João José Braz Sobral Eusébio

Licenciado em Ciências da Engenharia Eletrotécnica e de Computadores

Geradores de Sinais Aleatórios Baseados em Caos para Aplicações em Telecomunicações

Dissertação para obtenção do Grau de Mestre em Engenharia Eletrotécnica e de Computadores

Orientador:	Prof. Doutor João Goes, Professor Auxiliar com Agregação, FCT-UNL
Co-orientador:	Prof. Doutor Paulo Montezuma, Professor Auxiliar com Agregação, FCT-UNL

Júri:

Presidente:	Prof. Doutora Maria Helena Silva Fino
Arguentes:	Prof. Doutor Raúl Eduardo Capelo Tello Rato

FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE NOVA DE LISBOA

Março, 2017

Geradores de Sinais Aleatórios Baseados em Caos para Aplicações em Telecomunicações

Ao meu filho Gabriel, a quem não cheguei a ter a oportunidade de dizer o quanto o amava…

Agradecimentos

Este espaço é dedicado a todos os que acompanharam o desenvolvimento do meu percurso académico e em particular desta dissertação.

O meu primeiro agradecimento é dirigido aos Professores João Goes e Paulo Montezuma pelo trabalho exemplar que tiveram para comigo. Um profundo obrigado, por todo o tempo despendido, por toda a paciência, compreensão e dedicação que tiveram ao longo de todo o processo de desenvolvimento e escrita desta dissertação.

De seguida gostaria de agradecer aos meus pais, que sempre fizeram tudo para que eu terminasse o curso, sem nunca desistir de mim. Aos meus irmãos Rui e Nuno, obrigado especialmente pelo incentivo que me deram para terminar o curso.

Um especial obrigado à minha querida esposa Madalena, que para além de me incentivar sempre a terminar o curso, esteve sempre ao meu lado em todos os momentos.

Um agradecimento ao Edgar Silva, por toda a sua disponibilidade para me ajudar a ultrapassar os obstáculos que foram surgindo durante todo o período de elaboração da dissertação.

Por fim, um obrigado a todos os meus colegas que me acompanharam no meu percurso académico, em especial atenção ao Ricardo Laires, Fábio Oliveira, José Gonçalves, Diogo Silva, Cristiano Pereira, Carlos Simão, Pedro Viegas, Hugo Pereira e Luís Paiva que para além de me terem ajudado ao longo de todo o curso, sempre me ajudar a manter o espírito a académico.

A todos vós, um muito obrigado.

Resumo

Atualmente existe um enorme interesse pela segurança da informação mais sensível por parte de diversas entidades. Este interesse levou à procura de melhores formas de encriptação da informação transmitida entre entidades a nível de *software* e de *hardware*. No entanto, a combinação entre *hardware* e *software* para uma encriptação mais completa e complexa apresenta um enorme desafio.

Nos dias que decorrem, a encriptação tem sido alvo de ataques informáticos constantes. Desta forma, para além de se transmitir uma mensagem encriptada, resolveu criar-se um circuito analógico independente que conduzirá a forma como a mesma será transmitida, utilizando os princípios da teoria de caos.

A utilização de aleatoriedade em dispositivos eletrónicos associa-se à implementação de geradores eletrónicos de números aleatórios, cujo objetivo é gerar uma sequência de números aleatórios independentes, com a característica de que quando estes sejam gerados não produzam sempre as mesmas sequências, ou seja, que exista a "não-repetibilidade".

Esta dissertação propõe o estudo de um circuito analógico desenvolvido com base na teoria do caos, onde o mesmo gera uma sequência aleatória consoante as suas condições iniciais, com o intuito de utilizar a sequência gerada para criar uma difusão aleatória da transmissão. Com base no modelo Chua com díodo de Matsumoto, comprovou-se que o modelo é caótico. Para ser possível o mesmo se realizar em circuito integrado, reduziu-se os valores de grandeza dos elementos que armazenam energia, nomeadamente os condensadores e a bobine, para que a dimensão física destes não fosse um obstáculo.

Palavras-chave: Segurança, Caos, Aleatoriedade, Geradores, Difusão Aleatória

Abstract

Nowadays there is a huge interest in the security of the most sensitive information by several entities. This interest has led to better ways of encrypting information transmitted between entities at software and hardware level. However, a combination of hardware and software for more complete and complex encryption presents a huge challenge.

Currently, encryption has been the target of constant computer attacks. So, in addition to transmitting an encrypted message, it was decided to create an independent analog circuit that will lead to how a message will be transmitted using the principals of chaos theory.

The use of randomness in electronic devices is an association of electronic generators of random number, whose purpose is to generate a sequence of independent numbers with a characteristic that when they are generated do not always produce the same sequences, that there is non-repeatability.

This dissertation proposes the study of an analog circuit based on the chaos theory, where it generates a random sequence according to its own initial instructions, in order to use the sequence to create a random transmission diffusion. According to the Chua model with diode of Matsumoto, it was verified that the behavior of the model is chaotic. In order to be able to realize the circuit as an integrated circuit, the values of magnitude of the energy storage elements, namely capacitors and coil, have been reduced so that their sizing (capacitance and inductance values) was not a barrier.

Keywords: Security, Chaos, Randomness, Generators, Random Diffusion

Índice Geral

Agradecimentos ..... **i**

Resumo ..... **ii**

Abstract ..... **iii**

Índice Geral ..... **iv**

Índice de Figuras ..... **v**

1 Introdução **1**

1.1 Motivação e Objetivos 4

1.2 Organização da Dissertação 5

1.3 Contribuições 6

2 Estado da arte **7**

2.1 Caos 8

2.1.1 GNA's Existentes *10*

2.2 Modelos de circuitos caóticos 11

2.2.1 Double Scroll *12*

2.2.2 Folded Torus *19*

2.3 Diferença entre *Double Scroll* e *Folded Torus* 23

3 Circuito eletrónico **24**

3.1 Gerador de números aleatórios 25

3.2 Bobine Ativa 29

3.3 Bootstraping 32

4 Implementação: Análise de Resultados e Aplicações **34**

4.1 Análise de Resultados 35

4.2 Aplicações 39

5 Conclusões e Trabalho Futuro **42**

Referências Bibliográficas **45**

Índice de Figuras

Figura 1.1 - Árvore de categorização de geradores aleatórios de números 2
Figura 2.1 (a-d) - Trajetórias caóticas [3],[5]. 9
Figura 2.2 - Circuito autónomo simples com um atrator caótico [5],[25]..... 12
Figura 2.3 - Atrator observado. Voltagem: 2V/div. Corrente: 2mA/div [5]. 14
Figura 2.4 - Formas de onda no tempo medido. Escala horizontal: 1 ms/div [3],[5]. 14
Figura 2.5 - Outra realização do circuito representado na figura 2.2 [3],[5]. 15
Figura 2.6 - Circuito oscilador amortecido. 15
Figura 2.7 - Circuito não linear com dois díodos. 17
Figura 2.8 - Conversor de impedância negativa. 18
Figura 2.9 Circuito simples autónomo de terceira ordem que apresenta um anel fechado [3]. 19
Figura 2.10 - Realização física do circuito mostrado na figura 2.9 [5]. 21
Figura 2.11 - Atratores observados a partir do circuito da figura 2.9 projetado sobre o plano $vC1, vC2$. Escala horizontal: 0.5 V/div. Escala vertical: 0.5 V/div. Apenas um dos dois atratores é mostrado [5]. 22
Figura 2.12 - Secções transversais $iL = 0, vC2 < 0$, das trajetórias do sinal correspondentes da figura 2.11, no plano $vC1, vC2$ [5]. 22
Figura 2.13 Diferença entre Double Scroll e Folded Torus. 23
Figura 3.1 - Imagem de p versus q para o mapa logístico $xn + 1 = \mu xn\,(1 - xn)$. Esquerda (a): dinâmica regular em $\mu = 3{,}55$; Direita (b): dinâmica caótica em $\mu = 3{,}9$. Neste teste foram utilizados 5000 pontos de dados [16]. 26
Figura 3.2 - Circuito Chua com o díodo de Matsumoto. 27
Figura 3.4 - Histograma de valores gerados aleatoriamente pelo circuito Chua com díodo de Matsumoto com bobine ideal. 28
Figura 3.3 - Sinal $VOUT$ do circuito ilustrado na figura 3.2. 28
Figura 3.5 – *Gyrator* 29
Figura 3.6 – Circuito que implementa a bobine ativa. 30
Figura 3.7 - Circuito de substituição de condensador de 47 nF por 47 pF. 33
Figura 4.1 - Circuito Chua com díodo Matsumoto utilizando bobine ativa. 35
Figura 4.2 - Sinal $VOUT$ do circuito ilustrado na figura 4.1. 35
Figura 4.3 - Histograma de valores gerados aleatoriamente pelo circuito Chua com díodo de Matsumoto com bobine ativa. 36
Figura 4.4 - Circuito com bobine ativa, $C1$, $C2$ e $C3$ de ordem pF. 37
Figura 4.5 - Atrator de Lorenz resultante das simulações do circuito da figura 4.4. 37
Figura 4.6 -Sinal $VOUT$ do circuito ilustrado na figura 4.4. 38
Figura 4.7 - Sistema de transmissão. 41

1

1 Introdução

Aleatoriedade, palavra utilizada em situações onde não existe uma causa, uma ordem ou uma previsibilidade. Por isso, um processo repetitivo, no qual é impossível encontrar um padrão determinístico que possa ser descrito denomina-se processo aleatório. Ao dizer-se que uma variável é aleatória, significa que a variável segue uma dada distribuição de probabilidade. Desta forma, o aleatório é diferente do arbitrário, visto que o arbitrário não implica uma distribuição de probabilidade determinável como o aleatório.

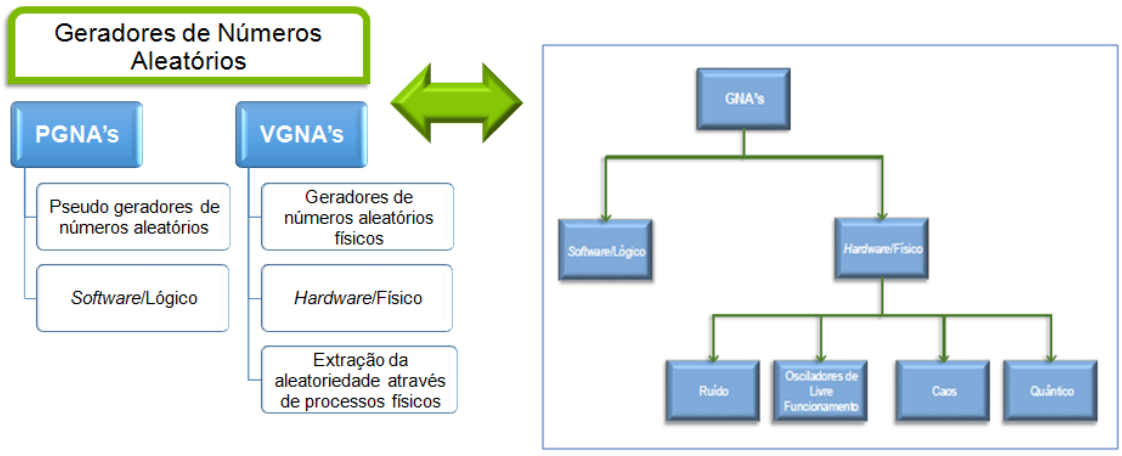
A utilização de aleatoriedade em dispositivos eletrónicos associa-se à implementação de geradores eletrónicos de números aleatórios. Por definição, os Geradores de Números Aleatórios (GNA's) são uma classe restrita nos diversos equipamentos eletrónicos, cujo objetivo é gerar uma sequência de dados perfeitamente independentes e identicamente distribuídos, com a característica de que quando estes sejam reiniciados, os mesmos não reproduzam sempre as mesmas sequências, isto é, que exista a "não-repetibilidade". Os GNAs têm várias aplicações a nível de engenharia, sendo a sua aplicação mais usual nos jogos de azar. No caso de Tecnologias de Informação e Comunicação (TIC) são abundantemente aplicados em testes e simulações. Estes podem ser utilizados para gerar tráfegos de rede simulados com determinadas propriedades estatísticas, com o intuito de realizar um teste *off-line* de um determinado dispositivo na rede pretendida. Adicionalmente, podem ainda ser usados para introduzir desvios do comportamento ideal e perfeitamente determinista de um sistema, imitando assim, um sistema real. Por outras palavras, podem ser usados para simulações de ruído no referido sistema.

Na implementação de geradores de números aleatórios analógicos existem diversas abordagens, nomeadamente o modelo PGNA (pseudo gerador de números aleatório) que consiste num circuito onde o gerador de números cria uma sequência repetitiva de valores que parecem ser de forma aleatória. O VGNA (verdadeiro gerador números aleatório), onde o gerador de números cria uma sequência aleatória, não sendo esta previsível. No PGNA temos um circuito denominado por LFSR (*linear feedback shift register*). Este circuito é composto por

uma cadeia de *flip-flops* onde, cada saída de *flip-flop,* é ligada à entrada do seguinte. Todos são regulados pelo mesmo *clock* (sinal de relógio), sendo que, a entrada do primeiro *flip-flop* é uma ligação direta das saídas de um ou mais *flip-flops* presentes na cadeia. Se o *feedback* for escolhido corretamente, consegue-se obter um LFSR com o máximo comprimento. Este valor obtido entrará num ciclo de onde resultará sempre um valor de saída idêntico a um contador, mas de forma aleatória. Estes valores de saída parecem ser aleatórios, mas podem ser previsíveis matematicamente, desse facto provém o nome PGNA [1].

Tal como a figura 1.1 mostra, os geradores de números aleatórios são compostos por PGNA's e VGNA's. No que diz respeito aos PGNA's (representado na figura por *software*/lógico), estes são pseudo-geradores de números aleatórios e os VGNA's são geradores de números aleatórios físicos. Os referidos por último, são compostos por quatro subcategorias: pelos geradores com base no ruído, com base no caos, com base em osciladores de livre funcionamento, e finalmente, pelos geradores de efeitos quânticos. Em contraste com os PGNA's, os VGNA's extraem a sua aleatoriedade do seu *hardware* de processos físicos que têm comportamentos não determinísticos. Desta forma, estes equipamentos são vistos como sendo melhores candidatos para geração de números aleatórios [2]. Os VGNA's podem repartir-se em quatro categorias, como indicado na figura 1.1:

1. Ruído GNA's;
2. Oscilador de livre funcionamento GNA's;
3. Caos GNA's
4. Quântico GNA's.



.

Figura 1.1 - Árvore de categorização de geradores aleatórios de números

Abstraindo das restantes categorias, cingimo-nos aos Caos GNAS visto que o circuito selecionado para tema da dissertação está enquadrado nessa categoria

Provavelmente o princípio que levanta mais dúvidas para o processo de gerar números aleatórios de forma física, é a obtenção dos mesmos a partir de medições repetidas de um sistema físico no caos. O problema filosófico que surge é que o caos significa encontrar ordem no que é aparentemente aleatório. Com base neste conceito utilizou-se o circuito caótico de Chua com o díodo Matsumoto como gerador de números aleatórios. Esta categoria de GNA's caóticos detém uma mistura conceptual de caos e aleatoriedade. Estas características, aliadas à robustez de certos sistemas caóticos, conseguem produzir níveis mínimos de ruído facilmente utilizáveis para gerar números aleatórios, essencialmente através de métodos de geração de ruído GNA.

Frequentemente, são efetuadas interpretações de forma errónea relativamente ao conceito de Caos, referindo-se a este, como sendo uma desordem ou, até mesmo, algo aleatório. Matematicamente, este é um sistema determinístico, dado que é possível anotar todas as equações de evolução. Apresenta duas características que mais nenhum sistema mostra, uma vez que, tem a presença de trajetórias irregulares aperiódicas e uma extrema sensibilidade às condições iniciais. Anteriormente, foi enunciado que, para existir imprevisibilidade é necessário existir falta de periodicidade, que é uma das características dos sistemas caóticos. Relativamente à sensibilidade do sistema às condições iniciais, este efeito é denominado efeito de borboleta e ocorre quando dois sistemas idênticos, com início em condições iniciais iguais, perante uma pequena alteração quase insignificante, poderão ter evoluções ao longo do tempo completamente distintas. Consequentemente, uma previsão a longo prazo de um sistema caótico pode-se revelar praticamente impossível. No entanto, se analisarmos uma fração do tempo, observando um sistema real, é possível medir a condição ideal com precisão limitada [1].

Pode argumentar-se que o GNA com base no Caos e o PGNA podem ser semelhantes devido ao facto de ambos, terem por base um algoritmo determinístico. Porém, existem duas diferenças significativas. Uma delas é a quantização, que é uma operação irreversível, onde não é possível recuperar o estado interno do sistema com base nos valores quantificados. Outra diferença é que, sendo o circuito caótico um circuito analógico, este é afetado pelo ruído. Mesmo que se ignore o ruído durante os testes, este modifica continuamente o estado interno do sistema, e assim, a evolução do sistema ao longo do tempo. Considerando que a evolução inicial do sistema tem por base o ruído existente no arranque do sistema, este regula toda a evolução do sistema de forma a considerar-se este gerador como VGNA. De acordo com este ponto de vista, um GNA baseado no Caos, não é diferente de um gerador baseado na observação direta de um fenómeno idêntico ao ruído.

1.1 Motivação e Objetivos

Como mencionado na introdução, os VGNA's subdividem-se em quatro tipos diferentes. O funcionamento do VGNA com base no caos, foi o gerador de números aleatórios que permitiu o estudo a nível de eletrónica analógica, onde é utilizado um método aleatório singular. Este tipo de GNA é possível implementar em *hardware* como sendo um bloco independente, dando origem a um gerador de números aleatórios caótico inacessível, aumentando assim a dificuldade de descodificação por parte de quem tenta capturar a mensagem enviada, sendo que, esta é a finalidade do estudo que será efetuado nesta dissertação.

A encriptação é crucial para a segurança de informação confidencial. Desta forma, para além de transmitir-se uma mensagem encriptada, resolveu-se criar um circuito analógico independente, que conduzirá a forma como a mesma será transmitida, utilizando a teoria de caos. A implementação de geradores eletrónicos de números aleatórios, tem como objetivo gerar uma sequência de números aleatórios independentes, com a particularidade de que quando estes sejam gerados não produzam sempre as mesmas sequências, para que exista a não repetibilidade. Assim sendo, a solução desenvolvida e aqui apresentada, consiste na criação de um circuito que, analogicamente, origine números aleatórios, números estes que servirão para definir qual o conjunto de antenas (*array* de antenas) a ser utilizado. A forma como o circuito é formado permite ter os bits que forem desejados para qualquer tipo de *array* de antenas. Para o caso de 3 bits, ficam disponíveis 8 números para definir 8 *array's* de antenas. Assim sendo, cada número poderá corresponder a 1 conjunto de antenas. Tendo o recetor acesso a este número e à forma de encriptação, saberá automaticamente em que conjunto de antenas estará parte da mensagem enviada, podendo deste modo organizar e recriar a mesma, sem qualquer interferência de outras transmissões.

Com esta solução, utilizando o circuito físico e não sob a forma de *software*, existe uma maior segurança para toda a transmissão da mensagem. Esta forma de transmissão traz vantagens a nível de velocidade, em comparação com as encriptações baseadas em *software*. Outra mais-valia a sublinhar, é o facto de que, sendo o circuito físico, o único acesso ter de ser realizado fisicamente, evitando ser alvo de espionagem industrial, garantindo assim a segurança da informação que se pretende preservar.

1.2 Organização da Dissertação

A dissertação é composta por cinco capítulos, na qual se inclui a presente introdução. Nesta é efetuada uma referência à aleatoriedade e a sua aplicação em dispositivos eletrónicos, contém também uma breve análise sobre as redes de telecomunicações onde é mencionado o tema da difusão aleatória de transmissão através de um circuito analógico. Neste capítulo é ainda descrita a origem do interesse pelo projeto, descrevendo o problema e uma possível solução para o mesmo, e por fim a estrutura adotada que se adequa a esta dissertação.

No segundo capítulo, são caracterizados os sistemas caóticos, sendo realizado um estudo sobre os circuitos analógicos existentes, aplicações onde os mesmos podem ser utilizados, nomeadamente na vertente de telecomunicações.

O terceiro capítulo contém a informação detalhada sobre o circuito, nomeadamente, as suas características e os seus componentes que o constituem. Adicionalmente, é realizada uma descrição detalhada da teoria subjacente ao circuito desenvolvido e apresentado no quarto capítulo, nomeadamente, a aplicação de uma bobine ativa e a utilização da técnica *bootstrapping*.

O quarto capítulo consiste na apresentação dos resultados e gráficos resultantes das simulações realizadas em *software*, após a substituição da bobine ideal por uma bobine ativa, de forma a verificar a influência destas no circuito, tal como a diminuição dos condensadores da ordem dos Nano Farad (nF) para os Pico Farad (pF).

No quinto capítulo serão apresentadas as conclusões relativas às análises realizadas no quarto capítulo. Adicionalmente é efetuada a comparação entre o circuito que se encontra no terceiro capítulo, o circuito original com o circuito modificado, onde foram efetuadas alterações nos componentes que o constituem, que está presente no quarto capítulo. Por fim, ainda no capítulo quinto, serão apresentadas as propostas para trabalhos futuros.

1.3 Contribuições

As principais contribuições desta dissertação são:

- os circuitos geradores de números aleatórios, nomeadamente caóticos, detêm uma mistura conceitual de caos e aleatoriedade. A robustez deste tipo de circuitos analógicos permite gerar números aleatórios com maior velocidade do que as abordagens digitais criadas para o mesmo efeito;

- sendo o circuito analógico e estando este em contacto direto com a antena, após a implementação que originará uma seleção aleatória do *array* de antenas, a transmissão de dados será muito mais eficiente quer a nível de segurança quer de velocidade.

2

2 Estado da arte

Neste capítulo pretende-se descrever o que é a Teoria do Caos, qual o seu impacto no objeto em estudo, analisar GNAS que se baseiem nesta teoria, verificar o seu funcionamento, dar a conhecer e comparar dois casos distintos de circuitos e elucidar o porquê de se optar por um deles.

Este capítulo está relacionado com o estudo da Teoria do Caos, para tal optou-se por dividir o capítulo em secções onde a primeira é uma introdução ao Caos em que se explica a sua base e o seu funcionamento. Neste ponto é descrito o que é um sistema caótico, quais as especificações que o mesmo deve apresentar, tal como as suas características. De seguida, são apresentados diferentes tipos de GNAS existentes. No ponto seguinte, é feita uma análise sobre dois modelos de circuitos caóticos autónomos. A comparação entre os dois circuitos é realizada no ponto posterior, onde se justifica qual o motivo de se ter optado por um dos circuitos para servir como base de estudo para esta dissertação.

Esta dissertação tem como objetivo mostrar como direcionar a informação proveniente do emissor utilizando um circuito analógico baseado na teoria de caos.

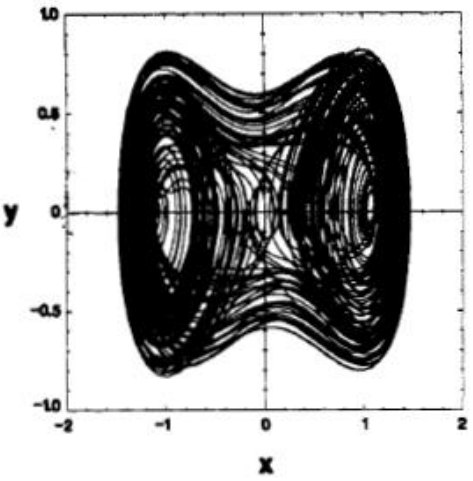
2.1 Caos

O caos é a ciência das surpresas, do não-linear e do imprevisível. Ensina-nos a esperar o inesperado. Enquanto a ciência mais tradicional lida com fenómenos supostamente previsíveis, como a gravidade, eletricidade ou reações químicas, a teoria do caos lida com situações não lineares que são, efetivamente, impossíveis de prever ou controlar, como o clima, a turbulência, o mercado de ações, os nossos estados cerebrais e assim por diante. Estes fenómenos são frequentemente descritos pela matemática fractal, que tenta capturar a complexidade infinita da natureza [1],[2],[3].

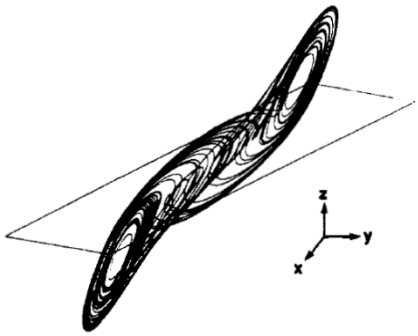
A Teoria do Caos é um padrão de organização dentro de um fenómeno desorganizado, ou seja, dentro de uma aparente causalidade. Nos dias de hoje, no meio que nos rodeia, vemos fenómenos que não podem ser descritos ou previstos pelas leis matemáticas, denominando-se estes por fenómenos caóticos. De um modo simplificado, o caos pode ser definido como comportamento de estado estacionário delimitado (estado estacionário - estado que não muda com o tempo, ou, estado para o qual o comportamento do sistema se torna assintótico à medida que o tempo passa para o infinito), que não é um ponto de equilíbrio, não é periódico (não tem um período constante), nem quasi-periódico (não se consegue no infinito prever o seu período), sendo difícil a sua definição. Na figura 2.1 (a) (onde y representa o sinal de saída e x o sinal de entrada) e (c) (onde y representa o sinal de saída, x o sinal de entrada e z o tempo), apresentam-se dois exemplos de trajetórias caóticas. A ilustração (a) representa um atrator de segunda ordem e a (c) um atrator de terceira ordem, que é uma característica de sistemas caóticos, segundo Lorenz. O atrator é fundamental na análise do caos. No espaço de fase, um atrator mostra o comportamento a longo prazo de um sistema. É uma imagem compacta e global de todos os possíveis estados estacionários de um sistema. De modo sucinto, pode dizer-se que o atrator é o cartão de identificação de um sistema. É um conjunto de pontos contidos numa forma, que se estabelece no espaço de fase, ocupando apenas certas zonas dentro do espaço de fase delimitado. Assim, um atrator caótico é uma unidade composta de todas as trajetórias caóticas. As trajetórias podem originar-se em qualquer lugar dentro da bacia de atração do atrator, sendo que nunca chegam a cruzar-se. Se tal acontecesse, o sistema poderia comportar-se de modos distintos sempre que as condições no ponto de passagem se repetissem. As trajetórias caóticas gravitam em direção ao atrator ao longo do tempo. Além disso, produzem dobras quando atingem o seu limite de espaço de fase. Um atrator caótico tem uma estrutura interna complexa e irregular de muitas camadas. Tem uma distribuição de probabilidade invariante - um histograma que representa a frequência relativa a longo prazo com que o sistema visita as suas várias colocações possíveis de espaço de fase, para um dado valor do critério de controle. Um atrator caótico é bastante reprodutível e mostra extrema sensibilidade às condições iniciais e a sua trajetória pode ser periódica ou não periódica.

Observando as ilustrações presentes na figura 2.1 (b) e (d) é notório que os sinais são de facto não periódicos, e que não têm uma distribuição uniforme, característica das soluções quase periódicas. Apesar da última afirmação, o comportamento quasi-periódico não está descartado [1],[4].

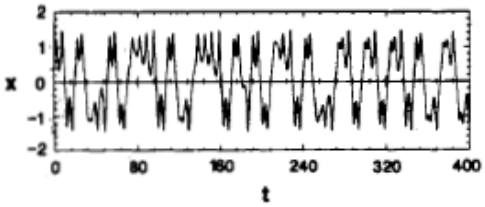
A dependência das condições iniciais é outra característica dos sistemas caóticos, já que, tendo em conta, duas condições iniciais diferentes, arbitrariamente perto uma da outra, as trajetórias que daí provêm são obrigatoriamente diferentes. Na prática, o estado inicial de um sistema nunca pode ser descrito de modo preciso, mas apenas dentro de uma determinada tolerância $\epsilon > 0$. Se duas condições iniciais, x_0 e $\hat{x}_{0,}$ estão contidas uma na outra, não podem ser diferenciadas. No entanto, após uma quantidade de tempo finita, $\phi_t\,(x_0)$ e $\phi_t\,(\hat{x}_0)$, vão divergir tornando-se distintas. Assim conclui-se, que não importa a precisão com que as condições iniciais são conhecidas, pois o comportamento a longo prazo de um sistema caótico nunca pode ser previsto. É desta imprevisibilidade que se fala quando se descrevem os sistemas caóticos como sistemas determinísticos que exibem comportamento aleatório [3],[5].



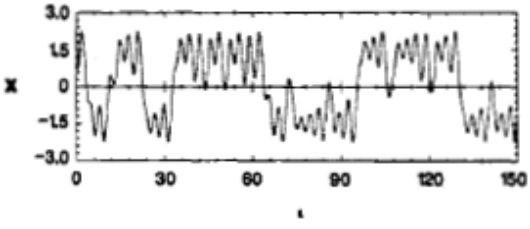
(a) Trajetória de segunda ordem de um sistema não autónomo.



(c) Trajetória caótica de terceira ordem do sistema autónomo.



(b) Forma de onda do tempo do primeiro componente de (a)



(d) Forma de onda do tempo do primeiro componente de (c).

Figura 2.1 (a-d) - Trajetórias caóticas [3],[5].

Um circuito para ser considerado caótico tem que obedecer a três condições [5]:

- ter três ou mais elementos que consigam armazenar energia;
- ter pelo menos um elemento não linear;
- e ter uma ou mais resistências localmente ativas.

A sequência de números gerada pelo circuito analógico em estudo é impossível de prever, porque para além de respeitar as condições acima mencionadas, o sistema por ele gerado tem as seguintes propriedades:

- uma pequena diferença nos parâmetros iniciais que resultará num comportamento completamente diferente de um sistema complexo;
- o princípio da incerteza proíbe a precisão. Portanto, a situação inicial de um sistema complexo não pode ser determinada com precisão, assim como a sua evolução não pode ser precisamente prevista;
- sistemas complexos muitas vezes procuram resolver uma situação específica. Esta situação pode ser estática ou dinâmica, que será possível visualizar nos atratores gerados pelos diferentes tipos de sistemas.

2.1.1 GNAS Existentes

Neste ponto irão ser enumerados diferentes tipos de GNAS existentes, sendo feita uma breve descrição de cada um deles para uma melhor compreensão (tendo em conta a figura 1.1).

No caso do PGNA BBS (*Blum Blum Shub*), estamos perante um gerador pseudoaleatório proposto em 1986 por Leonore Blum, Manuel Blum e Michael Shub [6],[7],[8]. É descrito por:

$$x_{n+1} = (x_n)^2 \bmod M, \tag{2.1}$$

onde $M = pq$ é o produto de dois grandes números primos p e q. A cada etapa do algoritmo, alguma saída é derivada de x_n; a saída é geralmente a paridade de bit de x_n, ou um ou mais dos bits menos significativos de x_n.

Este gerador é apropriado para ser utilizado em criptografia, uma vez que é possível provar a sua segurança. A prova de segurança, relaciona a qualidade do gerador com a dificuldade computacional de factoração de inteiros [7].

O PGNA KISS (*Keep It Simple Stupid*), é um gerador, que deve o seu nome ao princípio empírico: a simplicidade é um trunfo e um objetivo essencial em qualquer sistema. Este tipo de gerador é bastante conhecido em engenharia e no *software*. Este termo, KISS, significa "mantem-no simples, estúpido". Este gerador foi elaborado por George Marsaglia utilizando uma arquitetura muito simples e surge da combinação de alguns geradores pseudoaleatórios

simples, com o objetivo de se obter comportamentos mais complexos em relação aos geradores originais [7].

Relativamente ao modelo do gerador aleatório *VIA Padlock*, este usa os novos processadores de VIA, que incluem o *PadLock Security Engine*, nomeadamente os processadores C3, C5P e C7. Esta tecnologia consiste num bloco de primitivas de *hardware* projetado para implementar diversos recursos relacionados com a segurança. Este gerador tem a componente de *VIA PadLock RNG*, sendo este baseado no *Jitter* de dois osciladores de correntes livres, onde o primeiro é muito rápido e o segundo muito lento. O oscilador lento é utilizado para provar o rápido. Como os osciladores não podem atingir a sincronização, os valores amostrados dependem do *Jitter* do lento, dando assim origem a bits aleatórios. Estes bits são pós processados por um determinado algoritmo [7],[8].

Por fim, existe ainda o gerador aleatório *quantis*, elaborado pela empresa *idQuantique SA*. Trata-se de um gerador que utiliza valores baseados na reflexão de um único fotão num espelho semitransparente [7].

2.2 Modelos de circuitos caóticos

Nesta secção são apresentados dois circuitos de modelos caóticos e autónomos. Entenda-se por sistema autónomo um circuito que não necessita de impulsos para entrar em funcionamento. Neste caso fornece-se alimentação ao circuito e o mesmo começa a oscilar de forma independente.

O teste desses circuitos mostra que existe uma baixa ordem determinística (Newtoniana), uma vez que estes sistemas são imprevisíveis, pois uma ligeira alteração na condição inicial pode originar uma trajetória absolutamente distinta. Comparativamente, no caso dos osciladores periódicos, toda a trajetória pode convergir para a mesma órbita periódica independentemente da condição inicial, sendo por isso previsíveis. Além disso, relativamente aos circuitos imprevisíveis, também é possível verificar que podem produzir ruído determinístico [5]. Nestes circuitos eletrónicos, podem observar-se fenómenos caóticos. A simplicidade dos mesmos permite a sua fácil construção e implementação, possibilitando a confirmação dos fenómenos obtidos através de simulação em elemento digital e, em alguns casos, provar com rigor, que o circuito é de facto caótico. Entende-se por caótico, um circuito que admite uma oscilação não periódica. Podem, deste modo, destacar-se dois circuitos caóticos:

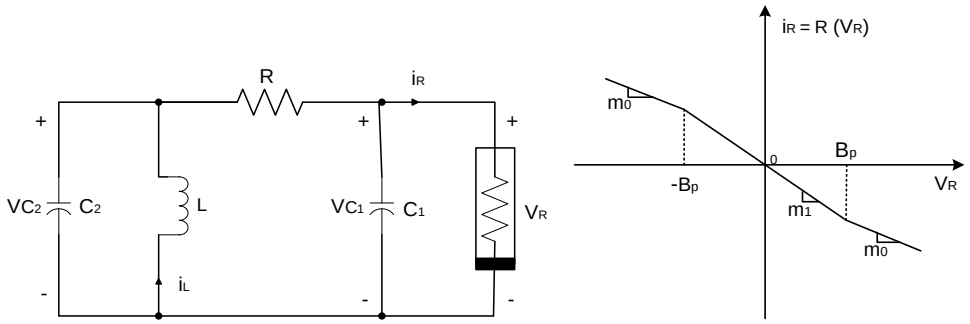
I) *Double scroll* [5],[25]

II) *Folded torus* [5],[25].

Nestes circuitos, a corrente e a tensão de cada elemento do circuito desempenham papéis críticos na dinâmica do sistema, uma vez que não pertencem a um elemento analógico.

2.2.1 Double Scroll

O circuito *Double Scroll* é um dos poucos sistemas físicos que obedece na íntegra às características de um circuito simples. O circuito genérico encontra-se apresentado na figura 2.2 (a), onde pode verificar-se que é constituído por duas partes. A primeira parte composta por um oscilador, nomeadamente formado por C_2, C_1, L e R e a segunda parte que contêm apenas um elemento não linear representado por V_R, que faz com que, a sua característica seja uma resistência não linear com dois pontos de quebra indicados na figura 2.2 (b) [5]. A explicação do circuito é realizada na sequência da figura 2.6 nomeadamente nas secções A,B e C.



(a) O circuito

(b) Característica $v - i$ da resistência não linear.

Figura 2.2 - Circuito autónomo simples com um atrator caótico [5],[25].

O princípio terá como base de funcionamento o atrator de Lorenz que tem como finalidade gerar um mapa caótico baseado num sistema dinâmico que evolui com um padrão complexo. As equações que demonstram o andamento de um atrator de Lorenz num eixo tridimensional com base no tempo percorrido são [5],[9],[10]:

$$\frac{dx}{dt} = \sigma(y - x), \tag{2.2}$$

$$\frac{dy}{dt} = x(\rho - z) - y, \tag{2.3}$$

$$\frac{dz}{dt} = xy - \beta z, \tag{2.4}$$

onde σ é chamado o número de Prandtl [11] e ρ o número de Rayleigh. Todos σ, ρ e $\beta > 0$, mas usualmente $\sigma = 10, \beta = \frac{8}{3} e\, \rho$ é variado. O sistema exibe comportamento caótico para $\rho > 28$ e exibe órbitas para outros valores.

Segundo Jaime E. Villate [12], um atrator não tem principio nem fim, tem evolução infinita. Este ocupa uma região de espaço de fase e não tendo principio nem fim significa que a oscilação é sempre diferente sem chegar nunca a repetir-se (período infinito) [12],[13]. Consequentemente a presença de um atrator revela um sistema caótico.

Se fizermos a analogia com o circuito representado na figura 2.2 obtemos o conjunto de equações de Chua descritas por:

$$x = \sigma\big(y - x - R(x)\big), \tag{2.5}$$

$$y = x - y + z, \tag{2.6}$$

$$z = -\beta y, \tag{2.7}$$

e se analisarmos o andamento da característica $v - i$ representados na figura 2.2 b), temos que:

$$R(x) = \begin{cases} m_0 x + m_0 - m_1, & \text{se } x \leq -1, \\ m_1 x, & \text{se } -1 \leq x \leq 1, \\ m_0 x + m_1 - m_0, & \text{se } 1 \leq x. \end{cases} \tag{2.8}$$

Tendo em conta os elementos do circuito com o andamento da característica $v - i$, temos como resultante:

$$v_1 = [1/(R.C_1)]\big((v_2 - v_1) - R.R(v_1)\big), \tag{2.9}$$

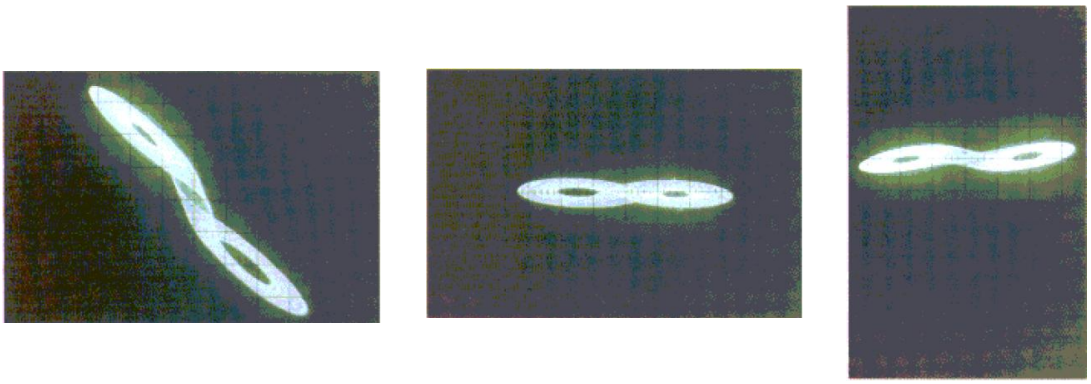
$$v_2 = [1/(R.C_2)](v_1 - v_2 + R.i_L), \tag{2.10}$$

$$i_L = [1/(L)](-v_2), \tag{2.11}$$

$$R(v_1) = \begin{cases} m_0 v_1 + (m_0 - m_1)B_P, & \text{se } v_1 \leq -B_P, \\ m_1 v_1, & \text{se } -B_P < v_1 < B_P, \\ m_0 v_1 + (m_1 - m_0)B_P, & \text{se } B_P \leq v_1. \end{cases} \tag{2.12}$$

As grandezas intervenientes acima referidas: $v_1 = Vc_1$ e $v_2 = Vc_2$, representam a tensão aos terminais dos condensadores C_1 e C_2. $R(v_1)$ representa a função transferência de V_R representada na figura 2.2 (a) e B_P corresponde à tensão limiar de condução dos díodos apresentados na secção B na figura 2.7.

A figura 2.3 apresenta o atrator observado para o circuito da figura 2.2, e na figura 2.4 são visualizadas as formas de onda no tempo, correspondentes ao andamento descrito pelas equações de Chua referidas em (2.5), (2.6) e (2.7) relativamente ao circuito da figura 2.2:

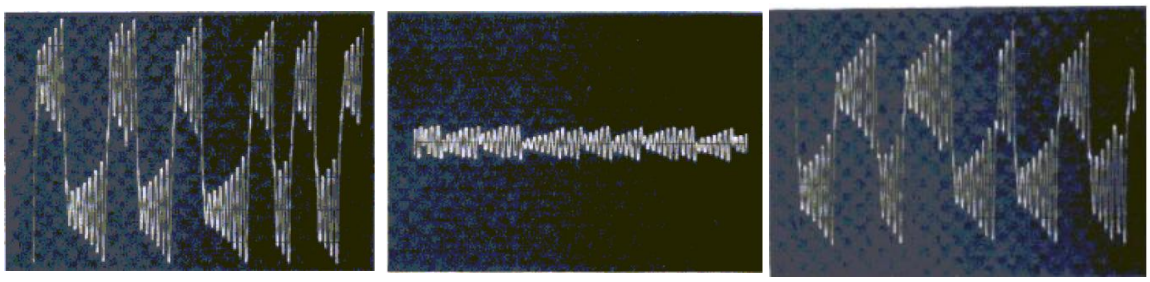


(a) Projeção sobre o plano (i_L, v_{C_1}).(a) Trajetória caótica

(b) Projeção sobre o plano (i_L, v_{C_2}).

(c) Projeção sobre o plano (v_{C_1}, v_{C_2}).

Figura 2.3 - Atrator observado. Voltagem: 2V/div. Corrente: 2mA/div [5].



(a) $v_{C_1}(t)$. Escala vertical: 2 V/div.

(b) $v_{C_2}(t)$. Escala vertical: 2 V/div.

(c) $i_L(t)$. Escala vertical: 2 mA/div.

Figura 2.4 - Formas de onda no tempo medido. Escala horizontal: 1 ms/div [3],[5].

Na figura 2.3 estão representados os atratores resultantes da implementação apresentada na figura 2.2, sendo que, na imagem 2.3 (b) está representado o sinal de saída em função do sinal de entrada. A figura 2.4 ilustra o andamento do sinal ao longo do tempo, comprovando que o mesmo não é periódico.

Na figura 2.5 apresenta-se de forma mais minuciosa o circuito apresentado na figura 2.2 (a):

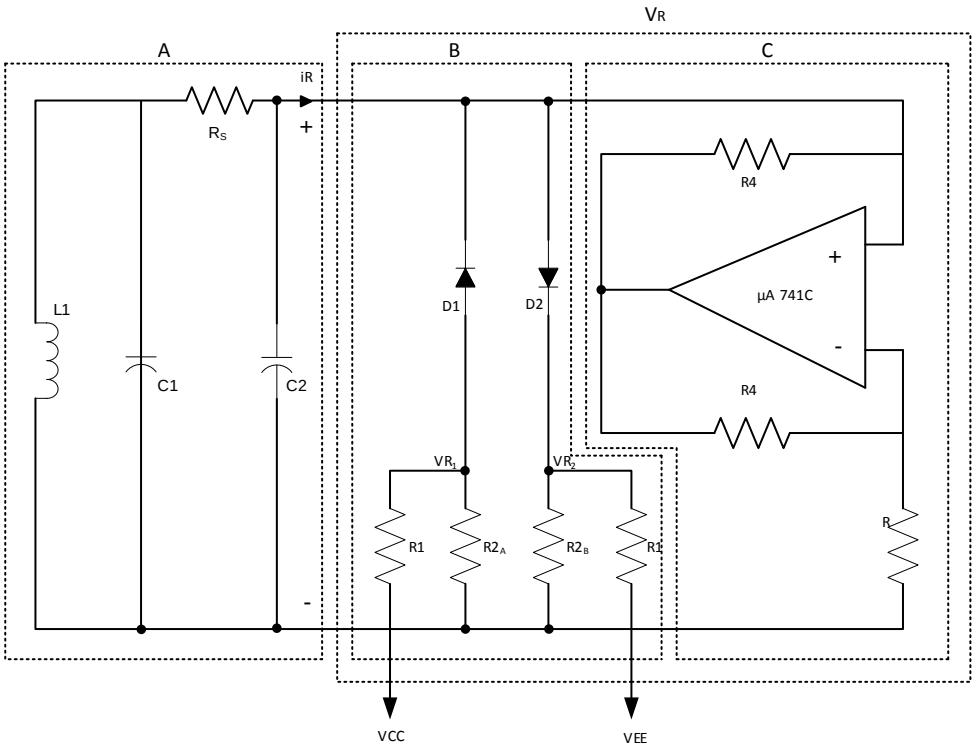


Figura 2.5 - Outra realização do circuito representado na figura 2.2 [3],[5].

Este circuito é constituído por três secções: a primeira de oscilação (A); uma segunda de emulação de um elemento não linear conforme referido (B); e, a terceira, uma de fonte de energia para a parte dinâmica do circuito (C), de referir que (B) e (C) constituem o V_R apresentado na figura 2.2 (a).

Seguidamente é realizada uma breve análise de cada secção que compõe este circuito.

- <u>Secção (A) – Oscilação:</u>

  Esta secção, é obtida pelo circuito representado na figura 2.6:

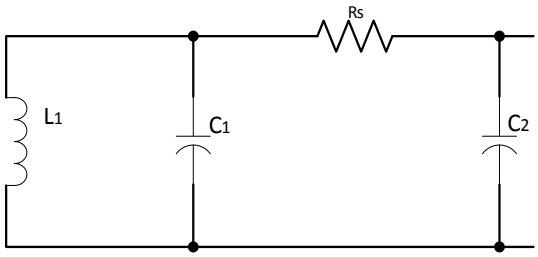


Figura 2.6 - Circuito oscilador amortecido.

O circuito oscilador é constituído por uma bobine (L_1), dois condensadores (C_1 e C_2) e R_s uma resistência, onde a tensão entre R_s e C_2 será o sinal de saída (V_{OUT}), como representado na figura 2.6, tendo como função oscilar a uma determinada frequência (f) [14].

Esta frequência (a que o circuito irá oscilar) é a frequência de ressonância entre os componentes em causa, que ocorre quando as suas reactâncias são iguais. Logo:

$$\mathrm{X_L} = 2\pi f L\,, \qquad \mathrm{X_C} = \frac{l}{2\pi f C}\,, \tag{2.13}$$

definindo os dois iguais entre si, representando uma condição de reatância igual (ressonância),

$$2\pi f L = \frac{l}{2\pi f C}\,, \tag{2.14}$$

multiplicando ambos os lados por f, elimina o termo f no denominador da fração,

$$2\pi f^2 L = \frac{1}{2\pi C}\,, \tag{2.15}$$

dividindo ambos os lados por $2\pi L$, obtém-se

$$f^2 = \frac{l}{2\pi 2\pi LC}\,, \tag{2.16}$$

pelo que temos,

$$f = \frac{l}{2\pi\sqrt{LC}}\,. \tag{2.17}$$

Com $C \approx C_1 + C_2$.

- <u>Secção (B) - Emulação de um elemento não linear:</u>

Esta secção que gera a parte caótica do circuito deve-se à inclusão de um elemento não linear. Isto é realizado através do circuito da figura 2.7:

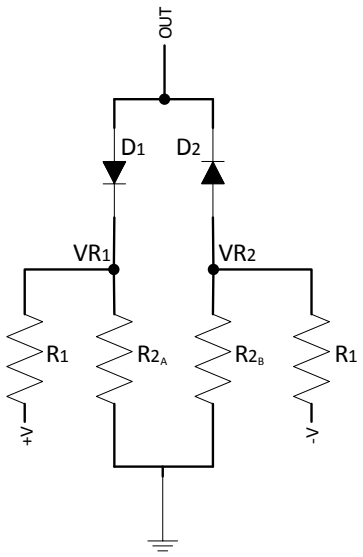


Figura 2.7 - Circuito não linear com dois díodos.

No circuito a tensão em V_{OUT} ultrapassa o valor do limiar de condução do díodo (tanto na parte negativa como na positiva), para D_1 e D_2. Este valor do limiar de condução do díodo é dado por:
na parte positiva:

$$\left(\frac{R1}{R1+R2}\cdot V^{+}\right)+V_{FD1}, \tag{2.18}$$

e na parte negativa:

$$\left(\frac{R2}{R2+R1}\cdot V^{-}\right)-V_{FD2}. \tag{2.19}$$

O díodo apenas conduz quando V_{OUT} é superior a $V_{FD}+V_{R1}$, onde V_{FD} representa a tensão no díodo e V_{R1} a tensão em $R1$.

Quando o díodo começa a conduzir, as resistências $R2_A$ ou $R2_B$ começam a afetar o funcionamento do circuito o que faz com que influencie a impedância do mesmo, ou seja, a impedância varia no instante em que uma das resistências, $R2_A$ ou $R2_B$, começam a afetar a dinâmica do circuito. Por esse motivo o circuito apresentado, é considerado o elemento não linear, visto que provoca uma variação da característica $V-I$, conforme é demostrado na figura 2.2 (b). O declive m_0 é quando as resistências influenciam o funcionamento e o declive m_1 ocorre quando as resistências em causa não têm qualquer impacto no circuito.

- Secção (C) – Fonte de energia para a parte dinâmica do circuito:

Esta secção é obtida através de um conversor de impedância negativa (CIN), que basicamente, é um circuito que utiliza um amplificador operacional (op-amp) que funciona como uma carga negativa. Isto é, conseguido através da introdução de um desvio de fase de $180°$ (inversão), entre a tensão e a corrente, para uma fonte de sinal. Existem duas versões deste circuito: com inversão de tensão (VCIN) e com inversão de corrente (ICIN). O circuito básico de um ICIN e a respetiva análise é apresentado na figura 2.8.

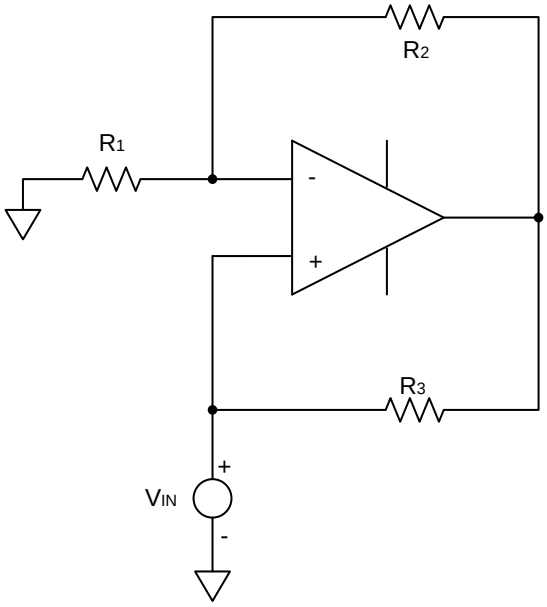


Figura 2.8 - Conversor de impedância negativa.

O ICIN é um amplificador não inversor (amplificador operacional e um divisor de tensão R_1, R_2 na figura 2.8) com uma resistência (R_3) conectada entre a sua saída e entrada. A tensão de saída do amplificador operacional é

$$V_{opamp} = V_{in}\left(1 + \frac{R_2}{R_1}\right). \tag{2.20}$$

A corrente que vai da saída do amplificador operacional através da resistência R_3 para a fonte V_{in} é - I_{in}, visto que, a tensão de saída do amplificador operacional é superior à sua tensão de entrada, o que faz com que o sentido de corrente seja da direita para a esquerda de R3,

$$I_{in} = \frac{V_{opamp} - V_{in}}{R_3} = V_{in}\frac{\frac{R_2}{R_1}}{R_3} \quad . \tag{2.21}$$

Por conseguinte, a entrada V_{in} experimenta uma corrente de oposição - I_{in} que é proporcional a V_{in}, e o circuito age como um resistor com resistência negativa

$$R_{in} = \frac{V_{in}}{I_{in}} = -R_3 \frac{R_1}{R_2}. \tag{2.22}$$

De um modo geral, R_1, R_2 e R_3 não precisam ser resistências puras (ou seja, podem ser condensadores, indutores ou redes de impedância), mas, neste caso recorre-se à utilização de elementos resistivos.

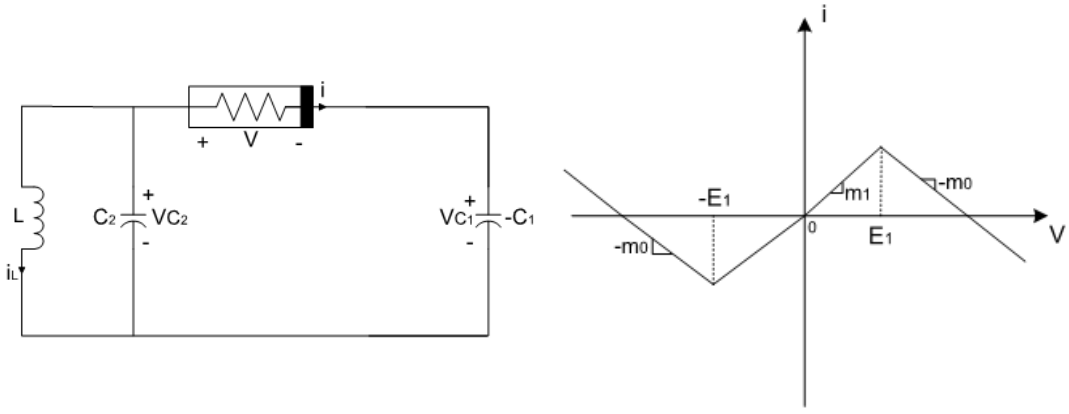
2.2.2 Folded Torus

Uma das possibilidades é ter um mecanismo de caos com base num gerador que tem como princípio uma órbita, que quando se muda os parâmetros obtemos uma bifurcação para um regime de quasi-periódico. As equações diferenciais que descrevem este comportamento são:

$$\frac{dx}{dt} = -\alpha f(y - x), \tag{2.23}$$

$$\frac{dy}{dt} = -f(y - x) - z, \tag{2.24}$$

$$\frac{dz}{dt} = \beta y. \tag{2.25}$$



(a) Implementação do circuito

(b) Resistência não linear com característica $v - i$

Figura 2.9 Circuito simples autónomo de terceira ordem que apresenta um anel fechado [3].

Se fizermos a analogia com o circuito representado na figura 2.9 é possível escrever:

$$C_1 \frac{dv_{C_1}}{dt} = -g\left(v_{C_2} - v_{C_1}\right), \tag{2.26}$$

$$C_2 \frac{dv_{C_2}}{dt} = -g\left(v_{C_2} - v_{C_1}\right) i_L, \tag{2.27}$$

$$L = \frac{di_L}{dt} = v_{C_2}, \tag{2.28}$$

e se analisarmos o andamento da característica $v - i$ temos que:

$$R(v) = -m_0 v + 0.5(m_0 + m_1)[|v + E_1| - |v - E_1|]. \tag{2.29}$$

Dos quatro elementos que compreendem o circuito apresentado na figura 2.9 (a), apenas um é não linear: a resistência linear por partes indicada pela figura 2.9 (b). Enquanto a capacidade C_1 tem um valor negativo (– C_1), os elementos lineares L e C_2 são passivos e E_1 corresponde à tensão de condução dos díodos. A dinâmica do circuito é descrita por:

$$C_1 \frac{dv_{C_1}}{dt} = -g\left(v_{C_2} - v_{C_1}\right), \tag{2.30}$$

$$C_2 \frac{dv_{C_2}}{dt} = -g\left(v_{C_2} - v_{C_1}\right) i_L, \tag{2.31}$$

$$L = \frac{di_L}{dt} = v_{C_2}, \tag{2.32}$$

onde v_{C_1}, v_{C_2} e i_L, representam respetivamente, a tensão através de C_1, a tensão através de C_2 e a corrente através de L. A função $R(\cdot)$ indica a característica de $v - i$ da resistência não linear e é representada por:

$$R(v) = -m_0 v + 0.5(m_0 + m_1)[|v + E_1| - |v - E_1|]. \tag{2.33}$$

Este circuito tem o funcionamento idêntico ao do *double scroll* sendo, as diferenças explicadas no subcapítulo 2.3. Apesar da capacidade ser positiva no lado direito, na figura 2.9, o sub-circuito N evidenciado na figura 2.10, induze-o a proceder como uma capacidade negativa quando observado a partir do lado esquerdo de N.

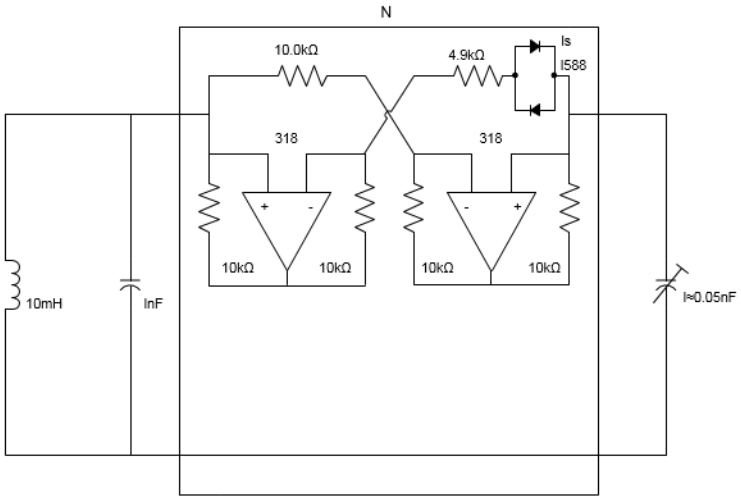
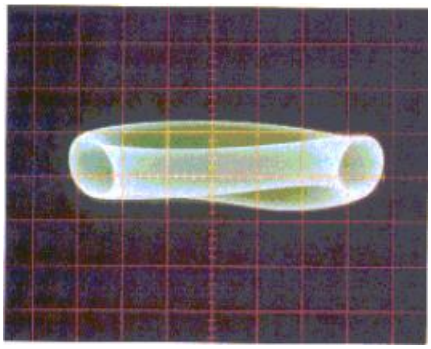
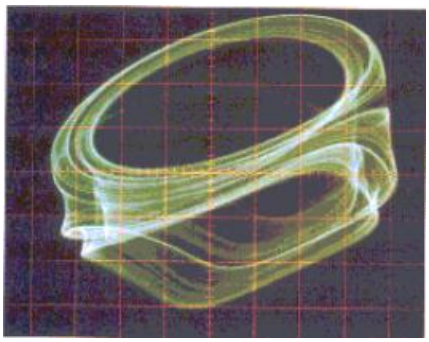


Figura 2.10 - Realização física do circuito mostrado na figura 2.9 [5].

A figura 2.11 apresenta duas imagens de anéis, com dois valores diferentes de C_1. A figura 2.11 (a) mostra 2 anéis, enquanto a figura 2.11 (b) indica um anel fechado. Clarificando: a figura 2.12 mostra as secções transversais das trajetórias correspondentes no $i_L = 0, v_{C_2} < 0$, tornando-se assim evidente que a figura 2.12 (a) representa 2 anéis, enquanto que a figura 2.12 (b) se parece com um anel dobrado [5]. De notar que as imagens que se seguem, são resultados do circuito representado na figura 2.9 (a).



(a) 2 anéis



(b) Anel fechado

Figura 2.11 - Atratores observados a partir do circuito da figura 2.9 projetado sobre o plano (v_{C_1}, v_{C_2}). Escala horizontal: 0.5 V/div. Escala vertical: 0.5 V/div. Apenas um dos dois atratores é mostrado [5].

(a) 2 anéis

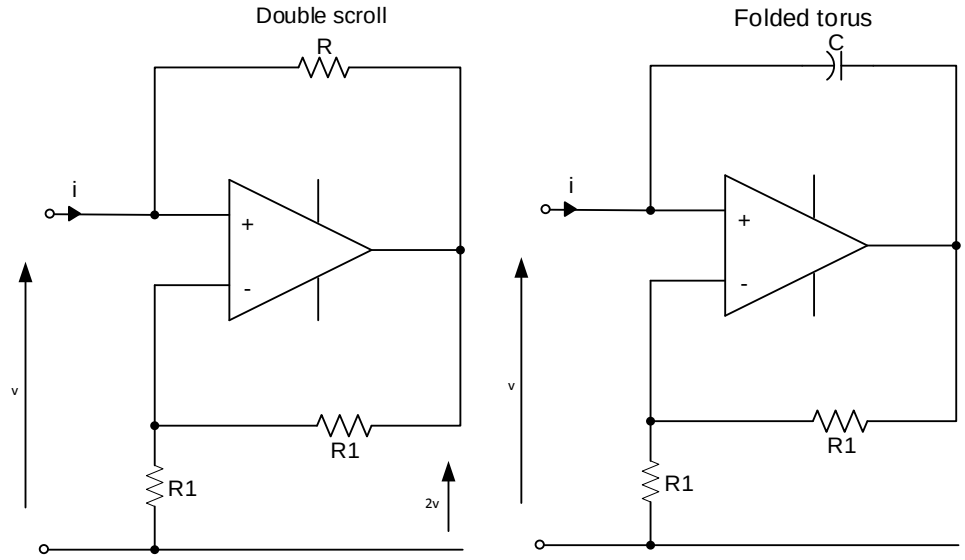
(a) Anel fechado

Figura 2.12 - Secções transversais $i_L = 0, v_{C_2} < 0$, das trajetórias do sinal correspondentes da figura 2.11, no plano (v_{C_1}, v_{C_2}) [5].

2.3 Diferença entre *Double Scroll* e *Folded Torus*

A resistência negativa $(R_{in} = -R)$,é invariante enquanto a capacidade negativa depende da frequência, como se pode observar pelas fórmulas apresentadas na figura 2.13. Outra característica, é que o circuito *double scroll,* tem órbita hiperbólica periódica e o *torus* tem uma orbita quasi-periódica. Por estas duas razões, o circuito escolhido foi o *double scroll*.

É possível visualizar no caso do *Double Scroll* que a resistência não depende de nada a não ser dela própria, ao passo que a impedância no *Folded Torus* não depende apenas do valor da capacidade do condensador.



(a) Circuito de resistência negativa

$$R_{in} = \frac{v}{i} = -R$$

(b) Circuito de capacidade negativa

$$Z_{in} = \frac{v}{i} = \frac{j}{\omega C}$$

Figura 2.13 Diferença entre Double Scroll e Folded Torus.

3

3 Circuito eletrónico

Este capítulo tem como objetivo demonstrar o funcionamento do circuito *double scroll*, estudado anteriormente. Mediante uma análise mais detalhada o nível de implementação, pretende-se gerar uma sequência de números aleatórios, o sinal V_{OUT}. Desta forma, optou-se por fazer uma breve introdução ao tema na secção 3.1, de seguida o fundamento teórico do teste 0-1 para caos. A implementação do circuito em *software* é apresentada de seguida, tal como o seu sinal de saída. É elaborado um histograma com o intuito de demonstrar a repetição das amostras retiradas do sinal de saída. Na secção 3.2, para permitir que o circuito seja passível de se tornar num circuito integrado, é feita uma alusão ao tema *gyrator* (bobine ativa) que permite diminuir o tamanho de uma bobine, e por ultimo na secção 3.3 é descrita a técnica de *bootstraping* que nos permite diminuir os valores dos condensadores de nF (Nano-Farad) para pF (Pico-Farad) (unidades de medição do condensador).

3.1 Gerador de números aleatórios

OS osciladores caóticos contínuos são usados inúmeras vezes para a formação de números aleatórios e sequências de bits caóticos. São implementados com placas de circuitos impresso, em vez de dispositivos dedicados especializados, devido à simplicidade da sua estrutura. Desempenham funções de elevada relevância e são de extrema importância ao garantirem a confiabilidade das sequências de bits formadas e a segurança do processo de geração contra quaisquer alterações não outorgadas das placas de circuito impresso, que possam colocar em risco o bom funcionamento dos geradores. As alterações ilícitas de *hardware* acontecem com mudanças de diagrama de circuito ou nas formas de parâmetros, sendo designadas como ataques de *hardware* ou *trojans*. A prevenção e deteção de alterações em sistemas com placas analógicas é um problema que persiste. Já em sistemas digitais reconfiguráveis este processo está facilitado devido ao desenvolvimento de técnicas especiais [15].

Após um abreve introdução aos osciladores caóticos, é apresentado o teste 0-1 utilizado para comprovação de que o circuito onde esta dissertação se baseia é efetivamente caótico. Neste tipo de teste não existe a necessidade de saber as equações dos sistemas não lineares (geradores), para conseguir realizar a distinção entre dinâmica regular e caótica, tal como, não é necessária uma etapa de reconstrução, pois o teste 0-1 opera apenas em amostras de tempo série (vetor) $\phi(j), j = 1, \dots, N$, assinalados durante o procedimento de medição. Com base no vetor $\phi(j)$, são definidas as variáveis de tradução p_c e q_c.

$$p_c(n) = \sum_{j=1}^{n} \phi(j)\cos(jc), \quad q_c(n) = \sum_{j=1}^{n} \phi(j)\sin(jc), \tag{3.1}$$

para $n = 1, \dots, N$, sendo n o número de amostras, com C sendo um valor escolhido aleatoriamente, pertencente ao intervalo $(0, \pi)$. Para detetar a ocorrência do caos, pode-se utilizar o método de regressão ou o de correlação. para a tradução das variáveis de p_c e q_c. O resultado é obtido sob duas formas: gráfica e numérica. A gráfica, é o andamento bidimensional de q_c contra o p_c para $n = 1, \dots, N$. Se o sinal analisado é caótico, então o andamento $q_c - p_c$ é um tipo de movimento Browniano com configuração irregular. A numérica, retorna um único número, $K \approx 1$, se o sinal analisado é caótico e $K \approx 0$ para sinal não-caótico [16],[17].

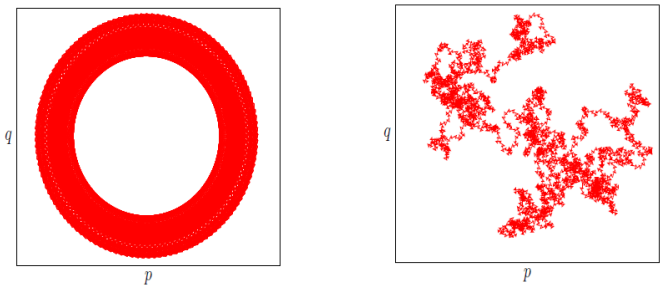
Seguidamente descreve-se a implementação do teste. Realiza-se a seguinte sequência de passos:

1. Para $c \in (0, \pi)$, calculamos as variáveis de tradução

$$p_c(n) = \sum_{j=1}^{n} \phi(j)\cos(jc), \quad q_c(n) = \sum_{j=1}^{n} \phi(j)\sin(jc), \tag{3.2}$$

para $n = 1, 2, \ldots, N$. Imagens típicas de p e q para a dinâmica regular e caótica são dadas na figura 3.1.

2. O comportamento difusivo (ou não-difusivo) de p_c e q_c pode ser investigado através da análise da média de deslocamento quadrado $M_c(n)$. A teoria adjacente do teste assegura que, se a dinâmica é regular, então o deslocamento quadrático médio é uma função limitada no tempo, enquanto que se a dinâmica é caótica, então, o deslocamento quadrático médio escala linearmente com o tempo.



(a) (b)

Figura 3.1 - Imagem de p versus q para o mapa logístico $x_{n+1} = \mu x_n (1 - x_n)$. Esquerda (a): dinâmica regular em $\mu = 3{,}55$; Direita (b): dinâmica caótica em $\mu = 3{,}9$. Neste teste foram utilizados 5000 pontos de dados [16].

3. Em seguida, calcular a taxa de crescimento assintótica K_c do deslocamento quadrático médio.

4. Os passos 1-3 são realizados para os valores N_c de c escolhidos aleatoriamente no intervalo $(0, \pi)$. Na prática, $N_c = 100$ é suficiente. Em seguida, calcular a média desses valores N_c de K_c para calcular o resultado final $K = \text{mediana}\,(K_c)$. O teste indica que um valor de $K \approx 0$ indica dinâmica regular, e $K \approx 1$ indica dinâmica caótica [16].

Olhando mais detalhadamente, quando é utilizado o método de regressão para calcular K, para o valor selecionado de C primeiro calcula-se o deslocamento médio quadrado:

$$M_c(n) = \frac{1}{N} \lim_{N\to\infty} \sum_{j=1}^{N} ([p(j+n) - p(j)]^2 + [q(j+n) - q(j)]^2) \,, \qquad (3.3)$$

onde $n = 1, 2, \ldots, n_{cut}$; $n_{cut} \ll N$. Se há presença de uma dinâmica caótica, então o deslocamento médio quadrado, escala linearmente com o tempo, ou seja, temos $K_c =$

$\lim_{n\to\infty}(\log M_c(n)/\log(n)) = 1$. Os valores de K_c são calculados para n_c números escolhidos aleatoriamente $c \in (0,\pi)$. O valor final K é obtido como a mediana de todos os valores de K_c.

Calculando K através do método de correlação, deve-se construir dois vetores $\xi = \{1,2,\ldots,n_{cut}\}$ e $\Delta = \{M_c(1), M_c(2),\ldots,M_c(n_{cut})\}$. Dado quaisquer dois vetores de x e y, cada um de comprimento r, definimos a sua covariância como $\mathrm{cov}(x,y) = (1/r)\sum_{j=1}^{r}(x(j) - \bar{x})(y(j) - \bar{y})$, onde $\bar{x} = (1/r)\sum_{j=1}^{r} x(j), \bar{y} = (1/r)\sum_{j=1}^{r} y(j)$ e a variância $\mathrm{var}(x) = \mathrm{cov}(x,x)$. Os valores n_c de K_c são, assim, obtidos a partir de $K_c = \mathrm{corr}(\xi,\Delta) = \left(\mathrm{cov}(\xi,\Delta)/\sqrt{\mathrm{var}(\xi)\mathrm{var}(\Delta)}\right)$, a partir do qual, tal como anteriormente, calculamos a media de todos os valores de K_c [15].

O circuito que foi utilizado para esta experimentação foi o circuito de caos Chua com o díodo de Matsumoto [15],[16].

A figura 3.2 representa a montagem do circuito Chua com o díodo de Matsumoto, utilizando uma bobine ideal (L). Este gerador de números aleatórios foi o circuito utilizado para base de estudo nesta dissertação.

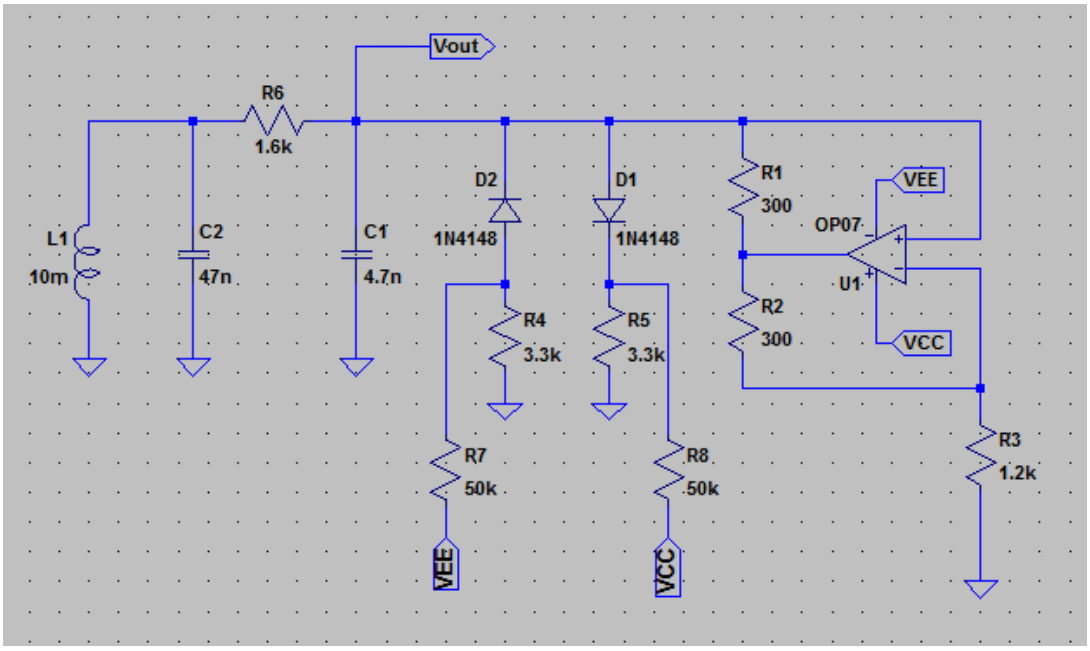


Figura 3.2 - Circuito Chua com o díodo de Matsumoto.

Na ilustração que se segue visualiza-se o sinal de saída V_{OUT} mediante o dimensionamento disponível na figura 3.2, onde R6 tem o valor de 1.6kΩ, C_1 e C_2 4.7 nF e 47 nF respetivamente, com L_1 a ser definida com 10 mH [18].

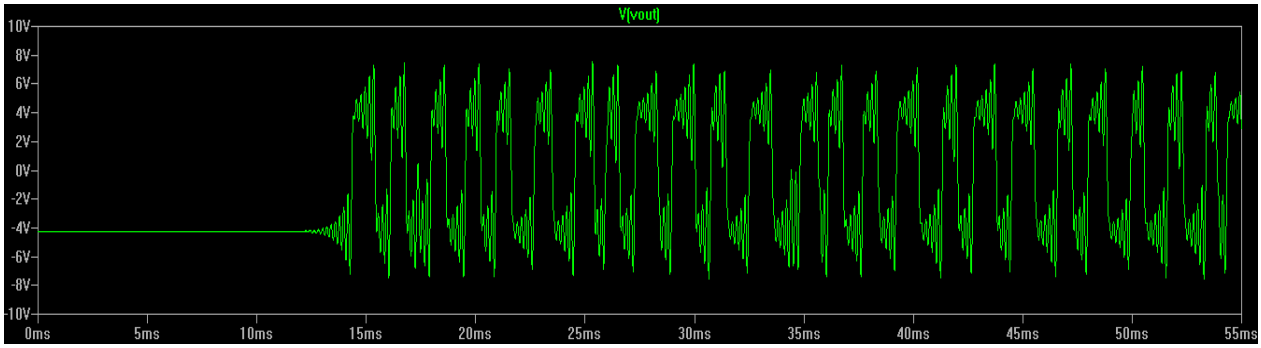


Figura 3.3 - Sinal V_{OUT} do circuito ilustrado na figura 3.2.

Observando o V_{OUT} (Sinal de saída) do circuito, verifica-se que este entra em funcionamento após sensivelmente 12ms, começando então a gerar a sequência aleatória de valores. Analisando os valores de saída V_{OUT} do GNA em estudo, elaborou-se um histograma, representado na figura 3.4, para verificar a repetição de valores entre diferentes gamas.

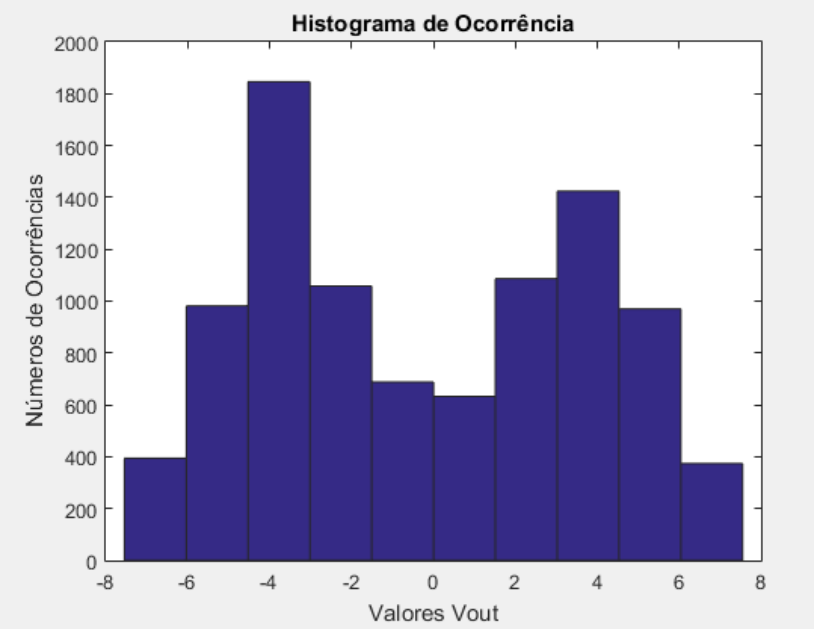


Figura 3.4 - Histograma de valores gerados aleatoriamente pelo circuito Chua com díodo de Matsumoto com bobine ideal.

O histograma representado na figura 3.4, tem como objetivo ilustrar que não existe uma distribuição homogénea ao longo do tempo, sendo que estamos perante uma análise de 10000 pontos de referência, de notar que a gama dos valores de tensão estão compreendidos no intervalo de -8V a 8V tal como se pretendia.

Para se transformar o circuito ilustrado na figura 3.2 num circuito integrado, é imperativo que se reduza os valores do condensador para a ordem dos Pico-Farad (pF), e que se substituía a bobine ideal por uma ativa, visto a bobine ideal ter o problema do seu tamanho e não poder fazer parte de um circuito integrado por afetar o custo do mesmo.

3.2 Bobine Ativa

Com o fim de diminuir o tamanho de uma bobine ideal, visto este ocupar imenso espaço num circuito integrado, utilizou-se um circuito denominado por *gyrator* tal como representado na figura 3.5. Este circuito consiste no facto de que, a resistência de carga ligada à terra, do primeiro Conversor de Impedância Negativa (ICIN - inversor de corrente), (onde Z – Impedância) é substituída por outro CIN (VCIN – inversor de tensão). Assim, para compreender o circuito: primeiro, o papel do segundo CIN B (VCIN) e posteriormente, a carga da resistência de carga ligada à terra da primeira CIN A (ICIN).

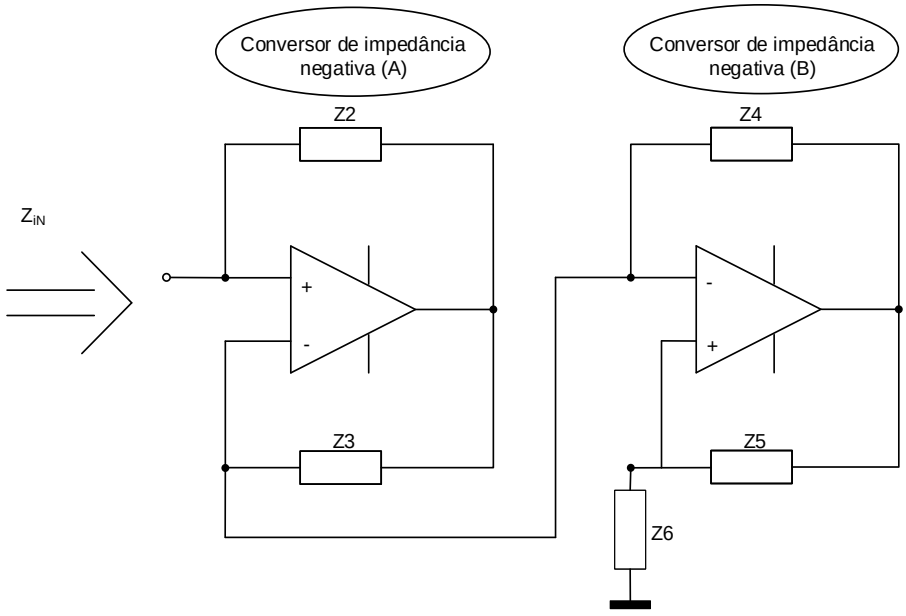


Figura 3.5 – *Gyrator*

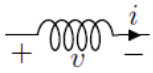
Considerando a segunda CIN (VCIN), assumindo que Z5 é um condensador. Este circuito atua como um indutor negativo, uma vez que o amplificador operacional adiciona uma tensão ao circuito anterior (ligado à sua entrada inversora) igual à queda de tensão através da resistência com ligação à massa Z6. Esta tensão representa a queda de tensão através de um indutor (esta é uma propriedade do circuito RC simples, onde a queda de tensão complementar

através da resistência comporta-se ao longo do tempo como a queda de tensão através de um indutor).

Aplicando esta breve introdução de *gyrator* de modo a criar uma bobine ativa, através das seguintes deduções matemáticas será explicado como esta bobine ativa substitui a bobine ideal.

Um indutor pode ser descrito mencionando dois domínios de energia: elétrico e magnético [18],[19]. Não se está a tentar utilizar os campos magnéticos que o indutor origina, o foco é o relacionamento da corrente para tensão no circuito que o indutor usa [18]. A corrente para a relação da tensão do indutor é:

$$v(t) = L\frac{di(t)}{dt}. \tag{3.4}$$



Esta equação tem como objetivo mostrar um circuito que tenha esta relação nos terminais.

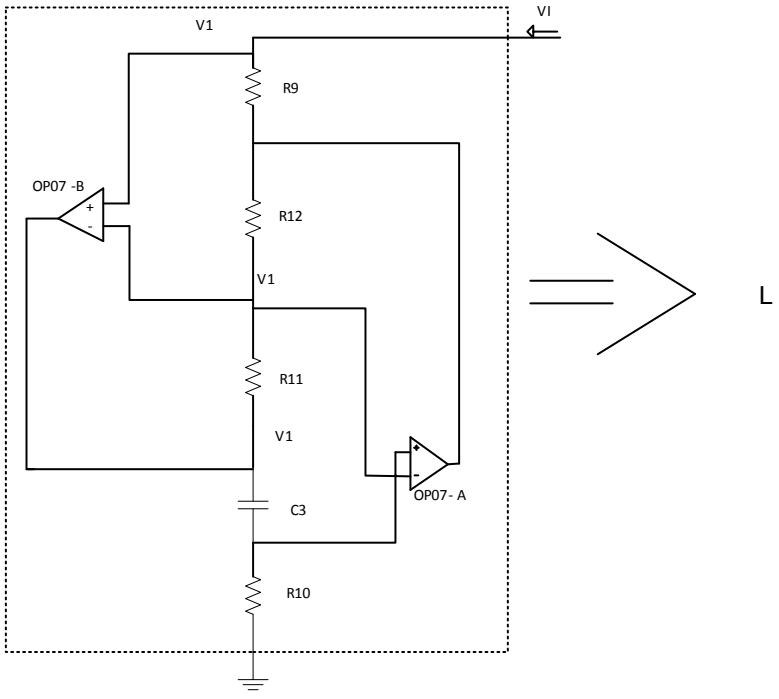


Figura 3.6 – Circuito que implementa a bobine ativa.

Utilizou-se este circuito, porque a sua relação (a relação entre V_1 e I_1) é a mesma que um indutor, isto é, pode-se mostrar que:

$$V_1(t) = L_1\frac{dI_1(t)}{dt}. \tag{3.5}$$

Observe-se a relação terminal de um indutor de maneira ligeiramente diferente, aplicando a transformada de Laplace. Pode dizer-se que a relação corrente para a tensão do indutor é

$$\frac{V(s)}{I(s)} = Ls. \tag{3.6}$$

Portanto, para ver a relação terminal:

$$\frac{V_1(s)}{I_1(s)} = L_1 s. \tag{3.7}$$

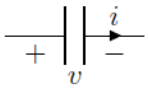
Tendo como ponto de partida o modelo ideal op-amp, sabe-se que a tensão no terminal + e - de um op-amp é o mesmo.

Neste ponto, podemos aplicar a Lei de Ohm para descobrir a corrente que passa por R_{10}, $\frac{V_1}{R_{10}}$.

A corrente passa através do terminal positivo de OP07-A (figura 3.6), pelos pressupostos de um op-amp ideal, sabe-se que é zero. A partir disso, conclui-se que a corrente está a passar por C_3 [19].

A relação terminal de um condensador é:

$$i(t) = C\frac{dv(t)}{dt}. \tag{3.8}$$



Aplicando a transformada de Laplace a essa relação terminal, obtém-se:

$$I(s) = CsV(S), \tag{3.9}$$

ou,

$$V(s) = \frac{I(s)}{Cs}. \tag{3.10}$$

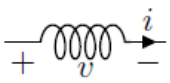
Relativamente à tensão entre C_3 e a tensão no nó entre R_{11} e R_9. Sabendo que a corrente passa por C_3, sabe-se que a tensão através de C_3 é:

$$V_{C_3} = \frac{\frac{V_1}{R_{10}}}{C_3 s} = \frac{V_1}{R_{10}}\frac{1}{C_3 s}, \tag{3.11}$$

e a tensão no nó entre R_{11} e C_3 é a tensão através de C_3 mais a tensão ao longo R_{10} que é:

$$V_{C_3} + V_1 = \frac{V_1}{R_{10}}\frac{1}{C_3 s} + V_1, \tag{3.12}$$

o resultado atingido é um circuito que tem a mesma relação de terminal como um indutor [19],



$$v(t) = L\frac{di(t)}{dt}, \tag{3.13}$$

$$\frac{V(s)}{I(s)} = sL. \tag{3.14}$$

Neste caso:

$$\frac{V_1(s)}{I_1(s)} = \frac{V_1}{\frac{V_1 R_{12}}{sC_3 R_9 R_{11} R_{10}}}, \tag{3.15}$$

$$\frac{V_1(s)}{I_1(s)} = \frac{sC_3 R_{11} R_9 R_{10}}{R_{12}}. \tag{3.16}$$

Desta forma, a função apresentada em (3.16) irá ser aplicada para que seja possível diminuir o valor de C_3, que é um dos objetivos desta dissertação, ter todos os condensadores com valores de grandezas abaixo dos Nano-Farad (nF).

3.3 Bootstraping

Tendo resolvido o problema da bobine ideal, substituindo-a pelo circuito representado na figura 3.5, o espaço que a mesma ocupava foi reduzido para tamanhos aceitáveis. Resta, assim, o problema dos condensadores com valor de capacidade elevada. Sempre orientado para a implementação do circuito Chua com o díodo de Matsumoto em circuito integrado, foi aplicado um multiplicador de capacidade representado na figura 3.7 que utiliza o efeito de "*Bootstrapping*", com o intuito de diminuir os condensadores ligados à massa. Para diminuir os valores dos condensadores, é necessário aumentar as resistências como se pode ver na equação (3.17).

Neste circuito é utilizado a técnica de "*Bootstrapping*", para que o condensador C_1 seja visto como um condensador muito maior. "*Bootstrap*" reside no facto do nó inferior do condensador C_1 não estar ligado à massa, mas sim estar ligado à saída de um amplificador inversor, que amplifica e inverte a tensão no nó superior do condensador. Desta forma, o nó inferior do condensador é diminuído. Assim sendo, vai ser necessário mais corrente para carregar o condensador dando a imagem que o condensador é muito maior. Devido a este facto, é possível baixar os valores dos condensadores para a ordem dos pF, tal como

pretendido [20]. Para se diminuir os condensadores C_1 , C_2 e C_3, da figura 4.4, o circuito utilizado está representado na figura 3.7, a equação que o define é:

$$Cap = \left(1 + \frac{RA}{RB}\right).C1. \tag{3.17}$$

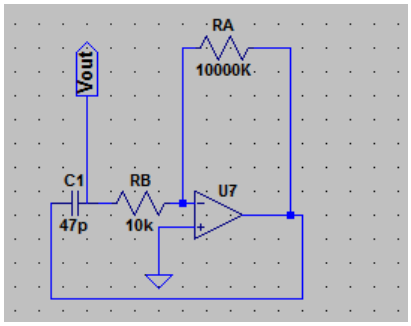


Figura 3.7 - Circuito de substituição de condensador de 47 nF por 47 pF.

4

4 Implementação: Análise de Resultados e Aplicações

No presente capítulo, com o intuito de rentabilizar o circuito, tornando-o mais pequeno a nível de dimensões físicas, com o propósito de criar um circuito integrado com baixo custo, pretende-se apresentar os resultados do circuito de Chua com díodo de Matsumoto utilizando um *gyrator* e aplicando a técnica de *bootstrapping* em condensadores que estivessem ligados diretamente à massa.

Pretende mostrar-se as alterações por fases, na secção 4.1 é aplicado o *gyrator* no circuito, substituindo assim, a bobine ideal. É elaborado um histograma com o intuito de demonstrar a repetição das amostras retiradas do sinal de saída e analisar os resultados de toda a implementação. Numa segunda fase, aplicar a técnica de *bootstrapping* nos condensadores ligados à massa e reduzir os seus valores da ordem de nF para os pF. De seguida, aplicar o teorema de Lorenz, e comprovar que com o sinal de saída (V_{OUT}) em função do sinal de entrada (V_{in}), resultante das alterações anteriormente realizadas, é originado um atrator. Atrator este, que nos comprova que o circuito continua a ser caótico. E na secção 4.2, será descrita a aplicabilidade do circuito estudado.

4.1 Análise de Resultados

Tendo em conta as considerações que foram apresentadas no capítulo 3, começou por aplicar-se o *gyrator* no circuito, substituindo assim a bobine ideal por uma bobine ativa.

Deste modo, substituiu-se L_1 pela bobine ativa, representada na figura 3.5, dando origem ao circuito da figura 4.1, circuito de *Chua* com o díodo de Matsumoto utilizando bobine ativa.

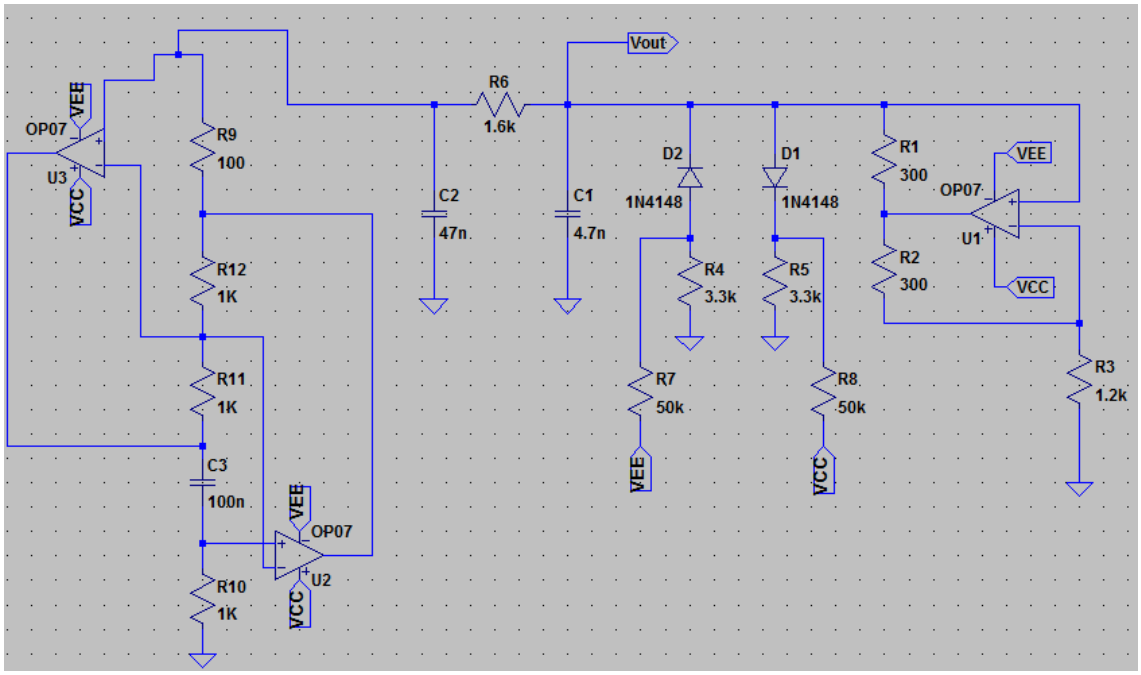


Figura 4.1 - Circuito Chua com díodo Matsumoto utilizando bobine ativa.

Na figura 4.2, visualiza-se o sinal de saída V_{OUT} mediante a parametrização disponível na figura 4.1, onde R_6 tem o valor de 1.6 kΩ, e C_1, C_2 e C_3 têm os valores 4.7 nF, 47 nF e 100 nF, respetivamente.

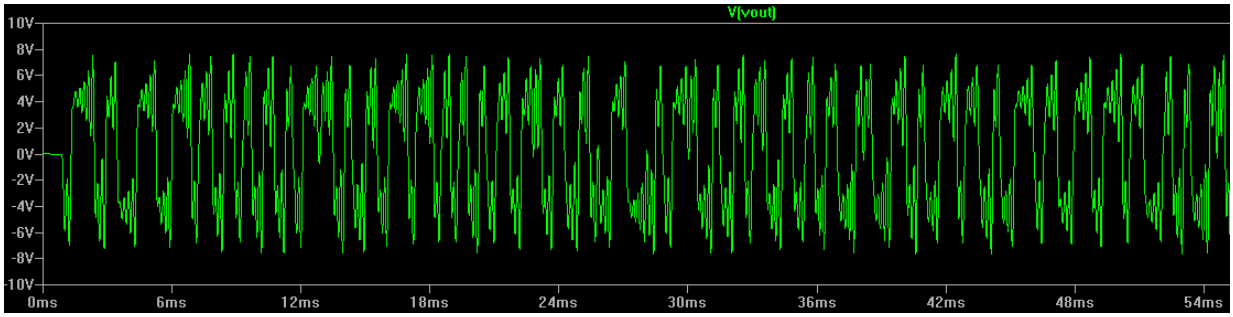


Figura 4.2 - Sinal V_{OUT} do circuito ilustrado na figura 4.1.

Em comparação com o circuito original apresentado na figura 3.1, que usa uma bobine ideal, este tem uma velocidade de resposta muito mais rápida, com uma redução na ordem dos 10 ms, originando tal como o circuito original, uma sequência de valores aleatória sem previsibilidade.

Analisando os valores de saída V_{OUT} do GNA em estudo, elaborou-se um histograma representado na figura 4.3, para verificar a repetição de valores entre diferentes gamas utilizando a bobine ativa. O histograma, tem como objetivo ilustrar que continua a não existir uma distribuição homogénea ao longo do tempo tal como apresentado na figura 3.4. Estamos perante uma análise de 10000 pontos de referência e tendo alterado as condições iniciais é possível comparar os dois histogramas e perceber que existe diferença entre os números de ocorrências e os valores de V_{OUT} relativamente ao histograma apresentado na figura 3.4. Esta situação é devida ao facto de ter-se alterado as condições iniciais, ao trocar a bobine ideal por uma bobine ativa.

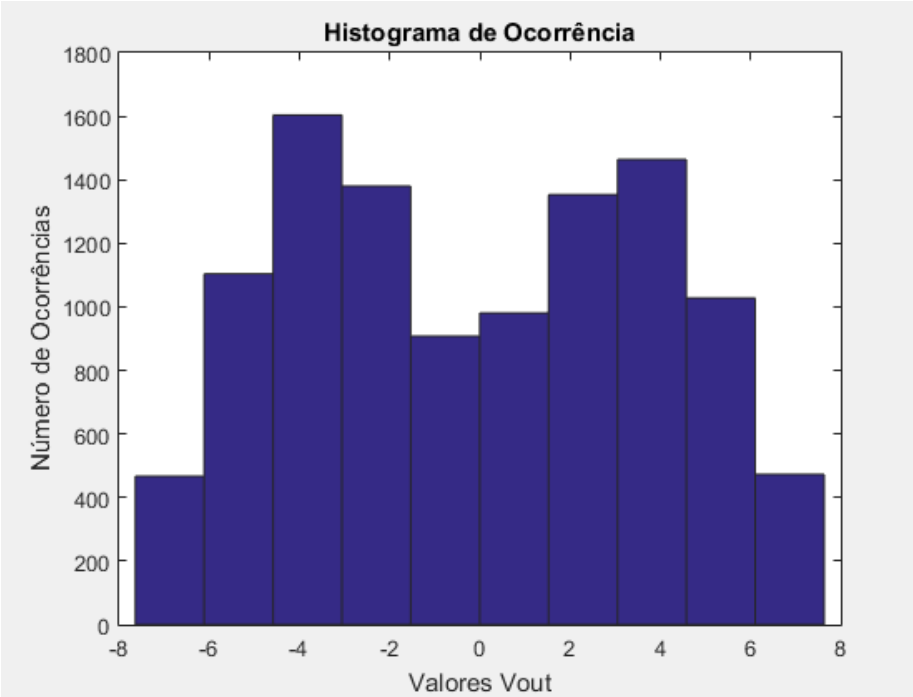


Figura 4.3 - Histograma de valores gerados aleatoriamente pelo circuito Chua com díodo de Matsumoto com bobine ativa.

De seguida, passou-se para a fase dois da implementação, que consiste na utilização para técnica *bootstraping*, que permitiu que se conseguisse diminuir o valor dos condensadores, nomeadamente os condensadores C_1 e C_2, pois são os únicos que estão ligados à massa. Esta técnica apenas pode ser utilizada nos casos em que o condensador está

ligado à massa. A capacidade do condensador C_3 foi diminuída pela equação (3.17) apresentada no capítulo 3.

Aplicando esta técnica ao circuito em estudo, obtém-se:

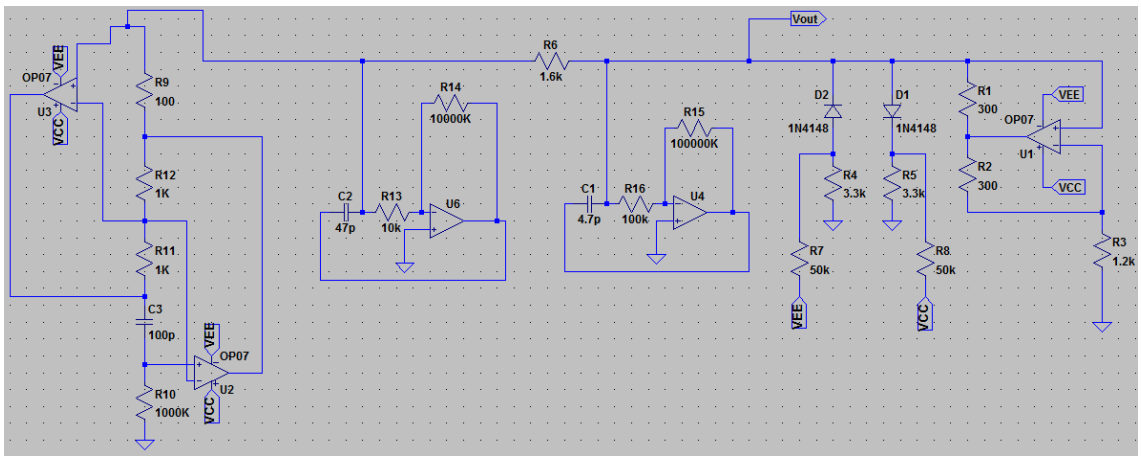


Figura 4.4 - Circuito com bobine ativa, C_1, C_2 e C_3 de ordem pF.

A figura 4.5, mostra o atrator de Lorenz resultante do circuito apresentado na figura 4.4. É possível visualizar o andamento do sinal de saída (V_{OUT}) em função do sinal de entrada (V_{in}). Tendo em conta a análise efetuada no capítulo 2, este é um mapa caótico onde pode observar-se, como um sistema dinâmico evolui no tempo com um padrão complexo não repetitivo [9],[11].

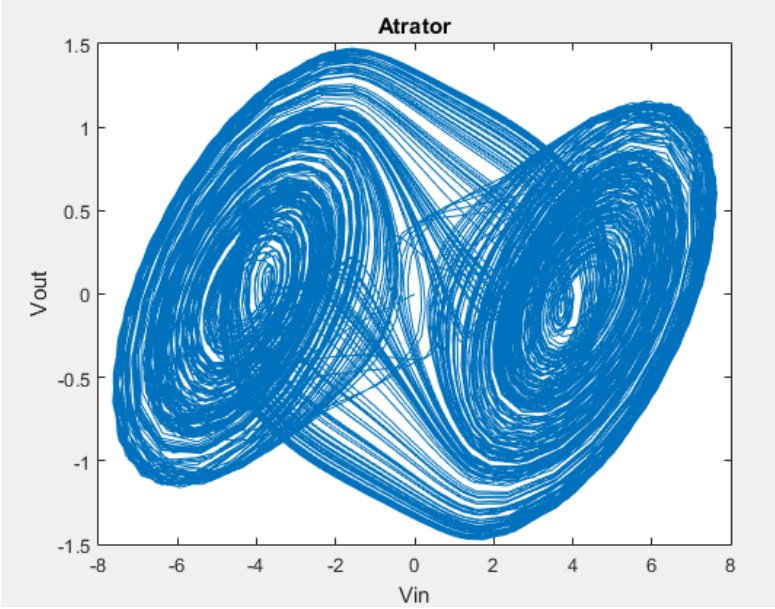


Figura 4.5 - Atrator de Lorenz resultante das simulações do circuito da figura 4.4.

O andamento de V_{OUT}/V_{in} segundo um atrator de Lorenz é um indicador de que o sistema é caótico. Não tem principio nem fim, tem evolução infinita, o que significa que a oscilação é sempre diferente e sem repetição (período infinito) [12],[13].

É possível visualizar na imagem 4.5 que o sinal desloca-se em torno de dois centros ($V_{in} = -4$ e $V_{in} = 4$), sendo esta é uma das características de um sistema caótico, isto é, existir um atrator de Lorenz com um sinal contínuo em torno de 2 pontos descrevendo a "imagem de um oito"[11], tal como explicado anteriormente no capítulo 2, na figura 2.2 (a) e nas fórmulas diferenciais em (2.5), (2.6) e (2.7). Na teoria, usualmente, $\sigma = 10, \beta = \frac{8}{3} e\ \rho$ é variado, onde o sistema exibe comportamento caótico para $\rho > 28$. Após aplicar esta teoria na prática, a imagem resultante do nosso sistema está ilustrada na figura 4.5, comprovando o facto do sistema em estudo ser caótico. Caso a imagem resultasse apenas em órbitas, seria apenas mais um sistema dinâmico [11],[21],[22]. Comparando a figura 4.5 com a figura 2.1 (a), ambas são de segunda ordem e os resultados são similares, o que revalida o facto de estar-se perante um gerador de números aleatório caótico.

Na ilustração que se segue, visualiza-se o sinal de saída V_{OUT} resultante da parametrização disponível na figura 4.4, onde R6 tem o valor de 1.6 kΩ, C_1, C_2 e C_3 têm os valores 4.7 pF, 47 pF e 100 pF, respetivamente.

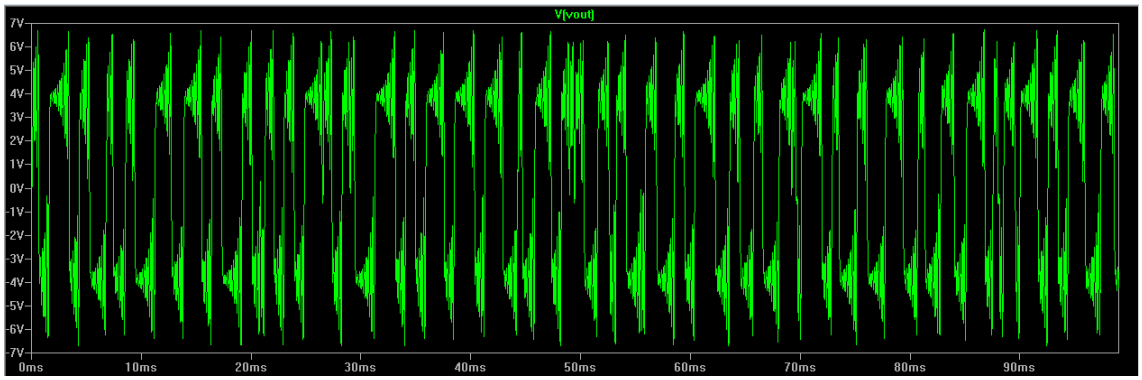


Figura 4.6 -Sinal V_{OUT} do circuito ilustrado na figura 4.4.

Na figura 4.6, pode visualizar-se uma maior rapidez de resposta, bem como uma maior variação de picos de tensão em relação ao V_{OUT} do circuito original, ilustrado na figura 3.3. No caso apresentado na figura 4.6, o valor de tensão diminui perto de 1V em relação ao circuito apresentado na figura 4.1. Como se trata de uma simulação em *software*, os condensadores não retêm energia para nova simulação, o que impossibilita a realização uma nova simulação com valores de tensão remanescentes que estariam presentes nos mesmos, inviabilizando assim, mostrar a sua sensibilidade às condições iniciais.

4.2 Aplicações

Nos últimos anos, tem sido notório o aumento da pesquisa sobre a sincronização caótica de sistemas caóticos de tempo contínuo e discreto, devido à sua aplicabilidade em comunicações seguras. Devido à sua sensibilidade às condições iniciais e ao comportamento aleatório dos sinais caóticos, assim como, ao espetro da banda larga, admitia-se que a mensagem a ser transmitida pudesse ser ocultada de modo eficiente no caos [23].

Assim, foram desenvolvidos três modos principais de codificação de mensagens:

1. Dissimulação caótica: a mensagem transmitida é adicionada a um sinal caótico muito forte para encobrir a informação e o sinal geral é então transmitido ao recetor;
2. *Chaos shift keying*: o sinal transmitido é adquirido por comutação entre N geradores caóticos de acordo com o nível de informação de uma mensagem N-*ary* (geralmente mensagens binárias são usadas com dois geradores caóticos);
3. Modulação do caos: a mensagem modifica o estado ou os critérios do gerador caótico através de um procedimento invertido, assim, o sinal caótico formado contém inerentemente a informação na mensagem transmitida.

Qualquer um destes esquemas, é utilizado em criptografia de mensagens, devendo estar disponível, no lado do recetor, um duplicado do sinal caótico do transmissor de modo a reconstruir a mensagem, ou seja, o recetor deve sincronizar com o transmissor.

Comunicação de caos utilizando sistemas analógicos, revelaram graves fragilidades principalmente nos que têm por base a dissimulação caótica. Neste caso, a reconstrução da mensagem depende maioritariamente do erro de sincronização, sendo que este, pode ser facilmente corrompido pelo ruído do canal. Deste modo, a pesquisa para a utilização de sistemas caóticos discretos adquiriu relevo. Um método de comunicação robusto que usa a modulação por mensagem digital, foi proposto por Parlitz e Ergezinger [23]. No entanto, para que possa existir sincronização, ambos os sistemas do transmissor e do recetor, devem iniciar ao mesmo tempo e com as mesmas condições iniciais, sendo que tal é inexequível. Além da problemática anterior, a mensagem é transmitida a uma taxa baixa devido à redundância. São necessárias N amostras caóticas para transmitir uma amostra de informação.

Liao e Huang sugeriram um esquema de modulação, que tem por base a sincronização baseada em observador, no qual é adicionada uma mensagem discreta à saída caótica, posteriormente, o sinal resultante é enviado de volta para o sistema transmissor e, ao mesmo tempo, é direcionado para o sistema recetor. A redundância é evitada. Apesar de ser um esquema bem sucedido, por vezes tem desvantagens, tais como: apenas é possível a transmissão de mensagens de baixa potência, o que torna o esquema vulnerável a distorcer o ruído do canal; e o *feedback* da mensagem aplicado a certos sistemas caóticos (como o mapa de Hénon) pode levar a desvio dos estados inicialmente caóticos [23].

O estudo efetuado nesta dissertação foi cingido na forma como a transmissão de mensagens é efetuada e não na transmissão e receção das mesmas. Desta forma de seguida são apresentados dois modelos de codificação de mensagens fazendo referência á forma como é transmitida e rececionada a informação. De notar que a as funções que definem a parte da transmissão são tridimensionais tal como ao longo desta dissertação tem-se vindo a demonstrar.

Apresentando dois esquemas diferentes de codificação de mensagens com base na modulação caótica: 1. Modulação por multiplicação e 2. Modulação por multiplicação e *feedback*. Nestes sistemas são utilizadas a sincronização de condução da resposta e a sincronização baseada num observador. O sistema de condução é usado como um transmissor e o sistema de resposta é o recetor. A sequência caótica de condução utilizada para a sincronização é modulada por uma mensagem binária, sendo necessária uma ligeira modificação do sistema transmissor-recetor para conseguir a sincronização.
Seguidamente apresenta-se uma breve descrição dos dois esquemas:

1. Modulação por multiplicação: são utilizados sistemas caóticos de tipo Lur'e. A sequência de saída caótica é multiplicada pela sequência de mensagens que é codificada em binário e satisfaz a seguinte hipótese:
   - Hipótese 1 - a mensagem transmitida é codificada em binário com $(-1, +1)$ são os únicos valores admitidos.
   - Hipótese 2 - A é estável e a não linearidade do sistema caótico é par, onde A representa uma matriz constante de dimensões apropriadas e $f: \mathbb{R} \to \mathbb{R}^n$ é o campo do vetor real.
2. Modulação por multiplicação e *feedback*: a saída caótica é multiplicada pela sequência de mensagens e a sequência obtida é simultaneamente enviada ao recetor e devolvida ao transmissor. O sistema de comunicação é descrito pelas seguintes equações, em que a sequencia modelada é o sinal portador de informação que ativa o recetor.

Estes são dois esquemas de modulação caótica para transmissão de mensagem digital. Usando a habilidade de sincronizar sistemas caóticos discretos com o conceito de condução da resposta, uma mensagem binária digital modula a sequência discreta caótica por meio de multiplicação simples. Este esquema está inserido numa classe especifica de sistemas caóticos. No sentido de ampliar a classe de sistemas caóticos envolvidos, o procedimento de modulação foi alterado, incluindo um *feedback loop* para injetar o sinal transmitido ao transmissor. Para recuperar a mensagem um demodulador baseado num observador é usado para sincronizar com o sistema transmissor. Este novo esquema de comunicação caótica pode ser aplicado a uma vasta classe de sistemas caóticos discretos. Alguns sistemas que podem divergir devido ao *feedback loop* podem ser ligeiramente modificados para satisfazer os

requisitos do esquema de comunicação [23]. Este é um esquema de comunicação de um único utilizador, no entanto, pode abranger um esquema multiutilizador. Nesse caso, é fundamental a escolha de um sistema caótico com propriedades estatísticas adequadas, para obtenção de um esquema de comunicação viável.

A aplicação do circuito em estudo na área das telecomunicações, pode ser para implementação de um esquema de pseudo hopping da orientação dos feixes de radiação de um conjunto de antenas. De forma a manter a complexidade baixa, pode-se utilizar a sucessão de números gerados, e através de um comutador selecionar diferentes *arrays* de antenas com feixes otimizados segundo direcções distintas, onde cada array o seu feixe orientado segundo uma determinada direcção (que consiste numa técnica de processamento de um sinal utilizada em sensores de *arrays* para direcionar o sinal de transmissão ou de receção). Desta forma é possível o envio de dados usando sequências de direções aleatórias mediante a selecção dos diferentes *arrays* de antenas ligados ao comutador. Dado que os números caóticos gerados ancontram-se no intervalo -8 a 8, é conveniente recorrer a 16 arrays planares e uniformes de 16 antennas com uma largura de feixe de 12º, de modo a que uma comutação abrangendo a totalidade dos arrays em presença consiga cobrir 180º. Na figura 4.7 é ilustrado o sistema que se pretende implementar, de acordo com as especificações acima mencionadas.

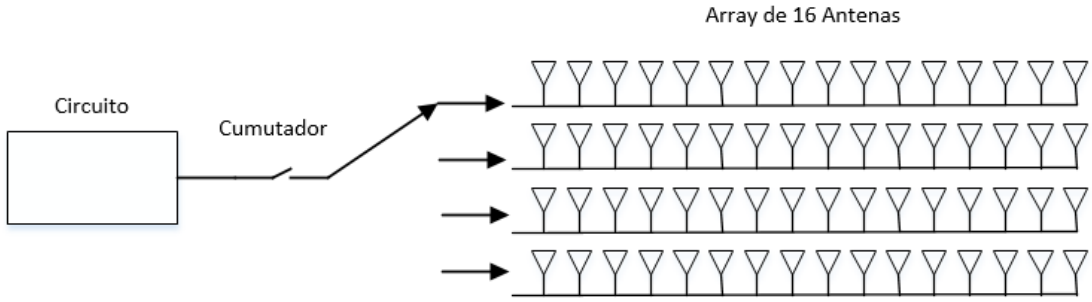


Figura 4.7 - Sistema de transmissão.

Para evitar efeitos de acoplamento entre antenas o espaçamento entre estas deve ser superior ou igual $d = \frac{\lambda}{2}$, em que λ representa o comprimento de onda e pesos de ($\mathbf{a} = [1,1,\ldots,1]$) entre elementos foram considerados [24]. Desta forma consegue-se implementar um esquema de segurança de nível fisico simples, no qual somente os recetores que detenham informação sobre a orientação do feixe do array ativo, em cada instante, são capazes de receber com sucesso a informação transmitida.

5

5 Conclusões e Trabalho Futuro

De acordo com o estudo efetuado sobre o tema proposto, conclui-se que a sequência gerada pelo GNA é efetivamente caótica. Após a análise de resultados verifica-se que existe uma aleatoriedade onde não existe um padrão definido nos valores obtidos. Tendo em conta os valores que eram apresentados inicialmente relativamente à resposta do circuito, com a alteração dos elementos que armazenam a energia do circuito, conseguiu-se obter uma maior velocidade de resposta do sistema, embora tenha-se perdido cerca de 1V na amplitude de saída do mesmo.

Analisando a sequência caótica gerada pelo circuito, chega-se à conclusão de que é possível ter um número indeterminado de *arrays* de antenas ligados a um comutador, o elemento que recebe a sequência de números caóticos do GNA e associa ao respetivo array, visto a sequência ter uma alta gama de valores. Desta forma, será possível ter uma seleção aleatória de diretividade relativamente à transmissão de dados com os *arrays* de antenas que se pretender.

Algumas características de um circuito integrado são: não ter condensadores com valores superiores de 1nF; as resistências terem de estar compreendidas entre grandezas inferiores a 1M Ohm; e, bobines ideais por ocuparem muito espaço. Foi necessário trocar a bobine inicialmente apresentada como sendo uma bobine ideal por uma bobine ativa, e alterar os condensadores ideais por condensadores ativos.

O maior desafio para colocar o circuito com os parâmetros desejados, foi efetivamente, diminuir as grandezas dos condensadores de nF para pF, uma vez que para atingir estes valores teve que existir um *tradeoff* entre os condensadores ideais e as resistências dos circuitos que compõem os condensadores ativos. Tal significa, que tiveram que se aumentar algumas resistências para que os condensadores em questão pudessem diminuir as suas grandezas. Para percutir a implementação do circuito analógico discreto em estudo num circuito integrado, existe uma última tarefa a nível de dimensionamento, que será substituir as resistências que têm as suas grandezas na ordem dos M Ohms por resistências ativas. Após a alteração destes elementos (a bobine ideal, os condensadores ideais e as resistências com

grandezas superiores a 1M Ohm) será então possível realizar o circuito analisado, em circuito integrado.

Para trabalho futuro, fica o desafio de:

- ✓ reduzir todas as resistências que tenham valores superiores a 1MOhm. Consequentemente a transformação do circuito analisado num circuito integrado;
- ✓ aplicar o circuito estudado nas diferentes aplicações mencionadas no subcapítulo 4.2, nomeadamente, no tipo de codificação de dissimulação caótica, em *chaos shift keying* e na modulação do caos.

Referências Bibliográficas

[1] S. Mitchum, “Digital Implementation of a True Random Number Generator,” *Dissertation for the degree of Doctor of Philosophy in Electrical and Computer Engineering, Virginia Commonwealth University*, pp. 5-89, 2010.

[2] M. Stipčević and Ç. Koç, “True Random Number Generators,” *Open Problems in Mathematics and Computational Science*, Ç. K. Koç, editor, Springer, pp.275–315, 2014.

[3] T. S. Parker and L. Chua, “Chaos : A Tutorial for Engineers Part I : Theoretical Aspects,” *Proc. IEEE*, vol. 75, no. 8, pp. 982 - 1008, 1987.

[4] H. Kantz and T. Schreiber, “Nonlinear Time Series Analysis,” *Cambridge University Press*. p. 388, 2004.

[5] T. Matsumoto, “Chaos in Electronic Circuits,” *Proc. IEEE*, vol. 75, no. 8, pp. 1033–1057, 1987.

[6] N. Nisan and A. Ta-Shma, “Extracting Randomness: A Survey and New Constructions,” *J. Comput. Syst. Sci.*, vol. 58, no. 1, pp. 148–173, 1999.

[7] F. Pareschi, “Chaos-Based Random Number Generators: Monolithic Implementation, Testing and Applications,” *PHD Thesis in Program in Information Technology, Alma Mater Studiorum Università Di Bologna*, pp. 1 - 139, 2006.

[8] Cryptography Research, Inc. “Evaluation of VIA C3 Nehemiah: Random Number Generator,” San Francisco, CA 94105,Feb. 2003, em: http://www.rambus.com/wp-content/uploads/2015/08/VIA_rng.pdf.

[9] T. Ziemer, “The Development and Numerical Modeling of a Chua Circuit as a Pedagogical Tool,” *The Physics Department at the College of Wooster USA*, pp. 1–9, 2014, em: http://physics.wooster.edu/JrIS/Files/Web_Article_Ziemer.pdf

[10] I. Stewart, “The Lorenz attractor exists,” *Nature*, vol. 406, no. August, pp. 948–949, 2000.

[11] I. Petráš, "Fractional-Order Nonlinear Systems: Modeling, Analyses and Simulation". *Spinger*. 2010.

[12] J. E. Villate, Introdução aos Sistemas Dinâmicos, *Versão 1.2, Faculdade de Engenharia da Universidade do Porto*, vol. 1. 2007.

[13] D. Saey, R. Debigaré, P. LeBlanc, M. J. Mador, C. H. Côté, J. Jobin, and F. Maltais, *Chaos Theory Tamed*, vol. 168, no. 4. 2003.

[14] A. Sevgen, “Damped and Forced Oscillations", pp. 5-30, 2009, em:http://www.phys.boun.edu.tr/~sevgena/p202/docs/Damped_and_Forced_Oscillations.pdf.

[15] M. Melosik and W. Marszalek, “Using the 0-1 test for chaos to detect hardware trojans in chaotic bit generators,” *Electronics Letters*, vol. 52, no. 11, pp. 919–921, 2016.

[16] G. A. Gottwald, “On the Implementation of the 0 – 1 Test for Chaos", *SIAM Journal on Applied Dynamical Systems, vol.* 8, no. 1, pp. 129–145, 2009.

[17] I. Falconer, G. A. Gottwald, I. Melbourne, and K. Wormnes, "Application of the 0-1 test for chaos to experimental data", *Siam Journal On Applied Dynamical Systems,* vol. 6, no. 2, pp. 395 - 402 , 2006.

[18] I. M. Filanovsky, M. Reja, and L. B. Oliveira, “New Non-Gyrator Type Active Inductors With Applications,” *Circuits and Systems (MWSCAS), IEEE 54th International Midwest Symposium* pp. 1 - 4, 2011.

[19] V. Siderskiy, “The Antoniou Inductance-Simulation Circuit Derivation”, http://www.chuacircuits.com, pp. 1–10, 2012, em: http://www.chuacircuits.com/PDFs/Antoniou%20Inductance-Simulation%20Circuit.pdf.

[20] Q. C. Zhong, “Active capacitors: Concept and implementation,” *IEEE Int. Symp. Ind.*

Electron., pp. 149–153, 2012.

[21] T. Ghys, “The Lorenz attractor, a paradigm for chaos,” *Prog. Math. Phys.*, vol. 66, pp. 1–54, 2013.

[22] Z. M. Ge and C. Y. Ou, “Chaos in a fractional order modified Duffing system,”: *Chaos, Solitons and Fractals*, *Elsevier*, vol. 34, no. 2, pp. 262–291, 2007.

[23] M. Feki, B. Robert, G. Gelle, and M. Colas, “Secure digital communication using discrete-time chaos synchronization,” *Chaos, Solitons and Fractals*, vol. 18, no. 4, pp. 881–890, 2003.

[24] A. M. Ferreira, “Double layer transmitter structure for millimeter wave communications,” *Dissertation for the degree of Doctor of Philosophy in Electrical Engineering and Computer Sciences*, *University of California, Berkeley*. 2014.

[25] G. Adrucioli, “Caracterização Experimental Do Caracterização Experimental Do Sistema Caótico de Chua”, *Monografia de Graduação em Engenharia de Controle e Automação*,UFOP, 2008.