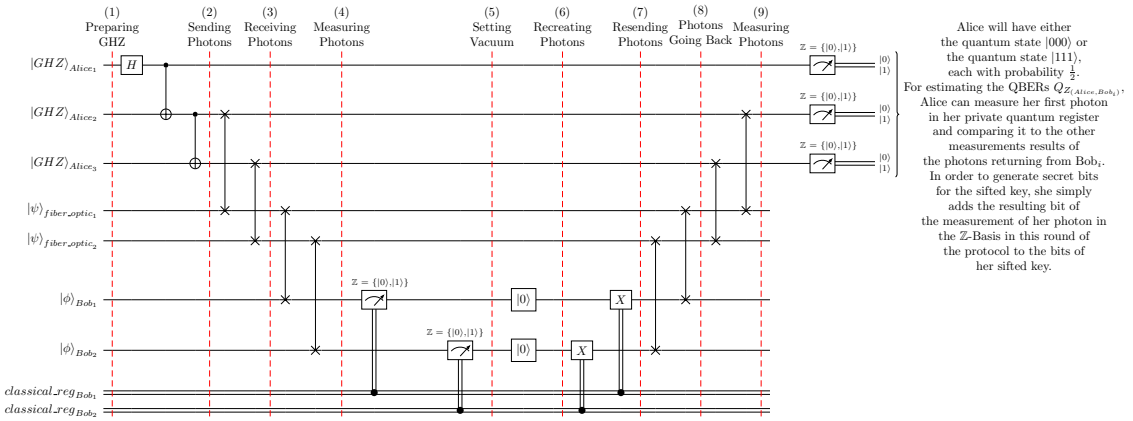


Figure 4.2: The Quantum Circuit for a SIFT round of the BKMPS22 protocol with GHZ states for 3 parties (Alice, Bob_1 and Bob_2) in Noiseless Scenarios. In this case, Alice and Bobs will extract a common secret bit for their sifted key, or will estimate the QBERs $Q_{\mathbb{Z}_{(Alice,Bob_i)}}$.

In a real-world implementation, the party p_i, with $2 \leq i \leq P$ (i.e., Bob_i), is not required to have quantum resources. In particular, p_i only needs a simple measurement device, such as Photodetectors. However, for a circuit-based simulation of our protocol, p_i needs to have a quantum register to measure the incoming qubit q_i in the $\mathbb{Z}$-Basis for the SIFT rounds.

Additionally, note that in the simulation of the SIFT rounds showed in Figure 4.2, right after p_i measures the qubit q_i in the $\mathbb{Z}$-Basis, it needs to create the quantum state equivalent to the classical bit obtained. More specifically, p_i also applies or not the Pauli-X gate to the qubit q_i created again, based on the classical bit got and kept in the classical register of p_i.

For the CTRL rounds, following the strategy $S = SWAP_{TEST}$, note that p_1 (i.e., Alice) has two quantum registers installed a *priori* in its endpoint (i.e., $|GHZ\rangle_{p_1}$ and $|GHZ\rangle_{p_1,SWAP}$) and creates an equal GHZ state in them (i.e., the $|GHZ_P\rangle$ state and $|GHZ_{P,SWAP}\rangle$ state, respectively). For the Quantum Transmission, p_1 only sends the qubits of GHZ state in the quantum register $|GHZ\rangle_{p_1}$ to the other respective p_i, with $2 \leq i \leq P$ (i.e., Bob_i), while keeping the other GHZ state in the quantum register $|GHZ\rangle_{p_1,SWAP}$. When those qubits of the GHZ state $|GHZ_P\rangle$ return from the other p_i to the quantum register $|GHZ\rangle_{p_1}$, p_1 performs a SWAP Test between the $|GHZ_P\rangle$ and $|GHZ_{P,SWAP}\rangle$ states. For a better understanding, we show the

quantum circuit for these rounds with the strategy $S = SWAP_{TEST}$ in the following Fig. 4.3:

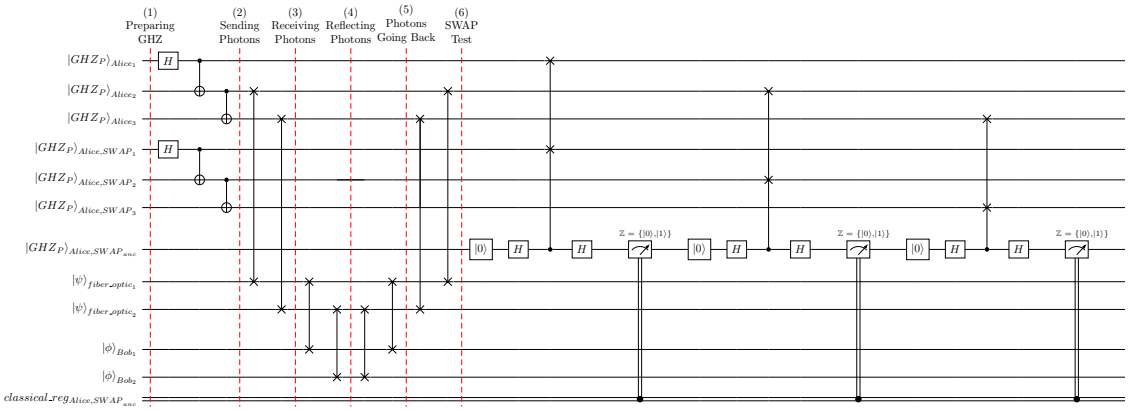


Figure 4.3: The Quantum Circuit for a SIFT round of the BKMPS22 protocol with GHZ states for 3 parties (Alice, Bob_1 and Bob_2) in Noiseless Scenarios, following the $SWAP_{TEST}$ strategy. In this case, Alice creates two quantum registers with two equal GHZ states, sending one of them to Bobs and keeping the other to herself. After the returning of the GHZ state in the reverse quantum communication medium, Alice can compare it with GHZ state kept in her private quantum register, to estimate the QBERs $Q_{CTRL_{(Alice,Bob_i)}}$.

On the other hand, for the CTRL rounds, following the strategy $S = GHZ_{MEAS}$, p_1 (i.e., Alice) only needs to have a single quantum register installed a *priori* at its endpoint (i.e., $|GHZ\rangle_{p_1}$) and creates a single GHZ state in it (i.e., the $|GHZ_P\rangle$ state). For a better comprehension, we show the quantum circuit for this type of rounds with the strategy $S = GHZ_{MEAS}$ in Figure 4.4:

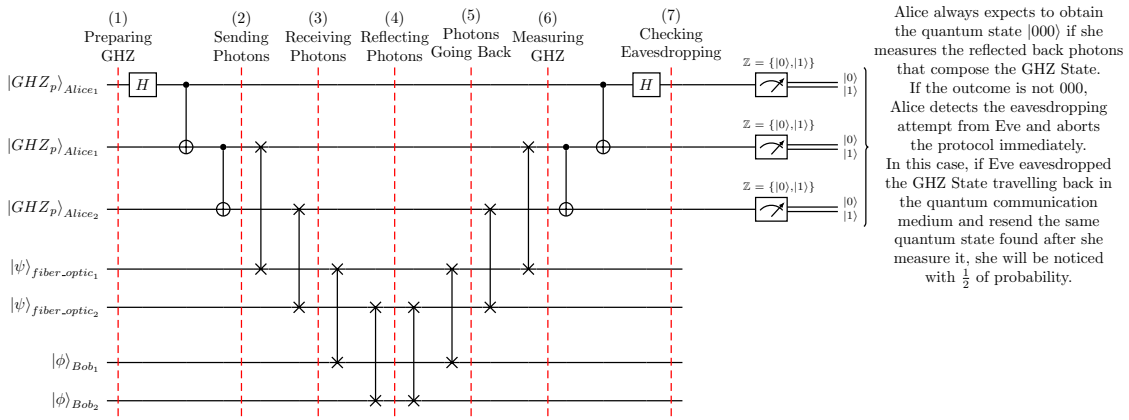


Figure 4.4: The Quantum Circuit for a CTRL round of the BKMPS22 protocol with GHZ states for 3 parties (Alice, Bob_1 and Bob_2) in Noiseless Scenarios, following the GHZ_{MEAS} strategy. In this case, Alice can perform an unitary transformation of the returning GHZ state to transform it back in the initial quantum state $|000\rangle$, to estimate the QBERs $Q_{CTRL_{(Alice,Bob_i)}}$.

Here, p_1 sends the qubits of GHZ state in the quantum register $|GHZ\rangle_{p_1}$ to the other respective p_i, with $2 \leq i \leq P$ (i.e., Bob_i). When those qubits returns from the other respective p_i to the quantum register $|GHZ\rangle_{p_1}$, p_1 measures the $|GHZ_P\rangle$ state in the GHZ-Basis.

4.3 Security Analysis

In this section, we will demonstrate the Security Analysis performed for our BKMPS22 Protocol, for which we consider an Adversary Model, and elaborate on the respective Security Proof.

4.3.1 Adversary Model

In this Master Thesis, the IR (Intercept-and-Resend) and the DoS (Denial-of-Service) Attacks (see Sections 3.6.1 and 3.6.2) will be the only ones considered for the Adversary Model of our protocol. These two attacks are the ones that are not directly related to imperfections on the quantum hardware used in these types of quantum cryptographic protocols. For this reason, the other remaining attacks introduced previously in this document (see Section 3.6) are out of the scope of the Adversary Model of our protocol and will not be considered in this section.

4.3.1.1 Security Countermeasures for Intercept-and-Resend (IR) Attacks

For the IR (Intercept-and-Resend) Attacks, first note that our protocol uses a random short pre-shared key not known by the eavesdropper e (e.g., Eve). All the parties use this pre-shared key to determine which operations they will perform in each round of the protocol. Therefore, the best strategy for e to eavesdrop on these rounds is to guess the respective type of operation at random. Additionally, the qubit q_1 is always kept private locally by p_1 (e.g., Alice), and thus, is not accessible to e. Namely, e only knows that p_1 (e.g., Alice) will create a GHZ state, and the other parties p_i will jointly perform a $\mathbb{Z}$-Basis (Standard Computational Basis) measurement on their respective qubits q_i or simply reflect them, on their endpoints, with $2 \leq i \leq P$. Moreover, for the `CTRL` rounds, the GHZ states prepared by p_1 remain maximally entangled until the end of the round, when p_1 measures that quantum state on the GHZ-Basis, undoing that quantum entanglement. Thus, an eavesdropper e has only two choices, measuring some qubit(s) q_i in the $\mathbb{Z}$-Basis or simply letting it (or them) return to p_1. In the end, we have a total of four possibilities, where we can exclude a *priori* the cases in which e let the qubit(s) q_i simply pass in the medium, since that it is equivalent to e not performing an IR Attack at all. So, we need to focus only on the cases in which an e measures the qubit(s) q_i in the $\mathbb{Z}$-Basis.

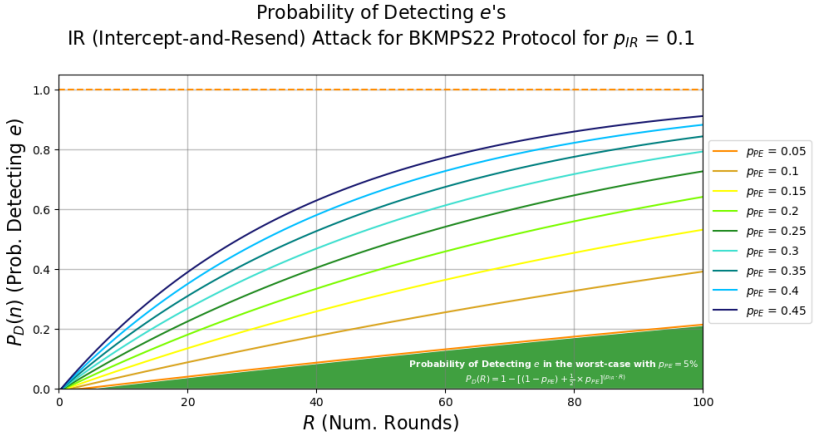
For the `SIFT` rounds, which happen more frequently, if e measures some qubit(s) of the GHZ state with the form $|GHZ_P\rangle = \frac{1}{\sqrt{2}}(|00...0\rangle + |11...1\rangle)$ in the $\mathbb{Z}$-Basis, it will collapse into the quantum states $|00...0\rangle$ or $|11...1\rangle$, with equal probability (i.e., 50%), being equivalent to correlated classical bits. If e do that interception in the forward direction of the quantum communication medium, resending an equivalent quantum state to the respective p_i, then, p_1 and p_i will jointly measure the quantum state which was already "observed" and obtain the same classical bits obtained by e, with $2 \leq i \leq P$, and thus, e can obtain the secret bit of that round without being noticed. The same happens with e doing that interception in the reverse direction of the quantum communication medium. If e intercepts the returning qubit(s) q_i already measured in the $\mathbb{Z}$-Basis by the respective p_i, it will be able to obtain the same classical

bit "observed" by all p_i, with $2 \leq i \leq P$. Here, all the parties will not notice e since p_1 will also obtain the same classical bit observed previously by all p_i in their respective endpoints.

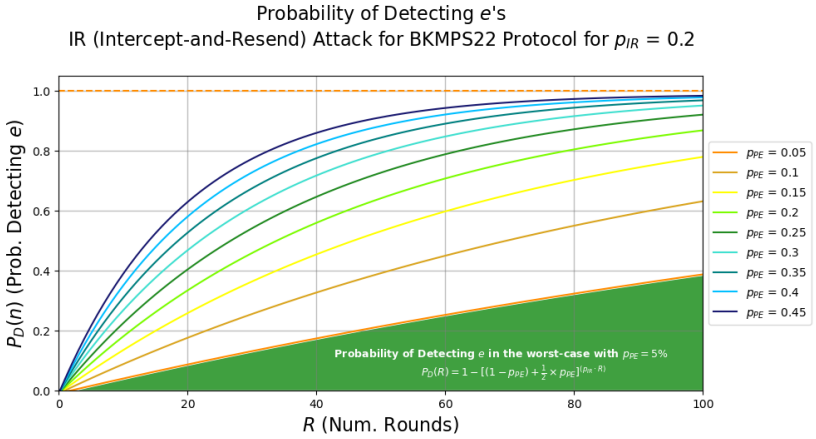
However, considering the CTRL rounds, which happen less frequently, e are not able to always intercept some qubit(s) q_i without being noticed, with $2 \leq i \leq P$. If e measures some qubit(s) q_i traveling in the forward direction of the quantum communication medium in the $\mathbb{Z}$-Basis, resending an equivalent quantum state (i.e., $|00...0\rangle$ or $|11...1\rangle$) to the respective p_i, then, p_i will reflect that quantum state back to p_1, which will be measured in the GHZ-Basis, resulting in the quantum states with the form $|\psi\rangle = \frac{1}{\sqrt{2}}\big(|00...0\rangle \pm |00...1\rangle\big)$, for the cases on which e obtained the quantum states $|0\rangle$ or $|1\rangle$ for the intercepted qubit, respectively. In both cases, it allows to p_1 detect the eavesdropping attempt from e with 50% of probability (i.e., where p_1 "observed" the quantum state $|11...1\rangle$, after the GHZ-Basis measurement). If, in addition, e tries to flip some qubit(s) q_i after measure them, regarding the classical outcome "observed", it ends being detected with the same probability, since p_1 always expect to obtain the quantum state $|00...0\rangle$. And even if e tries to replace the qubits q_i by a maximally entangled state such as a EPR pair (if $P = 2$) or a GHZ state (if $P > 2$), it ends being detected with a probability of 75%. Remember that if the protocol has R rounds, these probabilities of detect an interception of e are verified for each one of the $p_{PE} \cdot R$ CTRL rounds, what difficult even more the chances of e be constantly intercepting some qubit(s). This same analysis is also valid if e intercepts and resend some qubit(s) in the reverse direction of the quantum communication medium, since the quantum state reflected is the same travelling on the forward direction of that same quantum communication medium between the parties.

Therefore, considering this type of attack, the only cases on which e can intercept and resend some qubit(s) without being noticed is if it correctly guesses that it is a SIFT round, which happens with probability $(1 - p_{PE})$, or if it e guesses wrongly that it is SIFT round (i.e., when is actually a CTRL round), what happens with probability p_{PE}, and considering that p_1 obtains the quantum state $|00...0\rangle$, what happens in a further 50% of probability (i.e., $p_{PE} \times 50\%$), not noticing that e intercepted some qubit(s) in that round. Additionally, we can see that it is not a good strategy for e to try to always guess the type of the current round in order to perform the IR attack since the CTRL rounds, that represent the only cases where the parties can detect the presence of e, only happens in p_{PE} of the time. But we assume e does not have any knowledge about the pre-shared key, and consequently, about p_{PE}. In this case, her best strategy is to try to guess at random, considering a probability P_{IR}. In the end, for each round of the protocol, the total probability of e intercepting some qubit(s) without being noticed is given by $\big[(1 - p_{PE}) + \frac{1}{2} \times p_{PE}\big]$. So, the probability for e to be able to constantly intercept and resend qubit(s) during all the $p_{IR} \cdot R$ rounds of the protocol is given by $\big[(1 - p_{PE}) + \frac{1}{2} \times p_{PE}\big]^{(p_{IR} \cdot R)}$. If, as usual, we take the probability of the opposite event, the expression $P_D(R) = 1 - \big[(1 - p_{PE}) + \frac{1}{2} \times p_{PE}\big]^{(p_{IR} \cdot R)}$ gives us the probability of detecting e during the execution of our protocol. Notice that, in some cases, when p_{PE} is close to 50%, it is not a good choice to e choose a very high probability p_{IR}. However, we will demonstrate the analysis for all the cases by fixing several probabilities p_{IR} for e and the respective functions

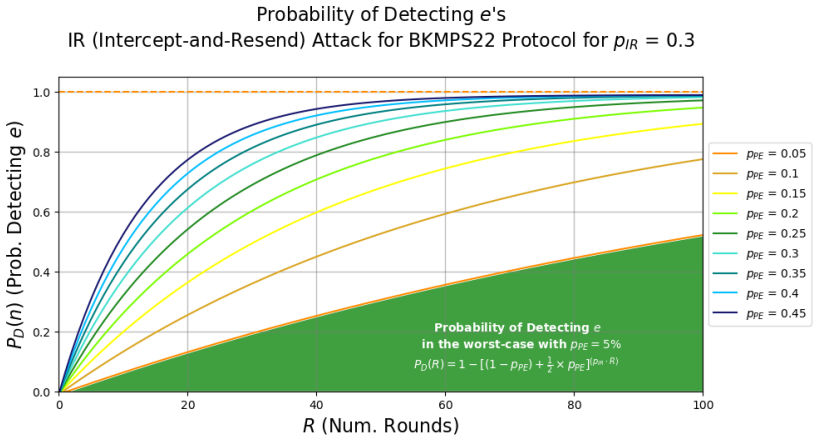
considering several $0 < p_{PE} < 0.5$. We show the behavior of these functions in Figure 4.5:



(a) Probability of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol with $p_{IR} = 0.1$.

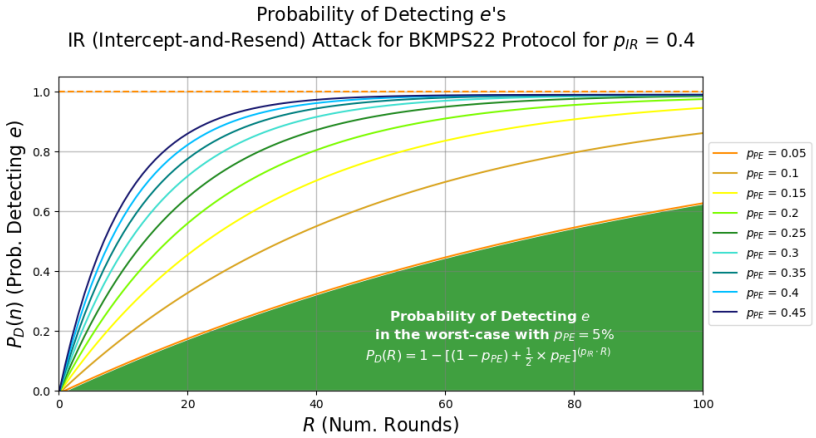


(b) Probability of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol with $p_{IR} = 0.2$.

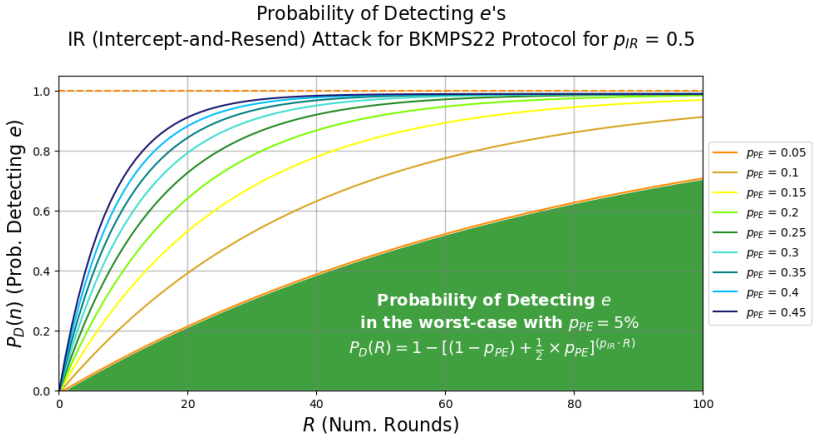


(c) Probability of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol with $p_{IR} = 0.3$.

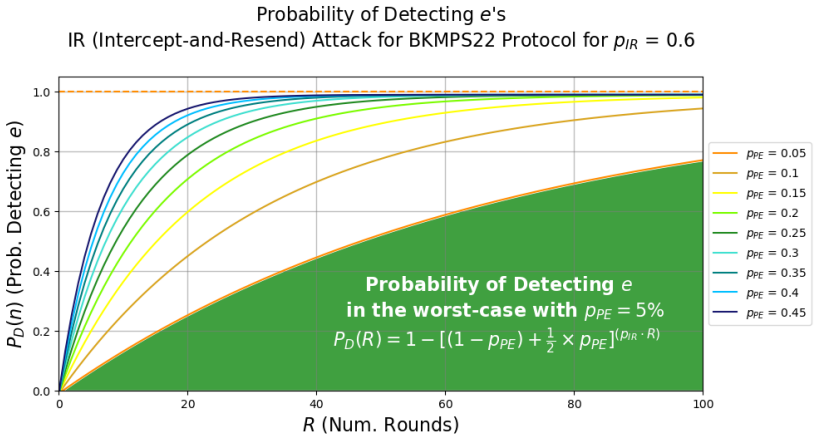
Figure 4.5: Probability of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol.



(d) Probability of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol with $p_{IR} = 0.4$.

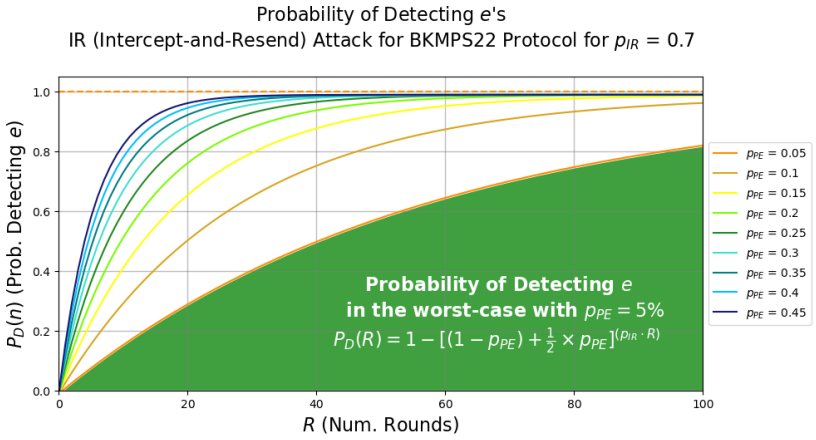


(e) Probability of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol with $p_{IR} = 0.5$.

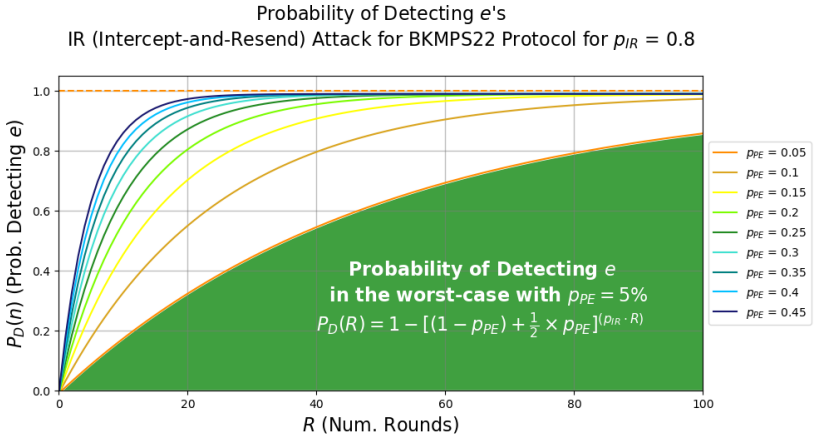


(f) Probability of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol with $p_{IR} = 0.6$.

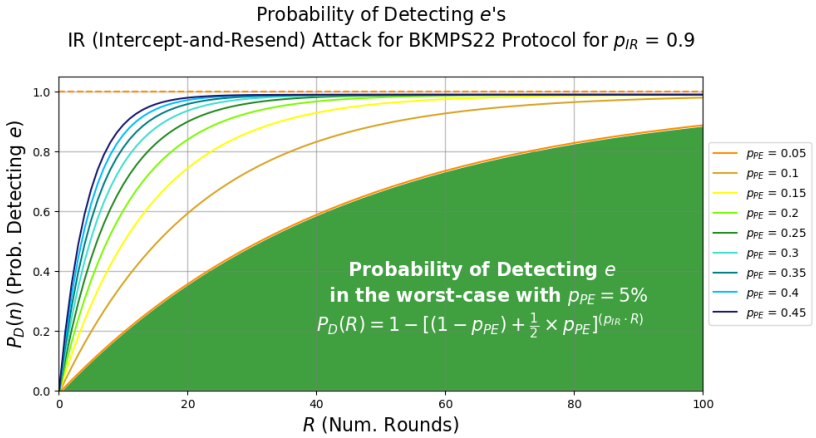
Figure 4.5: Probability of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol (cont.).



(g) Probability of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol with $p_{IR} = 0.7$.

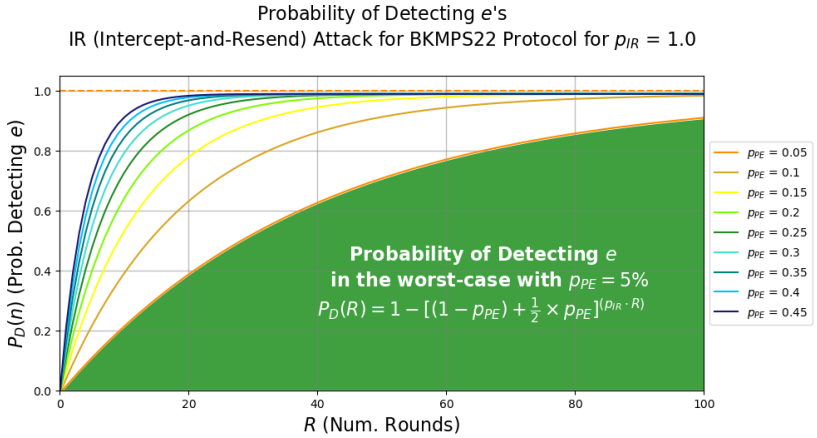


(h) Probability of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol with $p_{IR} = 0.8$.



(i) Probability of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol with $p_{IR} = 0.9$.

Figure 4.5: Probability of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol (cont.).



(j) Probability of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol with $p_{IR} = 1.0$.

Figure 4.5: Probability of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol (cont.).

Therefore, if we consider an infinite R, we have $\lim_{n \to +\infty} P_D(R) = 1$. Once again, with only $R = 20$, we have $P_D(20) = 1 - \left[(1 - p_{PE}) + \frac{1}{2} \times p_{PE}\right]^{(p_{IR} \cdot 20)}$, we wave the probabilities of detecting the eavesdropper e, for the several p_{IR} and p_{PE}, demonstrated in Table 4.1:

p_{IR}	0.1					0.275				
p_{PE}	0.05	0.15	0.25	0.35	0.45	0.05	0.15	0.25	0.35	0.45
$p_D(20)$	0.039	0.134	0.224	0.309	0.389	0.119	0.338	0.51	0.642	0.743
p_{IR}	0.45					0.625				
p_{PE}	0.05	0.15	0.25	0.35	0.45	0.05	0.15	0.25	0.35	0.45
$p_D(20)$	0.193	0.494	0.689	0.812	0.889	0.261	0.612	0.801	0.899	0.948
p_{IR}	0.8					0.975				
p_{PE}	0.05	0.15	0.25	0.35	0.45	0.05	0.15	0.25	0.35	0.45
$p_D(20)$	0.323	0.702	0.871	0.943	0.973	0.379	0.771	0.916	0.966	0.983

Table 4.1: Probabilities of Detecting e's IR (Intercept-and-Resend) Attack for BKMPS22 Protocol with $R = 20$.

As expected and similar to the standard observed in quantum cryptographic protocols, how more qubits an eavesdropper "intercepts-and-resend" (for higher p_{IR} values), the more will be the probability of detecting its presence. Additionally, we can see that if an eavesdropper tries to perform this attack in more than half of the rounds, if we use a $0.25 \leq p_{PE} \leq 0.35$, the probability of detecting its presence will be extremely high (above 80%) just for $R = 20$ rounds.

4.3.1.2 Security Countermeasures for Denial-of-Service (DoS) Attacks

Another attack that an eavesdropper can perform is the DoS (Denial-of-Service) Attack during the execution of our protocol. Here, it pretends not to allow the agreement of the conference key among all the parties. There are basically two ways that an eavesdropper e can achieve that. The first is by blocking some quantum communication medium(s) qcm_k between p_1 and

p_i, with $k = 1, ..., (P-1)$ and $i = (k+1)$ (e.g., cutting the corresponding fiber optic cable(s) or obstructing the corresponding direct line-of-sight paths in free-space optical mediums). The second is simply by intercepting the qubit(s) propagating in the quantum communication medium(s) constantly and on purpose, forcing the parties to always abort the protocol. One solution to this problem is to use other available quantum communication medium(s) once this attack is detected. In order to handle this attack on large scales correctly is crucial the implementation of metropolitan Quantum Communication Networks (or the global Quantum Internet itself), as well as every protocol they involve, such as Quantum Routing [259, 522–528], Topology Configuration [524, 529–542], and Shortest Path [543] protocols, or even, Quantum Teleportation, Quantum Entanglement Swapping and Quantum Entanglement Distillation protocols (see Sections 2.2.5.3 to 2.2.5.5). The major difficulty is how to detect these attempts of DoS Attacks and how to keep constantly updated information about alternative links.

In fact, we can detect the first case by simply introducing "alarms" into our protocol. Note that if an eavesdropper e blocks some quantum communication medium(s), no qubit(s) will propagate after the blocking point. In that case, the respective party who should expect to receive the qubit in some quantum state will always receive that same qubit in a vacuum state (i.e., $|0\rangle$), independently of the quantum state transmitted before the blocking point. And knowing this, we can assume that if a party keeps receiving qubits in the vacuum state in several consecutive rounds, assuming a threshold, probably the quantum communication medium where those qubits are propagating is blocked, and an "alarm" should be triggered. In that case, the harmed party should notify the other remaining parties of the situation. Then, they should abort the protocol immediately and possibly retry it using other available quantum communication medium for that party. Finally, the blocked quantum communication medium should be reported as unavailable, and nobody should not use it until being operational again.

4.3.2 Security Proof

For the security proof of our BKMPS22 protocol with GHZ States, we introduce a new notation for a better understanding. Let $\phi(P, \lambda, \mu) = \left|g^P(\lambda, \mu)\right\rangle = \frac{1}{\sqrt{2}}|0\rangle\left|\vec{\mu}\right\rangle + \frac{(-1)^\lambda}{\sqrt{2}}|1\rangle\left|(\vec{\neg\mu})\right\rangle$, where $P \geq 2$, $\lambda \in \{0,1\}$ and $\mu \in \{0,1\}$, from which we have $\vec{\mu} = \vec{0} = \left[0...0\right]^T$ and $\vec{\mu} = \vec{1} = \left[1...1\right]^T$, for $\mu = 0$ and $\mu = 1$, respectively. Additionally, $\neg\mu$ is the bitwise complement of μ, from which we have $\neg\mu = 1$ and $\neg\mu = 0$, for $\mu = 0$ and $\mu = 1$, respectively. In this notation, $\vec{\mu}$ corresponds to a column-vector with $(P-1)$ elements, which represents the bits expected to be shared among the parties regarding the GHZ State. Note this introduced mathematical formulation is nothing more than the generalized GHZ-Basis on P photons. However, if we have $P = 2$, this mathematical formulation represents the equivalent to an EPR pair (see Section 2.2.4.1) as the entangled state to be shared among the parties, which possibly corresponds to an instance of a SQKD (see Section 3.4). For our security proof, we assume that there is Alice, who is a quantum entity, as well as $(P-1)$ Bob(s), who is/are classical entity/entities. As usual, the parties have a small and random pre-shared secret key Θ, which determines the coordinated operation to be performed in each round of the protocol. From this pre-shared key, all the parties can pick

a shared and secret bit $\vec{\Theta}_r$, for a current round r of the protocol, where $1 \leq r \leq R$. The value of this secret bit may be biased so that $\vec{\Theta}_r = 0$ is more often than $\vec{\Theta}_r = 1$. If $\vec{\Theta}_r = 0$, Bobs will measure-and-resend the incoming photons, from which they derive a secret key bit. Otherwise, when $\vec{\Theta}_r = 1$, they just reflect back the photons to Alice, not "disturbing" its quantum state. The detailed description of our BKMPS22 Protocol with GHZ States is given in Section 4.1.1.1

In the end, we consider our BKMPS22 protocol with GHZ States a two-way semi-quantum cryptographic protocol between $P \geq 2$ parties. Therefore, for simplification, we can denote our original protocol as BKMPS22-GHZ^P. But now, consider instead the following one-way fully quantum cryptographic protocol between only $P' = 2$ parties, namely a single Alice and a single Bob[4], denoted as OW-QKD-GHZ^P, where $P \neq P'$ and $P \geq 2$. In simple terms, we can think of OW-QKD-GHZ^P protocol as a reduction of the BKMPS22-GHZ^P protocol. Namely, we reduce our BKMPS22 protocol from multipartite to bipartite scenarios for the same number of P photons.

4.3.2.1 Reduction to the One-Way QKD with GHZ States (OW-QKD-GHZ^P) Protocol

The high-level description of OW-QKD-GHZ^P (One-Way QKD with GHZ States) protocol is:

1) **Quantum Transmission**:

   i. *Preparation of Quantum States:*

   - Bob prepares a GHZ State with $(2P-1)$ entangled photons, also defined by $\phi\big((2P-1),0,0\big) = \big|g^{(2P-1)}(0,0)\big\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|\,\vec{0}\rangle + |1\rangle|\,\vec{1}\rangle\big)$ for each round r of the protocol, where $1 \leq r \leq R$. Afterward, he keeps $(P-1)$ of these photons (e.g., the first $(P-1)$ one(s)) to himself in his private quantum register.

   ii. *Transmission of Quantum States:*

   - Bob sends the other remaining P photons to Alice through the single quantum communication medium qcm shared between him and Alice, until all those photons reach Alice's endpoint, and her respective private quantum register.

   iii. *Secret Bit Generation or Eavesdropping Checking from Quantum States:*

   - Bob and Alice, according to their pre-shared key ($PSK = PSK_{Bob} = PSK_{Alice}$), will either choose to measure the photons in their possession in the $\mathbb{Z}$-Basis (equivalent to the original Measure-and-Resend operation) or not (equivalent to the original Reflect operation), with the following described purposes:
     - The rounds on which Bob and Alice choose the equivalent to the original Measure-and-Resend operation happen with higher frequency (i.e., with probability of $(1-p_{PE})$), are denoted as SIFT rounds and are used to set up the secret bits that will compose the final secret key between Bob and Alice. Here, Bob will measure all his $(P-1)$ photon(s) in the $\mathbb{Z}$-Basis, while Alice will perform the same measurement on the first of her P photons. For

[4] In the reduction from the BKMPS22-GHZ^P protocol to the OW-QKD-GHZ^P protocol, the single Bob is also called "super-Bob". This "super-Bob" simulates all the Bobs from the original BKMPS22-GHZ^P protocol during the reduction.

Bob, the results of these measurements in the $\mathbb{Z}$-Basis will handle a secret bit, for each one of the "simulated" Bobs from the original BKMPS22-GHZ^P protocol. In this case, Bob expects to have the same bit outcome for all his measured $(P-1)$ photons. On the other hand, Alice has P photons, which in general do not need to have the same outcome bit after being measured. Obviously, this can happen due to noise in the quantum communication medium qcm or to possible eavesdropping attempts made by Eve.

– The rounds on which Bob and Alice choose the equivalent to the original Reflect operation happen with lower frequency (i.e., with probability p_{PE}), are denoted as CTRL rounds and are used to check an eavesdropping made by Eve. Here, Bob will measure his $(P-1)$ photon(s) in the $\mathbb{X}$-Basis, while Alice will measure her P photons in the GHZ-Basis (see Section 2.2.4.2).

2) **Classical Post-Processing:**

i. *Secret Key Sifting and Parameter Estimation:*

- Bob checks a possible eavesdropping attempt from Eve on every CTRL rounds, on which he aborts the execution of the protocol if just one of the outcomes from his measurements in the $\mathbb{X}$-Basis produces the quantum state $|-\rangle$. Note that, though the probability of aborting is high, it is strictly less than 100%. Then, Alice and Bob discard the CTRL rounds since they will not use them to compose the secret key. Next, Bob selects a random sample of SIFT rounds and publicly announces them to Alice. Afterward, Alice checks which of her photons is the most correlated with all of $(P-1)$ Bob's photons. For the most correlated pairs of photons regarding each round, Alice computes the global QBER $Q_{\mathbb{Z}}$ and if this QBER exceeds a predefined threshold (ϵ for Noiseless Scenarios and $\eta + \epsilon$ for Noisy Scenarios), Alice should notify Bob to abort or retry the protocol. Otherwise, they discard the rounds of this sample and should continue the execution of the protocol. After this step, Bob and Alice will have their sifted keys which may still contain some bits with errors.

ii. *Information Reconciliation:*

- Bob sends an Error Correction Code to Alice, which should be applied locally by Alice to the secret bits that compose her respective distilled sifted key, to match the Bob's secret bits and agree on a common error-free reconciled key.

iii. *Privacy Amplification:*

- Bob and Alice randomly choose a Two-Universal Hash Function to apply to their reconciled key, to eliminate any remaining leakage of information during the Transmission of Quantum States or Information Reconciliation steps, and partial knowledge Eve may have about that reconciled key, finally resulting in their final common symmetric secret key (i.e., $(sk_{Bob} = sk_{Alice})$).

The simulation of the OW QKD protocol with GHZ States is given as follows:

Simulation of Protocol 2 One-Way QKD protocol with GHZ States

***Inputs*:**

(i) The number $P \geq 2$ of qubits of the GHZ State for each round in the BKMPS22 Protocol.

***Setup*:**

(i) p_1 and p_2 are the parties of the protocol, where p_1 is the `sender` and p_2 is the `receiver`.

(ii) qcm is the quantum communication medium between p_1 and p_2.

(iii) R is the number of rounds of the protocol, with $R \geq 1$.

(iv) e is a possible `eavesdropper`, who can perform attacks on the quantum communication medium qcm, during the different r rounds. If e is `NULL`, there is no `eavesdropper`.

(v) PSK_{p_i} is the pre-shared key among p_i, with $i = 1, 2$ and $PSK_{p_1} = PSK_{p_2}$.

***Steps*:**

a) For each round r of the protocol, with $1 \leq r \leq R$:

1) p_1 prepares a $|GHZ_{(2P-1)}\rangle$ state on its private quantum register.

2) p_1 sends $(P-1)$ qubit(s) of the $|GHZ_{(2P-1)}\rangle$ state to p_2, through the respective quantum communication medium qcm, keeping the other P qubits to itself.

3) If $e \neq$ `NULL`, it can perform an attack on the quantum communication medium qcm (see Section 4.3.1).

4) p_2 will perform one of the following enumerated operations, according to the bit r of its pre-shared key PSK_{p_2}:

(i) If $PSK_{p_2,r} = 0$ (`SIFT` round), p_2 performs the operation equivalent to the Measure-and-Resend operation:

- p_2 measures the first of its P qubits in the $\mathbb{Z}$-Basis.
- p_2 keeps the remaining $(P-1)$ qubit(s) in its private quantum register.

(ii) Otherwise, if $PSK_{p_2,r} = 1$ (`CTRL` round), p_2 performs operation equivalent to the Reflect operation:

- p_2 measures its P qubits in the GHZ-Basis (see Section 2.2.4.2).

5) Similarly, regarding the type of the round r, known from the bit r of the pre-shared key PSK_{p_1}, the party p_1 will perform one of the following enumerated operations:

(i) If $PSK_{p_1,r} = 0$ (`SIFT` round), p_1 performs the operation equivalent to the Secret Bit Generation operation:

- p_1 measures all its $(P-1)$ qubit(s) in the $\mathbb{Z}$-Basis.
- The most correlated bits resulting from the measurement of these qubits are added to its sifted key.

(ii) Otherwise, if $PSK_{p_1,r} = 1$ (`CTRL` round), p_1 performs the operation equivalent to the Eavesdropping Checking operation:

- p_1 measures its $(P-1)$ qubit(s) in the $\mathbb{X}$-Basis.

Steps (cont.) ***:***

b) After all the rounds of the protocol be completed, p_1 checks a possible eavesdropping attempt from e on the CTRL rounds and its respective measurements in the $\mathbb{X}$-Basis. If p_1 founds an outcome obtained from a quantum state $|+\rangle$, it aborts the protocol and communicate it to p_2. Then, p_1 and p_2 publicly announce to each other a random sample of the bits obtained in the SIFT rounds, on which they should estimate the QBER $Q_{\mathbb{Z}}$. If the QBER $Q_{\mathbb{Z}} \leq (\eta + \varepsilon)$, the party p_1 and p_2 should abort the protocol. Otherwise, they discard these rounds and the corresponding bits, keeping the remaining bits to compose their sifted keys sk_{p_1} and sk_{p_2}, which may still contain some errors among them.

c) p_1 choose a random Error Correction Code and announce it to p_2 to apply it to the bits of their sifted keys sk_{p_2} to agree on a common reconciled key rk_{p_i}, where $i = 1, 2$.

d) p_1 choose a random Two-Universal Hash Function and announce it to p_2 to be applied to the bits of their reconciled keys rk_{p_i}, extracting the final secret key k_{p_i}, where $i = 1, 2$.

Namely, η represents the amount of noise present in the quantum communication medium. Similarly, ε represents the amount of noise introduced by possible eavesdropping attempts. This parameter is the additional noise we consider acceptable for successful key exchange without compromising the key. Additionally, note that, for Noiseless Scenarios, we have $\eta = 0$.

From the specification of the OW-QKD-GHZ^P protocol, we now claim that BKMPS22-GHZ^P and the OW-QKD-GHZ^P protocols are equivalent in terms of security. Namely, for any attack on the BKMPS22-GHZ^P protocol, there is an attack against the OW-QKD-GHZ^P protocol, such that Alice, Bobs, and Eve cannot distinguish between these two protocols assuming, of course, that the latter does not abort. Therefore, if we prove the security of the OW-QKD-GHZ^P protocol, we will also achieve the security proof of our original BKMPS22-GHZ^P protocol since there can only be more attacks against the OW-QKD-GHZ^P protocol as we show. Note that proving the security of the OW-QKD-GHZ^P protocol involves determining the entropy of Alice's quantum physical system conditioned on Eve's knowledge about it, assuming that the protocol does not abort.

Security Proof against Collective Attacks

Before we demonstrate the complete proof of mentioned claim regarding the reduction of our BKMPS22-GHZ^P protocol, we show some intuition for the simple case with $R = 1$ round. In other words, this case corresponds to having just one signal pulse during the protocol, which results in a valid security proof for the already mentioned Collective Attacks (see Section 3.7.3). Here, Alice prepares a GHZ state with P entangled photons denoted by the quantum state $\phi(0,0) = \left|g^P(0,0)\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \left|\vec{0}\right\rangle_T + |1\rangle_A \left|\vec{1}\right\rangle_T\right)$[5]$= \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\ldots0\rangle_T + |1\rangle_A|1\ldots1\rangle_T\right)$, where A is the Alice's quantum register and T denotes the quantum register representing the photons in transit between the parties (i.e., Alice and Bob(s)). Namely, we assume the photon(s), in the quantum register T, is/are sent to Bob(s), but Eve will attack it/them by performing some

[5]Here, for the sake of simplicity of notation during the proofs, we use interchangeability of vector notation ($\vec{u}$) to represent a quantum physical system of more than one photon/qubit.

unitary operation U evolving the quantum state $\phi(0,0)$ to the following enumerated one:

$$U\big(\phi(0,0)\big) = \frac{1}{\sqrt{2}}\Bigg(|0\rangle_A \otimes \sum_{\vec{b}\in\{0,1\}^{(P-1)}} \sqrt{p(\vec{b}|0)}|\vec{b}\rangle_T |E_{(0,\vec{b})}\rangle_E + \\ + |1\rangle_A \otimes \sum_{\vec{b}\in\{0,1\}^{(P-1)}} \sqrt{p(\vec{b}|1)}|\vec{b}\rangle_T |E_{(1,\vec{b})}\rangle_E\Bigg), \text{ where } P \geq 2. \tag{4.3.2.1.1}$$

In this case, we make no assumptions on the quantum states $|E_{(a,\vec{b})}\rangle_E$ which are part of Eve's private ancilla quantum register E. Each Bob will obtain one photon from the quantum register T during the Quantum Transmission step. However, it changes nothing at this stage, if we look at them as one single party. This "super-Bob" chooses the operation according to the bit of the pre-shared key $\vec{\Theta}_r = \neg PSK_r$ corresponding to the round r of the protocol, where $1 \leq r \leq R$. Namely, if $\vec{\Theta}_r = 1$, "super-Bob" measures each quantum register T, which is equivalent to each Bob separately measuring his respective photon in the quantum register T in the original protocol. Otherwise, Bob reflects back the photons in quantum register T. We may equivalently represent this as "super-Bob" performing a CNOT gate. Each photon of the quantum register T controls this CNOT gate, which has as the target a new ancilla quantum register initialized as $|0\ldots0\rangle_B$. This ancilla quantum register B has one photon for each Bob of the original protocol. Later, "super-Bob" measuring the photons in the ancilla quantum register in the $\mathbb{Z}$-Basis, it will be equivalent to Bobs measuring the photons in the quantum register T. Thus, we can model this physical system as the following pure quantum state:

$$\frac{1}{\sqrt{2}}\Bigg(|0\rangle_A \otimes \sum_{\vec{b}\in\{0,1\}^{(P-1)}} \sqrt{p(\vec{b}|0)}|\vec{b}\rangle_T \big|(\vec{b}\wedge\vec{\Theta}_r)\big\rangle_B |E_{(0,\vec{b})}\rangle_E + \\ + |1\rangle_A \otimes \sum_{\vec{b}\in\{0,1\}^{(P-1)}} \sqrt{p(\vec{b}|1)}|\vec{b}\rangle_T \big|(\vec{b}\wedge\vec{\Theta}_r)\big\rangle_B |E_{(1,\vec{b})}\rangle_E\Bigg), \text{ where } P \geq 2. \tag{4.3.2.1.2}$$

Here, $(\vec{b}\wedge\vec{\Theta}_r)$ means the binary classical logic conjunction (i.e., the AND operation) of each bit of the vector $\vec{b}$ with the bit $\vec{\Theta}_r$, namely $(\vec{b}\wedge\vec{\Theta}_r) = (\vec{b}_1\wedge\vec{\Theta}_r), (\vec{b}_2\wedge\vec{\Theta}_r), ..., (\vec{b}_{(P-1)}\wedge\vec{\Theta}_r)$.

Now, Eve can also attack the returning signal pulses from Bobs, still corresponding to the quantum register T. However, this attack also depends on the quantum state of her private ancilla quantum register E initialized during the first attack. In this case, we assume Alice did not prepare the initial quantum state and send $(P-1)$ photons of that quantum state to Bob. Instead, we can claim that "super-Bob" could have prepared the following quantum state:

$$\frac{1}{\sqrt{2}}\Bigg(\sum_{\vec{b}\in\{0,1\}^{(P-1)}} \sqrt{p(\vec{b}|0)}\big|0,\vec{b}\big\rangle_T \big|(\vec{b}\wedge\vec{\Theta}_r)\big\rangle + \sum_{\vec{b}\in\{0,1\}^{(P-1)}} \sqrt{p(\vec{b}|1)}\big|1,\vec{b}\big\rangle_T \big|(\vec{b}\wedge\vec{\Theta}_r)\big\rangle\Bigg). \tag{4.3.2.1.3}$$

Next, "super-Bob" sends to Alice the photons of the quantum register T, which now consists of P photons. In this previous quantum state, we assume Eve has control only of the classical probability values $p(\vec{b}|a)$, which are related to the quantum state itself. However, note that Eve did not entangle this quantum state with her quantum physical system at this point.

Then, Eve intercepts the photons of the quantum register T and attacks the protocol using the unitary operator $\left(I_{T_0} \otimes U_R\right) \cdot V$, where the unitary operator V is defined by the action $V|a,\vec{b}\rangle = |a,\vec{b}\rangle_T |E_{(a,\vec{b})}\rangle$. Note that T_0 is the left-most photon in the quantum register T, namely Alice's quantum physical system. In this attack, Eve resends all the P photons to Alice. As obvious, it is clear that the resulting quantum state is identical to the previous one. Of course, Eve does not need to attack this one-way protocol using the previous unitary operator V. But for any attack on a real SQCKA protocol, an equivalent attack exists for this protocol. Thus, if we can prove the security of this protocol, we can also prove the security of the SQCKA protocol since it will include any of these attacks. In general, Eve may attack all P photons using a general unitary operator U', which may not consist of the above V unitary operator. In fact, this unitary operation U' evolves the quantum state to the following quantum state:

$$\begin{aligned} U'\left(\phi(a,\vec{b})\right) &= U'\left|a,\vec{b}\right\rangle = \\ &= \frac{1}{\sqrt{2}}\left(\sum_{a\in\{0,1\}} \sum_{\vec{b}\in\{0,1\}^{(P-1)}} \sqrt{p(\vec{b}|a)}\left|(\vec{b}\wedge\vec{\Theta}_r)\right\rangle_B \sum_{\vec{c}\in\{0,1\}^P} |\vec{c}\rangle_A |F^{\vec{c}}_{(a,\vec{b})}\rangle_E \right). \end{aligned} \tag{4.3.2.1.4}$$

Note that to derive this formulation, we simply used the abstract mathematical definition $U'\left|a,\vec{b}\right\rangle = \sum_{\vec{c}\in\{0,1\}^P} |\vec{c},F^{c}_{(a,\vec{b})}\rangle$ after which the P photons in the quantum physical system $|\vec{c}\rangle$ are sent to Alice. However, this one-way quantum cryptographic protocol depends on the bit $\vec{\Theta}_r$ being chosen *before* Bob prepares the quantum state. This protocol behaves differently from the $\texttt{OW-QKD-GHZ}^P$ protocol, where Bob can choose the bit $\vec{\Theta}_r$ after preparing the quantum state. This detail is important since we actually want to prove the security of the one-way case in the event of Eve preparing the quantum state. Clearly, if Eve attacks the protocol by also preparing the quantum system, it cannot depend on the secret bit $\vec{\Theta}_r$ and its use must come up after the legitimate parties, namely Alice and "super-Bob", receive the quantum system.

Thus, we have one more reduction of the above "half-way" one-way QKD protocol to the $\texttt{OW-QKD-GHZ}^P$ protocol. Now, consider Bob prepares the quantum state $\phi(0,0) = \left|g^{(2P-1)}(0,0)\right\rangle$ and sends P photons of that quantum state to Alice, keeping $(P-1)$ photons private. Here, this quantum state does not depend on the bit $\vec{\Theta}_r$. In particular, Eve attacks the protocol using the unitary operation U', which evolves the quantum state to the following enumerated one:

$$\begin{aligned} U'\left(\phi(a,\vec{b})\right) &= U'\left|a,\vec{b}\right\rangle = \\ &= \frac{1}{\sqrt{2}}\left(\sum_{a\in\{0,1\}} \sum_{\vec{b}\in\{0,1\}^{(P-1)}} \sqrt{p(\vec{b}|a)}\left|\vec{b}\right\rangle_B \sum_{\vec{c}\in\{0,1\}^P} |\vec{c}\rangle_A |F^{\vec{c}}_{a,\vec{b}}\rangle_E \right). \end{aligned} \tag{4.3.2.1.5}$$

Then, "super-Bob" picks the action of Measure-and-Resend or Reflect, denoted by $\vec{\Theta}_r$, which corresponds to all Bobs performing the same action in our original protocol. Obviously, if $\vec{\Theta}_r = 1$, the parties will use the current round of the protocol to generate a secret bit. In this case, the Equation (4.3.2.1.4) ends up being equal to Equation (4.3.2.1.5). If $\vec{\Theta}_r = 0$, Bob will measure the photons of his quantum register in the $\mathbb{X}$-Basis, from which we can rewrite the

previous Equation (4.3.2.1.5) with an unitary operator U'' as we demonstrate bellow:

$$\begin{aligned} U''\Big(U'\big(\phi(a,\vec{b})\big)\Big) &= U''\Big(U'\big|a,\vec{b}\big\rangle\Big) = \\ &= \frac{1}{\sqrt{2^{(P-1)}}}|\vec{+}\rangle_B \otimes \left(\sum_{a\in\{0,1\}} \sum_{\vec{b}\in\{0,1\}^{(P-1)}} \sqrt{p(\vec{b}|\vec{a})} \sum_{\vec{c}\in\{0,1\}^P} |\vec{c}, F^{\vec{c}}_{(\vec{a},\vec{b})}\rangle \right) + \\ &\quad + \sum_{\vec{x}\neq\vec{+}} |\vec{x}\rangle_B \otimes |\psi_{\vec{x}}\rangle_{AE}, \text{ where } P \geq 2. \end{aligned} \tag{4.3.2.1.6}$$

If "super-Bob" measures and observes all the individual superposed quantum states $|+\rangle$'s from the general quantum state $|\vec{+}\rangle_B$ in his private quantum register, this general quantum state will collapse exactly to the one which is expressed in Equation (4.3.2.1.4). Otherwise, if he observes anything else, the OW-QKD-GHZ^P protocol aborts. As obvious, the probability for "super-Bob" does not abort this protocol is only $\frac{1}{2^{(P-1)}}$. However, we are only interested to prove that OW-QKD-GHZ^P protocol is secure and not bound the key rate. Thus, we will not argue if the OW-QKD-GHZ^P protocol is efficient, which it most certainly is not. However, if we can prove the security of the OW-QKD-GHZ^P protocol, then the security of the "middle" one-way protocol also holds. Here, we can make such a claim since we can translate any attack against that protocol to an attack on the OW-QKD-GHZ^P protocol. Therefore, this mathematical deduction automatically also implies the security of our original BKMPS22-GHZ^P protocol.

Then, we show this assumption holds for any number R of rounds of the protocol and respective light pulses. First, we demonstrate the reduction to the "middle-ground" one-way protocol, where the preparation of the quantum state of "super-Bob" depends on knowing $\vec{\Theta}_r$.

In our BKMPS22-GHZ^P protocol, Alice prepares the quantum state modeled as follows:

$$\phi(0,0) = \big|g^P(0,0)\big\rangle^{\otimes R} = \frac{1}{\sqrt{2^R}} \sum_{\vec{a}\in\{0,1\}^R} \big|\overbrace{a_1\dots a_1}^{P}\big\rangle\big|\overbrace{a_2\dots a_2}^{P}\big\rangle\dots\big|\overbrace{a_R\dots a_R}^{P}\big\rangle, \tag{4.3.2.1.7}$$

where $P \geq 2$ and $R \geq 1$.

Then, by permuting sub-spaces of the resulting quantum state, we may also rewrite it as:

$$|\psi_0\rangle = \frac{1}{\sqrt{2^R}} \sum_{\vec{a}\in\{0,1\}^R} |a_1 a_2 \dots a_R\rangle_A |\overbrace{a_1\dots a_1}^{(P-1)}\rangle_{T_1} |\overbrace{a_2\dots a_2}^{(P-1)}\rangle_{T_2} \dots \big|\overbrace{a_R\dots a_R}^{(P-1)}\big\rangle_{T_R} \tag{4.3.2.1.8}$$

where $P \geq 2$ and $R \geq 1$.

Next, Eve will first attack this collection of quantum registers $T = T_1 T_2 \dots T_R$. Then, she sends the resulting quantum state to "super-Bob", which we can define as shown following:

$$\frac{1}{\sqrt{2^R}} \sum_{\vec{a}\in\{0,1\}^R} |\vec{a}\rangle_A \otimes \sum_{\vec{b}\in\{0,1\}^{(P-1)\cdot R}} \sqrt{p(\vec{b}|\vec{a})} |\vec{b}_1\rangle_{T_1} |\vec{b}_2\rangle_{T_2} \dots |\vec{b}_R\rangle_{T_R} |E_{(\vec{a},\vec{b})}\rangle \tag{4.3.2.1.9}$$

where $P \geq 2$ and $R \geq 1$.

Here, for simplicity of the equation, we have $|\vec{a}\rangle = |a_1 a_2 \dots a_R\rangle$, which corresponds to the photons of all rounds held by Alice. The same idea also applies to the T quantum registers held by all Bobs for all rounds of the protocol, i.e., $|\vec{b}_r\rangle = |\vec{b}_r^1 \vec{b}_r^2 \dots b_r^{(\vec{P}-1)}\rangle_{T_r}$, with $1 \leq r \leq R$.

At this point, all Bobs choose the binary pre-shared key $\vec{\Theta} \in \{0,1\}^R$. Then, if $\vec{\Theta}_r = 1$, they will measure-and-resend the quantum register T_r for the current round, where $1 \leq r \leq R$. Otherwise, all Bobs reflect this individual quantum register T_r. As before, we simulate this behavior by using CNOT gates, therefore evolving the quantum state into the following one:

$$|\psi_1\rangle = \frac{1}{\sqrt{2^R}} \sum_{\vec{a}\in\{0,1\}^R} |\vec{a}\rangle_A \sum_{\vec{b}\in\{0,1\}^{(P-1)\cdot R}} \sqrt{p(\vec{b}|\vec{a})} |\vec{b_1}\rangle_{T_1} |\vec{b_2}\rangle_{T_2} \dots |\vec{b_R}\rangle_{T_R} \\ \left|(\vec{b_1} \wedge \vec{\Theta_1})\right\rangle_B \left|(\vec{b_2} \wedge \vec{\Theta_2})\right\rangle_B \dots \\ \dots \left|(\vec{b_R} \wedge \vec{\Theta}_r)\right\rangle_B |E_{(\vec{a},\vec{b})}\rangle \\ \text{where } P \geq 2 \text{ and } R \geq 1. \tag{4.3.2.1.10}$$

In this previous equation, we mean $(\vec{b_r} \wedge \vec{\Theta}_r) = (\vec{b_r^1} \wedge \vec{\Theta}_r), (\vec{b_r^2} \wedge \vec{\Theta}_r), \dots, (b_r^{(\vec{P}-1)} \wedge \vec{\Theta}_r)$.

Afterward, the quantum register T will return to Eve, who is free to attack all the light pulses again using a unitary operator U_R. This unitary operator acts on all the R quantum registers T and Eve's private ancilla quantum register E from the first attack. Then, after Eve attach this seconds probe, the quantum registers T return to Alice. Let $|\psi_2\rangle = I_A \otimes I_B \otimes U_R |\psi_1\rangle$ denote the final joint quantum state before Alice perform the respective measurements on her side.

Now, we demonstrate that there is an attack against the "middle-ground" one-way protocol, which also produces the same joint quantum state $|\psi_2\rangle$. For this different protocol variant, Bob chooses randomly the pre-shared key $\vec{\Theta}$ and prepares the following quantum state:

$$|\delta_1\rangle = \frac{1}{\sqrt{2^R}} \sum_{\vec{a}\in\{0,1\}^R} |\vec{a}\rangle \sum_{\vec{b}\in\{0,1\}^{(P-1)\cdot R}} \sqrt{p(\vec{b}|\vec{a})}\, |\vec{b_1}\rangle_{T_1} |\vec{b_2}\rangle_{T_2} \dots |\vec{b_R}\rangle_{T_R} \\ \left|(\vec{b_1} \wedge \vec{\Theta_1})\right\rangle_B \left|(\vec{b_2} \wedge \vec{\Theta_2})\right\rangle_B \dots \\ \dots \left|(\vec{b_R} \wedge \vec{\Theta}_r)\right\rangle_B \\ \text{where } P \geq 2 \text{ and } R \geq 1. \tag{4.3.2.1.11}$$

In this case, $p(\vec{b}, \vec{a})$ is a classical probability distribution chosen by Eve, who has some partial control over Bobs' devices. However, note this previous quantum state is not entangled with Eve's private ancilla quantum register. In particular, the quantum register T is sent to Alice but intercepted by Eve, who may attack the protocol using the unitary operator $(I_A \otimes U_R) \cdot R_w$, where $R_w|\vec{a}, \vec{b}\rangle = |\vec{a}, \vec{b}, E_{(\vec{a},\vec{b})}\rangle$. Clearly, this represents a unitary operation, and the resulting quantum state is identical to the quantum state $|\psi_2\rangle$ from the real BKMPS22-GHZ^P protocol.

Finally, we demonstrate that for every attack on the "middle-ground" one-way protocol, there is an equivalent attack on OW-QKD-GHZ^P. For now, consider the "middle-ground" protocol. After Bob prepares the physical quantum system described above, Eve may attack using a general unitary operator U. This unitary operator acts on the entire quantum register T, including the quantum register T_0 traveling to Alice. This unitary operation U may or not

be of the form consisting of R_w. After this attack, the quantum state becomes the following:

$$|\sigma_1\rangle = \frac{1}{\sqrt{2^R}} \sum_{\vec{a}\in\{0,1\}^R} \sum_{\vec{b}\in\{0,1\}^{R\cdot(P-1)}} \sqrt{p(\vec{b}|\vec{a})} \left|(\vec{b_1} \wedge \vec{\Theta}_1)\right\rangle_B \left|(\vec{b_2} \wedge \vec{\Theta}_2)\right\rangle_B \ldots \\ \ldots \left|(\vec{b_R} \wedge \vec{\Theta}_r)\right\rangle_B \sum_{\vec{c}\in\{0,1\}^{(P-1)\cdot R}} |\vec{c}, e^{\vec{c}}_{(\vec{a},\vec{b})}\rangle \quad (4.3.2.1.12)$$

where $P \geq 2$ and $R \geq 1$.

Here, $\vec{b_r}$ are binary strings of length $(P-1)$ and $\vec{c}$ is a binary string of length $(P-1)\cdot R$. We also use the abstract action of the unitary operator U to be $U|\vec{a},\vec{b}\rangle = \sum_{\vec{c}\in\{0,1\}^{(P-1)\cdot R}} |\vec{c}, e^{\vec{c}}_{(\vec{a},\vec{b})}\rangle$. Note that these quantum states $|\vec{c}, e^{\vec{c}}_{(\vec{a},\vec{b})}\rangle$ are not necessarily normalized or orthogonal. In the BKMPS22-GHZ^P protocol, the resulting quantum state would have been the following one:

$$|\tau_1\rangle = \frac{1}{\sqrt{2^R}} \sum_{\vec{a}\in\{0,1\}^R} \sum_{\vec{b}\in\{0,1\}^{R\cdot(P-1)}} \sqrt{p(\vec{b}|\vec{a})} |\vec{b_1}\rangle_B |\vec{b_2}\rangle_B \ldots |\vec{b_R}\rangle_B \sum_{\vec{c}\in\{0,1\}^{(P-1)\cdot R}} |\vec{c}, e^{\vec{c}}_{(\vec{a},\vec{b})}\rangle, \quad (4.3.2.1.13)$$

where $P \geq 2$ and $R \geq 1$.

This quantum state is independent of the secret bits $\vec{\Theta}_r$, where $1 \leq r \leq R$. We claim that, if Bob measures each of his $(P-1)$ photon(s) in the r^{th} quantum register for all $\vec{\Theta}_r = 0$ in the $\mathbb{X}$-Basis and conditioned on him receiving the quantum state $|\vec{+}\rangle$, the post measured quantum state will be of the form $|\phi_1\rangle$. Otherwise, if Bob receives a quantum state different from $|\vec{+}\rangle$, he aborts the protocol. This observation is clear since by permuting the quantum systems, so that $\vec{\Theta} = \left[0, 0, \ldots, 0, 1, 1, \ldots, 1\right]$, with k bits $\vec{\Theta}_r$ equal to 0 on the left side and the remaining $(R-k)$ ones equal to 1 on the right side, we end up having the following quantum state:

$$|\sigma_1\rangle \cong \overbrace{|\vec{0}\rangle_B |\vec{0}\rangle_B \ldots |\vec{0}\rangle_B}^{k \text{ quantum register(s)}} \sum_{\vec{b}\in\{0,1\}^{(R-k)\cdot(P-1)}} |\vec{b}_{(k+1)}\rangle_B |\vec{b}_{(k+2)}\rangle_B \ldots |\vec{b}_R\rangle_B \quad (4.3.2.1.14)$$

where $R \geq 1$ and $1 \leq k \leq R$.

Then, if we change the basis in the first k quantum register(s) in Bob's possession, for which we had $\vec{\Theta}_r$ equal to 0 respectively, we end up having the following enumerated quantum state:

$$|\tau_1\rangle \cong \overbrace{|\vec{+}\rangle_B |\vec{+}\rangle_B \ldots |\vec{+}\rangle_B}^{k \text{ quantum register(s)}} \left(\sum_{\substack{\vec{a}\in\{0,1\}^R \\ \vec{b}\in\{0,1\}^{(R-k)\cdot(P-1)}}} |\vec{b}_{(k+1)}\rangle_B |\vec{b}_{(k+2)}\rangle_B \ldots |\vec{b}_R\rangle_B \sum_{\vec{c}\in\{0,1\}^{(P-1)\cdot R}} |\vec{c}, e^{\vec{c}}_{(\vec{a},\vec{b})}\rangle \right) \quad (4.3.2.1.15)$$

$+ |\tau'\rangle_{ABE}$, where $R \geq 1$ and $1 \leq k \leq R$.

Here, $|\tau'\rangle$ has no component in the first k quantum register(s) in the Bob's side with the form $|\vec{+}\rangle$. In other words, it is the post-measurement quantum state with the protocol aborting since Bob would have measured a quantum state $|-\rangle$. Clearly, we can see that this post-measured quantum state is equal to the one got in the "middle-ground" QKD protocol.

Therefore, we have shown, for every attack on the BKMPS22-GHZ^P protocol, from which we want to the respective security, there is an equivalent attack on the OW-QKD-GHZ^P protocol. Additionally, we show the latter protocol induces the same amount of noise and executes on the same quantum systems for all the legitimate parties. In this case, we always assume that the OW-QKD-GHZ^P protocol does not abort. In particular, there may be more attacks against the OW-QKD-GHZ^P protocol different from the ones studied in this analysis. However, given a certain observed amount of noise, by proving the security of the OW-QKD-GHZ^P protocol, the security of the BKMPS22-GHZ^P protocol must also follow. Note that there is no attack Eve can do which would cause OW-QKD-GHZ^P protocol to always abort except the DoS Attack (see Section 3.6.2).

Now, we prove the security of the OW-QKD-GHZ^P protocol in the asymptotic setting. More specifically, we assume that, instead of Bob preparing the physical quantum system, will be Eve to prepare it. Then, she sends the respective quantum states to Alice and Bob, keeping a private ancilla quantum register to herself. By letting Alice and Bob permute their physical quantum systems, we may assume that the quantum state prepared by Eve is i.i.d (independently and identically distributed) of the form $|\phi\rangle^{\otimes R}$ for sufficiently large R with $|\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$. Here, the Hilbert Space $\mathcal{H}_A$ is of dimension 2^P and the Hilbert Space $\mathcal{H}_B$ is of dimension $2^{(P-1)}$. Ideally, the preparation of the quantum state $|\phi\rangle = \left|g^{(2P-1)}(0,0)\right\rangle$ is independent of Eve. But it is obvious that Eve can also prepare anything in its place. Note that in the OW-QKD-GHZ^P protocol, we cannot test the fidelity of the quantum state. Normally, we can do this fidelity test by measuring and testing all $(2P-1)$ photons in the $\mathbb{X}$-Basis while looking at the parity of the outcomes. Indeed, the OW-QKD-GHZ^P protocol actually aborts if Bob measures a single quantum state $|-\rangle$ on some of those photons. Therefore, we must prove the security of this protocol being conditioned on Bob always observing the quantum state $|+\rangle$ if he chooses to measure it on the $\mathbb{X}$-Basis. This detail simulates the weakness of the OW-QKD-GHZ^P protocol, where Bob, who is a "classical entity", cannot perform all the required measurements.

Security from Key Generation and Parameter Estimation

For the parameter estimation step and generation of the sifted key, Alice and Bobs perform measurements in the $\mathbb{Z}$-Basis on their respective photons. During the *cut-and-choose*[6] procedure, a fixed number of $p_{PE} \cdot R$ randomly chosen rounds, out of the total number of R rounds, is used to exchange, via an authenticated classical channel, the classical outcomes obtained by the parties. By doing this, Alice and Bobs evaluate the experimentally observed probabilities $p_{\vec{i},\vec{j}}$ (see Equation (4.3.2.1.18)), for the parameter estimation step and calculation of the QBER $Q_{\mathbb{Z}}$. They also verify that $p_{\vec{i},\vec{j}}$ is not a product distribution, i.e., that the classical outcomes obtained by Alice and Bobs are not uncorrelated (see bellow for more details).

[6]The *cut-and-choose* is a protocol in which one party tries to convince other parties that some data the earlier sent to the former ones was honestly constructed according to an agreed upon method, such as occurring during the Parameter Estimation step.

Security from Eavesdropping Checking with GHZ States

Now, we analyze the case of the OW-QKD-GHZ^P protocol in which all Bobs measure in the $\mathbb{X}$-Basis, each obtaining the $|+\rangle$ result. Let us first consider a single round in a total of R rounds. This case of the protocol consists of four steps. Once again, we will consider all $(P-1)$ Bobs in the protocol as a single "super-Bob" for simplicity. These steps are described bellow.

Step 1: "Super-Bob" prepares a quantum state of $(2P-1)$ photons with the following form:

$$\left|g^{(2P-1)}(0,0)\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes(2P-1)} + |1\rangle^{\otimes(2P-1)}\right) \equiv \left|\text{GHZ}_{(2P-1)}\right\rangle, \text{ where } P \geq 2\ . \quad (4.3.2.1.16)$$

Then, "super-Bob" divides the photons of the previous quantum state into two parts. Namely, P photons of that quantum state are sent to Alice, while the remaining $(P-1)$ photons are kept private by himself. Therefore, we can re-write the previous quantum state as follows:

$$\left|\text{GHZ}_{(2P-1)}\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\vec{0}\rangle_A|\vec{0}\rangle_B + |\vec{1}\rangle_A|\vec{1}\rangle_B\right)\ . \quad (4.3.2.1.17)$$

Once again, we use the vector notation to denote strings of bits whose respective labels of the kets determine their lengths. Here, A and B correspond to P and $(P-1)$ photons of the physical systems of Alice and "super-Bob", respectively. Due to inevitable implementation imperfections, "super-Bob" prepares the following quantum state rather than the previous:

$$|\Psi\rangle_{AB} = \sum_{\vec{j},\vec{k}} \sqrt{p_{\vec{j},\vec{k}}}\, e^{i\theta_{\vec{j},\vec{k}}} |\vec{j}\rangle_A |\vec{k}\rangle_B, \text{ such that } \sum_{\vec{j},\vec{k}} p_{\vec{j},\vec{k}} = 1\ . \quad (4.3.2.1.18)$$

Note that, in order for the protocol to have any potential use, the probability distribution from Equation (4.3.2.1.18) cannot be the product one, i.e., $p_{\vec{j},\vec{k}} \neq p^A_{\vec{j}} \cdot p^B_{\vec{k}}$. Otherwise, the quantum state $|\Psi\rangle_{AB}$ would factor, and "super-Bob" and Alice would be uncorrelated.

Step 2: Upon "super-Bob" sending photons to Alice, Eve entangles her photons with them, and the overall quantum state of the quantum physical system ABE looks like the following one:

$$|\Psi\rangle_{ABE} = \sum_{\vec{j},\vec{k}} \sqrt{q_{\vec{j}}}\sqrt{p_{\vec{j},\vec{k}}}\, e^{i\left(\chi_{\vec{j}}+\theta_{\vec{j},\vec{k}}\right)} |\vec{j}\rangle_A |\vec{k}\rangle_B |E_{\vec{j}}\rangle_E, \text{ such that } \sum_{\vec{j},\vec{k}} q_{\vec{j}} \cdot p_{\vec{j},\vec{k}} = 1\ . \quad (4.3.2.1.19)$$

Now, we can make several comments about this mathematical formulation:

1. Note that Eve entangles her photons directly *only* to Alice's P photons. Recall that the $(P-1)$ photons belonging to "super-Bob" are always kept private. Thus, if certain $\vec{k}_0$ is absent from the initial quantum state $|\Psi\rangle_{AB}$ prepared by "super-Bob", i.e., $(\forall\vec{k})p_{\vec{j},\vec{k}_0} = 0$, then it will be absent from the eavesdropped quantum state $|\Psi\rangle_{ABE}$ as well.

2. Additionally, we can absorb the phases $e^{i\chi_{\vec{j}}}$ of Equation (4.3.2.1.19) into the quantum state $|E_{\vec{j}}\rangle_E$, and make the substitution $q_{\vec{j}} \cdot p_{\vec{j},\vec{k}} \longmapsto p_{\vec{j},\vec{k}}$ to simplify this formulation.

3. The "rescaled" probability distribution $p_{\vec{j},\vec{k}}$ can now be defined as a product one, i.e., it is now possible that $p_{\vec{j},\vec{k}} = p^A_{\vec{j}} \cdot p^B_{\vec{k}}$. This product possibility is for the case in which the outcomes obtained by Bobs are completely uncorrelated with those obtained by Alice. In practice, this possibility comes from Eve sending P different photons than ones labeled by A, prepared in an appropriate quantum state, possibly entangled with other quantum physical systems kept by Eve. Although our analysis is general, sending different photons to Alice is equivalent to swapping their quantum state with the one from the photons labeled initially by A. Finally, the crucial consequence of the possibility of completely "de-correlate" Alice with Bobs in the original protocol is that Alice's projection onto the quantum state $\left|\text{GHZ}_P\right\rangle$ with probability 1 (see Step 4) does not guarantee the generation of any key, let alone secret. Note that Eve can send photons to Alice that are uncorrelated with those of Bobs, prepared in the quantum state $\left|\text{GHZ}_P\right\rangle$. Therefore, we must include the outcome results of the measurements in the $\mathbb{Z}$-Basis in the secret key estimation.

Hereupon, the Equation (4.3.2.1.19) can now be further rewritten as follows:

$$|\Psi\rangle_{ABE} = \sum_{\vec{j},\vec{k}} \sqrt{p_{\vec{j},\vec{k}}} e^{i\theta_{\vec{j},\vec{k}}} |\vec{j}\rangle_A |\vec{k}\rangle_B |E_{\vec{j}}\rangle_E, \text{ such that } \sum_{\vec{j},\vec{k}} p_{\vec{j},\vec{k}} = 1 \,. \tag{4.3.2.1.20}$$

Afterward, Eve proceeds to forward those eavesdropped photons to Alice.

Step 3: Then, Bobs measure the incoming photons in the $\mathbb{X}$-Basis. Recall, we are interested in the outcome results $|\vec{+}\rangle \equiv |+\rangle^{\otimes(P-1)}$, which is obtained with the following probability:

$$\begin{aligned} p_{\vec{+}} = ||_B\langle\vec{+}|\Psi\rangle_{ABE}||^2 &= \frac{1}{2^{(P-1)}} \sum_{\vec{j},\vec{k},\vec{\ell},\vec{m}} \sqrt{p_{\vec{j},\vec{k}} p_{\vec{\ell},\vec{m}}}\; e^{i\left(\theta_{\vec{\ell},\vec{m}} - \theta_{\vec{j},\vec{k}}\right)}\, {}_A\langle \vec{j} | \vec{\ell} \rangle_A\, {}_E\langle E_{\vec{j}} | E_{\vec{\ell}} \rangle_E \\ &= \frac{1}{2^{(P-1)}} \sum_{\vec{j},\vec{k},\vec{m}} \sqrt{p_{\vec{j},\vec{k}} p_{\vec{j},\vec{m}}}\; e^{i\left(\theta_{\vec{j},\vec{m}} - \theta_{\vec{j},\vec{k}}\right)} \,. \end{aligned} \tag{4.3.2.1.21}$$

The last equality is a consequence of ${}_A\langle \vec{j} | \vec{\ell} \rangle_A = \delta_{\vec{j},\vec{m}}$[7] and ${}_E\langle E_{\vec{j}} | E_{\vec{j}} \rangle_E = 1$. The calculation of the probability $p_{\vec{+}}$ is straightforward. In this case, we only note that $(\forall \vec{k})\langle\vec{+}|\vec{k}\rangle = \frac{1}{\sqrt{2^{(P-1)}}}$.

Upon performing the measurement and obtaining the quantum state $|+\rangle^{\otimes(P-1)}$ as result, all Bobs will collapse the quantum state shared by Alice and Eve to the following one:

$$\begin{aligned} |\Psi\rangle_{ABE} \longrightarrow |\Psi\rangle_{AE} &= \frac{{}_B\langle\vec{+}|\Psi\rangle_{ABE}}{||_B\langle\vec{+}|\Psi\rangle_{ABE}||} \\ &= \frac{1}{\sqrt{2^{(P-1)} p_{\vec{+}}}} \left[\sum_{\vec{j}\in\{0,1\}^P} \left(\sum_{\vec{k}\in\{0,1\}^{(P-1)}} \sqrt{p_{\vec{j},\vec{k}}} e^{i\theta_{\vec{j},\vec{k}}} \right) |\vec{j}\rangle_A |E_{\vec{j}}\rangle_E \right] \\ &= \frac{1}{\sqrt{2^{(P-1)} p_{\vec{+}}}} \sum_{\vec{j}\in\{0,1\}^P} \alpha_{\vec{j}} |\vec{j}\rangle_A |E_{\vec{j}}\rangle_E \,. \end{aligned} \tag{4.3.2.1.22}$$

Regarding this equation, we have the equality $\alpha_{\vec{j}} \equiv \sum_{\vec{k}\in\{0,1\}^{(P-1)}} \sqrt{p_{\vec{j},\vec{k}}} e^{i\theta_{\vec{j},\vec{k}}}$. In particular, $\alpha_{\vec{0}} = \sum_{\vec{k}\in\{0,1\}^{(P-1)}} \sqrt{p_{\vec{0},\vec{k}}} e^{i\theta_{\vec{0},\vec{k}}}$ and $\alpha_{\vec{1}} = \sum_{\vec{k}\in\{0,1\}^{(P-1)}} \sqrt{p_{\vec{1},\vec{k}}} e^{i\theta_{\vec{1},\vec{k}}}$, for $\vec{j} = \vec{0}$ and $\vec{j} = \vec{1}$, respectively.

[7] This equality is also known as Kronecker Delta function in Quantum Mechanics.

Step 4: Now, Alice measures the observable $\hat{A} = |\text{GHZ}_P\rangle_A\langle\text{GHZ}_P|$ on her P photons. The probability of obtaining the outcome $\vec{1}$ (i.e., of projecting onto the quantum state $|\text{GHZ}_P\rangle_A$) is:

$$p_{\vec{1}} = p_{GHZ} = ||_A\langle\text{GHZ}_P|\Psi\rangle_{AE}||^2 = {}_{AE}\langle\Psi|\text{GHZ}_P\rangle_A\langle\text{GHZ}_P|\Psi\rangle_{AE} \, . \tag{4.3.2.1.23}$$

Additionally, we have that ${}_A\langle\vec{j}|\text{GHZ}_P\rangle_A = \frac{\left(\delta_{\vec{j},\vec{0}}+\delta_{\vec{j},\vec{1}}\right)}{\sqrt{2}}$. Thus, we are left with the following four terms, given by $(\vec{j},\vec{k}) \in \left\{(\vec{0},\vec{0}),(\vec{0},\vec{1}),(\vec{1},\vec{0}),(\vec{1},\vec{1})\right\}$. Therefore, we equivalently have:

$$p_{GHZ} = \frac{1}{2^P p_{\vec{+}}}\left[|\alpha_{\vec{0}}|^2 \, {}_E\langle E_{\vec{0}}|E_{\vec{0}}\rangle_E + |\alpha_{\vec{1}}|^2 \, {}_E\langle E_{\vec{1}}|E_{\vec{1}}\rangle_E + 2\text{Re}\left(\alpha^*_{\vec{0}}\alpha_{\vec{1}} \, {}_E\langle E_{\vec{0}}|E_{\vec{1}}\rangle_E\right)\right] \, . \tag{4.3.2.1.24}$$

Since ${}_E\langle E_{\vec{0}}|E_{\vec{0}}\rangle_E = {}_E\langle E_{\vec{1}}|E_{\vec{1}}\rangle_E = 1$, we finally have the following simplified equation:

$$p_{GHZ} = \frac{1}{2^P p_{\vec{+}}}\left[|\alpha_{\vec{0}}|^2 + |\alpha_{\vec{1}}|^2 + 2\text{Re}\left(\alpha^*_{\vec{0}}\alpha_{\vec{1}} \, {}_E\langle E_{\vec{0}}|E_{\vec{1}}\rangle_E\right)\right] \, . \tag{4.3.2.1.25}$$

Note that in the above equation, all parameters, apart from ${}_E\langle E_{\vec{0}}|E_{\vec{1}}\rangle_E$, are observable quantities. Namely, we obtain the probability p_{GHZ} by projecting the final quantum state $|\Psi\rangle_{AE}$ onto the GHZ-like quantum state $|\text{GHZ}_P\rangle_A$, while the probabilities $p_{\vec{+}}$, $\alpha_{\vec{0}}$ and $\alpha_{\vec{1}}$ are functions of the probabilities $p_{\vec{j},\vec{k}}$ that are obtained during the Parameter Estimation step, corresponding to measurements in the $\mathbb{Z}$-Basis. Thus, we use Equation (4.3.2.1.25) to evaluate ${}_E\langle E_{\vec{0}}|E_{\vec{1}}\rangle_E$, which occurs in the secure key estimation, in Equations (4.3.2.2.4) and (4.3.2.2.5).

Additionally, note that in the absence of noise and eavesdropping, "super-Bob" prepares a "perfect" quantum state. Namely, we should obtain the following enumerated quantities:

$$p_{\vec{0},\vec{0}} = p_{\vec{1},\vec{1}} = \frac{1}{2}, \; \theta_{\vec{0},\vec{0}} = \theta_{\vec{1},\vec{1}} = 0 \left(\text{i.e., } \alpha_{\vec{0}} = \alpha_{\vec{1}} = \frac{1}{\sqrt{2}}\right), \text{ and } {}_E\langle E_{\vec{0}}|E_{\vec{1}}\rangle_E = 1 \, . \tag{4.3.2.1.26}$$

Then, since in this case, we have the equality $p_{GHZ} = \frac{1}{2^{(P-1)}p_{\vec{+}}}$, and in order to have the probability $p_{GHZ} = 1$, it follows that $p_{\vec{+}} = \frac{1}{2^{(P-1)}}$, which can be straightforwardly obtained from Equation (4.3.2.1.21), by using the previous conditions mentioned in Equation (4.3.2.1.26).

Note also that if $p_{GHZ} = 1$, then we have $|\Psi\rangle_{AE} = |GHZ\rangle_A|E\rangle_E$ (in fact, this equality is true for any arbitrary quantum state $|\chi\rangle_A$, not just for the entangled quantum state $|GHZ\rangle_A$). But as noted in the comment 3. of Step 2, this observation alone does not mean that the parties can establish a secret key. Therefore, we must also include the results of the measurements in the $\mathbb{Z}$-Basis in the secret key analysis, and not just for the Parameter Estimation step.

4.3.2.2 Key Rate Calculation

Now, we can see how to estimate the key rate of our original BKMPS22 Protocol. In particular, the secure key in the asymptotic scenario is bounded by the following mathematical expression:

$$\kappa \geq S(A|E) - \min_j \max_k H(A_j|B_k) \, . \tag{4.3.2.2.1}$$

The latter term, $H(A_j|B_k)$, which corresponds to the Shannon Entropy, is nothing more than a simple mathematical function of the probabilities $p_{\vec{j},\vec{k}}$, obtained during the Parameter

Estimation step, in which the measurements are made in the $\mathbb{Z}$-Basis. Here, we minimize j in the second term because Alice chooses her photon such the secure key rate κ is as big as possible. However, Alice should actually choose the photon most correlated with all $(P-1)$ photons from Bobs to represent her secret key. For this reason, we take the maximization on k of Shannon Entropies over all Bobs to take the worst-case scenario of the secure key rate.

Here, we bound the Von Neumann Entropy, $S(A|E)$. Following the measurements made by Alice and Bob in the $\mathbb{Z}$-Basis on the initial quantum state from Equation (4.3.2.1.17), we have:

$$|\Psi\rangle_{ABE} = \sum_{\vec{j},\vec{k}} \sqrt{p_{\vec{j},\vec{k}}}\, e^{i\theta_{\vec{j},\vec{k}}} |\vec{j}\rangle_A |\vec{k}\rangle_B |E_{\vec{j}}\rangle_E, \text{ such that } \sum_{\vec{j},\vec{k}} p_{\vec{j},\vec{k}} = 1\ . \tag{4.3.2.2.2}$$

Then, by tracing out the photons in Bob's quantum register B, as well as all but the first of Alice's photons from her quantum register A, we get the following mathematical expression:

$$|0\rangle\langle 0|_{A_1} \otimes \left[\sum_{\vec{j}_0}\left(\sum_{\vec{k}} p_{\vec{j}_0,\vec{k}}\right)|E_{\vec{j}_0}\rangle\langle E_{\vec{j}_0}|_E\right] + |1\rangle\langle 1|_{A_1} \otimes \left[\sum_{\vec{j}_1}\left(\sum_{\vec{k}} p_{\vec{j}_1,\vec{k}}\right)|E_{\vec{j}_1}\rangle\langle E_{\vec{j}_1}|_E\right]\ . \tag{4.3.2.2.3}$$

In this equation, A_1 represents the first photon from Alice's quantum register A with P photons, $\vec{j}_0 = \left[0, j_2, j_3, ..., j_P\right]$ and $\vec{j}_1 = \left[1, j_2, j_3, ..., j_P\right]$, with $\vec{j}_i \in \{0,1\}$ for $i = 2, 3, ..., P$.

Then, using similar methods already used in some previous work proposals and mainly based on the Mach-Zehnder experiment [520], and assuming that relative phases are not relevant for the experimental results, we obtain the following mathematical formulation:

$$S(A|E) \geq \left(p_{\vec{0},\vec{0}} + p_{\vec{1},\vec{1}}\right)\left(H\left[\frac{p_{\vec{0},\vec{0}}}{\left(p_{\vec{0},\vec{0}} + p_{\vec{1},\vec{1}}\right)}\right] - H[\lambda]\right)\ . \tag{4.3.2.2.4}$$

In this previous equation, we have the following equality for the parameter λ:

$$\lambda = \frac{1}{2}\left(1 + \frac{\sqrt{\left(p_{\vec{0},\vec{0}} - p_{\vec{1},\vec{1}}\right)^2 + 4p_{\vec{0},\vec{0}}p_{\vec{1},\vec{1}}\mathrm{Re}^2\left(\langle E_{\vec{0}}|E_{\vec{1}}\rangle\right)}}{\left(p_{\vec{0},\vec{0}} + p_{\vec{1},\vec{1}}\right)}\right)\ . \tag{4.3.2.2.5}$$

Regarding the above equation, we also used the fact that $\langle E_{\vec{j}}|E_{\vec{j}}\rangle = 1$.

Finally, using the observable probabilities $p_{\vec{j},\vec{k}}$ and p_{GHZ}, and obtaining ${}_E\langle E_{\vec{0}}|E_{\vec{1}}\rangle_E$ from Equation (4.3.2.1.25), we can now estimate the secure key rate κ as we will show next.

4.3.3 Experimental Results

From the previous mathematical formulations, we can now simulate some experiments for an analysis of the secure key rate considering Noisy Scenarios and see how our protocol behaves under those conditions. For this Master Thesis, we will only consider "Symmetric Noise".

4.3.3.1 Numerical simulation assuming "Symmetric Noise"

In the following numerical simulation, we compute a secret key rate under the assumption of the "Symmetric Noise", as mentioned before. Thus, we make the following assumptions:

$$\begin{aligned} &p_{\vec{0},\vec{0}} = p_{\vec{1},\vec{1}} = a \leq \frac{1}{2}, \\ &p_{\vec{j},\vec{k}} = b, \text{ for } \left(\vec{j},\vec{k}\right) \notin \left\{\left(\vec{0},\vec{0}\right), \left(\vec{1},\vec{1}\right)\right\}, \text{ and} \\ &\theta_{\vec{j},\vec{k}} = 0, \text{ for all } \left(\vec{j},\vec{k}\right). \end{aligned} \tag{4.3.3.1.1}$$

Namely, the term $\theta_{\vec{j},\vec{k}} = 0$ denotes the fact we are not considering the relative phases for this numerical simulation. Additionally, note Alice holds P photons, while "super-Bob" has $(P-1)$ photons. Thus, the total Hilbert Space of Alice and "super-Bob", $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, has dimension $D = 2^{(2P-1)}$. From Equation (4.3.2.1.20), we have that there are D probabilities $p_{\vec{j},\vec{k}}$ as well. Therefore, the normalization $2a+(D-2)b = 1$ gives the following mathematical result:

$$b = \frac{(1-2a)}{(D-2)} = \frac{(1-2a)}{\left(2^{(2P-1)}-2\right)}. \tag{4.3.3.1.2}$$

Note that if the photons belonging to Alice and Bob are not entangled with those prepared by Eve, i.e., their quantum state is equal to Equation (4.3.2.1.18), we would have that $p_{GHZ} = 2a$. But here, we consider that those photons of Alice and Bob are entangled with those of Eve. In addition, the probability of obtaining a GHZ-like quantum state equal to Equation (4.3.2.1.16) is given by the expression from Equation (4.3.2.1.25). In other words, the probability of obtaining the GHZ-like state is not only a function of the probability distribution $p_{\vec{j},\vec{k}}$ but also of the real part of the overlap, $\mathcal{O} \equiv \text{Re}\left({}_E\langle E_{\vec{0}} | E_{\vec{1}} \rangle_E\right)$. From this observation, we now have two parameters a and $\mathcal{O}$. Thus, we can instead choose a somewhat more natural choice of a and p_{GHZ}.

Due to this symmetry, we end up having the following mathematical result:

$$\lambda = \frac{(1+\mathcal{O})}{2}. \tag{4.3.3.1.3}$$

And, since $H\left(\frac{1}{2}\right) = 1$, we consequently have the following mathematical simplification:

$$S(A|E) \geq 2a\left[1 - H\left(\frac{(1+\mathcal{O})}{2}\right)\right]. \tag{4.3.3.1.4}$$

Additionally, for the numerical simulation assuming the model of "Symmetric Noise", we have that all $H(A_1|B_i)$ are equal, and therefore we will consider only the following case:

$$H(A_1|B_1) = -\sum_{a_1,b_1=0}^{1} P_{a_1 b_1} \log_2\left(\frac{P_{a_1 b_1}}{P_{b_1}}\right). \tag{4.3.3.1.5}$$

Here, we obtain $P_{a_1 b_1}$ by tracing out all the photons from Alice and "super-Bob" but the first ones. Similarly, P_{b_1} is obtained by further tracing out Alice's photon A_1. Thus, we have:

$$\begin{aligned} P_{00} &= p_{\vec{0},\vec{0}} + \sum_{(\vec{p},\vec{q})\neq(\vec{0},\vec{0})} p_{0\vec{p},0\vec{q}} = a + \left(2^{(2P-3)} - 1\right) b = P_{11} \equiv A, \\ P_{01} &= P_{10} = 2^{(2P-3)} b \equiv B, \text{ and} \\ P_0 &= P_{00} + P_{01} = A + B = P_1 \, . \end{aligned} \tag{4.3.3.1.6}$$

In the previous equations, $\vec{p}$ and $\vec{q}$ are strings of length $(P-1)$ and $(P-2)$ bits, respectively. Therefore, from the previous equation, we finally have the following mathematical result:

$$H(A_1|B_1) = -2\left[A\log_2\left(\frac{A}{(A+B)}\right) + B\log_2\left(\frac{B}{(A+B)}\right)\right] \, . \tag{4.3.3.1.7}$$

Then, from Equation (4.3.2.1.25) we have the following mathematical result:

$$O = \frac{2^{(P-1)}\, p_{\vec{+}}\, p_{GHZ}}{\alpha_{\vec{0}}^2} - 1 \, . \tag{4.3.3.1.8}$$

Since $\alpha_{\vec{0}} = \alpha_{\vec{1}} = \sqrt{a} + \left(2^{(P-1)} - 1\right)\sqrt{b}$. In order to obtain $p_{\vec{+}} = \frac{1}{2^{(P-1)}} \sum_{\vec{j},\vec{k},\vec{m}} \sqrt{p_{\vec{j},\vec{k}} p_{\vec{j},\vec{m}}}$ from Equation (4.3.2.1.21), note that it depends only on $p_{\vec{j},\vec{m}}$, and that it has $N_{total} = 2^{(3P-1)}$ terms, since Alice's "index" $\vec{j}$ has 2^P values (i.e., it labels P photons), while Bobs' "indices" $\vec{k}$ and $\vec{m}$ have $2^{(P-1)}$ values each, considering we have $(P-1)$ Bobs. Since in the "symmetric noise", there are only two probabilities, a and b, there will be only three types of terms, listed below:

- For $\vec{j} = \vec{k} = \vec{m} \in \{0,1\}$, we have $\sqrt{p_{\vec{j},\vec{k}} p_{\vec{j},\vec{m}}} = a$. There are $N_a = 2$ such terms.
- For $\{0,1\} \ni \vec{j} = \vec{k} \neq \vec{m}$, or $\{0,1\} \ni \vec{j} = \vec{m} \neq \vec{k}$, we have $\sqrt{p_{\vec{j},\vec{k}}\, p_{\vec{j},\vec{m}}} = \sqrt{ab}$. There are $N_{ab} = 2 \times 2 \times (2^{(P-1)} - 1) = 4\,(2^{(P-1)} - 1)$ such terms.
- For all other choices of binary strings $\vec{j}$, $\vec{k}$ and $\vec{m}$, we have $\sqrt{p_{\vec{j},\vec{k}}\, p_{\vec{j},\vec{m}}} = b$. There are a total of $N_b = (N_{total} - N_a - N_{ab})$ such terms.

Therefore, we end up obtaining the following equation below:

$$p_+ = \frac{a + 2\left(2^{(P-1)} - 1\right)\sqrt{ab} + \left[2^{(3P-3)} - 2(2^{(P-1)} - 1) - 1\right] b}{2^{(P-1)-1}} \, . \tag{4.3.3.1.9}$$

As noted before, in the case of the "symmetric noise", the secure key rate κ is given by the two probabilities, $a \in \left[0, \frac{1}{2}\right]$ and $p_{\text{GHZ}} \in [0,1]$. Yet, they are not independent, as they are related by Equation (4.3.2.1.25), which connects the two probabilities through $O \in [-1,1]$, thus presenting an additional constraint. Since we have that $O = \frac{2^{(P-1)}\, p_{\vec{+}}\, p_{\text{GHZ}}}{\alpha_{\vec{0}}^2} - 1$, we see that $O \geq -1$ always. Then, the other inequality gives us the following equation below:

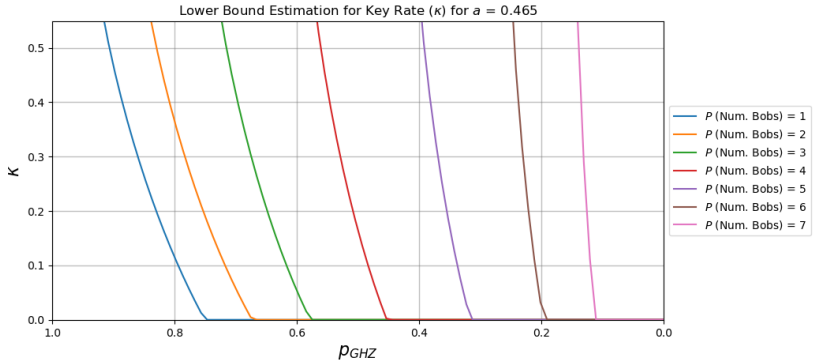
$$p_{GHZ} \leq \frac{\alpha_{\vec{0}}^2}{2^{(P-2)}\, p_{\vec{+}}} \equiv f\left(a, (P-1)\right), \text{ with } (P-1) \in \mathbb{N} \, . \tag{4.3.3.1.10}$$

Or, we can also equivalently have the following mathematical formulation:

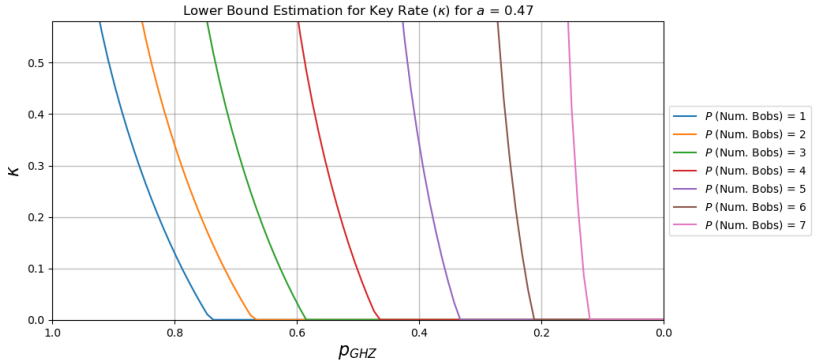
$$f\left(a,(P-1)\right)=\frac{\left(\sqrt{a}+\sqrt{\frac{\left(2^{(P-1)}-1\right)(1-2a)}{2\left(2^{(P-1)}+1\right)}}\right)^{2}}{a+\sqrt{\frac{2(2^{(P-1)}-1))a(1-2a)}{2^{(P-1)}+1}}+\left(2^{(3P-3)}-2^{P}+1\right)\frac{1-2a}{2(2^{2(P-1)}-1)}}. \tag{4.3.3.1.11}$$

Therefore, we can freely vary $a \in \left[0, \frac{1}{2}\right]$ and $(P-1) \in \mathbb{N}$, evaluating $f\left(a,(P-1)\right)$ given by Equation (4.3.3.1.11), choose $p_{\text{GHZ}} \leq f\left(a,(P-1)\right)$, and evaluate the lower bound for κ.

From all these mathematical derivations, we performed our numerical simulation assuming "symmetric noise". In the following plots, we have the estimations of the lower bounds for the key rate for some values of a and for some number P of Bobs of meaningful interest. We demonstrate some of those estimations in the following Figure 4.6:

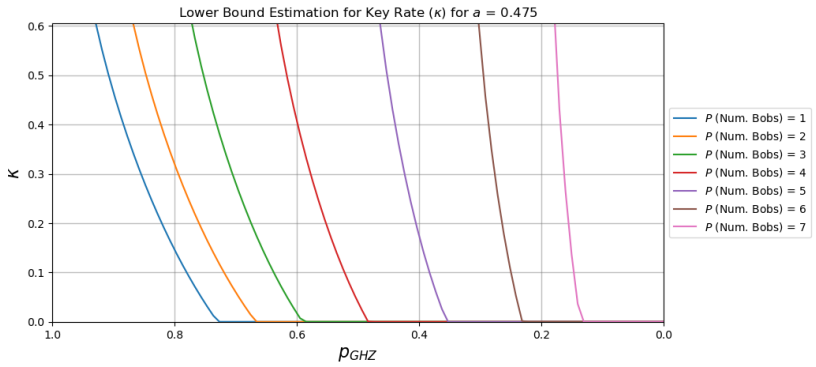


(a) Lower Bound Estimation for Key Rate (κ) for $a = 0.465$.

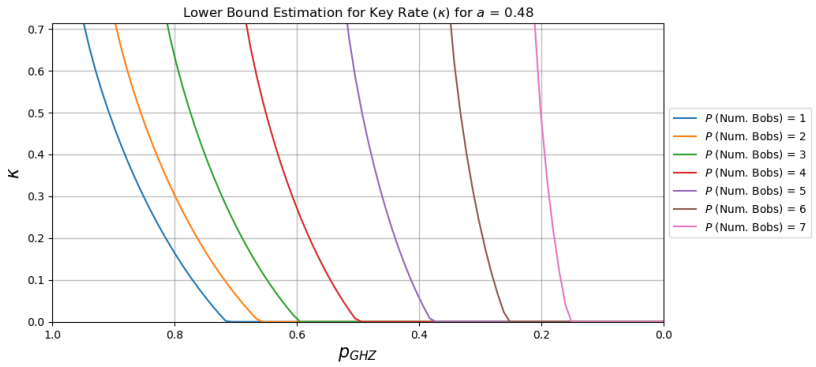


(b) Lower Bound Estimation for Key Rate (κ) for $a = 0.47$.

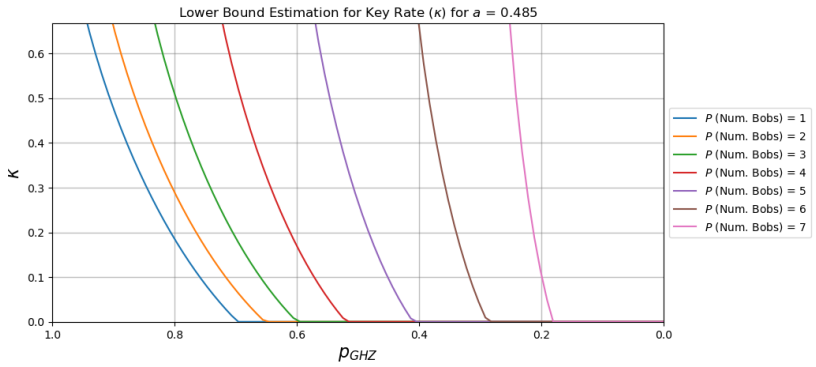
Figure 4.6: Lower Bound Estimation for Key Rate (κ) considering "Symmetric Noise".



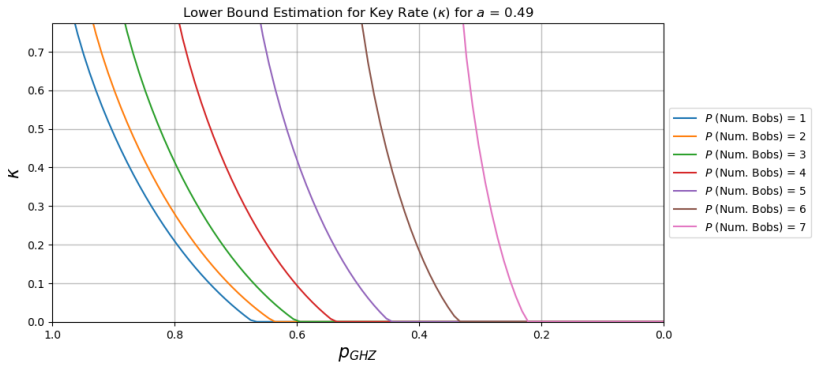
(c) Lower Bound Estimation for Key Rate (κ) for $a = 0.475$.



(d) Lower Bound Estimation for Key Rate (κ) for $a = 0.48$.

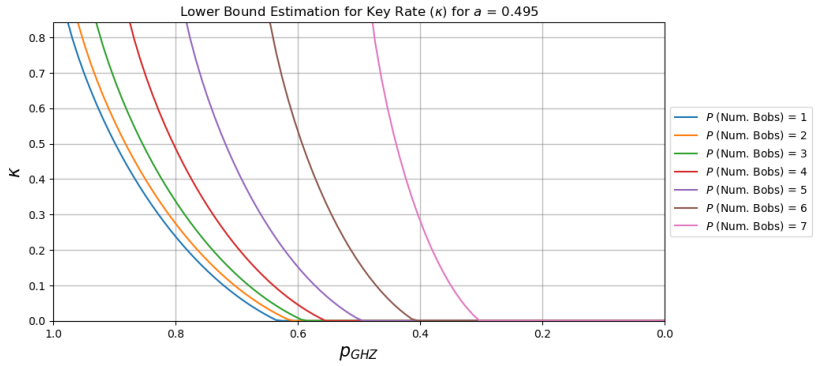


(e) Lower Bound Estimation for Key Rate (κ) for $a = 0.485$.

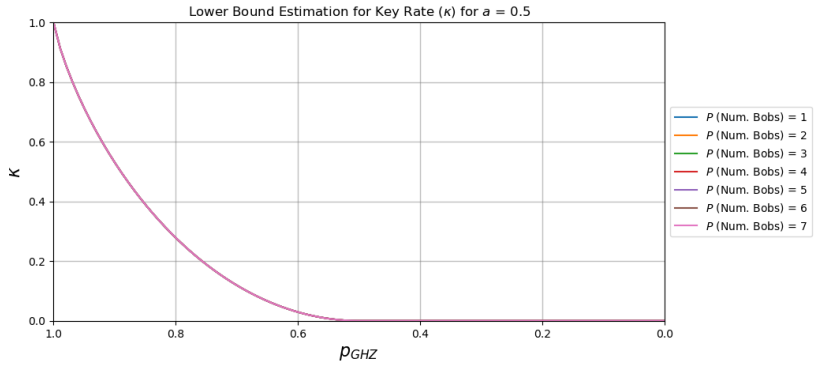


(f) Lower Bound Estimation for Key Rate (κ) for $a = 0.49$.

Figure 4.6: Lower Bound Estimation for Key Rate (κ) considering “Symmetric Noise” (cont.).



(g) Lower Bound Estimation for Key Rate (κ) for $a = 0.495$.



(h) Lower Bound Estimation for Key Rate (κ) for $a = 0.5$.

Figure 4.6: Lower Bound Estimation for Key Rate (κ) considering "Symmetric Noise" (cont.).

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

We are entering a new era of computation since quantum technologies are emerging and will be available soon at a large scale. There are many challenges in the current context of the growth of Quantum Computing, in particular, to develop secure applications for the future Quantum Internet, for example. Among those challenges is the design of the scalable extension of basic protocols like QKDs (Quantum Key Distributions) used in private communications between two users. From this need, we have what is known as QCKAs (Quantum Conference Key Agreements) that allow several parties to agree on a common private key (or conference key) used to communicate privately among them. As discussed in this Master's Thesis, the greatest advantage of using the quantum setting for the design of these types of protocols is that they can be much more secure when compared with their classical counterparts. In fact, its security does not rely on mathematical hardness assumptions but on laws of physics.

In this Master Thesis, we have proposed a new QCKA protocol performed among multiple users in a semi-quantum scenario. In this protocol, one party manipulates quantum resources, while the others are limited to performing measurements and resending the classical results, or simply reflecting the qubits. Since the approach proposed is semi-quantum, from a practical point of view, it has the advantage of simplicity and reduces the apparatus costs as it only requires one party to be quantum. Furthermore, we can enhance the possibility of a better performance at the security level by keeping at least that party as a quantum entity.

In particular, we proved that our SQCKA (Semi-Quantum Conference Key Agreement) protocol is secure when we consider standard adversary models. The proof of security used a reduction technique to an OWFQKD (One-Way Fully-Quantum Key Distribution) protocol which was especially developed to prove the security of our protocol. More specifically, we based this reduction technique on already similar existing techniques developed to prove the security of SQKD (Semi-Quantum Key Distribution) protocols. Using well-known theoretical

results, we analyzed the key rate of our proposal and computed a lower bound for it. The results obtained agree with others obtained for other quantum cryptographic proposals in the literature. In order to confirm this, we developed a library that can simulate our protocol and derived several numerical results. The source code, called Qis|krypt⟩[1], is available on GitHub. This library is also able to simulate other well-known quantum cryptographic protocols.

As Future Work, we can point to the following directions. One is to explore alternative approaches to improve the current estimated key rate lower bound. In particular, the method we assumed in this Master Thesis to compute this lower bound rate considers the security reduction mentioned before. This security reduction has the effect of exponentially decreasing that key rate with the number of Bobs and the estimation of the values of Von Neuman Entropy of a particular quantum state that is not as tight as possible. Both effects, the reduction and the computed estimation for the entropy, may be refined to improve the quality of the lower bound. One of the principal advantages of our proposal is the possibility of being realized with current technology and might be adapted to be implemented on a physical experimental setup. The particular realization of this quantum cryptographic protocol will require adjustments to the security analysis and recalculation of the respective key rate. Another direction is to consider other types of entanglement different from the GHZ States. In fact, from practical and security points of view, there are other types of quantum entanglements more robust than the GHZ States, which we can explore in the future, such as the W States. Regarding our Qis|krypt⟩ library, we aim to extend the current implementation to deal with more general Noisy Scenarios and include other different quantum (and semi-quantum) cryptographic protocols.

[1] See more information in: https://github.com/qiskrypt/qiskrypt/

Bibliography

[1] I. Newton. *Newton's Principia: The Mathematical Principles of Natural Philosophy*. Jussu Societatis Regiae ac Typis Josephi Streater; Prostat Apud Plures Bibliopolas Londini, 1687. URL: https://www.loc.gov/item/04014428/ (cit. on p. 2).

[2] T. Young. "The Bakerian Lecture: Experiments and Calculations Relative to Physical Optics". In: *Philosophical Transactions of the Royal Society of London* 94 (1804), pp. 1–16. DOI: 10.1098/rstl.1804.0001. URL: https://royalsocietypublishing.org/doi/abs/10.1098/rstl.1804.0001 (cit. on p. 2).

[3] G. Kirchhoff. "Über das Verhältniss Zwischen dem Emissionsvermögen und dem Absorptionsvermögen der Körper für Wärme und Licht". In: *Annalen der Physik* 185.2 (1860), pp. 275–301. DOI: https://doi.org/10.1002/andp.18601850205. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/andp.18601850205 (cit. on p. 2).

[4] W. Wien. "Eine Neue Beziehung der Strahlung Schwarzer Körper zum Zweiten Hauptsatz der Wärmetheorie". In: 1893. DOI: https://doi.org/10.1007/978-3-663-13885-3_12. URL: https://link.springer.com/chapter/10.1007/978-3-663-13885-3_12 (cit. on p. 2).

[5] W. Wien. "Über die Energievertheilung im Emissionsspectrum eines Schwarzen Körpers". In: *Annalen der Physik* 294.8 (1896), pp. 662–669. DOI: https://doi.org/10.1002/andp.18962940803. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/andp.18962940803 (cit. on p. 2).

[6] M. Planck. "Über Irreversible Strahlungsvorgänge". In: *Annalen der Physik* 306.1 (1900), pp. 69–122. DOI: https://doi.org/10.1002/andp.19003060105. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/andp.19003060105 (cit. on p. 2).

[7] M. Planck. "Ueber die Elementarquanta der Materie und der Elektricität". In: *Annalen der Physik* 309.3 (1901), pp. 564–566. DOI: https://doi.org/10.1002/andp.19013090311. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/andp.19013090311 (cit. on p. 2).

[8] A. Einstein. "Über Einen die Erzeugung und Verwandlung des Lichtes Betreffenden Heuristischen Gesichtspunkt". In: *Annalen der Physik* 322.6 (1905), pp. 132–148. DOI: https://doi.org/10.1002/andp.19053220607. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/andp.19053220607 (cit. on p. 2).

[9] A. Einstein. "Zur Theorie der Lichterzeugung und Lichtabsorption". In: *Annalen der Physik* 325.6 (1906), pp. 199–206. DOI: https://doi.org/10.1002/andp.19063250613. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/andp.19063250613 (cit. on p. 2).

[10] E. Rutherford. "The Scattering of α and β Particles by Matter and the Structure of the Atom". In: *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 21.125 (1911), pp. 669–688. DOI: 10.1080/14786440508637080. URL: https://doi.org/10.1080/14786440508637080 (cit. on p. 2).

[11] N. Bohr. "On the Constitution of Atoms and Molecules". In: *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 26.151 (1913), pp. 1–25. DOI: 10.1080/14786441308634955. URL: https://doi.org/10.1080/14786441308634955 (cit. on p. 2).

[12] A. Einstein. "Strahlungs-Emission und -Absorption nach der Quantentheorie". In: *Deutsche Physikalische Gesellschaft* 18 (1916), pp. 318–323. URL: http://cds.cern.ch/record/632330 (cit. on p. 2).

[13] E. Rutherford. "Collision of α Particles with Light Atoms". In: *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 37.222 (1919), pp. 581–587. DOI: 10.1080/14786440608635919. URL: https://doi.org/10.1080/14786440608635919 (cit. on p. 2).

[14] L. de Broglie. "A Tentative Theory of Light Quanta". In: *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 47.278 (1924), pp. 446–458. DOI: 10.1080/14786442408634378. URL: https://doi.org/10.1080/14786442408634378 (cit. on p. 2).

[15] W. Pauli. "Über den Zusammenhang des Abschlusses der Elektronengruppen im Atom mit der Komplexstruktur der Spektren". In: *Zeitschrift für Physik* 31.1 (1925), pp. 765–783. ISSN: 0044-3328. DOI: 10.1007/BF02980631. URL: https://doi.org/10.1007/BF02980631 (cit. on p. 2).

[16] W. Heisenberg. "Über Quantentheoretische Umdeutung Kinematischer und Mechanischer Beziehungen". In: *Zeitschrift für Physik* 33.1 (1925), pp. 879–893. ISSN: 0044-3328. DOI: 10.1007/BF01328377. URL: https://doi.org/10.1007/BF01328377 (cit. on p. 3).

[17] N. Bohr. "Atomic Theory and Mechanics". In: *Nature* 116.2927 (1925), pp. 845–852. ISSN: 1476-4687. DOI: 10.1038/116845a0. URL: https://doi.org/10.1038/116845a0 (cit. on p. 3).

[18] H. Kramers and W. Heisenberg. "Über die Streuung von Strahlung durch Atome". In: *Zeitschrift für Physik* 31.1 (1925), pp. 681–708. ISSN: 0044-3328. DOI: 10.1007/BF02980624. URL: https://doi.org/10.1007/BF02980624 (cit. on p. 3).

[19] E. Schrödinger. "An Undulatory Theory of the Mechanics of Atoms and Molecules". In: *Phys. Rev.* 28 (6 1926), pp. 1049–1070. DOI: 10.1103/PhysRev.28.1049. URL: https://link.aps.org/doi/10.1103/PhysRev.28.1049 (cit. on p. 3).

[20] M. Born. "Zur Quantenmechanik der Stoßvorgänge". In: *Zeitschrift für Physik* 37.12 (1926), pp. 863–867. ISSN: 0044-3328. DOI: 10.1007/BF01397477. URL: https://doi.org/10.1007/BF01397477 (cit. on p. 3).

[21] M. Born. "Quantenmechanik der Stoßvorgänge". In: *Zeitschrift für Physik* 38.11 (1926), pp. 803–827. ISSN: 0044-3328. DOI: 10.1007/BF01397184. URL: https://doi.org/10.1007/BF01397184 (cit. on p. 3).

[22] M. Born. "Das Adiabatenprinzip in der Quantenmechanik". In: *Zeitschrift für Physik* 40.3 (1927), pp. 167–192. ISSN: 0044-3328. DOI: 10.1007/BF01400360. URL: https://doi.org/10.1007/BF01400360 (cit. on p. 3).

[23] W. Heisenberg. "Über den Anschaulichen Inhalt der Quantentheoretischen Kinematik und Mechanik". In: *Zeitschrift für Physik* 43.3 (1927), pp. 172–198. ISSN: 0044-3328. DOI: 10.1007/BF01397280. URL: https://doi.org/10.1007/BF01397280 (cit. on pp. 3, 21).

[24] P. Dirac and R. Fowler. "The Quantum Theory of the Electron". In: *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character* 117.778 (1928), pp. 610–624. DOI: 10.1098/rspa.1928.0023. URL: https://royalsocietypublishing.org/doi/abs/10.1098/rspa.1928.0023 (cit. on p. 3).

[25] C. Anderson. "The Positive Electron". In: *Phys. Rev.* 43 (6 1933), pp. 491–494. DOI: 10.1103/PhysRev.43.491. URL: https://link.aps.org/doi/10.1103/PhysRev.43.491 (cit. on p. 3).

[26] E. Schrödinger. "Die Gegenwärtige Situation in der Quantenmechanik". In: *Naturwissenschaften* 23.50 (1935), pp. 844–849. ISSN: 1432-1904. DOI: 10.1007/BF01491987. URL: https://doi.org/10.1007/BF01491987 (cit. on p. 3).

[27] *Abacus*. URL: https://en.wikipedia.org/wiki/Abacus (cit. on p. 4).

[28] *Jacquard Machine*. URL: https://en.wikipedia.org/wiki/Jacquard_machine (cit. on p. 4).

[29] *Difference Engine*. URL: https://en.wikipedia.org/wiki/Difference_engine (cit. on p. 4).

[30] *Tabulating Machine*. URL: https://en.wikipedia.org/wiki/Tabulating_machine (cit. on p. 4).

[31] H. Hollerith. "An Electric Tabulating System". In: *The Origins of Digital Computers* (1982), pp. 133–143. DOI: 10.1007/978-3-642-61812-3_9 (cit. on p. 4).

[32] A. Church. "An Unsolvable Problem of Elementary Number Theory". In: *Journal of Symbolic Logic* 1.2 (1936), pp. 73–74. DOI: 10.2307/2268571 (cit. on p. 5).

[33] A. Church. "A Note on the Entscheidungsproblem". In: *Journal of Symbolic Logic* 1.1 (1936), pp. 40–41. DOI: 10.2307/2269326 (cit. on p. 5).

[34] A. Turing. "On Computable Numbers, with an Application to the Entscheidungsproblem". In: *Proceedings of the London Mathematical Society* s2-42.1 (1937), pp. 230–265. DOI: https://doi.org/10.1112/plms/s2-42.1.230. URL: https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/plms/s2-42.1.230 (cit. on p. 5).

[35] A. Turing. "Computability and λ-Definability". In: *The Journal of Symbolic Logic* 2.4 (1937), pp. 153–163. ISSN: 00224812. URL: http://www.jstor.org/stable/2268280 (cit. on p. 5).

[36] A. Burks and A. Burks. *The First Electronic Computer: The Atanasoff Story*. University of Michigan Press, 1989 (cit. on p. 5).

[37] A. Burks and A. Burks. "Atanasoff-Berry Computer". In: *Encyclopedia of Computer Science*. John Wiley and Sons Ltd., 2003, pp. 108–109. ISBN: 0470864125 (cit. on p. 5).

[38] J. Eckert and J. Mauchly. *US3120606A - Electronic Numerical Integrator And Computer*. 1947. URL: https://patents.google.com/patent/US3120606A/en (cit. on p. 5).

[39] M. Maynard. "Univac I". In: *Encyclopedia of Computer Science*. John Wiley and Sons Ltd., 2003, pp. 1813–1814. ISBN: 0470864125 (cit. on p. 5).

[40] J. von Neumann. "First Draft of a Report on the EDVAC". In: *IEEE Annals of the History of Computing* 15.4 (1945), pp. 27–75. DOI: 10.1109/85.238389 (cit. on p. 5).

[41] J. Bardeen and W. Brattain. "The Transistor, A Semi-Conductor Triode". In: *Phys. Rev.* 74 (2 1948), pp. 230–231. DOI: 10.1103/PhysRev.74.230. URL: https://link.aps.org/doi/10.1103/PhysRev.74.230 (cit. on p. 5).

[42] W. Shockley. "The Theory of p-n Junctions in Semiconductors and p-n Junction Transistors". In: *The Bell System Technical Journal* 28.3 (1949), pp. 435–489. DOI: 10.1002/j.1538-7305.1949.tb03645.x (cit. on p. 5).

[43] W. Shockley. "A Unipolar "Field-Effect" Transistor". In: *Proceedings of the IRE* 40.11 (1952), pp. 1365–1376. DOI: 10.1109/JRPROC.1952.273964 (cit. on p. 5).

[44] W. Shockley, J. Bardeen, and W. Brattain. *The Nobel Prize in Physics in 1956*. 1956. URL: https://www.nobelprize.org/prizes/physics/1956/summary/ (cit. on p. 5).

[45] F. Williams and T. Kilburn. "Electronic Digital Computers". In: *Nature* 162.4117 (1948), pp. 487–487. ISSN: 1476-4687. DOI: 10.1038/162487a0. URL: https://doi.org/10.1038/162487a0 (cit. on p. 5).

[46] T. Kilburn. "The University of Manchester Universal High-Speed Digital Computing Machine". In: *Nature* 164.4173 (1949), pp. 684–7 (cit. on p. 5).

[47] F. Williams, T. Kilburn, and G. Tootill. "Universal High-Speed Digital Computers: A Small-Scale Experimental Machine". In: *Proceedings of the IEE-Part II: Power Engineering* 98.61 (1951), pp. 13–28 (cit. on p. 5).

[48] J. Kilby. *US3138743A - Miniaturized Electronic Circuits*. 1959. URL: https://patents.google.com/patent/US3138743A/en (cit. on p. 5).

[49] 1959. URL: https://worldradiohistory.com/Archive-Electronics/50s/Electronics-1959-08-07.pdf (cit. on p. 5).

[50] R. Noyce. "Semiconductor Device-and-Lead Structure, Reprint of U.S. Patent 2,981,877 (Issued April 25, 1961. Filed July 30, 1959)". In: *IEEE Solid-State Circuits Society Newsletter* 12.2 (2007), pp. 34–40. DOI: 10.1109/N-SSC.2007.4785577 (cit. on p. 5).

[51] Z. Alferov, H. Kroemer, and J. Kilby. *The Nobel Prize in Physics in 2000*. 2000. URL: https://www.nobelprize.org/prizes/physics/2000/summary/ (cit. on p. 5).

[52] J. Kilby. *Jack Kilby - Nobel Lecture - nobelprize.org*. URL: https://www.nobelprize.org/uploads/2018/06/kilby-lecture.pdf (cit. on p. 5).

[53] M. Real, G. T. Kaye, and R. Warren. *A Revolution in Progress: A History of Intel to Date*. Intel Corp., Corporate Communications Dept., 1984 (cit. on p. 5).

[54] *Cisco Annual Internet Report (2018–2023) - White Paper*. 2020. URL: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (cit. on p. 6).

[55] *Optical Telegraph*. URL: https://en.wikipedia.org/wiki/Optical_telegraph (cit. on p. 6).

[56] *Electrical Telegraph*. URL: https://en.wikipedia.org/wiki/Electrical_telegraph (cit. on p. 7).

[57] *Morse Code*. URL: https://en.wikipedia.org/wiki/Morse_code (cit. on p. 7).

[58] URL: https://www.itu.int/rec/R-REC-M.1677-1-200910-I/ (cit. on p. 7).

[59] *Transatlantic Telegraph Cable*. URL: https://en.wikipedia.org/wiki/Transatlantic_telegraph_cable (cit. on p. 7).

[60] *Telephone*. URL: https://en.wikipedia.org/wiki/Telephone (cit. on p. 7).

[61] *Wireless Power Transfer*. URL: https://en.wikipedia.org/wiki/Wireless_power_transfer (cit. on p. 7).

[62] *Remote Control*. URL: https://en.wikipedia.org/wiki/Remote_control (cit. on p. 7).

[63] *Wireless Telegraphy*. URL: https://en.wikipedia.org/wiki/Wireless_telegraphy (cit. on p. 7).

[64] *Audion*. URL: https://en.wikipedia.org/wiki/Audion (cit. on p. 7).

[65] *Radio*. URL: https://en.wikipedia.org/wiki/Radio (cit. on p. 7).

[66] *DARPA*. URL: https://en.wikipedia.org/wiki/DARPA (cit. on p. 7).

[67] *ARPANET*. URL: https://en.wikipedia.org/wiki/ARPANET (cit. on p. 7).

[68] *Telstar*. URL: https://en.wikipedia.org/wiki/Telstar (cit. on p. 8).

[69] *Intelsat*. URL: https://en.wikipedia.org/wiki/Intelsat (cit. on p. 8).

[70] *Hypertext*. URL: https://en.wikipedia.org/wiki/Hypertext (cit. on p. 8).

[71] *Hypertext Editing System*. URL: https://en.wikipedia.org/wiki/Hypertext_Editing_System (cit. on p. 8).

[72] *Interface Message Processor*. URL: https://en.wikipedia.org/wiki/Interface_Message_Processor (cit. on p. 8).

[73] *Internet*. URL: https://en.wikipedia.org/wiki/Internet (cit. on p. 8).

[74] *World Wide Web*. URL: https://en.wikipedia.org/wiki/World_Wide_Web (cit. on p. 8).

[75] *Personal Computer*. URL: https://en.wikipedia.org/wiki/Personal_computer (cit. on p. 8).

[76] *Email*. URL: https://en.wikipedia.org/wiki/Email (cit. on p. 8).

[77] *Ethernet*. URL: https://en.wikipedia.org/wiki/Ethernet (cit. on p. 8).

[78] *WHOIS*. URL: https://en.wikipedia.org/wiki/WHOIS (cit. on p. 8).

[79] *Symbolics*. URL: https://en.wikipedia.org/wiki/Symbolics (cit. on p. 8).

[80] *HTML*. URL: https://en.wikipedia.org/wiki/HTML (cit. on p. 8).

[81] *File Transfer Protocol*. URL: https://en.wikipedia.org/wiki/File_Transfer_Protocol (cit. on p. 8).

[82] *Google Search*. URL: https://en.wikipedia.org/wiki/Google_Search (cit. on p. 8).

[83] *Google*. URL: https://en.wikipedia.org/wiki/Google (cit. on p. 8).

[84] *Hieroglyph*. URL: https://en.wikipedia.org/wiki/Hieroglyph (cit. on p. 9).

[85] *Pictogram*. URL: https://en.wikipedia.org/wiki/Pictogram (cit. on p. 9).

[86] *Scytale*. URL: https://en.wikipedia.org/wiki/Scytale (cit. on p. 9).

[87] *Caesar Cipher*. URL: https://en.wikipedia.org/wiki/Caesar_cipher (cit. on p. 10).

[88] *Alberti Cipher*. URL: https://en.wikipedia.org/wiki/Alberti_cipher (cit. on p. 10).

[89] *Vigenère Cipher*. URL: https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher (cit. on p. 10).

[90] *Jefferson Disk*. URL: https://en.wikipedia.org/wiki/Jefferson_disk (cit. on p. 10).

[91] *Zimmermann Telegram*. URL: https://en.wikipedia.org/wiki/Zimmermann_Telegram (cit. on p. 10).

[92] *Enigma Machine*. URL: https://en.wikipedia.org/wiki/Enigma_machine (cit. on p. 10).

[93] *Bomba Kryptologiczna (Cryptologic Bomb)*. URL: https://en.wikipedia.org/wiki/Bomba_(cryptography) (cit. on p. 11).

[94] *Type B Cipher Machine*. URL: https://en.wikipedia.org/wiki/Type_B_Cipher_Machine (cit. on p. 11).

[95] *William Friedman*. URL: https://en.wikipedia.org/wiki/William_F._Friedman (cit. on p. 11).

[96] *Lorenz Cipher*. URL: https://en.wikipedia.org/wiki/Lorenz_cipher (cit. on p. 11).

[97] *Colossus Computer*. URL: https://en.wikipedia.org/wiki/Colossus_computer (cit. on p. 11).

[98] T. Flowers. "The Design of Colossus (Foreword by Howard Campaigne)". In: *Annuals of the History of Computing* 5.3 (1983), pp. 239–252. DOI: 10.1109/MAHC.1983.10079 (cit. on p. 11).

[99] F. Miller. *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams*. C. M. Cornwell, 1882. URL: https://books.google.pt/books?id=tT9WAAAAYAAJ (cit. on p. 11).

[100] G. Vernam. *US1310719 - Secret Signaling System*. 1919. URL: https://patents.google.com/patent/US1310719/en (cit. on pp. 12, 67, 97).

[101] *Teleprinter*. URL: https://en.wikipedia.org/wiki/Teleprinter (cit. on p. 12).

[102] H. Feistel. *US3798359A - Block Cipher Cryptographic System*. 1971. URL: https://patents.google.com/patent/US3798359A/en (cit. on p. 12).

[103] H. Feistel. *US3798605A - Centralized Verification System*. 1971. URL: https://patents.google.com/patent/US3798605A/en (cit. on p. 12).

[104] H. Feistel. *US3798360A - Step Code Ciphering System*. 1971. URL: https://patents.google.com/patent/US3798360A/en (cit. on p. 12).

[105] H. Feistel. "Cryptography and Computer Privacy". In: *Scientific American* 228.5 (1973), pp. 15–23. ISSN: 00368733, 19467087. URL: http://www.jstor.org/stable/24923044 (cit. on p. 12).

[106] N. I. of Standards and T. (NIST). *Data Encryption Standard (DES)*. 1988. URL: https://csrc.nist.gov/publications/detail/fips/46/1/archive/1988-01-22 (cit. on p. 12).

[107] *EFF DES Cracker*. URL: https://en.wikipedia.org/wiki/EFF_DES_cracker (cit. on p. 12).

[108] M. Loukides and J. (F. F. Gilmore. *Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design*. O'Reilly & Associates, Inc., 1998. ISBN: 1565925203 (cit. on p. 12).

[109] J. Daemen and V. Rijmen. "The Block Cipher Rijndael". In: *Smart Card Research and Applications*. Ed. by J.-J. Quisquater and B. Schneier. Springer Berlin Heidelberg, 2000, pp. 277–284. ISBN: 978-3-540-44534-0 (cit. on pp. 12, 13, 97).

[110] C. Burwick et al. "MARS - A Candidate Cipher for AES". In: 1999 (cit. on p. 12).

[111] R. Rivest, M. Robshaw, R. Sidney, and Y. Yin. "The RC6 TM Block Cipher". In: 1998 (cit. on p. 12).

[112] R. Anderson, E. Biham, and L. Knudsen. "Serpent: A Proposal for the Advanced Encryption Standard". In: 1998 (cit. on p. 12).

[113] B. Schneier et al. "Twofish: A 128-Bit Block Cipher". In: *In First Advanced Encryption Standard (AES) Conference*. 1998 (cit. on p. 12).

[114] N. I. of Standards and T. (NIST). *Advanced Encryption Standard (AES)*. 2001. URL: https://csrc.nist.gov/publications/detail/fips/197/final (cit. on p. 13).

[115] W. Diffie and M. Hellman. "New Directions in Cryptography". In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638 (cit. on p. 13).

[116] R. Merkle. "Secure Communications over Insecure Channels". In: *Commun. ACM* 21.4 (1978), pp. 294–299. ISSN: 0001-0782. DOI: 10.1145/359460.359473. URL: https://doi.org/10.1145/359460.359473 (cit. on p. 13).

[117] R. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Commun. ACM* 21.2 (1977), pp. 120–126. ISSN: 0001-0782. DOI: 10.1145/359340.359342. URL: https://doi.org/10.1145/359340.359342 (cit. on pp. 13, 62).

[118] L. Lamport. *Constructing Digital Signatures from a One Way Function*. Tech. rep. CSL-98. 1979. URL: https://www.microsoft.com/en-us/research/publication/constructing-digital-signatures-one-way-function/ (cit. on pp. 13, 62).

[119] M. Rabin. *Digitalized Signatures and Public-Key Functions as Intractable as Factorization*. Tech. rep. 1979 (cit. on p. 13).

[120] V. Miller. "Use of Elliptic Curves in Cryptography". In: *Advances in Cryptology — CRYPTO '85 Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, pp. 417–426. ISBN: 978-3-540-39799-1 (cit. on p. 13).

[121] N. Koblitz. "Elliptic Curve Cryptosystems". In: *Mathematics of Computation* 48 (1987), pp. 203–209 (cit. on pp. 13, 62).

[122] A. Shamir, R. Rivest, and L. Adleman. "Mental Poker". In: *The Mathematical Gardner*. Ed. by D. A. Klarner. Springer US, 1981, pp. 37–43. ISBN: 978-1-4684-6686-7. DOI: 10.1007/978-1-4684-6686-7_5. URL: https://doi.org/10.1007/978-1-4684-6686-7_5 (cit. on p. 13).

[123] A. Yao. "Protocols for Secure Computations". In: *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*. 1982, pp. 160–164. DOI: 10.1109/SFCS.1982.38 (cit. on p. 13).

[124] O. Goldreich, S. Micali, and A. Wigderson. "How to Play ANY Mental Game". In: *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*. STOC '87. Association for Computing Machinery, 1987, pp. 218–229. ISBN: 0897912217. DOI: 10.1145/28395.28420. URL: https://doi.org/10.1145/28395.28420 (cit. on p. 13).

[125] L. Babai and S. Moran. "Arthur-Merlin Games: A Randomized Proof System, and a Hierarchy of Complexity Classes". In: *Journal of Computer and System Sciences* 36.2 (1988), pp. 254–276. ISSN: 0022-0000. DOI: https://doi.org/10.1016/0022-0000(88)90028-1. URL: https://www.sciencedirect.com/science/article/pii/0022000088900281 (cit. on p. 13).

[126] S. Goldwasser, S. Micali, and C. Rackoff. "The Knowledge Complexity of Interactive Proof Systems". In: *SIAM Journal on Computing* 18.1 (1989), pp. 186–208. DOI: 10.1137/0218012. URL: https://doi.org/10.1137/0218012 (cit. on p. 13).

[127] O. Goldreich, S. Micali, and A. Wigderson. "Proofs That Yield Nothing but Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems". In: *J. ACM* 38.3 (1991), pp. 690–728. ISSN: 0004-5411. DOI: 10.1145/116825.116852. URL: https://doi.org/10.1145/116825.116852 (cit. on p. 13).

[128] T. Sander, A. Young, and M. Yung. "Non-Interactive Cryptocomputing for NC/Sup 1/". In: *40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039)*. 1999, pp. 554–566. DOI: 10.1109/SFFCS.1999.814630 (cit. on p. 13).

[129] L. Lamport, R. Shostak, and M. Pease. "The Byzantine Generals Problem". In: *ACM Trans. Program. Lang. Syst.* 4.3 (1982), pp. 382–401. ISSN: 0164-0925. DOI: 10.1145/357172.357176. URL: https://doi.org/10.1145/357172.357176 (cit. on p. 13).

[130] M. Fischer, N. Lynch, and M. Paterson. "Impossibility of Distributed Consensus with One Faulty Process". In: *J. ACM* 32.2 (1985), pp. 374–382. ISSN: 0004-5411. DOI: 10.1145/3149.214121. URL: https://doi.org/10.1145/3149.214121 (cit. on p. 13).

[131] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2009. URL: http://bitcoin.org/bitcoin.pdf (cit. on p. 13).

[132] V. Buterin. "A Next Generation Smart Contract & Decentralized Application Platform". In: 2015 (cit. on p. 13).

[133] S. Haber and S. Stornetta. "How to Time-Stamp a Digital Document". In: *Journal of Cryptology* 3.2 (1991), pp. 99–111. ISSN: 1432-1378. DOI: 10.1007/BF00196791. URL: https://doi.org/10.1007/BF00196791 (cit. on p. 13).

[134] D. Bayer, S. Haber, and S. Stornetta. "Improving the Efficiency and Reliability of Digital Time-Stamping". In: *Sequences II*. Ed. by R. Capocelli, A. De Santis, and U. Vaccaro. Springer New York, 1993, pp. 329–33. ISBN: 978-1-4613-9323-8 (cit. on p. 13).

[135] R. Rivest, L. Adleman, and M. Dertouzos. "On Data Banks and Privacy Homomorphisms". In: *Foundations of Secure Computation, Academia Press* (1978), pp. 169–179 (cit. on p. 13).

[136] C. Gentry. "Fully Homomorphic Encryption Using Ideal Lattices". In: *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*. STOC '09. Association for Computing Machinery, 2009, pp. 169–178. ISBN: 9781605585062. DOI: 10.1145/1536414.1536440. URL: https://doi.org/10.1145/1536414.1536440 (cit. on p. 13).

[137] C. Gentry. *A Fully Homomorphic Encryption Scheme*. Stanford university, 2009 (cit. on p. 13).

[138] M. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan. "Fully Homomorphic Encryption Over the Integers". In: *Annual international conference on the theory and applications of cryptographic techniques*. Springer. 2010, pp. 24–43 (cit. on p. 13).

[139] J. Fan and F. Vercauteren. "Somewhat Practical Fully Homomorphic Encryption". In: *IACR Cryptology ePrint Archive* (2012), p. 144. URL: http://eprint.iacr.org/2012/144 (cit. on p. 13).

[140] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. "Leveled Fully Homomorphic Encryption Without Bootstrapping". In: *ACM Transactions on Computation Theory (TOCT)* 6.3 (2014), pp. 1–36 (cit. on p. 13).

[141] Z. Brakerski and V. Vaikuntanathan. "Efficient Fully Homomorphic Encryption from (Standard) LWE". In: *SIAM Journal on computing* 43.2 (2014), pp. 831–871 (cit. on p. 13).

[142] R. Feynman. "Simulating Physics with Computers". In: *International Journal of Theoretical Physics* 21.6 (1982), pp. 467–488. ISSN: 1572-9575. DOI: 10.1007/BF02650179. URL: https://doi.org/10.1007/BF02650179 (cit. on pp. 14, 21, 22).

[143] R. Ingarden. "Quantum Information Theory". In: *Reports on Mathematical Physics* 10.1 (1976), pp. 43–72. ISSN: 0034-4877. DOI: https://doi.org/10.1016/0034-4877(76)90005-7. URL: https://www.sciencedirect.com/science/article/pii/0034487776900057 (cit. on p. 14).

[144] P. Benioff. "Quantum Mechanical Hamiltonian Models of Turing Machines". In: *Journal of Statistical Physics* 29.3 (1982), pp. 515–546. ISSN: 1572-9613. DOI: 10.1007/BF01342185. URL: https://doi.org/10.1007/BF01342185 (cit. on p. 14).

[145] D. Deutsch and R. Penrose. "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer". In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400.1818 (1985), pp. 97–117. DOI: 10.1098/rspa.1985.0070. URL: https://royalsocietypublishing.org/doi/abs/10.1098/rspa.1985.0070 (cit. on pp. 14, 21).

[146] D. Deutsch and R. Jozsa. "Rapid Solution of Problems by Quantum Computation". In: *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 439.1907 (1992), pp. 553–558. DOI: 10.1098/rspa.1992.0167. URL: https://royalsocietypublishing.org/doi/abs/10.1098/rspa.1992.0167 (cit. on p. 14).

[147] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. "Quantum Algorithms Revisited". In: *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 454.1969 (1998), pp. 339–354. ISSN: 1471-2946. DOI: 10.1098/rspa.1998.0164. URL: http://dx.doi.org/10.1098/rspa.1998.0164 (cit. on p. 14).

[148] E. Bernstein and U. Vazirani. "Quantum Complexity Theory". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1411–1473. DOI: 10.1137/S0097539796300921. URL: https://doi.org/10.1137/S0097539796300921 (cit. on pp. 14, 15).

[149] D. Simon. "On the Power of Quantum Computation". In: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. SFCS '94. IEEE Computer Society, 1994, pp. 116–123. ISBN: 0818665807. DOI: 10.1109/SFCS.1994.365701. URL: https://doi.org/10.1109/SFCS.1994.365701 (cit. on pp. 14, 60, 62).

[150] P. Shor. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700 (cit. on pp. 15, 50, 51, 61, 62).

[151] P. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1484–1509. ISSN: 1095-7111. DOI: 10.1137/s0097539795293172. URL: http://dx.doi.org/10.1137/S0097539795293172 (cit. on pp. 15, 50, 51, 61, 62).

[152] L. Grover. "A Fast Quantum Mechanical Algorithm for Database Search". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. Association for Computing Machinery, 1996, pp. 212–219. ISBN: 0897917855. DOI: 10.1145/237814.237866. URL: https://doi.org/10.1145/237814.237866 (cit. on pp. 15, 51, 59, 62).

[153] D. Cory, A. Fahmy, and T. Havel. "Ensemble Quantum Computing by NMR Spectroscopy". In: *Proceedings of the National Academy of Sciences* 94.5 (1997), pp. 1634–1639. DOI: 10.1073/pnas.94.5.1634. URL: https://www.pnas.org/doi/abs/10.1073/pnas.94.5.1634 (cit. on p. 15).

[154] N. Gershenfeld and I. Chuang. "Quantum Computing with Molecules". In: *Scientific American* 278.6 (1998), pp. 66–71. ISSN: 00368733, 19467087. URL: http://www.jstor.org/stable/26057857 (cit. on p. 15).

[155] J. Jones and M. Mosca. "Implementation of a Quantum Algorithm on a Nuclear Magnetic Resonance Quantum Computer". In: *The Journal of Chemical Physics* 109.5 (1998), pp. 1648–1653. ISSN: 1089-7690. DOI: 10.1063/1.476739. URL: http://dx.doi.org/10.1063/1.476739 (cit. on p. 15).

[156] I. Chuang, N. Gershenfeld, and M. Kubinec. "Experimental Implementation of Fast Quantum Searching". In: *Phys. Rev. Lett.* 80 (15 1998), pp. 3408–3411. DOI: 10.1103/PhysRevLett.80.3408. URL: https://link.aps.org/doi/10.1103/PhysRevLett.80.3408 (cit. on p. 15).

[157] I. Chuang, L. Vandersypen, X. Zhou, D. Leung, and S. Lloyd. "Experimental Realization of a Quantum Algorithm". In: *Nature* 393.6681 (1998), pp. 143–146. ISSN: 1476-4687. DOI: 10.1038/30181. URL: http://dx.doi.org/10.1038/30181 (cit. on p. 15).

[158] J. Brooke, D. Bitko, T. Rosenbaum, and G. Aeppli. "Quantum Annealing of a Disordered Magnet". In: *Science* 284.5415 (1999), pp. 779–781. DOI: 10.1126/science.284.5415.779. URL: https://www.science.org/doi/abs/10.1126/science.284.5415.779 (cit. on p. 15).

[159] L. Vandersypen, M. Steffen, G. Breyta, C. Yannoni, M. Sherwood, and I. Chuang. "Experimental Realization of Shor's Quantum Factoring Algorithm using Nuclear Magnetic Resonance". In: *Nature* 414.6866 (2001), pp. 883–887. ISSN: 1476-4687. DOI: 10.1038/414883a. URL: https://doi.org/10.1038/414883a (cit. on p. 15).

[160] R. Raussendorf and H. Briegel. "A One-Way Quantum Computer". In: *Phys. Rev. Lett.* 86 (22 2001), pp. 5188–5191. DOI: 10.1103/PhysRevLett.86.5188. URL: https://link.aps.org/doi/10.1103/PhysRevLett.86.5188 (cit. on p. 15).

[161] C. Elliott. *The DARPA Quantum Network*. 2004. URL: https://arxiv.org/abs/quant-ph/0412029 (cit. on p. 16).

[162] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh. *Current Status of the DARPA Quantum Network*. 2005. URL: https://arxiv.org/abs/quant-ph/0503058 (cit. on p. 16).

[163] C. Elliott and H. Yeh. "DARPA Quantum Network Testbed". In: 2007 (cit. on p. 16).

[164] F. Koppens et al. "Driven coherent oscillations of a single electron spin in a quantum dot". In: *Nature* 442.7104 (2006), pp. 766–771. ISSN: 1476-4687. DOI: 10.1038/nature05065. URL: https://doi.org/10.1038/nature05065 (cit. on p. 16).

[165] G. Dutt et al. "Quantum Register Based on Individual Electronic and Nuclear Spin Qubits in Diamond". In: *Science* 316.5829 (2007), pp. 1312–1316. ISSN: 00368075, 10959203. URL: http://www.jstor.org/stable/20036388 (cit. on p. 16).

[166] V. Giovannetti, S. Lloyd, and L. Maccone. "Quantum Random Access Memory". In: *Physical Review Letters* 100.16 (2008). ISSN: 1079-7114. URL: http://dx.doi.org/10.1103/PhysRevLett.100.160501 (cit. on p. 16).

[167] M. Sillanpää, J. Park, and R. Simmonds. "Coherent Quantum State Storage and Transfer Between Two Phase Qubits via a Resonant Cavity". In: *Nature* 449.7161 (2007), pp. 438–442. ISSN: 1476-4687. DOI: 10.1038/nature06124. URL: http://dx.doi.org/10.1038/nature06124 (cit. on p. 16).

[168] J. Majer et al. "Coupling Superconducting Qubits via a Cavity Bus". In: *Nature* 449.7161 (2007), pp. 443–447. ISSN: 1476-4687. DOI: 10.1038/nature06184. URL: https://doi.org/10.1038/nature06184 (cit. on p. 16).

[169] M. Biercuk et al. "Optimized Dynamical Decoupling in a Model Quantum Memory". In: *Nature* 458.7241 (2009), pp. 996–1000. ISSN: 1476-4687. DOI: 10.1038/nature07951. URL: https://doi.org/10.1038/nature07951 (cit. on p. 16).

[170] X. Xu et al. "Optically Controlled Locking of the Nuclear Field via Coherent Dark-State Spectroscopy". In: *Nature* 459.7250 (2009), pp. 1105–1109. ISSN: 1476-4687. DOI: 10.1038/nature08120. URL: https://doi.org/10.1038/nature08120 (cit. on p. 16).

[171] H. Neven, V. Denchev, G. Rose, and W. Macready. *Training a Binary Classifier with the Quantum Adiabatic Algorithm*. 2008 (cit. on p. 17).

[172] H. Neven, V. Denchev, G. Rose, and W. Macready. *Training a Large Scale Classifier with the Quantum Adiabatic Algorithm*. 2009 (cit. on p. 17).

[173] D. Hanneke, J. Home, J. Jost, J. Amini, D. Leibfried, and D. Wineland. "Realization of a Programmable Two-Qubit Quantum Processor". In: *Nature Physics* 6.1 (2009), pp. 13–16. ISSN: 1745-2481. DOI: 10.1038/nphys1453. URL: http://dx.doi.org/10.1038/nphys1453 (cit. on p. 17).

[174] J. Home, D. Hanneke, J. Jost, J. Amini, D. Leibfried, and D. Wineland. "Complete Methods Set for Scalable Ion Trap Quantum Information Processing". In: *Science* 325.5945 (2009), pp. 1227–1230. ISSN: 1095-9203. DOI: 10.1126/science.1177077. URL: http://dx.doi.org/10.1126/science.1177077 (cit. on p. 17).

[175] L. DiCarlo et al. "Demonstration of Two-Qubit Algorithms with a Superconducting Quantum Processor". In: *Nature* 460.7252 (2009), pp. 240–244. ISSN: 1476-4687. DOI: 10.1038/nature08121. URL: http://dx.doi.org/10.1038/nature08121 (cit. on p. 17).

[176] *First Ever Commercial Quantum Computer Now Available for $10 Million.* 2011. URL: https://uk.pcmag.com/news/106505/first-ever-commercial-quantum-computer-now-available-for-10-million (cit. on p. 17).

[177] G. Fuchs, G. Burkard, P. Klimov, and D. Awschalom. "A Quantum Memory Intrinsic to Single Nitrogen-Vacancy Centres in Diamond". In: *Nature Physics* 7.10 (2011), pp. 789–793. ISSN: 1745-2481. DOI: 10.1038/nphys2026. URL: https://doi.org/10.1038/nphys2026 (cit. on p. 17).

[178] M. Mariantoni et al. "Implementing the Quantum Von Neumann Architecture with Superconducting Circuits". In: *Science* 334.6052 (2011), pp. 61–65. ISSN: 1095-9203. DOI: 10.1126/science.1208517. URL: http://dx.doi.org/10.1126/science.1208517 (cit. on p. 17).

[179] N. Harmut. *Launching the Quantum Artificial Intelligence Lab.* 2013. URL: https://ai.googleblog.com/2013/05/launching-quantum-artificial.html (cit. on p. 17).

[180] W. Pfaff et al. "Unconditional Quantum Teleportation Between Distant Solid-state Quantum Bits". In: *Science* 345.6196 (2014), pp. 532–535. ISSN: 1095-9203. DOI: 10.1126/science.1253512. URL: http://dx.doi.org/10.1126/science.1253512 (cit. on p. 17).

[181] T. Monz et al. "Realization of a Scalable Shor Algorithm". In: *Science* 351.6277 (2016), pp. 1068–1070. ISSN: 1095-9203. DOI: 10.1126/science.aad9480. URL: http://dx.doi.org/10.1126/science.aad9480 (cit. on p. 17).

[182] *IBM announces Advances to IBM Quantum Systems & Ecosystem.* 2017. URL: https://newsroom.ibm.com/2017-11-10-IBM-Announces-Advances-to-IBM-Quantum-Systems-Ecosystem (cit. on p. 18).

[183] E. Pednault et al. "Breaking the 49-qubit Barrier in the Simulation of Quantum Circuits". In: 15 (2017). URL: https://arxiv.org/pdf/1710.05867v1.pdf (cit. on p. 18).

[184] E. Pednault et al. "Pareto-Efficient Quantum Circuit Simulation using Tensor Contraction Deferral". In: (2017). URL: https://arxiv.org/pdf/1710.05867v4.pdf (cit. on p. 18).

[185] *The Future of Quantum Computing is Counted in Qubits.* 2018. URL: https://newsroom.intel.com/news/future-quantum-computing-counted-qubits/ (cit. on p. 18).

[186] *2018 CES: Intel Advances Quantum and Neuromorphic Computing Research.* 2018. URL: https://newsroom.intel.com/news/intel-advances-quantum-neuromorphic-computing-research/ (cit. on p. 18).

[187] S. Boixo et al. "Characterizing Quantum Supremacy in Near-Term Devices". In: *Nature Physics* 14.6 (2018), pp. 595–600. ISSN: 1745-2481. DOI: 10.1038/s41567-018-0124-x. URL: http://dx.doi.org/10.1038/s41567-018-0124-x (cit. on p. 18).

[188] *A Preview of Bristlecone, Google's New Quantum Processor*. 2018. URL: https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html (cit. on p. 18).

[189] B. Villalonga et al. "A Flexible High-Performance Simulator for Verifying and Benchmarking Quantum Circuits Implemented on Real Hardware". In: *npj Quantum Information* 5.1 (2019). ISSN: 2056-6387. DOI: 10.1038/s41534-019-0196-1. URL: http://dx.doi.org/10.1038/s41534-019-0196-1 (cit. on p. 18).

[190] *Intel Sees Promise of Silicon Spin Qubits for Quantum Computing*. 2018. URL: https://newsroom.intel.com/news/intel-sees-promise-silicon-spin-qubits-quantum-computing/ (cit. on p. 18).

[191] *National Quantum Initiative Act (2018 - H.R. 6227)*. 2018. URL: https://www.govtrack.us/congress/bills/115/hr6227 (cit. on p. 18).

[192] M. Giles. *President Trump has Signed a $1.2 Billion Law to Boost US Quantum Tech*. 2020. URL: https://www.technologyreview.com/2018/12/22/138149/president-trump-has-signed-a-12-billon-law-to-boost-us-quantum-tech/ (cit. on p. 18).

[193] P. Ball. "First Commercial Ion-Based Quantum Computer Built". In: *Physics World* 32.2 (2019), pp. 5–5. DOI: 10.1088/2058-7058/32/2/6. URL: https://doi.org/10.1088/2058-7058/32/2/6 (cit. on p. 18).

[194] F. Arute et al. "Quantum Supremacy Using a Programmable Superconducting Processor". In: *Nature* 574.7779 (2019), pp. 505–510. ISSN: 1476-4687. DOI: 10.1038/s41586-019-1666-5. URL: https://doi.org/10.1038/s41586-019-1666-5 (cit. on p. 18).

[195] *IBM Opens Quantum Computation Center in New York; Brings World's Largest Fleet of Quantum Computing Systems Online, Unveils New 53-Qubit Quantum System for Broad Use*. 2019. URL: https://newsroom.ibm.com/2019-09-18-IBM-Opens-Quantum-Computation-Center-in-New-York-Brings-Worlds-Largest-Fleet-of-Quantum-Computing-Systems-Online-Unveils-New-53-Qubit-Quantum-System-for-Broad-Use (cit. on p. 18).

[196] M. Bhaskar et al. "Experimental Demonstration of Memory-Enhanced Quantum Communication". In: *Nature* 580.7801 (2020), pp. 60–64. ISSN: 1476-4687. DOI: 10.1038/s41586-020-2103-5. URL: https://doi.org/10.1038/s41586-020-2103-5 (cit. on p. 18).

[197] F. Arute et al. "Hartree-Fock on a Superconducting Qubit Quantum Computer". In: *Science* 369.6507 (2020), pp. 1084–1089. ISSN: 1095-9203. DOI: 10.1126/science.abb9811. URL: http://dx.doi.org/10.1126/science.abb9811 (cit. on p. 19).

[198] H.-S. Zhong et al. "Quantum Computational Advantage Using Photons". In: *Science* 370.6523 (2020), pp. 1460–1463. ISSN: 1095-9203. DOI: 10.1126/science.abe8770. URL: http://dx.doi.org/10.1126/science.abe8770 (cit. on p. 19).

[199] H. Wang et al. "Boson Sampling with 20 Input Photons and a 60-Mode Interferometer in a 1014-Dimensional Hilbert Space". In: *Physical Review Letters* 123.25 (2019). ISSN: 1079-7114. DOI: 10.1103/physrevlett.123.250503. URL: http://dx.doi.org/10.1103/PhysRevLett.123.250503 (cit. on p. 19).

[200] F. Centrone, N. Kumar, E. Diamanti, and I. Kerenidis. "Experimental Demonstration of Quantum Advantage for NP Verification with Limited Information". In: *Nature Communications* 12.1 (2021), p. 850. ISSN: 2041-1723. DOI: 10.1038/s41467-021-21119-1. URL: https://doi.org/10.1038/s41467-021-21119-1 (cit. on p. 19).

[201] A. King et al. "Scaling Advantage Over Path-Integral Monte Carlo in Quantum Simulation of Geometrically Frustrated Magnets". In: *Nature Communications* 12.1 (2021), p. 1113. ISSN: 2041-1723. DOI: 10.1038/s41467-021-20901-5. URL: https://doi.org/10.1038/s41467-021-20901-5 (cit. on p. 19).

[202] H.-S. Zhong et al. "Phase-Programmable Gaussian Boson Sampling Using Stimulated Squeezed Light". In: *Phys. Rev. Lett.* 127 (18 2021). DOI: 10.1103/PhysRevLett.127.180502. URL: https://link.aps.org/doi/10.1103/PhysRevLett.127.180502 (cit. on p. 19).

[203] Y. Wu et al. "Strong Quantum Computational Advantage Using a Superconducting Quantum Processor". In: *Phys. Rev. Lett.* 127 (18 2021). DOI: 10.1103/PhysRevLett.127.180501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.127.180501 (cit. on p. 19).

[204] Q. Zhu et al. "Quantum Computational Advantage via 60-Qubit 24-Cycle Random Circuit Sampling". In: *Science Bulletin* 67.3 (2022), pp. 240–245. ISSN: 2095-9273. DOI: https://doi.org/10.1016/j.scib.2021.10.017. URL: https://www.sciencedirect.com/science/article/pii/S2095927321006733 (cit. on p. 19).

[205] J. Randall et al. "Many-Body–Localized Discrete Time Crystal with a Programmable Spin-Based Quantum Simulator". In: *Science* 374.6574 (2021), pp. 1474–1478. ISSN: 1095-9203. DOI: 10.1126/science.abk0603. URL: http://dx.doi.org/10.1126/science.abk0603 (cit. on p. 20).

[206] X. Mi et al. "Time-Crystalline Eigenstate Order on a Quantum Processor". In: *Nature* 601.7894 (2021), pp. 531–536. ISSN: 1476-4687. DOI: 10.1038/s41586-021-04257-w. URL: http://dx.doi.org/10.1038/s41586-021-04257-w (cit. on p. 20).

[207] J. Preskill. "Quantum Computing in the NISQ Era and Beyond". In: *Quantum* 2 (2018), p. 79. ISSN: 2521-327X. DOI: 10.22331/q-2018-08-06-79. URL: http://dx.doi.org/10.22331/q-2018-08-06-79 (cit. on p. 20).

[208] *Moore's Law*. URL: https://en.wikipedia.org/wiki/Moore%5C%27s_law (cit. on p. 21).

[209] G. Moore. "Cramming More Components Onto Integrated Circuits". In: *Proceedings of the IEEE* 86.1 (1995), pp. 82–85. DOI: 10.1109/JPROC.1998.658762 (cit. on p. 21).

[210] G. Moore. "Progress in Digital Integrated Electronics". In: *Electron Devices Meeting*. Vol. 21. 1975, pp. 11–13 (cit. on p. 21).

[211] *Transistor Count*. URL: https://en.wikipedia.org/wiki/Transistor_count (cit. on p. 21).

[212] *Quantum Tunneling*. URL: https://en.wikipedia.org/wiki/Quantum_tunnelling (cit. on p. 21).

[213] J. Tucker, C. Wang, and P. Carney. "Silicon Field-Effect Transistor Based on Quantum Tunneling". In: *Applied Physics Letters* 65.5 (1994), pp. 618–620. DOI: 10.1063/1.112250. URL: https://doi.org/10.1063/1.112250 (cit. on p. 21).

[214] W. Reddick and G. Amaratunga. "Silicon Surface Tunnel Transistor". In: *Applied Physics Letters* 67.4 (1995), pp. 494–496. DOI: 10.1063/1.114547. URL: https://doi.org/10.1063/1.114547 (cit. on p. 21).

[215] J. Powell. "The Quantum Limit to Moore's Law". In: *Proceedings of the IEEE* 96.8 (2008), pp. 1247–1248. DOI: 10.1109/JPROC.2008.925411. URL: https://ieeexplore.ieee.org/document/4567410 (cit. on p. 21).

[216] M. Waldrop. "The Chips are Down for Moore's Law". In: *Nature* 530.7589 (2016), pp. 144–147. DOI: 10.1038/530144a. URL: https://ui.adsabs.harvard.edu/abs/2016Natur.530..144W (cit. on p. 21).

[217] S. Sinha and W. Ditto. "Dynamics Based Computation". In: *Phys. Rev. Lett.* 81 (10 1998), pp. 2156–2159. DOI: 10.1103/PhysRevLett.81.2156. URL: https://link.aps.org/doi/10.1103/PhysRevLett.81.2156 (cit. on p. 21).

[218] T. Munakata, S. Sinha, and W. Ditto. "Chaos Computing: Implementation of Fundamental Logical Gates by Chaotic Elements". In: *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 49.11 (2002), pp. 1629–1633. DOI: 10.1109/TCSI.2002.804551. URL: https://ieeexplore.ieee.org/abstract/document/1046831 (cit. on p. 21).

[219] W. Ditto, K. Murali, and S. Sinha. "Chaos Computing: Ideas and Implementations". In: *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 366.1865 (2008), pp. 653–664. DOI: 10.1098/rsta.2007.2116. URL: https://doi.org/10.1098/rsta.2007.2116 (cit. on p. 21).

[220] L. Adleman. "Molecular Computation of Solutions to Combinatorial Problems". In: *Science* 266 5187 (1994), pp. 1021–4 (cit. on p. 21).

[221] L. Adleman. "On Constructing a Molecular Computer". In: *DNA Based Computers*. 1995 (cit. on p. 21).

[222] L. Kari. "DNA Computing: Arrival of Biological Mathematics". In: *Mathematical Intelligencer* 19.2 (1997), pp. 9–22 (cit. on p. 21).

[223] Q. Liu et al. "DNA Computing on Surfaces". In: *Nature* 403.6766 (2000), pp. 175–179. ISSN: 1476-4687. DOI: 10.1038/35003155. URL: https://doi.org/10.1038/35003155 (cit. on p. 21).

[224] G. Păun, G. Rozenberg, and A. Salomaa. *DNA Computing: New Computing Paradigms*. Springer Science & Business Media, 2005 (cit. on p. 21).

[225] G. Păun. *Membrane Computing: An Introduction*. Springer Science & Business Media, 2002 (cit. on p. 21).

[226] G. Ciobanu, G. Păun, and M. Pérez-Jiménez. *Applications of Membrane Computing*. Vol. 17. Springer, 2006 (cit. on p. 21).

[227] G. Păun. "Membrane Computing". In: *Scholarpedia* 5.1 (2010), p. 9259 (cit. on p. 21).

[228] J. Torrejon et al. "Neuromorphic Computing with Nanoscale Spintronic Oscillators". In: *Nature* 547.7664 (2017), pp. 428–431. ISSN: 1476-4687. DOI: 10.1038/nature23011. URL: https://doi.org/10.1038/nature23011 (cit. on p. 21).

[229] C. Schuman et al. "A Survey of Neuromorphic Computing and Neural Networks in Hardware". In: (2017). URL: https://ui.adsabs.harvard.edu/abs/2017arXiv170506963S (cit. on p. 21).

[230] G. Burr et al. "Neuromorphic Computing using Non-Volatile Memory". In: *Advances in Physics: X* 2.1 (2017), pp. 89–124. DOI: 10.1080/23746149.2016.1259585. URL: https://doi.org/10.1080/23746149.2016.1259585 (cit. on p. 21).

[231] C. Schuman et al. "Opportunities for Neuromorphic Computing Algorithms and Applications". In: *Nature Computational Science* 2.1 (2022), pp. 10–19. ISSN: 2662-8457. DOI: 10.1038/s43588-021-00184-y. URL: https://doi.org/10.1038/s43588-021-00184-y (cit. on p. 21).

[232] A. Einstein, B. Podolsky, and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" In: *Phys. Rev.* 47 (10 1935), pp. 777–780. DOI: 10.1103/PhysRev.47.777. URL: https://link.aps.org/doi/10.1103/PhysRev.47.777 (cit. on p. 44).

[233] J. Bell. "On the Einstein-Podolsky-Rosen Paradox". In: *Physics Physique Fizika* 1 (3 1964), pp. 195–200. DOI: 10.1103/PhysicsPhysiqueFizika.1.195. URL: https://link.aps.org/doi/10.1103/PhysicsPhysiqueFizika.1.195 (cit. on p. 44).

[234] D. Greenberger, M. Horne, and A. Zeilinger. "Going Beyond Bell's Theorem". In: *Bell's Theorem, Quantum Theory and Conceptions of the Universe*. Ed. by M. Kafatos. Springer, 1989, pp. 69–72. ISBN: 978-94-017-0849-4. DOI: 10.1007/978-94-017-0849-4_10. URL: https://doi.org/10.1007/978-94-017-0849-4_10 (cit. on p. 45).

[235] W. Dür, G. Vidal, and I. Cirac. "Three Qubits can be Entangled in two Inequivalent Ways". In: *Phys. Rev. A* 62 (6 2000), p. 062314. DOI: 10.1103/PhysRevA.62.062314. URL: https://link.aps.org/doi/10.1103/PhysRevA.62.062314 (cit. on p. 46).

[236] H. Briegel and R. Raussendorf. "Persistent Entanglement in Arrays of Interacting Particles". In: *Phys. Rev. Lett.* 86 (5 2001), pp. 910–913. DOI: 10.1103/PhysRevLett.86.910. URL: https://link.aps.org/doi/10.1103/PhysRevLett.86.910 (cit. on p. 47).

[237] M. Hein, J. Eisert, and H. Briegel. "Multiparty Entanglement in Graph States". In: *Physical Review A* 69.6 (2004). ISSN: 1094-1622. DOI: 10.1103/physreva.69.062311. URL: http://dx.doi.org/10.1103/PhysRevA.69.062311 (cit. on p. 47).

[238] M. Van den Nest, J. Dehaene, and B. De Moor. "Local Unitary versus Local Clifford Equivalence of Stabilizer States". In: *Physical Review A* 71.6 (2005). ISSN: 1094-1622. DOI: 10.1103/physreva.71.062323. URL: http://dx.doi.org/10.1103/PhysRevA.71.062323 (cit. on p. 47).

[239] S. Anders and H. Briegel. "Fast Simulation of Stabilizer Circuits Using a Graph-State Representation". In: *Physical Review A* 73.2 (2006). ISSN: 1094-1622. DOI: 10.1103/physreva.73.022334. URL: http://dx.doi.org/10.1103/PhysRevA.73.022334 (cit. on p. 47).

[240] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. Briegel. "Entanglement in Graph States and its Applications". In: (2006) (cit. on p. 47).

[241] I. Good. "The Interaction Algorithm and Practical Fourier Analysis". In: *Journal of the Royal Statistical Society. Series B (Methodological)* 20.2 (1958), pp. 361–372. ISSN: 00359246. URL: http://www.jstor.org/stable/2983896 (cit. on p. 49).

[242] J. Cooley and J. Tukey. "An Algorithm for the Machine Calculation of Complex Fourier Series". In: *Mathematics of Computation* 19 (1965), pp. 297–301 (cit. on p. 49).

[243] D. Coppersmith. "An Approximate Fourier Transform Useful in Quantum Factoring". In: 1994 (cit. on p. 50).

[244] A. Kitaev. "Quantum Measurements and the Abelian Stabilizer Problem". In: *Electron. Colloquium Comput. Complex.* 3 (1996) (cit. on p. 50).

[245] J. Hadamard. "Resolution d'une Question Relative aux Determinants". In: *Bull. des Sciences Math.* 2 (1893), pp. 240–246. URL: https://ci.nii.ac.jp/naid/20000814080/en/ (cit. on p. 51).

[246] J. Walsh. "A Closed Set of Normal Orthogonal Functions". In: *American Journal of Mathematics* 45.1 (1923), pp. 5–24. ISSN: 00029327, 10806377. URL: http://www.jstor.org/stable/2387224 (cit. on p. 51).

[247] B. Fino and R. Algazi. "Unified Matrix Treatment of the Fast Walsh-Hadamard Transform". In: *IEEE Transactions on Computers* C-25.11 (1976), pp. 1142–1146. DOI: 10.1109/TC.1976.1674569 (cit. on p. 51).

[248] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels". In: *Phys. Rev. Lett.* 70 (13 1993), pp. 1895–1899. DOI: 10.1103/PhysRevLett.70.1895. URL: https://link.aps.org/doi/10.1103/PhysRevLett.70.1895 (cit. on p. 51).

[249] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. "Experimental Quantum Teleportation". In: *Nature* 390.6660 (1997), pp. 575–579. ISSN: 1476-4687. DOI: 10.1038/37539. URL: http://dx.doi.org/10.1038/37539 (cit. on p. 51).

[250] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu. "Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels". In: *Physical Review Letters* 80.6 (1998), pp. 1121–1125. ISSN: 1079-7114. DOI: 10.1103/physrevlett.80.1121. URL: http://dx.doi.org/10.1103/PhysRevLett.80.1121 (cit. on p. 51).

[251] J.-G. Ren et al. "Ground-to-Satellite Quantum Teleportation". In: *Nature* 549.7670 (2017), pp. 70–73. ISSN: 1476-4687. DOI: 10.1038/nature23675. URL: http://dx.doi.org/10.1038/nature23675 (cit. on p. 51).

[252] T. Feng, Q. Xu, L. Zhou, M. Luo, W. Zhang, and X. Zhou. *Quantum Information Transfer between a Two-Level and a Four-Level Quantum System*. 2020 (cit. on p. 51).

[253] B. Yurke and D. Stoler. "Bell's-Inequality Experiments Using Independent-Particle Sources". In: *Phys. Rev. A* 46 (5 1992), pp. 2229–2234. DOI: 10.1103/PhysRevA.46.2229. URL: https://link.aps.org/doi/10.1103/PhysRevA.46.2229 (cit. on p. 53).

[254] M. Żukowski, A. Zeilinger, M. Horne, and A. Ekert. ""Event-Ready-Detectors" Bell Experiment via Entanglement Swapping". In: *Phys. Rev. Lett.* 71 (26 1993), pp. 4287–4290. DOI: 10.1103/PhysRevLett.71.4287. URL: https://link.aps.org/doi/10.1103/PhysRevLett.71.4287 (cit. on p. 53).

[255] M. Halder, A. Beveratos, N. Gisin, V. Scarani, C. Simon, and H. Zbinden. "Entangling Independent Photons by Time Measurement". In: *Nature Physics* 3.10 (2007), pp. 692–695. ISSN: 1745-2481. DOI: 10.1038/nphys700. URL: https://doi.org/10.1038/nphys700 (cit. on p. 53).

[256] H. Briegel, W. Dür, I. Cirac, and P. Zoller. "Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication". In: *Phys. Rev. Lett.* 81 (26 1998), pp. 5932–5935. DOI: 10.1103/PhysRevLett.81.5932. URL: https://link.aps.org/doi/10.1103/PhysRevLett.81.5932 (cit. on p. 54).

[257] Z. Zhao, T. Yang, Y.-A. Chen, A.-N. Zhang, and J.-W. Pan. "Experimental Realization of Entanglement Concentration and a Quantum Repeater". In: *Phys. Rev. Lett.* 90 (20 2003), p. 207901. DOI: 10.1103/PhysRevLett.90.207901. URL: https://link.aps.org/doi/10.1103/PhysRevLett.90.207901 (cit. on p. 54).

[258] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin. "Quantum Repeaters based on Atomic Ensembles and Linear Optics". In: *Rev. Mod. Phys.* 83 (1 2011), pp. 33–80. DOI: 10.1103/RevModPhys.83.33. URL: https://link.aps.org/doi/10.1103/RevModPhys.83.33 (cit. on p. 54).

[259] J. Kimble. "The Quantum Internet". In: *Nature* 453.7198 (2008), pp. 1023–1030. DOI: 10.1038/nature07127. URL: https://doi.org/10.1038%5C%2Fnature07127 (cit. on pp. 54, 125).

[260] S. Pirandola and S. Braunstein. "Physics: Unite to build a Quantum Internet". In: *Nature* 532.7598 (2016), pp. 169–171. ISSN: 1476-4687. DOI: 10.1038/532169a. URL: https://doi.org/10.1038/532169a (cit. on p. 54).

[261] S. Wehner, D. Elkouss, and R. Hanson. "Quantum Internet: A Vision for the Road Ahead". In: *Science* 362.6412 (2018) (cit. on p. 54).

[262] A. Dahlberg et al. "A Link Layer Protocol for Quantum Networks". In: *Proceedings of the ACM Special Interest Group on Data Communication*. SIGCOMM '19. Association for Computing Machinery, 2019, pp. 159–173. ISBN: 9781450359566. DOI: 10.1145/3341302.3342070. URL: https://doi.org/10.1145/3341302.3342070 (cit. on p. 54).

[263] W. Kozlowski and S. Wehner. "Towards Large-Scale Quantum Networks". In: *Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication* (2019). DOI: 10.1145/3345312.3345497. URL: http://dx.doi.org/10.1145/3345312.3345497 (cit. on p. 54).

[264] W. Kozlowski, A. Dahlberg, and S. Wehner. "Designing a Quantum Network Protocol". In: *Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies* (2020). DOI: 10.1145/3386367.3431293. URL: http://dx.doi.org/10.1145/3386367.3431293 (cit. on p. 54).

[265] C. Bennett, H. Bernstein, S. Popescu, and B. Schumacher. "Concentrating Partial Entanglement by Local Operations". In: *Physical Review A* 53.4 (1996), pp. 2046–2052. ISSN: 1094-1622. DOI: 10.1103/physreva.53.2046. URL: http://dx.doi.org/10.1103/PhysRevA.53.2046 (cit. on p. 54).

[266] C. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. Wootters. "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels". In: *Physical Review Letters* 76.5 (1996), pp. 722–725. ISSN: 1079-7114. DOI: 10.1103/physrevlett.76.722. URL: http://dx.doi.org/10.1103/PhysRevLett.76.722 (cit. on pp. 54–56).

[267] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters. "Mixed-State Entanglement and Quantum Error Correction". In: *Physical Review A* 54.5 (1996), pp. 3824–3851. ISSN: 1094-1622. DOI: 10.1103/physreva.54.3824. URL: http://dx.doi.org/10.1103/PhysRevA.54.3824 (cit. on pp. 54, 55).

[268] W. Dür and H. Briegel. "Entanglement Purification and Quantum Error Correction". In: *Reports on Progress in Physics* 70.8 (2007), pp. 1381–1424. ISSN: 1361-6633. DOI: 10.1088/0034-4885/70/8/r03. URL: http://dx.doi.org/10.1088/0034-4885/70/8/R03 (cit. on p. 54).

[269] N. Gisin. "Hidden Quantum Nonlocality Revealed by Local Filters". In: *Physics Letters A* 210.3 (1996), pp. 151–156. ISSN: 0375-9601. DOI: https://doi.org/10.1016/S0375-9601(96)80001-6. URL: https://www.sciencedirect.com/science/article/pii/S0375960196800016 (cit. on p. 55).

[270] F. Verstraete, J. Dehaene, and B. DeMoor. "Local Filtering Operations on Two Qubits". In: *Phys. Rev. A* 64 (1 2001). DOI: 10.1103/PhysRevA.64.010101. URL: https://link.aps.org/doi/10.1103/PhysRevA.64.010101 (cit. on p. 55).

[271] Z.-W. Wang et al. "Experimental Entanglement Distillation of Two-Qubit Mixed States under Local Operations". In: *Phys. Rev. Lett.* 96 (22 2006). DOI: 10.1103/PhysRevLett.96.220505. URL: https://link.aps.org/doi/10.1103/PhysRevLett.96.220505 (cit. on p. 55).

[272] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels". In: *Phys. Rev. Lett.* 77 (13 1996), pp. 2818–2821. DOI: 10.1103/PhysRevLett.77.2818. URL: https://link.aps.org/doi/10.1103/PhysRevLett.77.2818 (cit. on pp. 55, 57, 71).

[273] A. Kent. "Entangled Mixed States and Local Purification". In: *Phys. Rev. Lett.* 81 (14 1998), pp. 2839–2841. DOI: 10.1103/PhysRevLett.81.2839. URL: https://link.aps.org/doi/10.1103/PhysRevLett.81.2839 (cit. on p. 55).

[274] K. Vollbrecht and F. Verstraete. "Interpolation of Recurrence and Hashing Entanglement Distillation Protocols". In: *Phys. Rev. A* 71 (6 2005), p. 062325. DOI: 10.1103/PhysRevA.71.062325. URL: https://link.aps.org/doi/10.1103/PhysRevA.71.062325 (cit. on p. 55).

[275] E. Hostens, J. Dehaene, and B. De Moor. "Stabilizer States and Clifford Operations for Systems of Arbitrary Dimensions and Modular Arithmetic". In: *Phys. Rev. A* 71 (4 2005). DOI: 10.1103/PhysRevA.71.042315. URL: https://link.aps.org/doi/10.1103/PhysRevA.71.042315 (cit. on p. 55).

[276] E. Maneva and J. Smolin. "Improved Two-Party and Multi-Party Purification Protocols". In: (2000) (cit. on p. 55).

[277] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete. "Local Permutations of Products of Bell States and Entanglement Distillation". In: *Physical Review A* 67.2 (2003). ISSN: 1094-1622. DOI: 10.1103/physreva.67.022310. URL: http://dx.doi.org/10.1103/PhysRevA.67.022310 (cit. on p. 55).

[278] H. Bombín and M. Martin-Delgado. "Entanglement Distillation Protocols and Number Theory". In: *Physical Review A* 72.3 (2005). ISSN: 1094-1622. DOI: 10.1103/physreva.72.032313. URL: http://dx.doi.org/10.1103/PhysRevA.72.032313 (cit. on p. 55).

[279] E. Campbell and S. Benjamin. "Measurement-Based Entanglement under Conditions of Extreme Photon Loss". In: *Phys. Rev. Lett.* 101 (13 2008). DOI: 10.1103/PhysRevLett.101.130502. URL: https://link.aps.org/doi/10.1103/PhysRevLett.101.130502 (cit. on p. 57).

[280] N. Nickerson, J. Fitzsimons, and S. Benjamin. "Freely Scalable Quantum Technologies Using Cells of 5-to-50 Qubits with Very Lossy and Noisy Photonic Links". In: *Physical Review X* 4.4 (2014). ISSN: 2160-3308. DOI: 10.1103/physrevx.4.041041. URL: http://dx.doi.org/10.1103/PhysRevX.4.041041 (cit. on p. 57).

[281] J. Park. "The Concept of Transition in Quantum Mechanics". In: *Foundations of Physics* 1.1 (1970), pp. 23–33. ISSN: 1572-9516. DOI: 10.1007/BF00708652. URL: https://doi.org/10.1007/BF00708652 (cit. on p. 57).

[282] W. Wootters and W. Zurek. "A Single Quantum Cannot be Cloned". In: *Nature* 299.5886 (1982), pp. 802–803. ISSN: 1476-4687. DOI: 10.1038/299802a0. URL: https://doi.org/10.1038/299802a0 (cit. on p. 57).

[283] D. Dieks. "Communication by EPR Devices". In: *Physics Letters A* 92.6 (1982), pp. 271–272. ISSN: 0375-9601. DOI: https://doi.org/10.1016/0375-9601(82)90084-6. URL: https://www.sciencedirect.com/science/article/pii/0375960182900846 (cit. on p. 57).

[284] A. Pati and S. Braunstein. "Impossibility of Deleting an Unknown Quantum State". In: *Nature* 404.6774 (2000), pp. 164–165. ISSN: 0028-0836. DOI: 10.1038/35004532. URL: http://dx.doi.org/10.1038/35004532 (cit. on p. 58).

[285] S. Popescu and D. Rohrlich. "Causality and Nonlocality as Axioms for Quantum Mechanics". In: *Fundam. Theor. Phys.* 97 (1998). Ed. by G. Hunter, S. Jeffers, and J.-P. Vigier, pp. 383–389. DOI: 10.1007/978-94-017-0990-3_45 (cit. on p. 58).

[286] A. Peres and D. Terno. "Quantum Information and Relativity Theory". In: *Reviews of Modern Physics* 76.1 (2004), pp. 93–123 (cit. on p. 58).

[287] G. Brassard and P. Høyer. "An Exact Quantum Polynomial-Time Algorithm for Simon's Problem". In: *Proceedings of the Fifth Israeli Symposium on Theory of Computing and Systems* (). DOI: 10.1109/istcs.1997.595153. URL: http://dx.doi.org/10.1109/ISTCS.1997.595153 (cit. on pp. 59, 62).

[288] L. Grover. "Quantum Computers Can Search Rapidly by Using Almost Any Transformation". In: *Physical Review Letters* 80.19 (1998), pp. 4329–4332. ISSN: 1079-7114. DOI: 10.1103/physrevlett.80.4329. URL: http://dx.doi.org/10.1103/PhysRevLett.80.4329 (cit. on pp. 59, 62).

[289] G. Brassard, P. Høyer, M. Mosca, and A. Tapp. "Quantum Amplitude Amplification and Estimation". In: *Quantum Computation and Information* (2002), pp. 53–74. ISSN: 0271-4132. DOI: 10.1090/conm/305/05215. URL: http://dx.doi.org/10.1090/conm/305/05215 (cit. on pp. 59, 62).

[290] C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. "Strengths and Weaknesses of Quantum Computing". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1510–1523. ISSN: 1095-7111. DOI: 10.1137/s0097539796300933. URL: http://dx.doi.org/10.1137/S0097539796300933 (cit. on p. 59).

[291] D. Bernstein, J. Buchmann, and E. Dahmen. *Post Quantum Cryptography*. 1st. Springer Publishing Company, Incorporated, 2008. ISBN: 3540887016 (cit. on pp. 59, 62).

[292] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt. "Applying Grover's Algorithm to AES: Quantum Resource Estimates". In: *Post-Quantum Cryptography*. Ed. by T. Takagi. Springer International Publishing, 2016, pp. 29–43. ISBN: 978-3-319-29360-8 (cit. on p. 59).

[293] G. Leander and A. May. "Grover Meets Simon - Quantumly Attacking the FX-Construction". In: *Advances in Cryptology - ASIACRYPT 2017*. Ed. by T. Takagi and T. Peyrin. Springer International Publishing, 2017, pp. 161–178. ISBN: 978-3-319-70697-9 (cit. on pp. 59, 60).

[294] S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia. "Implementing Grover Oracles for Quantum Key Search on AES and LowMC". In: *Advances in Cryptology – EUROCRYPT 2020*. Ed. by A. Canteaut and Y. Ishai. Springer International Publishing, 2020, pp. 280–310. ISBN: 978-3-030-45724-2 (cit. on p. 59).

[295] D. Bernstein. "Cost Analysis of Hash Collisions: Will Quantum Computers make SHARCS Obsolete?" In: *SHARCS'09 Workshop Record (Proceedings 4th Workshop on Special-purpose Hardware for Attacking Cryptograhic Systems, Lausanne, Switzerland, September 9-10, 2009)*. 2009, pp. 105–116 (cit. on p. 60).

[296] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia. "Breaking Symmetric Cryptosystems Using Quantum Period Finding". In: *Advances in Cryptology – CRYPTO 2016*. Ed. by M. Robshaw and J. Katz. Lecture Notes in Computer Science (LNCS). Springer Berlin Heidelberg, 2016, pp. 207–237. ISBN: 978-3-662-53007-8. DOI: 10.1007/978-3-662-53008-5_8. URL: https://www.iacr.org/conferences/crypto2016/,%20https://www.iacr.org/conferences/crypto2016/index.html (cit. on p. 60).

[297] T. Santoli and C. Schaffner. "Using Simon's Algorithm to Attack Symmetric-Key Cryptographic Primitives". In: *Quantum Info. Comput.* 17.1–2 (2017), pp. 65–78. ISSN: 1533-7146 (cit. on p. 60).

[298] X. Bonnetain, A. Hosoyamada, M. Naya-Plasencia, Y. Sasaki, and A. Schrottenloher. "Quantum Attacks Without Superposition Queries: The Offline Simon's Algorithm". In: *Advances in Cryptology – ASIACRYPT 2019*. Ed. by S. Galbraith and S. Moriai. Springer International Publishing, 2019, pp. 552–583. ISBN: 978-3-030-34578-5 (cit. on p. 60).

[299] G. Brassard, P. Høyer, and A. Tapp. "Quantum Cryptanalysis of Hash and Claw-Free Functions". In: *Lecture Notes in Computer Science* (1998), pp. 163–169. ISSN: 1611-3349. DOI: 10.1007/bfb0054319. URL: http://dx.doi.org/10.1007/BFb0054319 (cit. on pp. 60, 62).

[300] A. Hosoyamada, Y. Sasaki, and K. Xagawa. "Quantum Multicollision-Finding Algorithm". In: *Advances in Cryptology – ASIACRYPT 2017*. Ed. by T. Takagi and T. Peyrin. Springer International Publishing, 2017, pp. 179–210. ISBN: 978-3-319-70697-9 (cit. on p. 61).

[301] A. Hosoyamada and Y. Sasaki. "Finding Hash Collisions with Quantum Computers by Using Differential Trails with Smaller Probability than Birthday Bound". In: *Advances in Cryptology – EUROCRYPT 2020*. Ed. by A. Canteaut and Y. Ishai. Springer International Publishing, 2020, pp. 249–279. ISBN: 978-3-030-45724-2 (cit. on p. 61).

[302] C. Pomerance. "A Tale of Two Sieves". In: *Notices Amer. Math. Soc* 43 (1996), pp. 1473–1485 (cit. on p. 61).

[303] N. I. of Standards and Technology. *Digital Signature Standard (DSS)*. 2013. URL: https://csrc.nist.gov/publications/detail/fips/186/4/final (cit. on p. 62).

[304] T. ElGamal. "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms". In: *IEEE Transactions on Information Theory* 31.4 (1985), pp. 469–472. DOI: 10.1109/TIT.1985.1057074 (cit. on p. 62).

[305] D. Johnson and A. Menezes. *The Elliptic Curve Digital Signature Algorithm (ECDSA)*. Tech. rep. 1999 (cit. on p. 62).

[306] E. Barker, D. Johnson, and M. Smid. *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. 2017. URL: https://www.nist.gov/publications/recommendation-pair-wise-key-establishment-schemes-using-discrete-logarithm (cit. on p. 62).

[307] D. Bernstein and T. Lange. "Post-Quantum Cryptography". In: *Nature* 549.7671 (2017), pp. 188–194. ISSN: 1476-4687. DOI: 10.1038/nature23461. URL: https://doi.org/10.1038/nature23461 (cit. on p. 62).

[308] S. Wiesner. "Conjugate Coding". In: *SIGACT News* 15.1 (1983), pp. 78–88. ISSN: 0163-5700. DOI: 10.1145/1008908.1008920. URL: https://doi.org/10.1145/1008908.1008920 (cit. on pp. 62, 65, 66).

[309] C. Bennett and G. Brassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing". In: *Theoretical Computer Science* 560 (1984), pp. 7–11. ISSN: 0304-3975. DOI: 10.1016/j.tcs.2014.05.025. URL: http://dx.doi.org/10.1016/j.tcs.2014.05.025 (cit. on pp. 62, 65, 66, 68, 75, 80, 85).

[310] F. Grasselli. *Quantum Cryptography: From Key Distribution to Conference Key Agreement*. Springer, 2021. ISBN: 978-3-030-64359-1 (cit. on p. 62).

[311] L. Kocarev. "Chaos-Based Cryptography: A Brief Overview". In: *IEEE Circuits and Systems Magazine* 1.3 (2001), pp. 6–21 (cit. on p. 62).

[312] L. Kocarev and S. Lian. *Chaos-Based Cryptography: Theory, Algorithms and Applications*. Vol. 354. Springer Science & Business Media, 2011 (cit. on p. 62).

[313] G. Xiao, M. Lu, L. Qin, and X. Lai. "New Field of Cryptography: DNA Cryptography". In: *Chinese Science Bulletin* 51.12 (2006), pp. 1413–1420. ISSN: 1861-9541. DOI: 10.1007/s11434-006-2012-5. URL: https://doi.org/10.1007/s11434-006-2012-5 (cit. on p. 62).

[314] L. Liu, Q. Zhang, and X. Wei. "A RGB Image Encryption Algorithm Based on DNA Encoding and Chaos Map". In: *Computers & Electrical Engineering* 38.5 (2012), pp. 1240–1248. ISSN: 0045-7906. DOI: 10.1016/j.compeleceng.2012.02.007. URL: http://dx.doi.org/10.1016/j.compeleceng.2012.02.007 (cit. on p. 62).

[315] M. Ajtai. "Generating Hard Instances of Lattice Problems". In: *In Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*. ACM, 1996, pp. 99–108 (cit. on p. 62).

[316] O. Goldreich, S. Goldwasser, and S. Halevi. "Public-Key Cryptosystems from Lattice Reduction Problems". In: *Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology*. CRYPTO '97. Berlin, Heidelberg: Springer-Verlag, 1997, pp. 112–131. ISBN: 3540633847 (cit. on p. 62).

[317] M. Ajtai and C. Dwork. "A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence". In: *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*. STOC '97. Association for Computing Machinery, 1997, pp. 284–293. ISBN: 0897918886. DOI: 10.1145/258533.258604. URL: https://doi.org/10.1145/258533.258604 (cit. on p. 62).

[318] J. Hoffstein, J. Pipher, and J. Silverman. *US6081597A - Public Key Cryptosystem Method and Apparatus*. 1998. URL: https://patents.google.com/patent/US6081597 (cit. on p. 62).

[319] J. Hoffstein, J. Pipher, and J. Silverman. "NTRU: A Ring-Based Public Key Cryptosystem". In: *ANTS*. 1998 (cit. on p. 62).

[320] O. Regev. "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography". In: STOC '05. Association for Computing Machinery, 2005, pp. 84–93. ISBN: 1581139608. DOI: 10.1145/1060590.1060603. URL: https://doi.org/10.1145/1060590.1060603 (cit. on p. 62).

[321] D. Micciancio. "Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions". In: *Comput. Complex.* 16.4 (2007), pp. 365–411. ISSN: 1016-3328. DOI: 10.1007/s00037-007-0234-9. URL: https://doi.org/10.1007/s00037-007-0234-9 (cit. on p. 62).

[322] C. Gentry, C. Peikert, and V. Vaikuntanathan. *Trapdoors for Hard Lattices and New Cryptographic Constructions*. 2007 (cit. on p. 62).

[323] V. Lyubashevsky and D. Micciancio. "Asymptotically Efficient Lattice-Based Digital Signatures". In: *Theory of Cryptography*. Ed. by R. Canetti. Springer Berlin Heidelberg, 2008, pp. 37–54. ISBN: 978-3-540-78524-8 (cit. on p. 62).

[324] V. Lyubashevsky, D. Micciancio, C. Peikert, and A. Rosen. "SWIFFT: A Modest Proposal for FFT Hashing". In: *Fast Software Encryption*. Ed. by K. Nyberg. Springer Berlin Heidelberg, 2008, pp. 54–72. ISBN: 978-3-540-71039-4 (cit. on p. 62).

[325] C. Peikert. "Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem". In: *Theoretical Foundations of Practical Information Security*. Ed. by R. Canetti, S. Goldwasser, G. Müller, and R. Steinwandt. Vol. 8491. Dagstuhl Seminar Proceedings (DagSemProc). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2009. DOI: 10.42

30/DagSemProc.08491.4. URL: https://drops.dagstuhl.de/opus/volltexte/2009/1892 (cit. on p. 62).

[326] T. Güneysu, V. Lyubashevsky, and T. Pöppelmann. "Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems". In: *Cryptographic Hardware and Embedded Systems – CHES 2012*. Ed. by E. Prouff and P. Schaumont. Springer Berlin Heidelberg, 2012, pp. 530–547. ISBN: 978-3-642-33027-8 (cit. on p. 62).

[327] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky. "Lattice Signatures and Bimodal Gaussians". In: *Advances in Cryptology – CRYPTO 2013*. Ed. by R. Canetti and J. Garay. Springer Berlin Heidelberg, 2013, pp. 40–56. ISBN: 978-3-642-40041-4 (cit. on p. 62).

[328] C. Peikert. "Lattice Cryptography for the Internet". In: *Post-Quantum Cryptography*. Ed. by M. Mosca. Springer International Publishing, 2014, pp. 197–219. ISBN: 978-3-319-11659-4 (cit. on p. 62).

[329] S. Akleylek, N. Bindel, J. Buchmann, J. Krämer, and G. Marson. "An Efficient Lattice-Based Signature Scheme with Provably Secure Instantiation". In: *Progress in Cryptology – AFRICACRYPT 2016*. Ed. by D. Pointcheval, A. Nitaj, and T. Rachidi. Springer International Publishing, 2016, pp. 44–60. ISBN: 978-3-319-31517-1 (cit. on p. 62).

[330] A. Chopra. *GLYPH: A New Instantiation of the GLP Digital Signature Scheme*. 2017 (cit. on p. 62).

[331] R. McEliece. "A Public-Key Cryptosystem Based On Algebraic Coding Theory". In: *Deep Space Network Progress Report* 44 (1978), pp. 114–116 (cit. on p. 62).

[332] H. Niederreiter. "Knapsack-Type Cryptosystems and Algebraic Coding Theory". In: *Prob. Contr. Inform. Theory* 15.2 (1986), pp. 157–166 (cit. on p. 62).

[333] E. Fujisaki and T. Okamoto. "Secure Integration of Asymmetric and Symmetric Encryption Schemes". In: *Advances in Cryptology — CRYPTO' 99*. Ed. by M. Wiener. Springer Berlin Heidelberg, 1999, pp. 537–554. ISBN: 978-3-540-48405-9 (cit. on p. 62).

[334] K. Kobara and H. Imai. "Semantically Secure McEliece Public-Key Cryptosystems - Conversions for McEliece PKC". In: *Public Key Cryptography*. Ed. by K. Kim. Springer Berlin Heidelberg, 2001, pp. 19–35. ISBN: 978-3-540-44586-9 (cit. on p. 62).

[335] N. Courtois, M. Finiasz, and N. Sendrier. "How to Achieve a McEliece-Based Digital Signature Scheme". In: *Advances in Cryptology — ASIACRYPT 2001*. Ed. by C. Boyd. Springer Berlin Heidelberg, 2001, pp. 157–174. ISBN: 978-3-540-45682-7 (cit. on p. 62).

[336] D. Augot, M. Finiasz, and N. Sendrier. *A Fast Provably Secure Cryptographic Hash Function*. 2003 (cit. on p. 62).

[337] B. Biswas and N. Sendrier. "McEliece Cryptosystem Implementation: Theory and Practice". In: *Post-Quantum Cryptography*. Ed. by J. Buchmann and J. Ding. Springer Berlin Heidelberg, 2008, pp. 47–62. ISBN: 978-3-540-88403-3 (cit. on p. 62).

[338] Y. Wang. "Quantum Resistant Random Linear Code Based Public Key Encryption Scheme RLCE". In: *2016 IEEE International Symposium on Information Theory (ISIT)*. 2016, pp. 2519–2523. DOI: 10.1109/ISIT.2016.7541753 (cit. on p. 62).

[339] R. Merkle. "A Certified Digital Signature". In: *Advances in Cryptology — CRYPTO' 89 Proceedings*. Ed. by G. Brassard. Springer New York, 1989, pp. 218–238. ISBN: 978-0-387-34805-6 (cit. on p. 62).

[340] F. Leighton and S. Micali. *US5432852A - Large Provably Fast and Secure Digital Signature Schemes Based on Secure Hash Functions*. 1994. URL: https://patents.google.com/patent/US5432852A/en (cit. on p. 62).

[341] A. Perrig. "The BiBa One-Time Signature and Broadcast Authentication Protocol". In: *Proceedings of the 8th ACM Conference on Computer and Communications Security*. CCS '01. Association for Computing Machinery, 2001, pp. 28–37. ISBN: 1581133855. DOI: 10.1145/501983.501988. URL: https://doi.org/10.1145/501983.501988 (cit. on p. 62).

[342] L. Reyzin and N. Reyzin. "Better than BiBa: Short One-Time Signatures with Fast Signing and Verifying". In: *Information Security and Privacy*. Ed. by L. Batten and J. Seberry. Springer Berlin Heidelberg, 2002, pp. 144–153. ISBN: 978-3-540-45450-2 (cit. on p. 62).

[343] J. Buchmann, L. García, E. Dahmen, M. Döring, and E. Klintsevich. "CMSS – An Improved Merkle Signature Scheme". In: *IN PROGRESS IN CRYPTOLOGY - INDOCRYPT 2006*. Springer-Verlag, 2006, pp. 349–363 (cit. on p. 62).

[344] J. Buchmann, E. Dahmen, E. Klintsevich, K. Okeya, and C. Vuillaume. "Merkle Signatures with Virtually Unlimited Signature Capacity". In: *Applied Cryptography and Network Security*. Ed. by J. Katz and M. Yung. Springer Berlin Heidelberg, 2007, pp. 31–45. ISBN: 978-3-540-72738-5 (cit. on p. 62).

[345] J. Buchmann, E. Dahmen, S. Ereth, A. Hülsing, and M. Rückert. "On the Security of the Winternitz One-Time Signature Scheme". In: *Progress in Cryptology – AFRICACRYPT 2011*. Ed. by A. Nitaj and D. Pointcheval. Springer Berlin Heidelberg, 2011, pp. 363–378. ISBN: 978-3-642-21969-6 (cit. on p. 62).

[346] J. Buchmann, E. Dahmen, and A. Hülsing. *XMSS - A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions*. 2011 (cit. on p. 62).

[347] A. Hülsing, L. Rausch, and J. Buchmann. "Optimal Parameters for XMSSMT". In: *Security Engineering and Intelligence Informatics*. Ed. by A. Cuzzocrea, C. Kittl, D. Simos, E. Weippl, and L. Xu. Springer Berlin Heidelberg, 2013, pp. 194–208. ISBN: 978-3-642-40588-4 (cit. on p. 62).

[348] D. Bernstein et al. *SPHINCS: Practical Stateless Hash-Based Signatures*. 2014 (cit. on p. 62).

[349] L. De Feo, D. Jao, and J. Plût. "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies". In: *Journal of Mathematical Cryptology* 8.3 (2014), pp. 209–247. DOI: doi:10.1515/jmc-2012-0015. URL: https://doi.org/10.1515/jmc-2012-0015 (cit. on p. 62).

[350] C. Costello, D. Jao, P. Longa, M. Naehrig, J. Renes, and D. Urbanik. *Efficient Compression of SIDH Public Keys*. 2016 (cit. on p. 62).

[351] R. Azarderakhsh, D. Jao, K. Kalach, B. Koziel, and C. Leonardi. *Key Compression for Isogeny-Based Cryptosystems*. 2016 (cit. on p. 62).

[352] T. Matsumoto and H. Imai. "Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption". In: *Advances in Cryptology — EUROCRYPT '88*. Springer Berlin Heidelberg, 1988, pp. 419–453. ISBN: 978-3-540-45961-3 (cit. on p. 62).

[353] J. Patarin. "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms". In: *Advances in Cryptology — EUROCRYPT '96*. Ed. by U. Maurer. Springer Berlin Heidelberg, 1996, pp. 33–48. ISBN: 978-3-540-68339-1 (cit. on p. 62).

[354] J. Patarin. "The Oil and Vinegar Signature Scheme". In: *Dagstuhl Workshop on Cryptography September, 1997*. 1997 (cit. on p. 62).

[355] A. Kipnis, J. Patarin, and L. Goubin. "Unbalanced Oil and Vinegar Signature Schemes". In: *Advances in Cryptology — EUROCRYPT '99*. Ed. by J. Stern. Springer Berlin Heidelberg, 1999, pp. 206–222. ISBN: 978-3-540-48910-8 (cit. on p. 62).

[356] J. Patarin, N. Courtois, and L. Goubin. "FLASH, a Fast Multivariate Signature Algorithm". In: *Proceedings of the 2001 Conference on Topics in Cryptology: The Cryptographer's Track at RSA*. CT-RSA 2001. Springer-Verlag, 2001, pp. 298–307. ISBN: 3540418989 (cit. on p. 62).

[357] J. Patarin, N. Courtois, and L. Goubin. "QUARTZ, 128-Bit Long Digital Signatures". In: *Proceedings of the 2001 Conference on Topics in Cryptology: The Cryptographer's Track at RSA*. CT-RSA 2001. Springer-Verlag, 2001, pp. 282–297. ISBN: 3540418989 (cit. on p. 62).

[358] B.-Y. Yang, J.-M. Chen, and Y.-H. Chen. "TTS: High-Speed Signatures on a Low-Cost Smart Card". In: *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings*. Vol. 3156. Lecture Notes in Computer Science. Springer, 2004, pp. 371–385. DOI: 10.1007/978-3-540-28632-5_27. URL: https://iacr.org/archive/ches2004/31560371/31560371.pdf (cit. on p. 62).

[359] J.-M. Chen and B.-Y. Yang. "A More Secure and Efficacious TTS Signature Scheme". In: *Information Security and Cryptology - ICISC 2003*. Ed. by J.-I. Lim and D.-H. Lee. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 320–338. ISBN: 978-3-540-24691-6 (cit. on p. 62).

[360] J. Ding and D. Schmidt. "Rainbow, a New Multivariable Polynomial Signature Scheme". In: *Applied Cryptography and Network Security*. Ed. by J. Ioannidis, A. Keromytis, and M. Yung. Springer Berlin Heidelberg, 2005, pp. 164–175. ISBN: 978-3-540-31542-1 (cit. on p. 62).

[361] M.-S. Chen, A. Hülsing, J. Rijneveld, S. Samardjiska, and P. Schwabe. *From 5-Pass MQ-Based Identification to MQ-Based Signatures*. 2016 (cit. on p. 62).

[362] A. Casanova et al. *GeMSS: A Great Multivariate Short Signature*. Tech. rep. 2017, pp. 1–4. URL: https://hal.inria.fr/hal-01662158 (cit. on p. 62).

[363] W. Beullens and B. Preneel. "Field Lifting for Smaller UOV Public Keys". In: *International Conference on Cryptology in India*. Springer. 2017, pp. 227–246 (cit. on p. 62).

[364] N. Wagner and M. Magyarik. "A Public Key Cryptosystem Based on the Word Problem". In: *Proceedings of CRYPTO 84 on Advances in Cryptology*. Springer-Verlag, 1985, pp. 19–36. ISBN: 0387156585 (cit. on p. 62).

[365] I. Anshel, M. Anshel, and D. Goldfeld. "An Algebraic Method for Public-Key Cryptography". In: *Mathematical Research Letters* 6 (1999), pp. 287–291 (cit. on p. 62).

[366] K. Ko et al. "New Public-Key Cryptosystem Using Braid Groups". In: *Advances in Cryptology — CRYPTO 2000*. Ed. by M. Bellare. Springer Berlin Heidelberg, 2000, pp. 166–183. ISBN: 978-3-540-44598-2 (cit. on p. 62).

[367] V. Shpilrain and G. Zapata. "Combinatorial Group Theory and Public Key Cryptography". In: *Applicable Algebra in Engineering, Communication and Computing* 17.3 (2006), pp. 291–302 (cit. on p. 62).

[368] M. Chase et al. "Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. CCS '17. Association for Computing Machinery, 2017, pp. 1825–1842. ISBN: 9781450349468. DOI: 10.1145/3133956.3133997. URL: https://doi.org/10.1145/3133956.3133997 (cit. on p. 62).

[369] E. Ben-Sasson, A. Chiesa, M. Riabzev, N. Spooner, M. Virza, and N. Ward. *Aurora: Transparent Succinct Arguments for R1CS*. 2018 (cit. on p. 62).

[370] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev. *Scalable, Transparent, and Post-Quantum Secure Computational Integrity*. 2018 (cit. on p. 62).

[371] A. Chiesa, D. Ojha, and N. Spooner. *Fractal: Post-Quantum and Transparent Recursive Proofs from Holography*. 2019 (cit. on p. 62).

[372] 2018. URL: https://www.accenture.com/_acnmedia/pdf-87/accenture-809668-quantum-cryptography-whitepaper-v05.pdf (cit. on p. 63).

[373] 2020. URL: https://www.accenture.com/_acnmedia/PDF-119/Accenture-SpeQtral-In-Quantum-We-Trust.pdf (cit. on p. 63).

[374] A. Ekert. "Quantum Cryptography Based on Bell's Theorem". In: *Physical Review Letters* 67 (1991), pp. 661–663 (cit. on pp. 65, 68, 86).

[375] C. Bennett. "Quantum Cryptography Using any Two Nonorthogonal States". In: *Phys. Rev. Lett.* 68 (21 1992), pp. 3121–3124. DOI: 10.1103/PhysRevLett.68.3121. URL: https://link.aps.org/doi/10.1103/PhysRevLett.68.3121 (cit. on pp. 65, 68, 79).

[376] C. Bennett, G. Brassard, and D. Mermin. "Quantum Cryptography Without Bell's Theorem". In: *Phys. Rev. Lett.* 68 (5 1992), pp. 557–559. DOI: 10.1103/PhysRevLett.68.557. URL: https://link.aps.org/doi/10.1103/PhysRevLett.68.557 (cit. on pp. 65, 68, 89).

[377] Y. Mu, J. Seberry, and Y. Zheng. "Shared Cryptographic Bits via Quantized Quadrature Phase Amplitudes of Light". In: *Optics Communications* 123.1 (1996), pp. 344–352. ISSN: 0030-4018. DOI: https://doi.org/10.1016/0030-4018(95)00688-5. URL: https://www.sciencedirect.com/science/article/pii/0030401895006885 (cit. on pp. 65, 68, 85).

[378] H. Bechmann-Pasquinucci and N. Gisin. "Incoherent and Coherent Eavesdropping in the Six-State Protocol of Quantum Cryptography". In: *Physical Review A* 59.6 (1999), pp. 4238–4248. ISSN: 1094-1622. DOI: 10.1103/physreva.59.4238. URL: http://dx.doi.org/10.1103/PhysRevA.59.4238 (cit. on pp. 65, 68, 83).

[379] W.-Y. Hwang. "Quantum Key Distribution with High Loss: Toward Global Secure Communication". In: *Physical Review Letters* 91.5 (2003). DOI: 10.1103/physrevlett.91.057901. URL: https://doi.org/10.1103%5C%2Fphysrevlett.91.057901 (cit. on pp. 65, 85).

[380] B.-G. Englert et al. *Efficient and Robust Quantum Key Distribution with Minimal State Tomography*. 2004. DOI: 10.48550/ARXIV.QUANT-PH/0412075. URL: https://arxiv.org/abs/quant-ph/0412075 (cit. on p. 65).

[381] J. Renes. "Spherical-Code Key-Distribution Protocols for Qubits". In: *Physical Review A* 70.5 (2004). DOI: 10.1103/physreva.70.052314. URL: https://doi.org/10.1103%5C%2Fphysreva.70.052314 (cit. on p. 65).

[382] V. Scarani, A. Acín, G. Ribordy, and N. Gisin. "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations". In: *Phys. Rev. Lett.* 92 (5 2004). DOI: 10.1103/PhysRevLett.92.057901. URL: https://link.aps.org/doi/10.1103/PhysRevLett.92.057901 (cit. on pp. 65, 85).

[383] K. Tamaki and H.-K. Lo. "Unconditionally Secure Key Distillation from Multiphotons". In: *Physical Review A* 73.1 (2006). DOI: 10.1103/physreva.73.010302. URL: https://doi.org/10.1103%5C%2Fphysreva.73.010302 (cit. on p. 65).

[384] M. Khan, M. Murphy, and A. Beige. "High Error-Rate Quantum Key Distribution for Long-Distance Communication". In: *New Journal of Physics* 11.6 (2009). DOI: 10.1088/1367-2630/11/6/063043. URL: https://doi.org/10.1088%5C%2F1367-2630%5C%2F11%5C%2F6%5C%2F063043 (cit. on p. 65).

[385] E. Serna. *Quantum Key Distribution Protocol with Private-Public Key*. 2009. DOI: 10.48550/ARXIV.0908.2146. URL: https://arxiv.org/abs/0908.2146 (cit. on p. 65).

[386] M. Lucamarini et al. “Efficient Decoy-State Quantum Key Distribution with Quantified Security”. In: *Opt. Express* 21.21 (2013), pp. 24550–24565. DOI: 10.1364/OE.21.024550. URL: http://opg.optica.org/oe/abstract.cfm?URI=oe-21-21-24550 (cit. on pp. 65, 85).

[387] M. Boyer, D. Kenigsberg, and T. Mor. “Quantum Key Distribution with Classical Bob”. In: *Phys. Rev. Lett.* 99 (14 2007). DOI: 10.1103/PhysRevLett.99.140501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.99.140501 (cit. on pp. 65, 91).

[388] M. Boyer, R. Gelles, D. Kenigsberg, and T. Mor. “Semiquantum Key Distribution”. In: *Phys. Rev. A* 79 (3 2009), p. 032341. DOI: 10.1103/PhysRevA.79.032341. URL: https://link.aps.org/doi/10.1103/PhysRevA.79.032341 (cit. on pp. 65, 91, 93, 94).

[389] X. Zou, D. Qiu, L. Li, L. Wu, and L. Li. “Semiquantum-Key Distribution Using Less than Four Quantum States”. In: *Phys. Rev. A* 79 (5 2009). DOI: 10.1103/PhysRevA.79.052312. URL: https://link.aps.org/doi/10.1103/PhysRevA.79.052312 (cit. on pp. 65, 94).

[390] W. Krawec. “Restricted Attacks on Semi-Quantum Key Distribution Protocols”. In: *Quantum Information Processing* 13.11 (2014), pp. 2417–2436. ISSN: 1570-0755. DOI: 10.1007/s11128-014-0802-2. URL: https://doi.org/10.1007/s11128-014-0802-2 (cit. on pp. 65, 96).

[391] X. Zou, D. Qiu, S. Zhang, and P. Mateus. “Semiquantum Key Distribution without Invoking the Classical Party’s Measurement Capability”. In: *Quantum Information Processing* 14.8 (2015), pp. 2981–2996. DOI: 10.1007/s11128-015-1015-z (cit. on pp. 65, 96).

[392] W. Zhang and D. Qiu. *A Single-State Semi-Quantum Key Distribution Protocol and its Security Proof*. 2016. DOI: 10.48550/ARXIV.1612.03087. URL: https://arxiv.org/abs/1612.03087 (cit. on pp. 65, 96).

[393] W. Krawec and E. Geiss. “Semi-Quantum Key Distribution with Limited Measurement Capabilities”. In: *2018 International Symposium on Information Theory and Its Applications (ISITA)*. 2018, pp. 462–466. DOI: 10.23919/ISITA.2018.8664264 (cit. on pp. 65, 96).

[394] A. Gagliano, W. Krawec, and H. Iqbal. *From Classical to Semi-Quantum Secure Communication*. 2019. DOI: 10.48550/ARXIV.1901.01611. URL: https://arxiv.org/abs/1901.01611 (cit. on pp. 65, 96).

[395] Z. Sun, C. Zhang, B. Wang, Q. Li, and D. Long. “Improvements on “Multiparty Quantum Key Agreement with Single Particles””. In: *Quantum Information Processing* 12.11 (2013), pp. 3411–3420. ISSN: 1573-1332. DOI: 10.1007/s11128-013-0608-7. URL: https://doi.org/10.1007/s11128-013-0608-7 (cit. on pp. 65, 101).

[396] G.-B. Xu, Q.-Y. Wen, F. Gao, and S.-J. Qin. “Novel Multiparty Quantum Key Agreement Protocol with GHZ States”. In: *Quantum Information Processing* 13.12 (2014), pp. 2587–2594. ISSN: 1573-1332. DOI: 10.1007/s11128-014-0816-9. URL: https://doi.org/10.1007/s11128-014-0816-9 (cit. on pp. 65, 101).

[397] Y.-F. He and W.-P. Ma. "Quantum Key Agreement Protocols with Four-Qubit Cluster States". In: *Quantum Information Processing* 14.9 (2015), pp. 3483–3498. ISSN: 1573-1332. DOI: 10.1007/s11128-015-1060-7. URL: https://doi.org/10.1007/s11128-015-1060-7 (cit. on pp. 65, 101).

[398] Z. Sun, J. Yu, and P. Wang. "Efficient Multi-Party Quantum Key Agreement by Cluster States". In: *Quantum Information Processing* 15.1 (2015), pp. 373–384. ISSN: 1573-1332. DOI: 10.1007/s11128-015-1155-1. URL: https://doi.org/10.1007/s11128-015-1155-1 (cit. on p. 65).

[399] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß. "Multi-Partite Entanglement can Speed Up Quantum Key Distribution in Networks". In: *New Journal of Physics* 19.9 (2017), p. 093012. ISSN: 1367-2630. DOI: 10.1088/1367-2630/aa8487. URL: http://dx.doi.org/10.1088/1367-2630/aa8487 (cit. on pp. 65, 98).

[400] H. Cao and W. Ma. "Multiparty Quantum Key Agreement Based on Quantum Search Algorithm". In: *Scientific Reports* 7.1 (2017). ISSN: 2045-2322. DOI: 10.1038/srep45046. URL: https://doi.org/10.1038/srep45046 (cit. on p. 65).

[401] F. Grasselli, H. Kampermann, and D. Bruß. "Finite-Key Effects in Multipartite Quantum Key Distribution Protocols". In: *New Journal of Physics* 20.11 (2018), p. 113014. DOI: 10.1088/1367-2630/aaec34. URL: https://doi.org/10.1088/1367-2630/aaec34 (cit. on pp. 65, 99).

[402] Y.-H. Chou, G.-J. Zeng, Z.-H. Chang, and S.-Y. Kuo. "Dynamic Group Multi-Party Quantum Key Agreement". In: *Scientific Reports* 8.1 (2018), p. 4633. ISSN: 2045-2322. DOI: 10.1038/s41598-018-21658-6. URL: https://doi.org/10.1038/s41598-018-21658-6 (cit. on pp. 65, 101).

[403] F. Grasselli, H. Kampermann, and D. Bruß. "Conference Key Agreement with Single-Photon Interference". In: *New Journal of Physics* 21.12 (2019). ISSN: 1367-2630. DOI: 10.1088/1367-2630/ab573e. URL: http://dx.doi.org/10.1088/1367-2630/ab573e (cit. on pp. 65, 100).

[404] F. Hahn et al. *Anonymous Conference Key Agreement in Quantum Networks*. 2020. DOI: 10.48550/ARXIV.2007.07995. URL: https://arxiv.org/abs/2007.07995 (cit. on pp. 65, 101).

[405] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß. "Quantum Conference Key Agreement: A Review". In: *Advanced Quantum Technologies* 3.11 (2020). DOI: 10.1002/qute.202000025. URL: https://doi.org/10.1002%5C%2Fqute.202000025 (cit. on pp. 65, 97, 98, 107, 108, 110).

[406] P. Singkanipa and P. Kok. *Quantum Conference Key Agreement with Photon Loss*. 2021. DOI: 10.48550/ARXIV.2101.01483. URL: https://arxiv.org/abs/2101.01483 (cit. on pp. 65, 101).

[407] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi. "Experimental Quantum Conference Key Agreement". In: *Science Advances* 7.23 (2021). DOI: 10.1126/sciadv.abe0395. URL: https://doi.org/10.1126%5C%2Fsciadv.abe0395 (cit. on p. 65).

[408] J. Dynes, Z. Yuan, A. Sharpe, and A. Shields. "A High Speed, Postprocessing Free, Quantum Random Number Generator". In: *Applied Physics Letters* 93.3 (2008), p. 031109. DOI: 10.1063/1.2961000. URL: https://doi.org/10.1063/1.2961000 (cit. on p. 65).

[409] M. Wayne and P. Kwiat. "Low-Bias High-Speed Quantum Random Number Generator via Shaped Optical Pulses". In: *Opt. Express* 18.9 (2010), pp. 9351–9357. DOI: 10.1364/OE.18.009351. URL: http://opg.optica.org/oe/abstract.cfm?URI=oe-18-9-9351 (cit. on p. 65).

[410] H. Fürst et al. "High Speed Optical Quantum Random Number Generation". In: *Opt. Express* 18.12 (2010), pp. 13029–13037. DOI: 10.1364/OE.18.013029. URL: http://opg.optica.org/oe/abstract.cfm?URI=oe-18-12-13029 (cit. on p. 65).

[411] C. Gabriel et al. "A Generator for Unique Quantum Random Numbers Based on Vacuum States". In: *Nature Photonics* 4.10 (2010), pp. 711–715. ISSN: 1749-4893. DOI: 10.1038/nphoton.2010.197. URL: https://doi.org/10.1038/nphoton.2010.197 (cit. on p. 65).

[412] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo. "Ultrafast Quantum Random Number Generation Based on Quantum Phase Fluctuations". In: *Opt. Express* 20.11 (2012), pp. 12366–12377. DOI: 10.1364/OE.20.012366. URL: http://opg.optica.org/oe/abstract.cfm?URI=oe-20-11-12366 (cit. on p. 65).

[413] S. Aaronson. "Quantum Copy-Protection and Quantum Money". In: *2009 24th Annual IEEE Conference on Computational Complexity*. IEEE. 2009, pp. 229–242 (cit. on p. 65).

[414] A. Lutomirski et al. "Breaking and Making Quantum Money: Toward a New Quantum Cryptographic Protocol". In: (2009). DOI: 10.48550/ARXIV.0912.3825. URL: https://arxiv.org/abs/0912.3825 (cit. on p. 65).

[415] S. Aaronson and P. Christiano. "Quantum Money from Hidden Subspaces". In: *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*. 2012, pp. 41–60 (cit. on p. 65).

[416] M. Zhandry. *Quantum Lightning Never Strikes the Same State Twice*. 2017. DOI: 10.48550/ARXIV.1711.02276. URL: https://arxiv.org/abs/1711.02276 (cit. on p. 65).

[417] A. Coladangelo. *Smart Contracts Meet Quantum Cryptography*. 2019. DOI: 10.48550/ARXIV.1902.05214. URL: https://arxiv.org/abs/1902.05214 (cit. on p. 65).

[418] C. Crépeau, D. Gottesman, and A. Smith. "Secure Multi-Party Quantum Computation". In: *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*. 2002, pp. 643–652 (cit. on p. 65).

[419] R. Colbeck. "Quantum and Relativistic Protocols for Secure Multi-Party Computation". In: (2009) (cit. on p. 65).

[420] D. Unruh. "Universally Composable Quantum Multi-Party Computation". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2010, pp. 486–505 (cit. on p. 65).

[421] H.-K. Lo and H. F. Chau. "Is Quantum Bit Commitment Really Possible?" In: *Physical Review Letters* 78.17 (1997), pp. 3410–3413. DOI: 10.1103/physrevlett.78.3410. URL: https://doi.org/10.1103%5C%2Fphysrevlett.78.3410 (cit. on p. 65).

[422] D. Mayers. "Unconditionally Secure Quantum Bit Commitment is Impossible". In: *Physical Review Letters* 78.17 (1997), pp. 3414–3417. DOI: 10.1103/physrevlett.78.3414. URL: https://doi.org/10.1103%5C%2Fphysrevlett.78.3414 (cit. on p. 65).

[423] H.-K. Lo. "Insecurity of Quantum Secure Computations". In: *Physical Review A* 56.2 (1997), pp. 1154–1162. DOI: 10.1103/physreva.56.1154. URL: https://doi.org/10.1103%5C%2Fphysreva.56.1154 (cit. on p. 65).

[424] H.-K. Lo and H. F. Chau. "Why Quantum Bit Commitment and Ideal Quantum Coin Tossing are Impossible". In: *Physica D: Nonlinear Phenomena* 120.1-2 (1998), pp. 177–187. DOI: 10.1016/s0167-2789(98)00053-0. URL: https://doi.org/10.1016%5C%2Fs0167-2789%5C%2898%5C%2900053-0 (cit. on p. 65).

[425] A. Kent. "Unconditionally Secure Bit Commitment". In: *Physical Review Letters* 83.7 (1999), pp. 1447–1450. DOI: 10.1103/physrevlett.83.1447. URL: https://doi.org/10.1103%5C%2Fphysrevlett.83.1447 (cit. on p. 65).

[426] A. Kent. "Coin Tossing is Strictly Weaker than Bit Commitment". In: *Physical Review Letters* 83.25 (1999), pp. 5382–5384. DOI: 10.1103/physrevlett.83.5382. URL: https://doi.org/10.1103%5C%2Fphysrevlett.83.5382 (cit. on p. 65).

[427] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp. "Authentication of Quantum Messages". In: *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.* IEEE Comput. Soc, 2002. DOI: 10.1109/sfcs.2002.1181969. URL: https://doi.org/10.1109%5C%2Fsfcs.2002.1181969 (cit. on p. 65).

[428] D. Boneh and M. Zhandry. "Quantum-Secure Message Authentication Codes". In: *Advances in Cryptology – EUROCRYPT 2013*. Ed. by T. Johansson and P. Nguyen. Springer Berlin Heidelberg, 2013, pp. 592–608. ISBN: 978-3-642-38348-9 (cit. on pp. 65, 71).

[429] F. Ablayev and A. Vasiliev. "Cryptographic Quantum Hashing". In: *Laser Physics Letters* 11.2 (2013), p. 025202. DOI: 10.1088/1612-2011/11/2/025202. URL: https://doi.org/10.1088/1612-2011/11/2/025202 (cit. on p. 65).

[430] Y.-G. Yang, P. Xu, R. Yang, Y.-H. Zhou, and W.-M. Shi. "Quantum Hash Function and its Application to Privacy Amplification in Quantum Key Distribution, Pseudo-Random Number Generation and Image Encryption". In: *Scientific Reports* 6.1 (2016). ISSN: 2045-2322. DOI: 10.1038/srep19788. URL: https://doi.org/10.1038/srep19788 (cit. on pp. 65, 71).

[431] D. Gottesman and I. Chuang. *Quantum Digital Signatures*. 2001. DOI: 10.48550/ARXIV.QUANT-PH/0105032. URL: https://arxiv.org/abs/quant-ph/0105032 (cit. on pp. 65, 71).

[432] X. Lü and D.-G. Feng. *Quantum Digital Signature based on Quantum One-Way Functions*. 2004. DOI: 10.48550/ARXIV.QUANT-PH/0403046. URL: https://arxiv.org/abs/quant-ph/0403046 (cit. on pp. 65, 71).

[433] G. Nikolopoulos and M. Fischlin. "Information-Theoretically Secure Data Origin Authentication with Quantum and Classical Resources". In: *Cryptography* 4.4 (2020). ISSN: 2410-387X. DOI: 10.3390/cryptography4040031. URL: https://www.mdpi.com/2410-387X/4/4/31 (cit. on p. 65).

[434] T. Okamoto, K. Tanaka, and S. Uchiyama. "Quantum Public-Key Cryptosystems". In: *Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*. CRYPTO '00. Springer-Verlag, 2000, pp. 147–165. ISBN: 3540679073 (cit. on pp. 65, 71).

[435] B. Huttner, N. Imoto, N. Gisin, and T. Mor. "Quantum Cryptography with Coherent States". In: *Phys. Rev. A* 51 (3 1995), pp. 1863–1869. DOI: 10.1103/PhysRevA.51.1863. URL: https://link.aps.org/doi/10.1103/PhysRevA.51.1863 (cit. on pp. 66, 103).

[436] G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders. "Security Aspects of Practical Quantum Cryptography". In: *Conference Digest. 2000 International Quantum Electronics Conference (Cat. No.00TH8504)*. 2000. DOI: 10.1109/IQEC.2000.907967 (cit. on pp. 66, 103).

[437] N. Lütkenhaus and M. Jahma. "Quantum Key Distribution with Realistic States: Photon-Number Statistics in the Photon-Number Splitting Attack". In: *New Journal of Physics* 4.1 (2002), p. 44 (cit. on p. 66).

[438] V. Makarov and D. Hjelme. "Faked States Attack on Quantum Cryptosystems". In: *Journal of Modern Optics* 52.5 (2005), pp. 691–705. DOI: 10.1080/09500340410001730986. URL: https://doi.org/10.1080/09500340410001730986 (cit. on pp. 66, 102, 103).

[439] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma. "Time-Shift Attack in Practical Quantum Cryptosystems". In: (2005). DOI: 10.48550/ARXIV.QUANT-PH/0512080. URL: https://arxiv.org/abs/quant-ph/0512080 (cit. on pp. 66, 103, 104).

[440] M. Mosca, A. Tapp, and R. de Wolf. *Private Quantum Channels and the Cost of Randomizing Quantum Information*. 2000 (cit. on pp. 67, 97).

[441] K. Inoue, E. Waks, and Y. Yamamoto. "Differential Phase Shift Quantum Key Distribution". In: *Phys. Rev. Lett.* 89 (3 2002). DOI: 10.1103/PhysRevLett.89.037902. URL: https://link.aps.org/doi/10.1103/PhysRevLett.89.037902 (cit. on p. 68).

[442] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden. "Fast and Simple One-Way Quantum Key Distribution". In: *Applied Physics Letters* 87.19 (2005), p. 194108. DOI: 10.1063/1.2126792. URL: https://doi.org/10.1063/1.2126792 (cit. on p. 68).

[443] V. Scarani et al. "The Security of Practical Quantum Key Distribution". In: *Rev. Mod. Phys.* 81 (3 2009), pp. 1301–1350. DOI: 10.1103/RevModPhys.81.1301. URL: https://link.aps.org/doi/10.1103/RevModPhys.81.1301 (cit. on pp. 68, 71, 77, 108).

[444] E. Diamanti and A. Leverrier. "Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations". In: *Entropy* 17.9 (2015), pp. 6072–6092. ISSN: 1099-4300. DOI: 10.3390/e17096072. URL: https://www.mdpi.com/1099-4300/17/9/6072 (cit. on p. 68).

[445] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan. "Practical Challenges in Quantum Key Distribution". In: *npj Quantum Information* 2.1 (2016), p. 16025. ISSN: 2056-6387. DOI: 10.1038/npjqi.2016.25. URL: https://doi.org/10.1038/npjqi.2016.25 (cit. on p. 68).

[446] X. Wang, S. Guo, P. Wang, W. Liu, and Y. Li. "Realistic Rate & Distance Limit of Continuous-Variable Quantum Key Distribution". In: *Opt. Express* 27.9 (2019), pp. 13372–13386. DOI: 10.1364/OE.27.013372. URL: http://opg.optica.org/oe/abstract.cfm?URI=oe-27-9-13372 (cit. on p. 68).

[447] S. Pirandola et al. "Advances in Quantum Cryptography". In: *Adv. Opt. Photon.* 12.4 (2020), pp. 1012–1236. DOI: 10.1364/AOP.361502. URL: http://opg.optica.org/aop/abstract.cfm?URI=aop-12-4-1012 (cit. on pp. 68, 71, 101–105).

[448] H. Yuen and V. Chan. "Noise in Homodyne and Heterodyne Detection". In: *Opt. Lett.* 8.3 (1983), pp. 177–179. DOI: 10.1364/OL.8.000177. URL: http://opg.optica.org/ol/abstract.cfm?URI=ol-8-3-177 (cit. on p. 69).

[449] G. Abbas, V. Chan, and T. Yee. "Local-Oscillator Excess-Noise Suppression for Homodyne and Heterodyne Detection". In: *Opt. Lett.* 8.8 (1983), pp. 419–421. DOI: 10.1364/OL.8.000419. URL: http://opg.optica.org/ol/abstract.cfm?URI=ol-8-8-419 (cit. on p. 69).

[450] M. Collett, R. Loudon, and C. Gardiner. "Quantum Theory of Optical Homodyne and Heterodyne Detection". In: *Journal of Modern Optics* 34.6-7 (1987), pp. 881–902. DOI: 10.1080/09500348714550811. URL: https://doi.org/10.1080/09500348714550811 (cit. on p. 69).

[451] G. Brassard and L. Salvail. "Secret-Key Reconciliation by Public Discussion". In: *Advances in Cryptology — EUROCRYPT '93*. Ed. by T. Helleseth. Springer Berlin Heidelberg, 1994, pp. 410–423. ISBN: 978-3-540-48285-7 (cit. on p. 71).

[452] D. Elkouss, J. Martinez-Mateo, and V. Martin. "Information Reconciliation for Quantum Key Distribution". In: (2010). DOI: 10.48550/ARXIV.1007.1616. URL: https://arxiv.org/abs/1007.1616 (cit. on p. 71).

[453] C. Berrou, A. Glavieux, and P. Thitimajshima. "Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes". In: *Proceedings of ICC '93 - IEEE International Conference on Communications*. Vol. 2. 1993, 1064–1070 vol.2. DOI: 10.1109/ICC.1993.397441 (cit. on p. 71).

[454] C. Berrou and A. Glavieux. "Near Optimum Error Correcting Coding and Decoding: Turbo-Codes". In: *IEEE Transactions on Communications* 44.10 (1996), pp. 1261–1271. DOI: 10.1109/26.539767 (cit. on p. 71).

[455] R. Gallager. "Low-Density Parity-Check Codes". In: *IRE Transactions on Information Theory* 8.1 (1962), pp. 21–28. DOI: 10.1109/TIT.1962.1057683 (cit. on p. 71).

[456] D. MacKay and R. Neal. "Near Shannon Limit Performance of Low Density Parity Check Codes". In: *Electronics Letters* 32 (18 1996), pp. 1645–1646. ISSN: 0013-5194. URL: https://digital-library.theiet.org/content/journals/10.1049/el_19961141 (cit. on p. 71).

[457] E. Arikan. "Channel Polarization: A Method for Constructing Capacity-Achieving Codes". In: *2008 IEEE International Symposium on Information Theory*. 2008, pp. 1173–1177. DOI: 10.1109/ISIT.2008.4595172 (cit. on p. 71).

[458] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer. "Generalized Privacy Amplification". In: *IEEE Transactions on Information Theory* 41.6 (1995), pp. 1915–1923. DOI: 10.1109/18.476316 (cit. on p. 71).

[459] J. Carter and M. Wegman. "Universal Classes of Hash Functions". In: *Journal of Computer and System Sciences* 18.2 (1979), pp. 143–154. ISSN: 0022-0000. DOI: https://doi.org/10.1016/0022-0000(79)90044-8. URL: https://www.sciencedirect.com/science/article/pii/0022000079900448 (cit. on pp. 71, 99, 101).

[460] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. "Quantum Cryptography". In: *Rev. Mod. Phys.* 74 (1 2002), pp. 145–195. DOI: 10.1103/RevModPhys.74.145. URL: https://link.aps.org/doi/10.1103/RevModPhys.74.145 (cit. on pp. 71, 108).

[461] R. Renner. *Security of Quantum Key Distribution*. 2005. DOI: 10.48550/ARXIV.QUANT-PH/0512258. URL: https://arxiv.org/abs/quant-ph/0512258 (cit. on pp. 71, 77, 107).

[462] H.-K. Lo and Y. Zhao. "Quantum Cryptography". In: (2008). DOI: 10.48550/ARXIV.0803.2507. URL: https://arxiv.org/abs/0803.2507 (cit. on p. 71).

[463] F. Xu, X. Zhang, H.-K. Lo, and J.-W. Pan. "Quantum Cryptography with Realistic Devices". In: 2019 (cit. on p. 71).

[464] C. Portmann and R. Renner. *Security in Quantum Cryptography*. 2021. DOI: 10.48550/ARXIV.2102.00021. URL: https://arxiv.org/abs/2102.00021 (cit. on pp. 71, 101, 103–107).

[465] R. Renner, N. Gisin, and B. Kraus. "An Information-Theoretic Security Proof for QKD Protocols". In: *Physical Review A* (2005) (cit. on p. 77).

[466] C. Branciard, N. Gisin, B. Kraus, and V. Scarani. "Security of Two Quantum Cryptography Protocols Using the Same Four Qubit States". In: *Phys. Rev. A* 72 (3 2005). DOI: 10.1103/PhysRevA.72.032301. URL: https://link.aps.org/doi/10.1103/PhysRevA.72.032301 (cit. on p. 77).

[467] P. Shor and J. Preskill. "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol". In: *Physical review letters* 85 2 (2000), pp. 441–4 (cit. on p. 77).

[468] K. Tamaki and N. Lütkenhaus. "Unconditional Security of the Bennett 1992 Quantum Key-Distribution Protocol Over a Lossy and Noisy Channel". In: *Phys. Rev. A* 69 (3 2004). DOI: 10.1103/PhysRevA.69.032316. URL: https://link.aps.org/doi/10.1103/PhysRevA.69.032316 (cit. on p. 77).

[469] J. Clauser, M. Horne, A. Shimony, and R. Holt. "Proposed Experiment to Test Local Hidden-Variable Theories". In: *Phys. Rev. Lett.* 23 (15 1969), pp. 880–884. DOI: 10.1103/PhysRevLett.23.880. URL: https://link.aps.org/doi/10.1103/PhysRevLett.23.880 (cit. on p. 86).

[470] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields. "Overcoming the Rate–Distance Limit of Quantum Key Distribution Without Quantum Repeaters". In: *Nature* 557.7705 (2018), pp. 400–403. ISSN: 1476-4687. DOI: 10.1038/s41586-018-0066-6. URL: http://dx.doi.org/10.1038/s41586-018-0066-6 (cit. on pp. 89, 100).

[471] W. Krawec. "Restricted Attacks on Semi-Quantum Key Distribution Protocols". In: *Quantum Information Processing* 13.11 (2014), pp. 2417–2436. ISSN: 1573-1332. DOI: 10.1007/s11128-014-0802-2. URL: https://doi.org/10.1007/s11128-014-0802-2 (cit. on p. 95).

[472] S. Bose, V. Vedral, and P. Knight. "Multiparticle Generalization of Entanglement Swapping". In: *Physical Review A* 57.2 (1998), pp. 822–829. DOI: 10.1103/physreva.57.822. URL: https://doi.org/10.1103%5C%2Fphysreva.57.822 (cit. on p. 98).

[473] K. Chen and H.-K. Lo. "Multi-partite Quantum Cryptographic Protocols with Noisy GHZ States". In: (2004). DOI: 10.48550/ARXIV.QUANT-PH/0404133. URL: https://arxiv.org/abs/quant-ph/0404133 (cit. on p. 98).

[474] K. Chen and H.-K. Lo. "Conference Key Agreement and Quantum Sharing of Classical Secrets with Noisy GHZ States". In: *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.* IEEE, 2005. DOI: 10.1109/isit.2005.1523616. URL: https://doi.org/10.1109%5C%2Fisit.2005.1523616 (cit. on p. 98).

[475] S. Zhao et al. "Phase-Matching Quantum Cryptographic Conferencing". In: *Physical Review Applied* 14.2 (2020). DOI: 10.1103/physrevapplied.14.024010. URL: https://doi.org/10.1103%5C%2Fphysrevapplied.14.024010 (cit. on p. 101).

[476] R. Alléaume et al. "Using Quantum Key Distribution for Cryptographic Purposes: A Survey". In: (2007). DOI: 10.48550/ARXIV.QUANT-PH/0701168. URL: https://arxiv.org/abs/quant-ph/0701168 (cit. on p. 102).

[477] H.-W. Li et al. "Attacking a Practical Quantum-Key-Distribution System with Wavelength-Dependent Beam-Splitter and Multiwavelength Sources". In: *Physical Review A* 84.6 (2011). DOI: 10.1103/physreva.84.062308. URL: https://doi.org/10.1103%5C%2Fphysreva.84.062308 (cit. on p. 102).

[478] M. Stipčević. *Preventing Detector Blinding Attack and other Random Number Generator Attacks on Quantum Cryptography by use of an Explicit Random Number Generator*. 2014. DOI: 10.48550/ARXIV.1403.0143. URL: https://arxiv.org/abs/1403.0143 (cit. on pp. 102, 103, 105).

[479] M. Koashi. *Simple Security Proof of Quantum Key Distribution via Uncertainty Principle*. 2005. DOI: 10.48550/ARXIV.QUANT-PH/0505108. URL: https://arxiv.org/abs/quant-ph/0505108 (cit. on p. 103).

[480] V. Makarov, A. Anisimov, and J. Skaar. "Effects of Detector Efficiency Mismatch on Security of Quantum Cryptosystems". In: *Physical Review A* 74.2 (2006) (cit. on pp. 103, 104).

[481] Y. Zhao, C.-H. Fung, B. Qi, C. Chen, and H.-K. Lo. "Quantum Hacking: Experimental Demonstration of Time-Shift Attack Against Practical Quantum-Key-Distribution Systems". In: *Physical Review A* 78.4 (2008). DOI: 10.1103/physreva.78.042333. URL: https://doi.org/10.1103%5C%2Fphysreva.78.042333 (cit. on pp. 103, 104).

[482] C.-H. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma. "Security Proof of Quantum Key Distribution with Detection Efficiency Mismatch". In: (2008). DOI: 10.48550/ARXIV.0802.3788. URL: https://arxiv.org/abs/0802.3788 (cit. on p. 103).

[483] L. Lydersen and J. Skaar. "Security of Quantum Key Distribution with Bit and Basis Dependent Detector Flaws". In: (2008). DOI: 10.48550/ARXIV.0807.0767. URL: https://arxiv.org/abs/0807.0767 (cit. on p. 103).

[484] L. Lydersen et al. "Hacking Commercial Quantum Cryptography Systems by Tailored Bright Illumination". In: *Nature Photonics* 4.10 (2010), pp. 686–689. DOI: 10.1038/nphoton.2010.214. URL: https://doi.org/10.1038%5C%2Fnphoton.2010.214 (cit. on p. 103).

[485] L. Lydersen et al. "Thermal Blinding of Gated Detectors in Quantum Cryptography". In: *Optics Express* 18.26 (2010). DOI: 10.1364/oe.18.027938. URL: https://doi.org/10.1364%5C%2Foe.18.027938 (cit. on pp. 103, 105).

[486] Z. Yuan, J. Dynes, and A. Shields. "Avoiding the Blinding Attack in QKD". In: *Nature Photonics* 4.12 (2010), pp. 800–801. ISSN: 1749-4893. DOI: 10.1038/nphoton.2010.269. URL: https://doi.org/10.1038/nphoton.2010.269 (cit. on pp. 103, 105).

[487] Z. Yuan, J. Dynes, and A. Shields. "Resilience of Gated Avalanche Photodiodes Against Bright Illumination Attacks in Quantum Cryptography". In: *Applied Physics Letters* 98.23 (2011). DOI: 10.1063/1.3597221. URL: https://doi.org/10.1063%5C%2F1.3597221 (cit. on p. 103).

[488] M. Rau et al. "Spatial Mode Side Channels in Free-Space QKD Implementations". In: *IEEE Journal of Selected Topics in Quantum Electronics* 21.3 (2015), pp. 187–191. DOI: 10.1109/JSTQE.2014.2372008 (cit. on p. 103).

[489] S. Sajeed et al. "Security Loophole in Free-Space Quantum Key Distribution due to Spatial-Mode Detector-Efficiency Mismatch". In: *Phys. Rev. A* 91 (6 2015). DOI: 10.1103/PhysRevA.91.062301. URL: https://link.aps.org/doi/10.1103/PhysRevA.91.062301 (cit. on pp. 103, 106).

[490] Y.-Y. Fei, X.-D. Meng, M. Gao, Z. Ma, and H. Wang. "Practical Decoy State Quantum Key Distribution with Detector Efficiency Mismatch". In: *The European Physical Journal D* 72.6 (2018), p. 107. ISSN: 1434-6079. DOI: 10.1140/epjd/e2018-90110-3. URL: https://doi.org/10.1140/epjd/e2018-90110-3 (cit. on p. 103).

[491] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter. "The Breakdown Flash of Silicon Avalanche Photodiodes-Back Door for Eavesdropper Attacks?" In: *Journal of Modern Optics* 48.13 (2001), pp. 2039–2047. DOI: 10.1080/09500340108240905. URL: https://doi.org/10.1080%5C%2F09500340108240905 (cit. on pp. 103, 104).

[492] A. Meda et al. "Quantifying Backflash Radiation to Prevent Zero-Error Attacks in Quantum Key Distribution". In: *Light: Science & Applications* 6.6 (2016), e16261–e16261. DOI: 10.1038/lsa.2016.261. URL: https://doi.org/10.1038%5C%2Flsa.2016.261 (cit. on pp. 103, 104).

[493] P. Pinheiro et al. "Eavesdropping and Countermeasures for Backflash Side Channel in Quantum Cryptography". In: *Optics Express* 26.16 (2018), p. 21020. DOI: 10.1364/oe.26.021020. URL: https://doi.org/10.1364%5C%2Foe.26.021020 (cit. on pp. 103, 104).

[494] V. Makarov. "Controlling Passively Quenched Single Photon Detectors by Bright Light". In: *New Journal of Physics* 11.6 (2009). DOI: 10.1088/1367-2630/11/6/065003. URL: https://doi.org/10.1088%5C%2F1367-2630%5C%2F11%5C%2F6%5C%2F065003 (cit. on pp. 103, 105).

[495] I. Gerhardt et al. "Full-Field Implementation of a Perfect Eavesdropper on a Quantum Cryptography System". In: *Nature Communications* 2.1 (2011). DOI: 10.1038/ncomms1348. URL: https://doi.org/10.1038%5C%2Fncomms1348 (cit. on pp. 103, 105).

[496] H. Weier et al. "Quantum Eavesdropping Without Interception: An Attack Exploiting the Dead Time of Single-Photon Detectors". In: *New Journal of Physics* 13.7 (2011). DOI: 10.1088/1367-2630/13/7/073024. URL: https://doi.org/10.1088%5C%2F1367-2630%5C%2F13%5C%2F7%5C%2F073024 (cit. on pp. 103, 105).

[497] A. Bugge et al. "Laser Damage Helps the Eavesdropper in Quantum Cryptography". In: *Physical Review Letters* 112.7 (2014). DOI: 10.1103/physrevlett.112.070503. URL: https://doi.org/10.1103%5C%2Fphysrevlett.112.070503 (cit. on pp. 103, 105).

[498] N. Lütkenhaus. "Security Against Individual Attacks for Realistic Quantum Key Distribution". In: *Physical Review A* 61.5 (2000). DOI: 10.1103/physreva.61.052304. URL: https://doi.org/10.1103%5C%2Fphysreva.61.052304 (cit. on pp. 103, 108).

[499] A. Müller et al. ""Plug and Play" Systems for Quantum Cryptography". In: *Applied Physics Letters* 70.7 (1997), pp. 793–795. DOI: 10.1063/1.118224. URL: https://doi.org/10.1063/1.118224 (cit. on p. 105).

[500] T. Nishioka, H. Ishizuka, and T. Hasegawa. ""Circular Type"Quantum Key Distribution". In: *IEEE Photonics Technology Letters* 14.4 (2002), pp. 576–578. DOI: 10.1109/68.992616. URL: https://doi.org/10.1109%5C%2F68.992616 (cit. on p. 105).

[501] C.-H. Fung, B. Qi, K. Tamaki, and H.-K. Lo. "Phase-Remapping Attack in Practical Quantum-Key-Distribution Systems". In: *Physical Review A* 75.3 (2007). DOI: 10.1103/physreva.75.032314. URL: https://doi.org/10.1103%5C%2Fphysreva.75.032314 (cit. on p. 106).

[502] F. Xu, B. Qi, and H.-K. Lo. "Experimental Demonstration of Phase-Remapping Attack in a Practical Quantum Key Distribution System". In: *New Journal of Physics* 12.11 (2010). DOI: 10.1088/1367-2630/12/11/113026. URL: https://doi.org/10.1088%5C%2F1367-2630%5C%2F12%5C%2F11%5C%2F113026 (cit. on p. 106).

[503] A. Vakhitov, V. Makarov, and D. Hjelme. "Large Pulse Attack as a Method of Conventional Optical Eavesdropping in Quantum Cryptography". In: *Journal of Modern Optics* 48.13 (2001), pp. 2023–2038. DOI: 10.1080/09500340108240904. URL: https://www.tandfonline.com/doi/abs/10.1080/09500340108240904 (cit. on p. 106).

[504] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. "Trojan-Horse Attacks on Quantum-Key-Distribution Systems". In: *Physical Review A* 73.2 (2006). DOI: 10.1103/physreva.73.022320. URL: https://doi.org/10.1103%5C%2Fphysreva.73.022320 (cit. on p. 106).

[505] N. Jain et al. "Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems". In: *IEEE Journal of Selected Topics in Quantum Electronics* 21.3 (2015), pp. 168–177. DOI: 10.1109/JSTQE.2014.2365585 (cit. on p. 106).

[506] M. Lucamarini et al. "Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution". In: *Physical Review X* 5.3 (2015). DOI: 10.1103/physrevx.5.031030. URL: https://doi.org/10.1103%5C%2Fphysrevx.5.031030 (cit. on p. 106).

[507] K. Tamaki, M. Curty, and M. Lucamarini. "Decoy-State Quantum Key Distribution with a Leaky Source". In: *New Journal of Physics* 18.6 (2016). DOI: 10.1088/1367-2630/18/6/065008. URL: https://doi.org/10.1088%5C%2F1367-2630%5C%2F18%5C%2F6%5C%2F065008 (cit. on p. 106).

[508] S. Vinay and P. Kok. "Extended Analysis of the Trojan-Horse Attack in Quantum Key Distribution". In: *Physical Review A* 97.4 (2018). DOI: 10.1103/physreva.97.042335. URL: https://doi.org/10.1103%5C%2Fphysreva.97.042335 (cit. on p. 106).

[509] M. Ben-Or, M. Horodecki, D. Leung, D. Mayers, and J. Oppenheim. "The Universal Composable Security of Quantum Key Distribution". In: (2004) (cit. on p. 107).

[510] R. Renner and R. Koenig. "Universally Composable Privacy Amplification Against Quantum Adversaries". In: (2004). DOI: 10.48550/ARXIV.QUANT-PH/0403133. URL: https://arxiv.org/abs/quant-ph/0403133 (cit. on p. 107).

[511] D. Mayers. *Quantum Key Distribution and String Oblivious Transfer in Noisy Channels*. 1996. DOI: 10.48550/ARXIV.QUANT-PH/9606003. URL: https://arxiv.org/abs/quant-ph/9606003 (cit. on p. 108).

[512] E. Biham and T. Mor. "Security of Quantum Cryptography against Collective Attacks". In: *Physical Review Letters* 78.11 (1997), pp. 2256–2259. DOI: 10.1103/physrevlett.78.2256. URL: https://doi.org/10.1103%5C%2Fphysrevlett.78.2256 (cit. on p. 108).

[513] C. Fuchs, N. Gisin, R. Griffiths, C.-S. Niu, and A. Peres. "Optimal Eavesdropping in Quantum Cryptography. I. Information Bound and Optimal Strategy". In: *Phys. Rev. A* 56 (2 1997), pp. 1163–1172. DOI: 10.1103/PhysRevA.56.1163. URL: https://link.aps.org/doi/10.1103/PhysRevA.56.1163 (cit. on p. 108).

[514] D. Mayers. "Unconditional Security in Quantum Cryptography". In: (1998). DOI: 10.48550/ARXIV.QUANT-PH/9802025. URL: https://arxiv.org/abs/quant-ph/9802025 (cit. on p. 108).

[515] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor. *Security of Quantum Key Distribution Against All Collective Attacks*. 1998. DOI: 10.48550/ARXIV.QUANT-PH/9801022. URL: https://arxiv.org/abs/quant-ph/9801022 (cit. on p. 108).

[516] H. Lu and Q.-Y. Cai. "Quantum Key Distribution with Classical Alice". In: *International Journal of Quantum Information* 06.06 (2008), pp. 1195–1202. DOI: 10.1142/S0219749908004353. URL: https://doi.org/10.1142/S0219749908004353 (cit. on p. 110).

[517] Z. Xian-Zhou, G. Wei-Gui, T. Yong-Gang, R. Zhen-Zhong, and G. Xiao-Tian. "Quantum Key Distribution Series Network Protocol with M-Classical Bobs". In: *Chinese Physics B* 18.6 (2009), pp. 2143–2148. DOI: 10.1088/1674-1056/18/6/006. URL: https://doi.org/10.1088/1674-1056/18/6/006 (cit. on p. 110).

[518] K.-N. Zhu, N.-R. Zhou, Y.-Q. Wang, and X.-J. Wen. "Semi-Quantum Key Distribution Protocols with GHZ States". In: *International Journal of Theoretical Physics* 57.12 (2018), pp. 3621–3631. ISSN: 1572-9575. DOI: 10.1007/s10773-018-3875-3. URL: https://doi.org/10.1007/s10773-018-3875-3 (cit. on pp. 110, 111).

[519] N.-R. Zhou, K.-N. Zhu, and X.-F. Zou. "Multi-Party Semi-Quantum Key Distribution Protocol With Four-Particle Cluster States". In: *Annalen der Physik* 531.8 (2019). DOI: https://doi.org/10.1002/andp.201800520. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/andp.201800520 (cit. on p. 110).

[520] F. Massa et al. *Experimental Semi-Quantum Key Distribution With Classical Users*. 2019. DOI: 10.48550/ARXIV.1908.01780. URL: https://arxiv.org/abs/1908.01780 (cit. on pp. 111, 139).

[521] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. "Quantum Fingerprinting". In: *Physical Review Letters* 87.16 (2001). DOI: 10.1103/physrevlett.87.167902. URL: https://doi.org/10.1103%5C%2Fphysrevlett.87.167902 (cit. on p. 116).

[522] R. Van Meter, T. Satoh, T. Ladd, W. Munro, and K. Nemoto. "Path Selection for Quantum Repeater Networks". In: *Networking Science* 3.1-4 (2013), pp. 82–95. DOI: 10.1007/s13119-013-0026-2. URL: https://doi.org/10.1007%5C%2Fs13119-013-0026-2 (cit. on p. 125).

[523] S. Perseguers, J. Lapeyre, D. Cavalcanti, M. Lewenstein, and A. Acín. "Distribution of Entanglement in Large-Scale Quantum Networks". In: *Reports on Progress in Physics* 76.9 (2013). DOI: 10.1088/0034-4885/76/9/096001. URL: https://doi.org/10.1088%5C%2F0034-4885%5C%2F76%5C%2F9%5C%2F096001 (cit. on p. 125).

[524] R. Van Meter. *Quantum Networking*. John Wiley & Sons, 2014 (cit. on p. 125).

[525] M. Caleffi. "Optimal Routing for Quantum Networks". In: *IEEE Access* 5 (2017), pp. 22299–22312 (cit. on p. 125).

[526] L. Gyongyosi and S. Imre. "Decentralized Base-Graph Routing for the Quantum Internet". In: *Physical Review A* 98.2 (2018). DOI: 10.1103/physreva.98.022310. URL: https://doi.org/10.1103%5C%2Fphysreva.98.022310 (cit. on p. 125).

[527] K. Chakraborty, F. Rozpedek, A. Dahlberg, and S. Wehner. *Distributed Routing in a Quantum Internet*. 2019. DOI: 10.48550/ARXIV.1907.11630. URL: https://arxiv.org/abs/1907.11630 (cit. on p. 125).

[528] M. Pant et al. "Routing Entanglement in the Quantum Internet". In: *npj Quantum Information* 5.1 (2019), pp. 1–9 (cit. on p. 125).

[529] S. Lloyd et al. "Infrastructure for the Quantum Internet". In: *Computer Communication Review* 34.5 (2004), pp. 9–20. ISSN: 0146-4833. DOI: 10.1145/1039111.1039118 (cit. on p. 125).

[530] P. Kok et al. "Linear Optical Quantum Computing with Photonic Qubits". In: *Reviews of Modern Physics* 79.1 (2007), pp. 135–174. DOI: 10.1103/revmodphys.79.135. URL: https://doi.org/10.1103%5C%2Frevmodphys.79.135 (cit. on p. 125).

[531] L. Bacsardi. "On the Way to Quantum-Based Satellite Communication". In: *IEEE Communications Magazine* 51.8 (2013), pp. 50–55. DOI: 10.1109/MCOM.2013.6576338 (cit. on p. 125).

[532] S. Pirandola. *Capacities of Repeater-Assisted Quantum Communications*. 2016. DOI: 10.48550/ARXIV.1601.00966. URL: https://arxiv.org/abs/1601.00966 (cit. on p. 125).

[533] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. "Fundamental Limits of Repeaterless Quantum Communications". In: *Nature Communications* 8.1 (2017), p. 15043. ISSN: 2041-1723. DOI: 10.1038/ncomms15043. URL: https://doi.org/10.1038/ncomms15043 (cit. on p. 125).

[534] R. Laurenza and S. Pirandola. "General Bounds for Sender-Receiver Capacities in Multipoint Quantum Communications". In: *Physical Review A* 96.3 (2017). DOI: 10.1103/physreva.96.032318. URL: https://doi.org/10.1103%5C%2Fphysreva.96.032318 (cit. on p. 125).

[535] L. Gyongyosi and S. Imre. "Topology Adaption for the Quantum Internet". In: *Quantum Information Processing* 17.11 (2018), pp. 1–12 (cit. on p. 125).

[536] L. Gyongyosi, S. Imre, and H. Nguyen. "A Survey on Quantum Channel Capacities". In: *IEEE Communications Surveys Tutorials* 20.2 (2018), pp. 1149–1205. DOI: 10.1109/COMST.2017.2786748 (cit. on p. 125).

[537] L. Gyongyosi and S. Imre. "Dynamic Topology Resilience for Quantum Networks". In: *Advances in Photonics of Quantum Computing, Memory, and Communication XI*. Ed. by Z. Hasan, P. Hemmer, A. Craig, and A. Migdall. Vol. 10547. International Society for Optics and Photonics. SPIE, 2018, pp. 89–95. DOI: 10.1117/12.2288707. URL: https://doi.org/10.1117/12.2288707 (cit. on p. 125).

[538] S. Pirandola et al. "Theory of Channel Simulation and Bounds for Private Communication". In: *Quantum Science and Technology* 3.3 (2018), p. 035009. DOI: 10.1088/2058-9565/aac394. URL: https://doi.org/10.1088%5C%2F2058-9565%5C%2Faac394 (cit. on p. 125).

[539] L. Gyongyosi and S. Imre. "Multilayer Optimization for the Quantum Internet". In: *Scientific Reports* 8.1 (2018). ISSN: 2045-2322. DOI: 10.1038/s41598-018-30957-x. URL: https://doi.org/10.1038/s41598-018-30957-x (cit. on p. 125).

[540] L. Gyongyosi and S. Imre. "Entanglement Availability Differentiation Service for the Quantum Internet". In: *Scientific Reports* 8.1 (2018). ISSN: 2045-2322. DOI: 10.1038/s41598-018-28801-3. URL: https://doi.org/10.1038/s41598-018-28801-3 (cit. on p. 125).

[541] M. Caleffi, A. Cacciapuoti, and G. Bianchi. "Quantum Internet: From Communication to Distributed Computing!" In: *Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication*. ACM, 2018. DOI: 10.1145/3233188.3233224. URL: https://doi.org/10.1145%5C%2F3233188.3233224 (cit. on p. 125).

[542] D. Castelvecchi. "The Quantum Internet has Arrived (and it hasn't)". In: *Nature* 554.7692 (2018), pp. 289–292. DOI: 10.1038/d41586-018-01835-3 (cit. on p. 125).

[543] E. Dijkstra. "A Note on Two Problems in Connexion with Graphs". In: *Numerische Mathematik* 1.1 (1959), pp. 269–271. ISSN: 0945-3245. DOI: 10.1007/BF01386390. URL: https://doi.org/10.1007/BF01386390 (cit. on p. 125).