
UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
UNIDADE ACADÊMICA DO CABO DE SANTO AGOSTINHO
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA FÍSICA

RICARDSON ALEXANDRE PEREIRA FEITOZA

# Geração e distribuição de chaves criptográficas simétricas através da sincronização intermitente de circuitos eletrônicos caóticos acoplados

Cabo de Santo Agostinho - PE
2022

RICARDSON ALEXANDRE PEREIRA FEITOZA

# Geração e distribuição de chaves criptográficas simétricas através da sincronização intermitente de circuitos eletrônicos caóticos acoplados

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Física da Unidade Acadêmica do Cabo de Santo Agostinho da Universidade Federal Rural de Pernambuco para a obtenção do título de Mestre em Engenharia Física.

Área de concentração: Optoeletrônica
Orientador: Prof. Dr. Weliton Soares Martins
Coorientador: Prof. Dr. Rafael Alves de Oliveira

Cabo de Santo Agostinho - PE
2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal Rural de Pernambuco
Sistema Integrado de Bibliotecas
Gerada automaticamente, mediante os dados fornecidos pelo(a) autor(a)

F311g Feitoza, Ricardson Alexandre Pereira
Geração e distribuição de chaves criptográficas simétricas através da sincronização intermitente de circuitos eletrônicos caóticos acoplados / Ricardson Alexandre Pereira Feitoza. - 2022.
74 f. : il.

Orientador: Weliton Soares Martins.
Coorientador: Rafael Alves de Oliveira.
Inclui referências.

Dissertação (Mestrado) - Universidade Federal Rural de Pernambuco, , Cabo de Santo Agostinho, 2022.

1. Criptografia. 2. Caos. 3. Sincronização. 4. Circuitos caóticos sincronizados. I. Martins, Weliton Soares, orient. II. Oliveira, Rafael Alves de, coorient. III. Título

CDD

RICARDSON ALEXANDRE PEREIRA FEITOZA

Geração e distribuição de chaves criptográficas simétricas através da sincronização intermitente de circuitos eletrônicos caóticos acoplados

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Física da Unidade Acadêmica do Cabo de Santo Agostinho da Universidade Federal Rural de Pernambuco para a obtenção do título de Mestre em Engenharia Física.

Aprovada em: 23/02/2022

Banca Examinadora

---

Prof. Dr. Weliton Soares Martins
Orientador

---

Prof. Dr. Rafael Alves de Oliveira
Coorientador

---

Profa. Dra. Fernanda Selingardi Matias
Examinador externo

---

Prof. Dr. Italo Roger Ferreira Moreno Pinheiro da Silva
Examinador interno

*Aos meus filhos, Caio e Gabriel,*
*dedico esta conquista.*

## AGRADECIMENTOS

Inicialmente agradeço a Deus pelo dom da vida e pela oportunidade de concluir este trabalho.

Agradeço aos meus pais, Sebastião Monteiro (em memória) e Maria do Carmo, pelo amor incondicional e pelos ensinamentos de vida.

Agradeço a minha esposa, Simone Oliveira, e aos meus filhos, Caio Henrique e Gabriel Luiz, pela compreensão dos momentos de ausência, pelo constante incentivo e simplesmente por existirem em minha vida.

Agradeço ao meu orientador, Prof. Weliton Soares Martins, pela paciência, pela brilhante orientação, pela sabedoria compartilhada comigo e pela amizade. Certamente, sua contribuição foi fundamental para que esse trabalho se tornasse realidade.

Agradeço ao meu co-orientador, Prof. Rafael Alves de Oliveira, pela revisão do trabalho e pela amizade.

Agradeço aos amigos Robson Oliveira e Hjuan Guilherme pela ajuda no desenvolvimento desta dissertação.

*“As invenções são, sobretudo, o resultado de um trabalho teimoso.”*

*Santos Dumont*

## RESUMO

O presente trabalho propõe um conceito de geração e distribuição de chaves criptográficas simétricas inovador e seguro. O conceito é inovador porque as chaves são geradas a partir dos eventos de perda de sincronia de dois osciladores caóticos acoplados e, diferentemente dos esquemas de criptografia de chaves simétricas tradicionais, não necessitam serem compartilhadas previamente entre o transmissor e o receptor. É seguro porque a chave gerada atende aos quatro requisitos do *one-time pad*, o que a torna inquebrável. Foi demonstrado numérica e experimentalmente que, uma vez alcançada a sincronização caótica entre o transmissor e o receptor, a mesma chave criptográfica aleatória pode ser gerada por amostragem do sinal dos eventos de dessincronização que ocorre entre o oscilador mestre e seu auxiliar, no lado do transmissor, e entre o oscilador escravo e seu auxiliar, no lado do receptor. A prova de conceito foi realizada utilizando como plataforma o oscilador caótico de Gauthier-Bienfang, mas poderia ter sido implementada em plataformas optoeletrônicas ou fotônicas. Como o maior interesse era provar a validade do conceito, optou-se por utilizar o oscilador caótico de Gauthier-Bienfang única e exclusivamente por ser um circuito eletrônico de modelagem matemática simples, fácil construção e principalmente baixo custo. O método de geração de chave a partir dos sinais caóticos é flexível e pode ser tornado tão robusto quanto se queira. Embora o método utilizado aqui tenha sido bastante simples, ele se mostrou eficaz quando submetido aos testes estatísticos da suíte de protocolo do *National Institute of Standards and Technology* (NIST). Os resultados alcançados nos testes do NIST deixam claro a aleatoriedade das chaves, o que é fundamental para qualquer sistema criptográfico. Face ao exposto, o sistema proposto no presente trabalho se apresenta como uma excelente alternativa à criptografia clássica e à criptografia quântica no tocante a garantir segurança da informação de pessoas, instituições e governos na Internet.



**Palavras-chave**: criptografia; caos; sincronização; circuitos caóticos sincronizados.

**ABSTRACT**

The present work proposes an innovative and secure symmetric cryptographic key generation and distribution concept. The concept is innovative because the keys are generated from the out-of-sync events of two chaotic coupled oscillators and, unlike traditional symmetric key encryption schemes, they do not need to be previously shared between the transmitter and the receiver. It is safe because the generated key meets the four requirements of the *one-time pad*, which makes it unbreakable. It has been shown numerically and experimentally that once chaotic synchronization between the transmitter and receiver is achieved, the same random cryptographic key can be generated by sampling the signal from the desynchronization events that occur between the master oscillator and its auxiliary, on the transmitter side. , and between the slave oscillator and its auxiliary, on the receiver side. The proof of concept was carried out using the Gauthier-Bienfang chaotic oscillator as a platform, but it could have been implemented on optoelectronic or photonic platforms. As the main interest was to prove the validity of the concept, it was decided to use the Gauthier-Bienfang chaotic oscillator solely and exclusively because it is an electronic circuit with simple mathematical modeling, easy construction and mainly low cost. The key generation method from chaotic signals is flexible and can be made as robust as you like. Although the method used here was quite simple, it proved effective when subjected to the statistical tests of the *National Institute of Standards and Technology* (NIST) protocol suite. The results achieved in NIST tests make clear the randomness of keys, which is fundamental for any cryptographic system. In view of the above, the system proposed in the present work presents itself as an excellent alternative to classical cryptography and quantum cryptography in terms of guaranteeing information security for people, institutions and governments on the Internet.

**Keywords**: cryptography; chaos; synchronization; synchronized chaotic circuits.

## LISTA DE ILUSTRAÇÕES

## LISTA DE TABELAS

## LISTA DE EQUAÇÕES

**SUMÁRIO**

# 1 INTRODUÇÃO

É natural esperar que a informação seja o principal ativo na Era da Informação, haja vista que governos, empresas e pessoas que possuem informação precisa e oportuna detêm poder, vantagem competitiva, entre outros diferenciais. Obviamente, por se tratar de um bem valioso, a informação é objeto de cobiça e alvo de ataques de toda ordem. Logo, protegê-la é necessário, principalmente, quando de sua transmissão pela rede mundial de computadores.

A criptografia é uma ferramenta de segurança indispensável para proteger informações sensíveis compartilhadas na Internet. A criptografia clássica, embora rápida e escalável, é quebrada por algoritmos quânticos. A criptografia quântica, apesar de inquebrável, é mais lenta e menos escalável, além de necessitar de uma infraestrutura mais cara do que as redes ópticas clássicas (FALCO et al., 2019). Logo, uma alternativa é a criptografia caótica, que passou a ser objeto de estudo, pesquisa e desenvolvimento a partir do trabalho de sincronização de sistemas caóticos de Pecora e Carroll (PECORA; CARROLL, 1990).

A criptografia caótica explora o fato de o caos ser extremamente sensível às condições iniciais e aos parâmetros do circuito, o que é ideal para ocultar informações e, consequentemente, transmiti-las com segurança em redes de telecomunicações inseguras. Ao longo do tempo, diferentes esquemas caóticos de comunicação segura foram propostos, dentre os quais se destacam o mascaramento caótico aditivo (CUOMO; OPPENHEIM; STROGATZ, 1993) e a modulação caótica (ARGYRIS et al., 2005), mas todos apresentaram algum tipo de problema de segurança, exceto o esquema conhecido como sistema criptográfico caótico proposto por Yang at al. (YANG; WU; CHUA, 1997). Para garantir maior grau de segurança, tal sistema associa técnicas da criptografia clássica e da sincronização caótica da seguinte forma: o sinal de texto claro m(t) é criptografado com um sinal de chave, c(t), que é gerado pelo sistema caótico no transmissor. O sinal criptografado então é usado para alterar a dinâmica caótica da variável de estado utilizada para realizar a sincronização entre o transmissor e o receptor. A variável de estado utilizada para realizar a sincronização é diferente da variável de estado utilizada para gerar a chave. Uma vez alcançada a sincronização, o sinal de texto claro m(t) pode ser recuperado no receptor (YANG, 2004).

O presente trabalho propõe um esquema análogo ao de Yang at al. (YANG; WU; CHUA, 1997), porém emprega um método inovador de geração de chave criptográfica ao utilizar a sincronização intermitente de circuitos eletrônicos caóticos acoplados (GAUTHIER; BIENFANG, 1996) e, diferentemente do proposto por Yang, não utiliza o sinal criptografado para alterar a dinâmica da variável de sincronização. Aqui, o sinal criptografado e o sinal da variável de sincronização trafegam por canais públicos distintos.

A presente dissertação está estruturada da seguinte forma: na seção 2, é apresentada uma abordagem teórica dos conceitos basilares de criptografia; na seção 3, é feita uma revisão teórica da sincronização de sistemas caóticos, do sistema Gauthier-Bienfang e do acoplamento unidirecional de dois sistemas Gauthier-Bienfang; na seção 4, o sistema proposto é descrito e apresentado por meio de um diagrama esquemático, bem como é mostrado os principais resultados numéricos e experimentais; na seção 5, é realizada uma discussão dos resultados numéricos e experimentais; e na seção 6, são apresentadas as conclusões e perspectivas do presente trabalho.

# 2 CRIPTOGRAFIA

Armazenar e enviar informação de forma segura sempre foi uma preocupação humana, haja vista que, desde meados do quinto século A.C, tem-se notícia de um sistema de criptografia militar (KAHN, 1996). Atualmente, dado ao crescimento exponencial de serviços e de usuários na Internet, garantir segurança da informação tornou-se, de um lado, uma necessidade, de outro, um desafio.

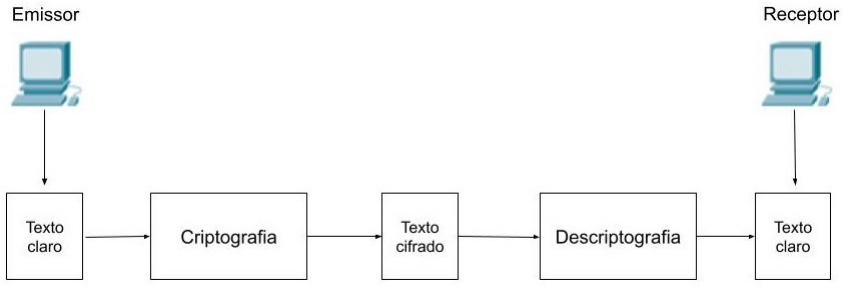
À medida que a quantidade de informações sensíveis armazenadas e compartilhadas na rede mundial de computadores aumenta, o número de pessoas mal-intencionadas e, consequentemente, de ataques crescem juntos. Portanto, a fim de garantir segurança, criptografar tais informações é fundamental, pois, mesmo que terceiros as obtenham, não conseguirão entendê-las.

A criptografia resolve grande parte dos problemas de segurança da informação e, felizmente, atualmente não está mais restrita apenas à proteção de informações governamentais, militares ou bancárias, como era antigamente. Hoje, ela está presente em todo tipo de sistema, de um simples aplicativo de troca de mensagens instantâneas a bolsa de valores, a fim de garantir segurança da informação de pessoas e instituições.

## 2.1 CONCEITOS BÁSICOS

A criptografia, do grego *kryptós* (esconder) e *grápho* (escrita), é a ciência que estuda e aplica técnicas de transformação de uma informação clara em uma informação obscura, para que terceiros, conhecido como atacante, ao obter essa informação de forma indevida não consiga compreendê-la. Na Fig. 1, mostram-se os componentes de um sistema criptográfico.

Figura 1 – Componentes de um sistema criptográfico.




Fonte: Autor.

A informação original é conhecida como texto claro, ao passo que a mensagem codificada é chamada de texto cifrado. O processo de converter um texto claro em um texto cifrado é conhecido como encriptação ou criptografia, e ocorre no momento da emissão. Restaurar o texto claro a partir do texto cifrado é decriptação ou descriptografia, e ocorre na recepção.

Os algoritmos de criptografia, também conhecidos como cifras, são responsáveis por transformar o texto claro no cifrado, no processo de encriptação, e por converter o texto cifrado no texto claro, no processo de decriptação.

A chave é um valor sem correlação alguma com o texto claro, com os algoritmos de criptografia e com o texto cifrado sobre o qual o algoritmo opera. Um texto cifrado é gerado a partir de um algoritmo de criptografia, uma chave e um texto claro. Já o texto claro original é revelado a partir de um algoritmo de descriptografia, uma chave e um texto cifrado.

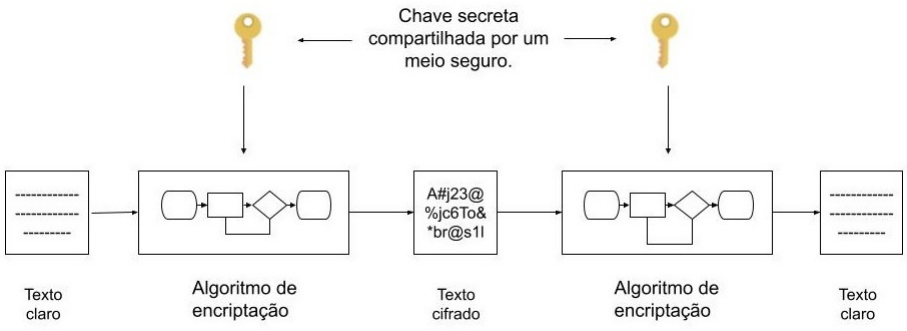
## 2.2 TIPOS DE CHAVES CRIPTOGRÁFICAS

Os algoritmos de criptografia podem ser agrupados basicamente em dois ramos: os algoritmos de chave simétrica, também conhecida como chave secreta, e os algoritmos de chave assimétrica, também denominada de chave-pública.

### 2.2.1 Chave Simétrica

A criptografia de chave simétrica é aquela em que a mesma chave secreta é utilizada tanto pelo emissor quanto pelo receptor. O emissor usa essa chave e o algoritmo de criptografia para encriptar o texto claro; o receptor usa a mesma chave e o algoritmo de descriptografia para obter o texto claro novamente. A segurança de tal tipo de criptografia reside na manutenção do segredo da chave, uma vez que o algoritmo utilizado para criptografar e descriptografar é conhecido pelo público em geral. Na Fig. 2, apresenta-se o diagrama esquemático da criptografia de chave simétrica.

Figura 2 – Criptografia de chave simétrica.



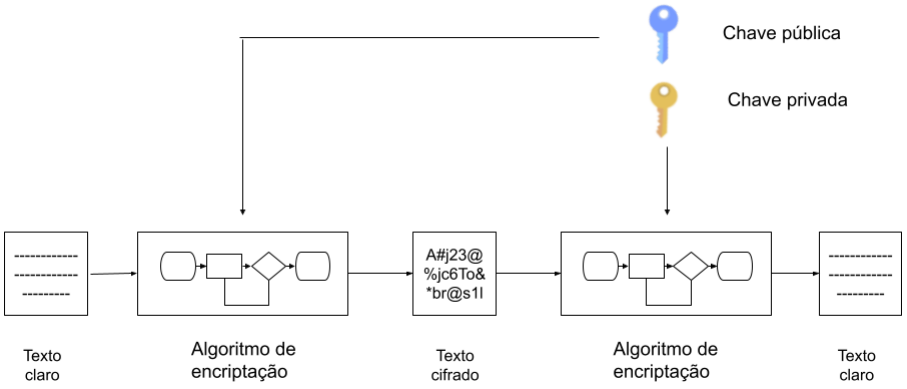

Fonte: Autor.

### 2.2.2 Chave Assimétrica

A criptografia de chave assimétrica é aquela em que duas chaves, uma chave privada e uma pública, são usadas. A chave pública é divulgada ao público em geral, ao passo que a chave privada é guardada secretamente pelo receptor. Quando o emissor quer enviar informação ao receptor, ele usa a chave pública do receptor para encriptar a

informação. Quando a mensagem é recebida pelo receptor, a chave privada é utilizada para decriptar a informação. As chaves pública e privada devem ser necessariamente diferentes. A segurança da criptografia de chave assimétrica está no fato de as chaves públicas e privadas não guardarem correlação alguma e da manutenção do segredo da chave privada, uma vez que a chave pública é divulgada. Na Fig. 3, apresenta-se o diagrama esquemático da criptografia de chave assimétrica.

Figura 3 – Criptografia de chave assimétrica.




Fonte: Autor.

O foco do presente trabalho é a geração e a distribuição de chaves secretas para ser utilizada na criptografia de chave simétrica. Logo, a partir deste ponto, trata-se única e exclusivamente da criptografia de chave simétrica.

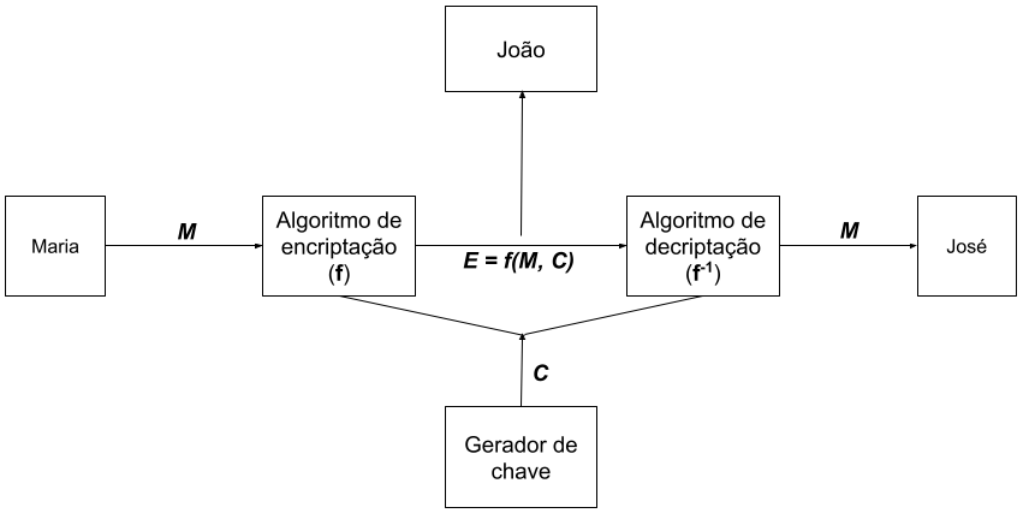
## 2.3 CRIPTOGRAFIA DE CHAVE SIMÉTRICA

O modelo básico de comunicação da criptografia de chave simétrica envolve três atores: Maria, José e João. A ideia básica é a seguinte: Maria e José precisam trocar informações confidenciais através de um canal de comunicação inseguro, ou seja, passível de interferências por João, que pode realizar um ataque passivo (análise de tráfego, por exemplo) ou ataque ativo (modificação de mensagem, por exemplo) para obter alguma vantagem indevida. Na Fig. 4, mostram-se os componentes de um sistema criptográfica simétrico.

Com a mensagem ***M*** e a chave de encriptação ***C*** como entradas, o algoritmo de encriptação produz o texto encriptado ***E = f(C, M)***. Essa notação indica que ***E*** é produzido usando-se o algoritmo de encriptação ***f*** como função do texto claro ***M*** e da chave ***C***. O receptor legítimo, de posse da chave, é capaz de inverter a transformação e obter $\boldsymbol{M = f^{-1}(C, E)}$.

O atacante, acessando ***E***, mas não tendo acesso a ***C*** ou ***M***, pode tentar recuperar ***M*** ou ***C***, ou ambos. Contudo, não terá sucesso, mesmo considerando que ele tenha conhecimento dos algoritmos de encriptação (***f***) e decriptação ($\boldsymbol{f^{-1}}$).

Figura 4 – Sistema criptográfico simétrico, em que *M*, *C*, *E*, *f* e $f^{-1}$ representam a mensagem, a chave, o texto encriptado, o algoritmo de encriptação e o algoritmo de decriptação, respectivamente.




Fonte: Autor.

O atacante pode utilizar a técnica de ***criptoanálise*** e/ou ***força bruta*** para decifrar a mensagem ou a chave, ou ambas. A criptoanálise busca analisar as características do algoritmo criptográfico para obter o texto claro ou, principalmente, a chave. A força bruta busca testar todas as possibilidades de chave em um trecho do texto cifrado para obter o texto claro. Vale destacar que as técnicas são quase sempre utilizadas em conjunto. Inicialmente, o criptoanalista usa a criptoanálise para reduzir o espaço amostral de chaves possíveis e, em seguida, ele usa a força bruta. Isso diminuirá o tempo de quebra do código consideravelmente, já que a quantidade de chaves a ser testada foi reduzida.

Obviamente que o atacante só terá sucesso se o texto cifrado possuir alguma informação que leve exclusivamente ao texto claro associado. Se o texto cifrado não possuir informação acerca do texto claro, independentemente da quantidade de texto cifrado ou de tempo que o atacante tenha, o código nunca será quebrado. Tal modelo de encriptação é conhecido como incondicionalmente seguro.

Na prática, no entanto, o máximo que se consegue é implementar modelos de encriptação computacionalmente seguro, que são aqueles em que o custo para quebrar o algoritmo de encriptação é maior que o próprio valor da informação ou o tempo exigido para quebrar o algoritmo de encriptação é maior que o tempo de vida útil da informação (STALLINGS, 2015).

## 2.4 MÉTODOS DE CRIPTOGRAFIA CLÁSSICA

Os métodos de criptografia clássica básicos são os de **cifras de substituição** e de **cifras de transposição**. A seguir será detalhada cada uma dessas cifras.

### 2.4.1 Cifras de Substituição

A cifra de substituição substitui um símbolo de texto claro por um outro símbolo de texto cifrado. Representa-se o texto claro com letras minúsculas, o texto cifrado com letras maiúsculas e a chave com letras minúsculas e itálico. São exemplos de cifras de substituição: a Cifra com Deslocamento (ou Cifra de César), a Cifra Monoalfabética, a Cifra Poligráfica e a Cifra Polialfabética.

- Cifra com Deslocamento (ou Cifra de César)

A cifra de substituição mais simples que existe é a cifra de Júlio César. A Cifra de César substitui cada letra do alfabeto por aquela que fica três posições adiante. Matematicamente, a encriptação na cifra de César é dada por

$$E = f(3, p) = (p + 3) \mod 26, \tag{2.1}$$

em que $E$ é o texto cifrado, $f$ é o algoritmo de encriptação e $p$ é o texto claro. Define-se $a \mod n$ como o resto da divisão de $a$ por $n$. Para uma abordagem mais completa sobre aritmética modular, consultar (PAAR; PELZL, 2010).

A decriptação é realizada facilmente retrocedendo três posições.

A Cifra de César pode ser generalizada permitindo-se que o deslocamento $k$ tenha qualquer magnitude entre 1 e 25. Logo, a encriptação é dada por

$$E = f(k, p) = (p + k) \mod 26, \tag{2.2}$$

e a decriptação por

$$p = f^{-1}(k, E) = (E - k) \mod 26, \tag{2.3}$$

em que $f^{-1}$ é o algoritmo de decriptação.

Observa-se que, por possuir apenas 25 chaves possíveis, que é exatamente o número de deslocamentos possíveis, a Cifra de César pode ser facilmente quebrada por Força Bruta.

- Cifra Monoalfabética

A cifra de substituição monoalfabética consiste na permutação das letras do alfabeto utilizado. Em geral, um conjunto com $n$ elementos permite $n!$ permutações. Levando em consideração que o alfabeto possui $26$ letras, então haverá $26!$, ou mais do que $4 \times 10^{26}$, chaves possíveis.

O problema da quebra da cifra por Força Bruta está resolvido, mas o problema da estrutura sobrevivente do texto claro no texto cifrado (a distribuição de frequência

do alfabeto, por exemplo) ainda permanece e poderá ser facilmente explorado pelo criptoanalista.

A forma de reduzir o impacto da estrutura sobrevivente do texto claro no texto cifrado é utilizando a técnica de encriptar várias letras do texto claro (Cifra Poligráfica) ou encriptar usando vários alfabetos de cifra (Cifra Polialfabética).

- Cifra Poligráfica

A cifra poligráfica substitui grupo de letras do texto claro por caracteres no texto cifrado. São exemplos de cifras poligráficas:

a) Cifra Playfair

A cifra de encriptação de múltiplas letras mais conhecida é a Playfair. Tal cifra utiliza uma matriz $5 \times 5$ preenchida com uma palavra-chave, excluindo-se as letras repetidas da palavra-chave, e com as letras do alfabeto latino. Inicialmente a palavra-chave é alocada da esquerda para a direita e de cima para baixo. Em seguida, as outras letras (em ordem alfabética) são colocadas até preencher a matriz por completo. As letras *i* e *j* contam como uma só. Geralmente a letra *j* é omitida. Por exemplo, se a palavra-chave for *segredo*, a matriz $5 \times 5$ será:

$$\begin{pmatrix} s & e & g & r & d \\ o & a & b & c & f \\ h & i & k & l & m \\ n & p & q & t & u \\ v & w & x & y & z \end{pmatrix} \tag{2.4}$$

O texto claro é encriptado com duas letras de cada vez, de acordo com as seguintes regras: 1 - Letras de texto claro repetidas que estão no mesmo par são separadas por uma de preenchimento, como x, de modo que, por exemplo, a palavra carro seria tratado como ca rx ro. 2 - Duas letras de texto claro que estejam na mesma linha da matriz são substituídas pela letra à direita, com o primeiro elemento da linha vindo após o último, de forma rotativa. Assim, no exemplo apresentado na matriz 2.4 para a palavra-chave *segredo*, as letras rd são encriptadas como DS. 3 - Duas letras de texto claro que estejam na mesma coluna são substituídas pela letra abaixo, com o elemento de cima da coluna vindo após o último, de forma rotativa. No exemplo da matriz 2.4, so é encriptado como OS. 4 - Caso contrário, cada letra de texto claro em um par é substituída por aquela que esteja em sua própria linha e na coluna ocupada pela outra letra de texto claro. Assim, cp na matriz 2.4 torna-se AT e he torna-se IS.

A cifra Playfair resolve o problema da distribuição de frequência das cifras anteriores, mas ainda conserva boa parte da estrutura do texto claro.

b) Cifra de Hill

Outra cifra poligráfica bastante interessante é a cifra de Hill. A cifra de Hill encripta $m$ letras de texto claro em $m$ letras de texto cifrado. Para isso, cada caractere do texto claro deve ser associado a um valor numérico, a = 0, b = 1, ..., z = 25. Em seguida, realiza-se a operação **C** = **P**K mod N, em que **P** e **C** são vetores $1 \times n$, representando o texto claro e o texto cifrado, respectivamente, K é uma matriz $n \times n$ invertível, indicando a chave de encriptação, e N é o número de letras do alfabeto utilizado. Por fim, converte-se cada número resultante em letra novamente.

Por exemplo, considere $m = 3$, N = 26 (o alfabeto latino), a sigla fab como texto claro e a matriz de encriptação

$$K = \begin{pmatrix} 19 & 5 & 7 \\ 18 & 5 & 4 \\ 15 & 19 & 5 \end{pmatrix}. \tag{2.5}$$

Aplicando a cifra de Hill, tem-se que

$$\mathbf{P} = (612). \tag{2.6}$$

Consequentemente,

$$\mathbf{C} = \begin{pmatrix} 6 & 1 & 2 \end{pmatrix} . \begin{pmatrix} 19 & 5 & 7 \\ 18 & 5 & 4 \\ 15 & 19 & 5 \end{pmatrix} \mod 26 \tag{2.7}$$

$$\mathbf{C} = \begin{pmatrix} 162 & 73 & 56 \end{pmatrix} \mod 26 \tag{2.8}$$

$$\mathbf{C} = \begin{pmatrix} 6 & 21 & 4 \end{pmatrix}. \tag{2.9}$$

Logo, o texto cifrado **C** será FUD.

Para decifrar, basta realizar a operação com a inversa da matriz K: **P** = **C**$K^{-1}$ $\mod 26$. Sendo

$$K^{-1} = \begin{pmatrix} -17/250 & 18/125 & -1/50 \\ -1/25 & -1/75 & 1/15 \\ 89/250 & -143/375 & 1/150 \end{pmatrix}, \tag{2.10}$$

tem-se

$$\mathbf{P} = \begin{pmatrix} 6 & 21 & 4 \end{pmatrix} . \begin{pmatrix} -17/250 & 18/125 & -1/50 \\ -1/25 & -1/75 & 1/15 \\ 89/250 & -143/375 & 1/150 \end{pmatrix} \mod 26 \tag{2.11}$$

$$\mathbf{P} = \begin{pmatrix} 22/125 & -353/375 & -188/125 \end{pmatrix} \mod 26 \tag{2.12}$$

$$\mathbf{P} = \begin{pmatrix} 22/125 & -353/375 & -188/125 \end{pmatrix} \mod 26 \tag{2.13}$$

$$\mathbf{P} = \begin{pmatrix} 6 & 1 & 2 \end{pmatrix}, \tag{2.14}$$

que é exatamente o texto claro original.

A cifra de Hill, assim como a cifra Playfair, resolve o problema da distribuição de frequência, mas ainda conserva boa parte da estrutura do texto claro.

- Cifras Polialfabéticas

A cifra polialfabética visa também minimizar o impacto da estrutura sobrevivente do texto claro no texto cifrado, com a vantagem de serem mais robusta que as cifras poligráficas, haja vista que consegue tornar o texto cifrado mais plano, ou seja, a distribuição de frequência das letras é praticamente a mesma. São cifras polialfabéticas:

a) Cifra de Vigenère

A cifra polialfabética mais popular é a cifra de Vigenère. Tal cifra funciona como múltiplas cifras de César, uma vez que cada letra do texto claro é encriptada com uma cifra de César diferente, a depender da letra da chave.

Matematicamente, a encriptação na cifra de Vigenère é dada por

$$C_i = (p_i + k_{i.mod(m)}) \mod 26, \tag{2.15}$$

e a decriptação por

$$p_i = (C_i - k_{i.mod(m)}) \mod 26, \tag{2.16}$$

em que $C_i$ é a letra do texto cifrado na posição $i$, $p_i$ é a letra do texto claro na posição $i$ e $k_{i.mod(m)}$ é a letra da chave na posição $i$.

A cifra de Vigenère exige que a chave possua o mesmo tamanho do texto claro. Logo, se a chave possuir um tamanho menor, ela deverá ser repetida até passar a ter o mesmo comprimento do texto claro.

Por exemplo, utilizando-se a palavra-chave *segredo*, amanhã será o dia d (texto claro) é encriptado da seguinte forma:

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| texto claro | 0 | 12 | 0 | 13 | 7 | 0 | 18 | 4 | 17 | 0 | 14 | 3 | 8 | 0 | 3 |
| chave | 18 | 4 | 6 | 17 | 4 | 3 | 14 | 18 | 4 | 6 | 17 | 4 | 3 | 14 | 18 |
| texto cifrado | 18 | 16 | 6 | 4 | 11 | 3 | 6 | 22 | 21 | 6 | 5 | 7 | 11 | 14 | 21 |

(2.17)

texto claro: amanhaseraodiad

chave: *segredosegredos*

texto cifrado: SQGELDGWVGFHLOV

Como se percebe no exemplo, uma grande vantagem dessa cifra é o fato de uma letra no texto claro poder ser levada a múltiplas letras no texto cifrado. Isso torna a ocultação da frequência das letras mais efetiva que a das cifras anteriores, mas não resolve o problema de forma definitiva.

Em virtude de a chave precisar ser repetida (geralmente ela é menor do que o texto claro), bem como de a chave e o texto claro possuírem a mesma natureza e, consequentemente, o mesmo problema da distribuição de frequências das letras, a cifra de Vigenère também é vulnerável a criptoanálise.

Para solucionar a questão da repetição da palavra-chave, Vigenère propôs a solução das auto-chave, que consistia em pegar parte do texto claro para complementar a palavra-chave:

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| texto claro | 0 | 12 | 0 | 13 | 7 | 0 | 18 | 4 | 17 | 0 | 14 | 3 | 8 | 0 | 3 |
| chave | 18 | 4 | 6 | 17 | 4 | 3 | 14 | 0 | 12 | 0 | 13 | 7 | 0 | 18 | 4 |
| texto cifrado | 18 | 16 | 6 | 4 | 11 | 3 | 6 | 4 | 3 | 0 | 1 | 10 | 8 | 18 | 7 |

(2.18)

texto claro: amanhaseraodiad

chave: *segredoamanhase*

texto cifrado: SQGELDGEDABKISH

Ressalta-se, no entanto, que a questão da distribuição de frequência permanece sem solução.

b) Cifra de Vernam

A fim de superar as limitações da cifra de Vernère, Vernam propôs que uma cifra robusta deveria possuir uma chave tão longa quanto o texto claro e zero relacionamento estatístico com ele. Ele abandonou a ideia de palavra e passou a trabalhar com fluxo de bits. Matematicamente, a encriptação na cifra de Vernam é dada por

$$c_i = p_i \oplus k_i, \tag{2.19}$$

e a decriptação por

$$p_i = c_i \oplus k_i, \tag{2.20}$$

em que $p_i$ = dígito binário na posição $i$ do texto claro, $k_i$ = dígito binário na posição $i$ da chave, $c_i$ = dígito binário na posição $i$ do texto cifrado e $\oplus$ = operação ou–exclusivo (XOR).

A cifra de Vernam chegou muito próximo da cifra ideal, mas pecou ao permitir que a chave pudesse ser reutilizada.

c) One-time Pad (OTP)

Joseph Mauborgne, a fim de aperfeiçoar a cifra de Vernam, propôs o esquema de encriptação denominado *one-time pad*. O *one-time pad* é um esquema de encriptação teórico, inquebrável, que sugere codificar o texto claro usando uma chave que seja: 1) completamente aleatória e sem correlação alguma com o texto claro; 2) tão longa quanto o texto claro; 3) nunca utilizada antes, no todo ou em parte; e 4) compartilhada por um meio seguro.

Levando em consideração que a chave seja mantida em sigilo, um atacante, mesmo tendo acesso a todo texto cifrado que julgar necessário e conhecimento da cifra, não pode quebrar o *one-time pad*, pelo simples fato de o texto cifrado não conter nenhuma informação acerca do texto claro.

O *one-time pad* fornece segurança completa, independentemente da cifra, mas há dois problemas práticos que tornam sua implementação um desafio, são eles: a geração e a distribuição das chaves.

Vale destacar que todo sistema de criptografia que pretende ser considerado incondicionalmente seguro deve atender aos quatro requisitos impostos pelo *one-time pad*.

### 2.4.2 Cifras de Transposição

A cifra de transposição busca permutar as letras do texto claro, consoante a regra específica da chave, para obter o texto cifrado. Há várias formas de realizar a cifra

de transposição, as duas mais comuns são a *rail fence* (cerca de trilho) e a transposição colunar simples.

- *Rail fence* (cerca de trilho)

Nesse tipo de transposição, as letras são dispostas numa sequências de diagonais e depois lidas horizontalmente. Por exemplo, para uma cerca de trilho com duas linhas, tem-se uma matriz com duas linhas e $n$ colunas:

Texto claro: amanhã será o dia d

Matriz:

| a | - | a | - | h | - | s | - | r | - | o | - | i | - | d |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| - | m | - | n | - | a | - | e | - | a | - | d | - | a | - |

(2.21)

Texto cifrado: AAHSROIDMNAEADA

- Transposição colunar simples

Nesse tipo de transposição, a mensagem é escrita linha por linha numa matriz de largura fixa e, depois de estabelecida a ordem de leitura das colunas, o texto cifrado será a leitura coluna por coluna seguindo essa ordem. Como exemplo, tem-se:

Texto claro: amanhã será o dia d

Matriz:

| 2 | 5 | 4 | 1 | 3 |
|---|---|---|---|---|
| a | m | a | n | h |
| a | s | e | r | a |
| o | d | i | a | d |

(2.22)

Texto cifrado: NRAAAOHADAEIMSD

Em virtude de apenas a ordem do texto ser alterada nas cifras de transposição simples, a distribuição de frequência das letras será praticamente a mesma da frequência da língua usada. Logo, tais cifras de transposição podem ser facilmente quebradas.

Para aumentar a robustez da cifra e dificultar o trabalho do criptoanalista, o ideal é realizar mais de um estágio de transposição, inclusive mesclando cifras de transposição diferentes, e até combinando cifras de transposição com cifras de substituição.

Face ao exposto, de todos os tipos cifras vistas acima, a única realmente segura é a *one-time pad*. Em virtude disso, o esquema de comunicação segura proposto no presente trabalho visa garantir a segurança proposta por tal cifra.

# 3 SINCRONIZAÇÃO DE SISTEMAS CAÓTICOS

A sincronização de sistemas caóticos tem sido objeto de estudo, pesquisa e desenvolvimento desde a década de 80, quando Fujisaka e Yamada (FUJISAKA; YAMADA, 1983) desenvolveram a teoria da estabilidade do movimento sincronizado em sistemas de osciladores acoplados. Ao longo dos anos subsequentes, relevantes contribuições acadêmicas sobre o assunto foram desenvolvidas, dentre as quais se destacam os trabalhos de Pecora e Carrol (PECORA; CARROLL, 1990), que trataram da sincronização em sistemas caóticos, e Gauthier e Bienfang (GAUTHIER; BIENFANG, 1996), que abordaram a sincronização intermitente em osciladores caóticos acoplados.

Certamente, a sincronização de sistemas caóticos passou a ser de grande interesse da comunidade cientifica, de um lado, por ser um fenômeno amplamente observado na natureza, uma vez que está presente em sistemas ecológicos, fisiológicos, meteorológicos (PIKOVSKY; ROSENBLUM; KURTHS, 2002), de outro, por ter inúmeras possibilidades de aplicações tecnológicas, tais como em óptica (ROY; THORNBURG, 1994), em redes neurais (BELYKH; LANGE; HASLER, 2005) e em comunicações (PECORA; CARROLL, 1990).

Sincronizar sistemas caóticos nada mais é do que ajustar a operação de dois ou mais sistemas caóticos que oscilam de forma independente, a fim de que passem a apresentar uma dinâmica relacionada. Ressalta-se que há diferentes tipos de sincronização, entre elas a sincronização idêntica (PECORA; CARROLL, 1990), a sincronização em fase (ROSENBLUM; PIKOVSKY; KURTHS, 1996), a sincronização com atraso (ROSENBLUM; PIKOVSKY; KURTHS, 1997), a sincronização antecipada (VOSS, 2000) e a sincronização generalizada (KOCAREV; PARLITZ, 1996).

A sincronização de sistemas caóticos ocorre através do acoplamento unidirecional ou bidirecional dos sistemas em questão. No acoplamento unidirecional, também conhecido como mestre-escravo, o sistema mestre controla a dinâmica do sistema escravo à medida que uma ou mais variáveis de estado do sistema mestre é passada ao sistema escravo de forma direta ou indiretamente. No bidirecional, a dinâmica dos sistemas sofrem influência mútua.

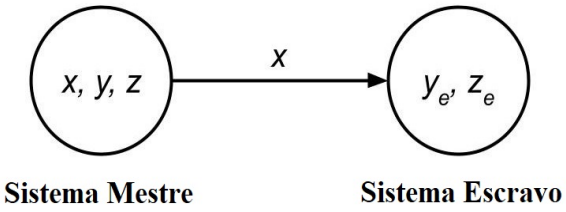
A partir de agora, aborda-se somente a sincronização idêntica por acoplamento unidirecional, que será tratada em detalhes na subseção 3.1, em virtude de ser a única utilizada no desenvolvimento do presente trabalho.

## 3.1 SINCRONIZAÇÃO IDÊNTICA POR ACOPLAMENTO UNIDIRECIONAL

A sincronização idêntica por acoplamento unidirecional é o tipo de sincronização na qual dois sistemas, lineares ou não, acoplados, apresentam soluções idênticas no decorrer do tempo, quando o primeiro sistema, denominado mestre, transmite algum

sinal ao segundo sistema, denominado escravo, conforme Fig. 5.

Figura 5 – Sincronização idêntica numa configuração mestre-escravo em que a variável $X$ é transmitida ao sistema escravo. $X$, $Y$ e $Z$ são variáveis de estado do sistema mestre e $Y_e$ e $Z_e$ são variáveis de estado do sistema escravo.




Fonte: Autor.

O processo de sincronização idêntica por acoplamento unidirecional pode ser demonstrado a partir da utilização de equações diferenciais ordinárias (PECORA; CARROLL, 1990). Logo, essa é a abordagem adotada a seguir.

Considere um sistema dinâmico autônomo n-dimensional

$$\dot{\mathbf{u}} = \mathbf{f}(\mathbf{u}). \tag{3.1}$$

Separe o sistema, arbitrariamente, em dois subsistemas,

$$\dot{\mathbf{v}} = \mathbf{g}(\mathbf{v}, \mathbf{w}) \quad e \quad \dot{\mathbf{w}} = \mathbf{h}(\mathbf{v}, \mathbf{w}), \tag{3.2}$$

em que $\mathbf{v} = (u_1,...,u_m)$, $\mathbf{g} = (f_1(u),...,f_m(u))$, $\mathbf{w} = (w_{m+1},...,w_n)$ e $\mathbf{h} = (f_{m+1}(u),...,f_n(u))$.

Agora crie um novo subsistema $\mathbf{w}'$, idêntico ao sistema $\mathbf{w}$, faça $\mathbf{v}' \to \mathbf{v}$ na função $\mathbf{h}$, e acrescente este novo subsistema às Eqs. 3.2:

$$\begin{aligned} \dot{\mathbf{v}} &= \mathbf{g}(\mathbf{v}, \mathbf{w}); \\ \dot{\mathbf{w}} &= \mathbf{h}(\mathbf{v}, \mathbf{w}); \ e \\ \dot{\mathbf{w}}' &= \mathbf{h}(\mathbf{v}, \mathbf{w}'). \end{aligned} \tag{3.3}$$

Examine a diferença, $\Delta\mathbf{w} = \mathbf{w}' - \mathbf{w}$. Os subsistemas componentes $\mathbf{w}$ e $\mathbf{w}'$ sincronizarão somente se $\Delta\mathbf{w} \to 0$ quando $t \to \infty$. No limite infinitesimal, isto leva a equação variacional do subsistema,

$$\dot{\boldsymbol{\xi}} = \mathbf{D}_w\mathbf{h}(\mathbf{v}(t), \mathbf{w}(t))\boldsymbol{\xi}, \tag{3.4}$$

em que $\Delta\mathbf{w} \equiv \boldsymbol{\xi}$ e $\mathbf{D}_w\mathbf{h}$ é o Jacobiano do campo vetorial do subsistema $\mathbf{w}$ em relação a $\mathbf{w}$ somente. O comportamento das trajetórias da Eq. 3.4 depende dos expoentes de Lyapunov do subsistema $\mathbf{w}$, uma vez que tais expoentes indicam a taxa de aproximação

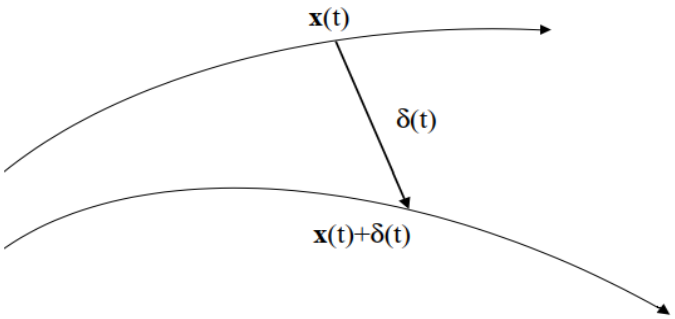
ou de afastamento entre trajetórias no espaço de fase. Para verificar como isso ocorre, suponha duas trajetórias iniciando seus movimentos nos pontos $x(t)$ e $x(t) + \delta(t)$, em que $\delta(t)$ é um vetor de comprimento inicial muito pequeno. Na Fig. 6, traz-se uma ideia de como seriam essas trajetórias no espaço de fase. Para verificar se as trajetórias se aproximam ou se afastam, basta analisar o comprimento do vetor $\delta(t)$, que é dado por:

$$|\delta(t)| \approx |\delta(0)|e^{\lambda t}, \tag{3.5}$$

em que $\lambda$ é o expoente de Lyapunov. Da Eq. 3.5, resta claro que o comprimento do vetor $\delta(t)$ ao longo do tempo depende do expoente de Lyapunov, haja vista que, se $\lambda < 0$, $\delta(t)$ reduz e, por conseguinte, as trajetórias se aproximam. Por outro lado, se $\lambda > 0$, $\delta(t)$ aumenta e, naturalmente, as trajetórias se afastam. Logo, em última instância, são os expoentes de Lyapunov que mostram o quão rápido ou lento uma trajetória se afasta ou se aproxima da outra.

Vale destacar que um sistema dinâmico terá tantos expoentes de Lyapunov quantas forem as suas dimensões, ou seja, um sistema com dimensão $n$ terá $n$ expoentes de Lyapunov que representam as taxas médias de convergência ou divergência das $n$ trajetórias independentes no espaço de fase. Observe que, se ao menos um dos expoentes de Lyapunov for positivo, as trajetórias serão divergentes. Logo, basta analisar o maior deles para concluir acerca do comportamento dinâmico das trajetórias. Para um tratamento completo acerca de expoentes de Lyapunov, consultar o livro *Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering* (STROGATZ, 2018).

Figura 6 – Evolução de duas trajetórias partindo de condições iniciais muito próximas.




Fonte: Autor.

Voltando aos subsistemas **w** e **w′**, conclui-se que eles só sincronizarão se os expoentes do subsistema **w** forem todos negativos, uma vez que é a negatividade dos expoentes que garantem a estabilidade do subsistema **w** e, consequentemente, a convergência de **w′**. Observe que esses expoentes dependerão da variável transmitida, **v**, e, portanto, são chamados de expoentes sub-Lyapunov (PECORA; CARROLL, 1990).

A negatividade dos expoentes de Lyapunov do subsistema **w** é condição necessária, mas não suficiente, para haver sincronização entre **w** e **w**′. O conjunto de condições iniciais de **w**′, que o faz sincronizar com **w**, deve ser levado em consideração também, pois, não é para qualquer conjunto de condições iniciais que **w**′ sincronizará com **w**.

Demonstra-se o processo de sincronização idêntica por meio do acoplamento unidirecional completo a partir do sistema de Lorenz, um sistema caótico dissipativo de dimensão $3$, cuja dinâmica é governada pelo seguinte conjunto de equações diferenciais de primeira ordem:

$$\begin{aligned} \dot{x} &= \sigma(y - x); \\ \dot{y} &= rx - y - xz;\ e \\ \dot{z} &= xy - bz, \end{aligned} \tag{3.6}$$

em que $\sigma$, $b$, $r > 0$ são os parâmetros das equações do sistema (STROGATZ, 2018).

Suponha dois sistemas de Lorenz idênticos. Então, transmita um sinal do primeiro sistema para o segundo. Deixe esse sinal ser a componente $x$ do primeiro sistema de Lorenz. No segundo sistema, em todos os lugares que houver um componente $x$, substitua pelo sinal do primeiro sistema. Essa técnica de acoplamento unidirecional é comumente chamada de *substituição completa* (PECORA et al., 1997). Isso resulta em um novo sistema composto de cinco equações:

$$\begin{aligned} \dot{x_1} &= \sigma(y_1 - x_1); \\ \dot{y_1} &= -x_1 z_1 + r x_1 - y_1; \quad \dot{y_2} = -x_1 z_2 + r x_1 - y_2; \\ \dot{z_1} &= x_1 y_1 - b z_1;\ e \qquad\quad \dot{z_2} = x_1 y_2 - b z_2, \end{aligned} \tag{3.7}$$

em que os subscritos $1$ e $2$ identificam o conjunto de equações dos sistemas mestre e escravo, respectivamente.

A variável $x_1$ é responsável pela condução do segundo sistema. Se o sistema de Eqs. 3.7 for iniciado com condições iniciais arbitrárias, então, analisando a solução numérica do sistema, verifica-se que $y_2$ converge para $y_1$, e $z_2$ para $z_1$, quando o sistema evolui. Depois de muito tempo, tem-se $y_2 = y_1$ e $z_2 = z_1$. Portanto, para um determinado conjunto de parâmetros ($\sigma$, $b$, $r$) que tornam a dinâmica caótica, observa-se dois sistemas caóticos sincronizados. Normalmente, essa situação é chamada de sincronização idêntica, uma vez que ambos os subsistemas $(y, z)$ são idênticos, o que se manifesta na igualdade dos componentes.

As equações $y_2 = y_1$ e $z_2 = z_1$ determinam um hiperplano no espaço de fase de cinco dimensões. A restrição do movimento no hiperplano é a imagem geométrica

da sincronização idêntica. Esse hiperplano é chamado de variedade de sincronização (PECORA et al., 1997). O espaço ortogonal à variedade de sincronização, conhecido como variedade transversal, tem coordenadas zero quando o movimento está na variedade de sincronização.

No exemplo de substituição completa de dois sistemas de Lorenz sincronizados, observa-se que as diferenças $|y_1 - y_2| \to 0$ e $|z_1 - z_2| \to 0$ no limite $t \to \infty$, em que $t$ é o tempo. Isso ocorre porque a variedade de sincronização é estável. Para verificar isso, transforma-se o sistema de equações para um novo conjunto de coordenadas:

$$\begin{aligned} x_1 &= x_1; \\ y_\perp &= y_1 - y_2; \qquad y_\parallel = y_1 + y_2; \\ z_\perp &= z_1 - z_2; \ e \quad z_\parallel = z_1 + z_2. \end{aligned} \tag{3.8}$$

No novo conjunto de coordenadas, as três coordenadas $(x_1, y_\parallel, z_\parallel)$ pertencem à variedade de sincronização e as outras duas $(y_\perp, z_\perp)$, a variedade transversal.

A condição de sincronização é satisfeita quando $y_\perp \to 0$ e $z_\perp \to 0$ em $t \to \infty$. Portanto, o ponto $(0, 0)$ da variedade transversal deve ser um ponto fixo da variedade. Isto leva a necessidade de os subsistemas dinâmicos $dy_\perp/dt$ e $dz_\perp/dt$ serem estáveis no ponto $(0, 0)$. A dinâmica do sistema na vizinhança desse ponto é descrita pela equação

$$\begin{pmatrix} \dot{y_\perp} \\ \dot{z_\perp} \end{pmatrix} = \begin{pmatrix} -1 & -x_1 \\ x_1 & -b \end{pmatrix} \begin{pmatrix} y_\perp \\ z_\perp \end{pmatrix}, \tag{3.9}$$

em que $y_\perp$ e $z_\perp$ são consideradas pequenas perturbações em torno do ponto $(0, 0)$. A solução dessa equação matricial dará a estabilidade - se $y_\perp$ ou $z_\perp$ cresce quando $t \to \infty$, tem-se que a dinâmica do sistema é instável, ao passo que, se $y_\perp$ e $z_\perp$ diminuem quando $t \to \infty$, a dinâmica do sistema é estável.

A condição mais geral e, ao que parece, mínima para a estabilidade é ter expoentes de Lyapunov negativos para a Eq. 3.9. Facilmente se verifica que isso é o mesmo que exigir que o subsistema de resposta $y_2$ e $z_2$ tenha expoentes negativos. Portanto, pode-se considerar o sistema escravo $(y_2, z_2)$ como um sistema dinâmico separado, conduzido pelo sinal $x_1$, e calcular os expoentes de Lyapunov para esse subsistema da maneira usual. Esses expoentes de Lyapunov depende de $x_1$, pois os valores dos expoentes sub-Lyapunov para um determinado sistema dinâmico depende da escolha da coordenada do sistema mestre que será substituída no sistema escravo.

Pode-se abordar a sincronização de dois sistemas caóticos sob um ponto de vista mais geral, no qual a técnica de substituição completa acima é um caso especial. Este é o acoplamento *difusivo unilateral*, também chamado de *controle de feedback*

*negativo*, que é obtido adicionando-se um termo de amortecimento ao sistema escravo da seguinte forma:

$$\dot{\mathbf{x}}_1 = \mathbf{F}(\mathbf{x}_1) \quad e \quad \dot{\mathbf{x}}_2 = \mathbf{F}(\mathbf{x}_2) + \alpha\hat{E}(\mathbf{x}_1 - \mathbf{x}_2) \tag{3.10}$$

em que $\hat{E}$ é uma matriz que determina a combinação linear dos componentes **x** que serão usados na diferença e $\alpha$ determina a força de acoplamento. Esse é o método utilizado para realizar a sincronização no presente trabalho.

Vale destacar que a força de acoplamento influencia diretamente a qualidade da sincronização (PIKOVSKY; ROSENBLUM; KURTHS, 2002; BOCCALETTI et al., 2002). Isto é, para forças de acoplamento abaixo de uma força de acoplamento crítica, os sistemas interagentes não sincronizam e evoluem de forma independente um do outro. Em contrapartida, para forças de acoplamento acima desse força crítica, os sistemas sincronizam e passam a apresentar comportamento dinâmico relacionados.

Há inúmeras outras técnicas de acoplamento unidirecional (PECORA et al., 1997) que, assim como o acoplamento bidirecional, não serão abordadas aqui em virtude de não serem utilizadas no desenvolvimento do presente trabalho.

Na próxima subseção, apresenta-se o sistema caótico que é utilizado para demonstrar a sincronização idêntica por acoplamento unidirecional.

## 3.2 SISTEMA DE GAUTHIER-BIENFANG

O sistema de Gauthier-Bienfang, oscilador caótico real utilizado como plataforma para a geração e distribuição das chaves criptográficas simétricas do presente trabalho, foi selecionado como equivalente elétrico em virtude de ser um excelente gerador de caos, além de possuir modelagem matemática simples, fácil construção e baixo custo. O sistema de Gauthier-Bienfang está apresentado na Fig. 7.

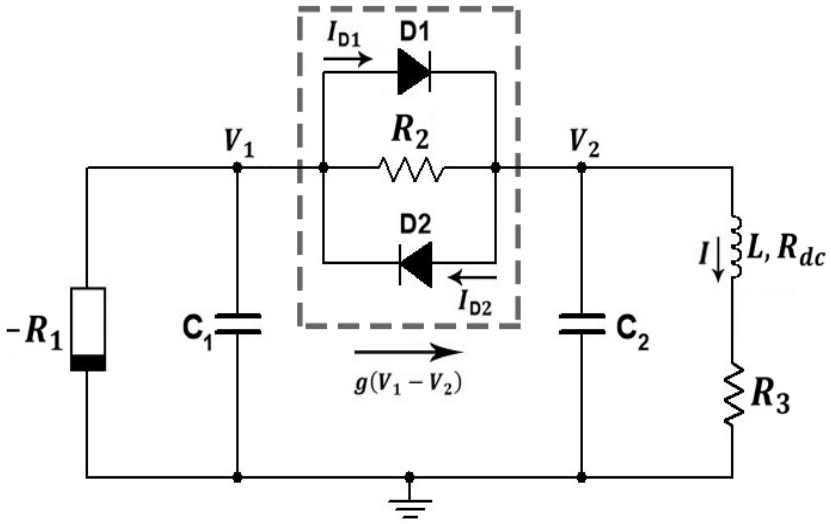
O oscilador de Gauthier-Bienfang é composto basicamente por um resistor negativo ativo, responsável pela manutenção da energia do circuito, por um elemento não-linear, responsável pela dinâmica complexa, e por um circuito RLC passivo, responsável pelas oscilações, conforme Fig. 7.

O resistor negativo, $R_1$, é implementado na prática a partir de um de Conversor de Impedância Negativa (CIN), que nada mais é do que um circuito amplificador operacional não inversor ideal acrescido do resistor $R_a$, consoante Fig. 8.

A partir da análise da Fig. 8, verifica-se que, uma vez aplicada a tensão de entrada, $V_{in}$, toda corrente resultante, $I_a$, flui por $R_a$, uma vez que o amplificador operacional é ideal. Aplicando a lei de Ohm, tem-se:

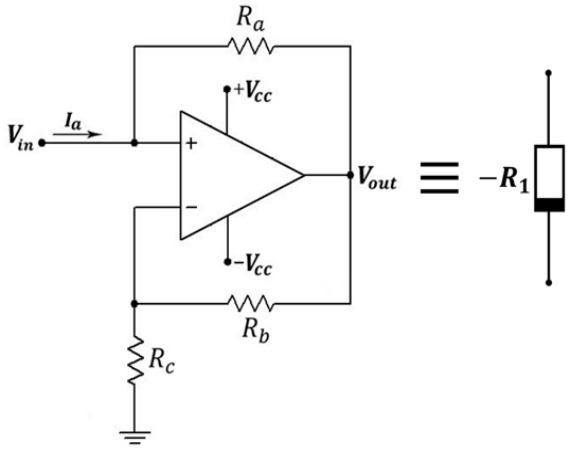
$$I_a = \frac{V_{in} - V_{out}}{R_a}. \tag{3.11}$$

Figura 7 – Oscilador eletrônico caótico que consiste de um resistor negativo $R_1 = 2814\ \Omega$, capacitores $C_1 = C_2 = C = 10$ nF, um indutor $L = 56$ mH (resistência dc de $353\ \Omega$), um resistor $R_3 = 100\ \Omega$ e um elemento não-linear passivo (resistor $R_2 = 8067\ \Omega$ e diodos tipo 1N914, caixa tracejada).




Fonte: Autor.

Figura 8 – Conversor de Impedância Negativa.




Fonte: Autor.

Sabendo que o amplificador operacional está em uma configuração não inversora e assumindo que $V_{in}$ provém de uma fonte de tensão ideal, obtém-se a tensão de saída $V_{out}$:

$$V_{out} = V_{in}(1 + \frac{R_b}{R_c}). \tag{3.12}$$

Substituindo a Eq. 3.12 na Eq. 3.11, pode-se mostrar que

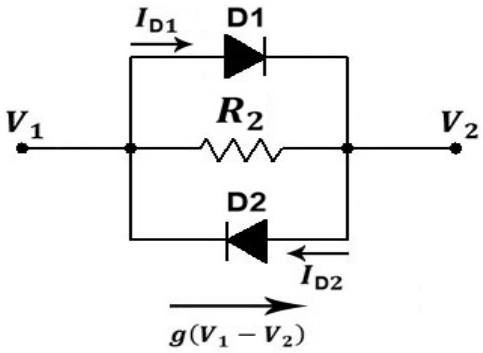
$$R_{in} = \frac{V_{in}}{I_a} = -\frac{R_a R_c}{R_b}. \tag{3.13}$$

Essa é a resistência de entrada do CIN e, consequentemente, do resistor negativo ($R_1$ = $R_{in}$). Observe que, se $R_b$ e $R_c$ forem iguais, a resistência de entrada

será simplesmente igual a -$R_a$ ($R_1$ = $R_{in}$ = -$R_a$). Ao passo que, se $R_a$ e $R_b$ forem iguais, a resistência de entrada será simplesmente igual a -$R_c$ ($R_1$ = $R_{in}$ = -$R_c$).

O elemento não-linear é constituído por dois diodos antiparalelo, D1 e D2, em paralelo ao resistor R2, conforme Fig. 9.

Figura 9 – Elemento não-linear composto pelos diodos antiparalelos e pelo resistor $R_2$.




Fonte: Autor.

Aplicando a lei dos nós de Kirchhoff à Fig. 9, obtém-se

$$g(V_1 - V_2) = I_{D1} + I_{R2} - I_{D2}. \tag{3.14}$$

Para diodos trabalhando na região de polarização direta, uma boa aproximação para a relação I - V é

$$I_d = I_s(e^{\frac{V}{nV_T}} - 1), \tag{3.15}$$

em que $V_T$ é a tensão térmica, $I_s$ é a corrente de saturação, $n$ é o número de diodo, parâmetros estes que variam de diodo para diodo, e $V$ é a tensão entre os terminais do diodo (SEDRA et al., 1998).

Logo, substituindo a Eq. 3.15 na Eq. 3.14, obtém-se

$$g(V_1 - V_2) = \frac{V_1 - V_2}{R_2} + I_s(e^{\frac{V_1 - V_2}{nV_T}} - e^{-\frac{V_1 - V_2}{nV_T}}), \tag{3.16}$$

consequentemente,

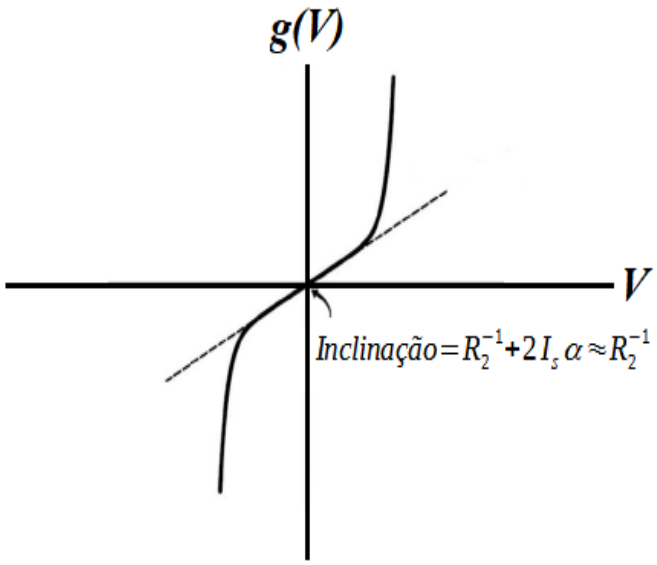
$$g(V) = VR_2^{-1} + 2I_s \sinh(\alpha V), \tag{3.17}$$

em que $\alpha = (nV_T)^{-1}$ e $V = V_1 - V_2$ é a diferença de potencial entre os terminais do elemento não-linear. A curva característica da Eq. 3.17 está apresentada na Fig. 10.

Observa que, para baixas tensões, a curva é aproximadamente linear devido ao fato de os diodos funcionarem como um circuito aberto. Logo, a corrente flui por $R_2$. Para tensões mais altas, a curva é não-linear porque os diodos passam a conduzir a corrente e, consequentemente, tira $R_2$ de operação.

Observa-se que $R_2$ desempenha um papel primordial na Eq. 3.17. Mantendo $V$ constante, tem-se que: 1) para $R_2$ pequeno, $g(V) \to V$. Logo, o termo linear da Eq. 3.17 domina o comportamento do elemento não-linear e o sistema de Gauthier-Bienfang passa a oscilar de forma periódica; e 2) Para $R_2$ grande, $g(V) \to 2I_s \sinh(\alpha V)$. Logo, o termo não-linear da Eq. 3.17 passa a dominar o comportamento do elemento não-linear e o sistema de Gauthier-Bienfang passa a oscilar de forma caótica.

Figura 10 – Curva característica de não-linearidade.



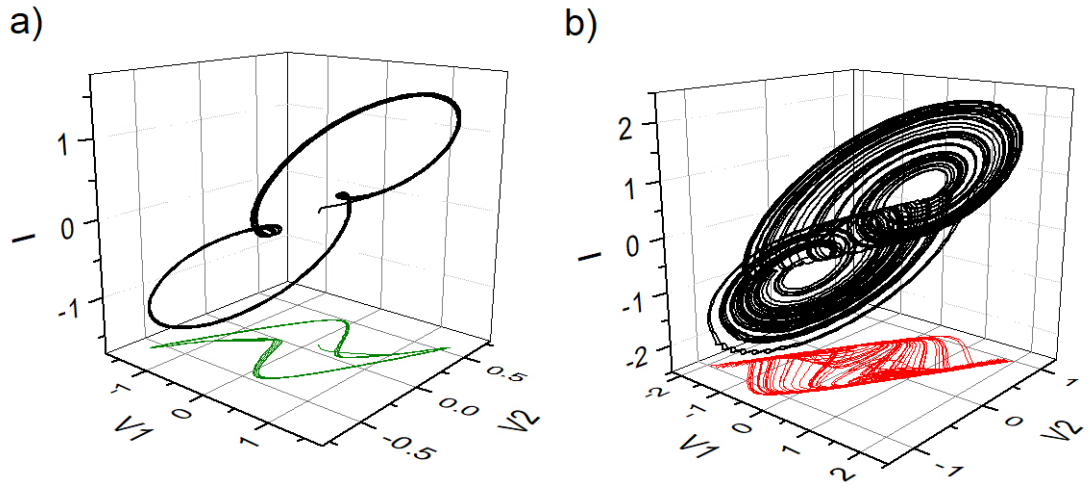

Fonte: Autor.

O circuito RLC, contido no sistema mostrado na Fig. 7, composto pelo capacitor $C_2$, pelo indutor $L$ e pelo resistor $R_3$, é um oscilador comum, que tem sua dinâmica influenciada pelo comportamento dinâmico do elemento não-linear.

Analisando a dinâmica do sistema de Gauthier-Bienfang, verifica-se que, ao alimentar o sistema, para uma pequena diferença de potencial entre $V_1$ e $V_2$, toda corrente do sistema flui através do resistor $R_2$, já que os diodos $D1$ e $D2$ estão funcionando como um circuito aberto, e o circuito RLC passa a operar em regime periódico. Após a diferença de potencial entre $V_1$ e $V_2$ aumentar e fazer os diodos funcionarem como um circuito fechado, o circuito RLC passa a operar em regime caótico. A dinâmica caótica do oscilador de Gauthier-Bienfang vem exatamente da impossibilidade de se prever o momento exato em que a diferença de potencial entre $V_1$ e $V_2$ é positiva, fazendo com que $D1$ conduza e $D2$ funcione como um circuito aberto, ou negativa, fazendo com que $D2$ conduza e $D1$ funcione como um circuito aberto. Na Fig. 11, apresenta-se o diagrama de fase demonstrando o comportamento periódico (Fig. 11(a)) e caótico (Fig. 11(b)) do sistema Gauthier-Bienfang.

Facilmente, aplicando as leis de Kirchhoff (lei das malhas e leis dos nós) ao circuito da Fig. 7, obtêm-se as equações diferenciais que governam a evolução dinâmica

Figura 11 – Retrato de fase: a) regime periódico, com $R_2 = 1{,}65$; e b) regime caótico, com $R_2 = 3{,}44$. Além do valor de $R_2$, os demais valores adimensionais dos resistores serão calculados mais a frente nesta subseção, são eles: $R_1 = 1{,}2$, $R_3 = 0{,}042$, $R_{dc} = 0{,}15$ e $R_4 = R_3 + R_{dc} = 0{,}192$.




Fonte: Autor.

do sistema:

$$\begin{aligned} C\dot{V}_1 &= V_1 R_1^{-1} - g(V_1 - V_2); \\ C\dot{V}_2 &= g(V_1 - V_2) - I;\ e \\ L\dot{I} &= V_2 - R_4 I, \end{aligned} \tag{3.18}$$

em que $V_1$ ($V_2$) representa a queda de tensão através do capacitor $C_1 = 10$ nF($C_2 = 10$ nF), $I$ representa a corrente fluindo através do indutor $L = 56$ mH, que possui resistência interna $R_{dc} = 353\ \Omega$, e do resistor $R_3 = 100\ \Omega$, $g(V_1 - V_2) = V/R_2 + I_s[\exp(\alpha.V) - \exp(-\alpha.V)]$ representa a corrente fluindo através da combinação paralela do resistor $R_2 = 8067\ \Omega$ e dos diodos de sinal (1N914), que possuem como parâmetros $I_s = 5{,}63$ nA, $V_d = 0{,}58$ V e $\alpha = 11{,}6$. O resistor negativo é $R_1 = 2814\ \Omega$, e $R_4 = R_1 + R_3 = 453\ \Omega$.

A análise do sistema é enormemente facilitada com as Eqs. 3.18 adimensionalizadas, haja vista que o número de parâmetros de controle é reduzido. Logo, dividindo as resistências por $R = \sqrt{L/C_1} = 2{,}37$ kΩ, as tensões por $V_d = 0{,}58$ V (tensão do diodo), as correntes por $I_d = V_d/R = 0{,}25$ mA (corrente do diodo) e o tempo por $\tau = \sqrt{LC_1} = 23{,}7\ \mu$s, obtêm-se as seguintes equações adimensionais:

$$\begin{aligned} \dot{V}_1 &= V_1 R_1^{-1} - g(V_1 - V_2); \\ \dot{V}_2 &= g(V_1 - V_2) - I;\ e \\ \dot{I} &= V_2 - R_4 I, \end{aligned} \tag{3.19}$$

em que os valores adimensionais das resistências são aproximadamente $R_1 = 1{,}2$, $R_2 = 3{,}4$, $R_3 = 0{,}042$, $R_{dc} = 0{,}15$ e $R_4 = 0{,}192$.

Os pontos fixos do sistema Gauthier-Bienfang são determinados impondo $(\dot{V}_1, \dot{V}_2, \dot{I}) = (0, 0, 0)$ nas Eqs. 3.19. Fazendo isso, obtém-se:

$$V_1^* = R_1 g(V_1^* - V_2^*); \tag{3.20}$$

$$I^* = g(V_1^* - V_2^*);\ e \tag{3.21}$$

$$V_2^* = R_4 I^*. \tag{3.22}$$

Para descobrir os pontos fixos a partir das Eqs. 3.20 - 3.22, é necessário resolver a Eq. 3.21 primeiro, uma vez que $V_1^*$ e $V_2^*$ são funções de $I^*$. Da Eq. 3.20 e Eq. 3.22, obtém-se:

$$V^* = V_1^* - V_2^* = R_1 I^* - R_4 I^* = (R_1 - R_4) I^*. \tag{3.23}$$

Substituindo a Eq. 3.17 na Eq. 3.21,

$$I^* = V^* R_2^{-1} + 2 I_s \sinh(\alpha V^*), \tag{3.24}$$

e, consequentemente, a Eq. 3.23 na Eq. 3.24,

$$I^* = (R_1 - R_4) I^* R_2^{-1} + 2 I_s \sinh(\alpha (R_1 - R_4) I^*), \tag{3.25}$$

após algumas manipulações matemáticas, pode-se chegar na equação

$$I^* = I_0 \sinh(\alpha (R_1 - R_4) I^*), \tag{3.26}$$

em que $I_0 = 2 I_r R_2 (R_4 - R_1 + R_2)^{-1}$, com $I_r \equiv I_s / I_d$.

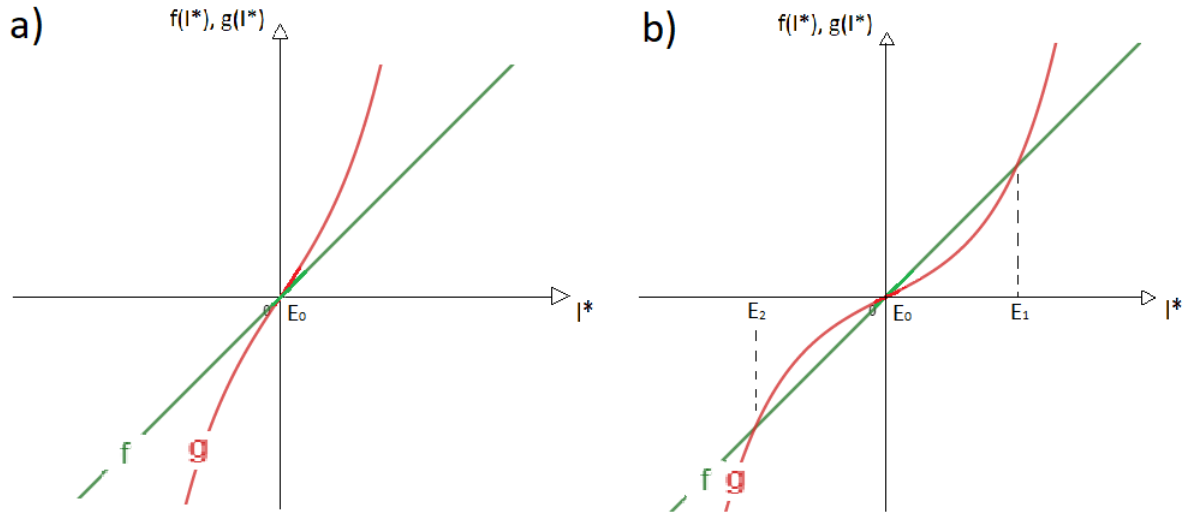
Verifica-se imediatamente que o ponto $E_0 = (0, 0, 0)$ é ponto fixo do sistema. O problema reside em saber se há outros pontos fixos. Para isso, é necessário resolver a Eq. 3.26, que, por ser transcendental, não pode ser resolvida analiticamente. Logo, adotada-se uma abordagem geométrica qualitativa para obtenção, se houver, dos demais pontos fixos. Para tanto, defina uma função

$$h(I) = I - I_0 \sinh(\alpha (R_1 - R_4) I). \tag{3.27}$$

Em seguida, faça $f(I) = I$ e $g(I) = I_0 \sinh(\alpha (R_1 - R_4) I)$, plote as funções $f(I)$ e $g(I)$ na mesma figura e varie $R_2$, conforme Fig. 12. Observe que a reta $I$ intercepta a curva $I_0 \sinh(\alpha (R_1 - R_4) I)$ onde $I = I_0 \sinh(\alpha (R_1 - R_4) I)$ e, portanto, $h(I) = 0$. Assim, as intersecções da linha e da curva correspondem aos pontos fixos do sistema.

Observando a Fig. 12, é evidente que o ponto $E_0$ é ponto fixo do sistema para todo valor de $R_2$, exceto para $R_2 = R_1 - R_4$, uma vez que a corrente $I_0$ não está definida.

Figura 12 – Gráfico da reta $f(I^*)$ e da curva $g(I^*)$ em função de $I^*$ para a) $R_2 = 0{,}5$ e b) $R_2 = 1{,}5$.




Fonte: Autor.

Além disso, em algum valor $R_2$ crítico, dois pontos fixos simétricos em relação à origem, $E_1 = (R_1 I^*, R_4 I^*, I^*)$ e $E_2 = (-R_1 I^*, -R_4 I^*, -I^*)$, surgem, o que implica dizer que uma bifurcação ocorre no sistema. Outro ponto importante a ser destacado é que, quando os pontos $E_1$ e $E_2$ surgem, a origem, $E_0$, tem sua estabilidade alterada para um tipo de estabilidade diferente da estabilidade desses pontos, haja vista que dois pontos fixos estáveis ou instáveis não podem coexistir próximos um do outro. Consequentemente, os pontos fixos $E_1$ e $E_2$ possuem a mesma estabilidade.

O valor de $R_2$ crítico, denominado $R_c$, que faz surgir um ponto de bifurcação pode ser determinado impondo a condição de que os gráficos de $f(I) = I$ e $g(I) = I_0 \sinh(\alpha(R_1 - R_4)I)$ se cruzem tangencialmente em torno do ponto fixo sob análise. Isso é conseguido igualando as funções $f(I)$ e $g(I)$, calculando a derivada de ambos os lados no ponto $E_0 = (0{,}0{,}0)$ e isolando $R_2$. Logo,

$$\frac{d}{dI}\left(\frac{I}{I_0}\right) = \frac{d}{dI}(\sinh(\alpha(R_1 - R_4)I)) \rightarrow R_2 = R_c = \frac{R_1 - R_4}{1 - 2I_r\alpha\,(R_1 - R_4)}. \tag{3.28}$$

Substituindo os valores dos parâmetros conhecidos, isto é, $R_1 = 1{,}2$, $R_4 = 0{,}192$, $I_r = 22{,}52 \times 10^{-6}$ e $\alpha = 11{,}6$, tem-se que o ponto de bifurcação ocorre para $R_2 = R_c \approx 1{,}01$.

Para avaliar a estabilidade local dos pontos fixos do sistema de Eqs. 3.19, basta linearizá-lo e, em seguida, calcular os autovalores da matriz jacobiana em torno dos

pontos fixos. A matriz jacobiana do sistema linearizado é dada por

$$J\left(V_1,V_2,I\right)=\begin{pmatrix} a-\mu & \mu & 0 \\ \mu & -\mu & -1 \\ 0 & 1 & -d \end{pmatrix}, \tag{3.29}$$

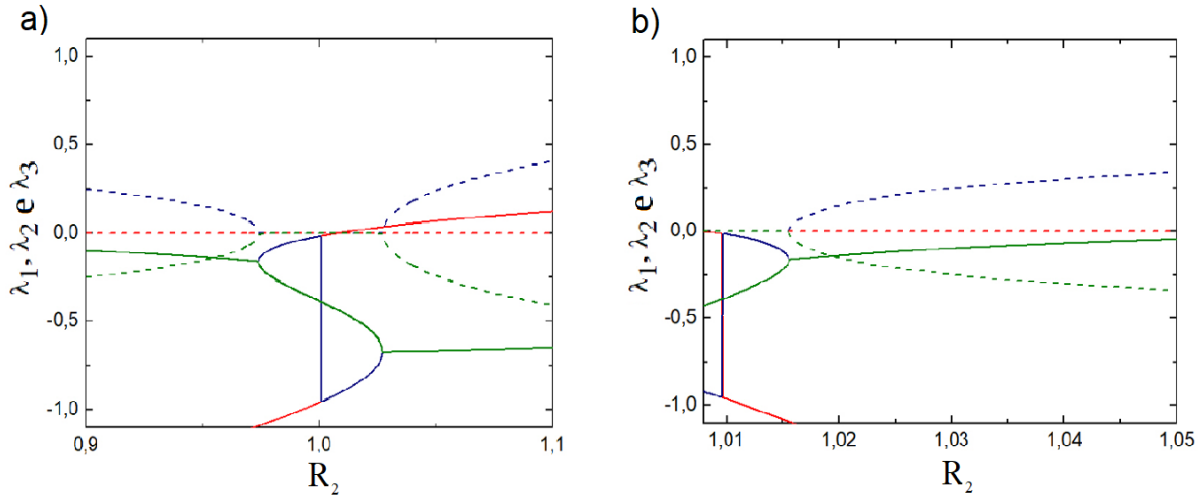
em que $\mu = R_2^{-1}+2I_r\alpha\cosh\left[\alpha\left(V_1-V_2\right)\right]$, $a=R_1^{-1}$ e $d=R_4$. Calculando $\det(J-\lambda I_3)=0$, obtém-se o polinômio característico $P\left(\lambda\right)$:

$$P\left(\lambda\right)=\lambda^3+a_2\lambda^2+a_1\lambda+a_0=0, \tag{3.30}$$

em que $a_2=(2\mu+d-a)$, $a_1=\left(1+\mu\left(2d-a\right)-ad\right)$, $a_0=\mu\left(1-ad\right)-a$.

Resolvendo numericamente a Eq. 3.30, obtém-se o diagrama de autovalores apresentados na Fig. 13.

Figura 13 – Diagrama de autovalores: (a) na origem e (b) nos pontos fixos simétricos. Há três autovalores: $\lambda_1$ (linha vermelha), $\lambda_2$ (linha verde) and $\lambda_3$ (linha azul). A parte real de cada um é representada pelo traço contínuo e a parte imaginária pelo traço tracejado.



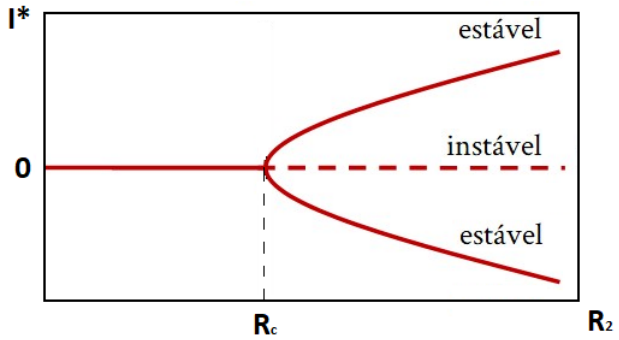

Fonte: Autor.

Observe que, para cada valor de $R_2$, tem-se um conjunto de três autovalores: $\lambda_1$, $\lambda_2$ e $\lambda_3$. Na Fig. 13(a), que mostra o diagrama de autovalores na origem, verifica-se que, para $R_2 < R_c$, a origem é estável, uma vez que todos os autovalores são negativos, e para $R_2 > R_c$, ela é instável, pois o autovalor $\lambda_1$ é positivo. Olhando agora para a Fig. 13(b), observa-se que os pontos fixos simétricos surgem estáveis, haja vista que os três autovalores são negativos logo após $R_2 = R_c$.

Após toda essa análise, conclui-se que o sistema sofre uma bifurcação de forquilha supercrítica em $R_2 = R_c$, consoante se observa no diagrama de bifurcação apresentado na Fig. 14.

Quando $R_2 < R_c$, só há um ponto fixo no sistema: a origem ($E_0$), que é estável. Em $R_2 = R_c$, ponto de bifurcação, a origem se torna fracamente estável. Quando

Figura 14 – Diagrama de bifurcação.




Fonte: Autor.

$R_2 > R_c$, a origem perde a estabilidade e dois novos pontos fixos ($E_1$ e $E_2$) estáveis aparecem simetricamente localizados em cada lado da origem.

Uma vez analisado em detalhe o oscilador Gauthier-Bienfang, na próxima subseção, utilizam-se dois desses osciladores para analisar a sincronização de sistemas caóticos.

## 3.3 ACOPLAMENTO ENTRE DOIS SISTEMAS GAUTHIER-BIENFANG

Para estudar a sincronização de circuitos caóticos, é necessário acoplá-los. Logo, por meio de uma acoplamento difusivo unilateral, realiza-se o acoplamento de dois sistemas Gauthier-Bienfang quase-idênticos (sistemas com uma diferença entre os parâmetros de, no máximo, $1\%$), cuja dinâmica do acoplamento pode ser descrita pelas seguintes equações diferenciais:

$$\dot{\mathbf{x}}_1 = \mathbf{F}(\mathbf{x}_1) \quad e \tag{3.31}$$

$$\dot{\mathbf{x}}_2 = \mathbf{F}(\mathbf{x}_2) + \alpha\hat{E}(\mathbf{x}_1 - \mathbf{x}_2), \tag{3.32}$$

em que $\mathbf{x}_1$ ($\mathbf{x}_2$) denota a posição no espaço de fase *n*-dimensional do oscilador mestre (escravo), **F** representa o fluxo dos osciladores, $\hat{E}$ é uma matriz de acoplamento $n$ x $n$, $\alpha$ é a força de acoplamento e $\mathbf{x}_i^T = (V_{1i}, V_{2i}, I_i)$.

Para facilitar a análise do processo de sincronização, os sistemas de Eqs. 3.31 e 3.32 são transformados para um novo conjunto de coordenadas:

$$\mathbf{x}_{\|} = \mathbf{x}_1 + \mathbf{x}_2 \quad e \tag{3.33}$$

$$\mathbf{x}_{\perp} = \mathbf{x}_1 - \mathbf{x}_2, \tag{3.34}$$

que especificam a dinâmica na variedade de sincronização e na variedade transversal, respectivamente.

A sincronização dos osciladores ocorre quando $\mathbf{x}_1(t) = \mathbf{x}_2(t)$, isto é, quando $|\mathbf{x}_\perp| = 0$, e, segundo Fujisaka and Yamada (FUJISAKA; YAMADA, 1983), sua estabilidade depende da negatividade do expoente transversal máximo de Lyapunov, ou seja, se $\lambda_\perp^1 \geq \lambda_\perp^2 \geq ...\lambda_\perp^n$ representam os expoentes transversais de Lyapunov, a sincronização é estável se $\lambda_\perp^1 \leq 0$. Os expoentes transversais de Lyapunov são os expoentes de Lyapunov no contexto da sincronização de sistemas. Eles fornecem informações a respeito da influência de perturbações que tiram o sistema da sincronização, indicando se essas perturbações são amortecidas ou não. Se as perturbações são amortecidas, a sincronização é estável. Caso contrário, é instável.

Vale destacar que, embora Fujisaka and Yamada tenham estabelecido a condição para que dois sistemas caóticos acoplados exibam sincronismo estável, Joshua Bienfang e Daniel Gauthier mostraram que o critério falha em alguns sistemas (GAUTHIER; BIENFANG, 1996).

Pode-se observar a estabilidade ou a instabilidade do sincronismo a partir da medida da distância escalar média $|\mathbf{x}_\perp|_{med}$ e máxima $|\mathbf{x}_\perp|_{max}$, que são sensíveis à estabilidade transversal global e local do estado sincronizado, respectivamente.

Em seguida, é analisada a qualidade do sincronismo de dois sistemas Gauthier-Bienfang acoplados por meio da variável $V_1$ em 3.3.1 e por meio da variável $V_2$ em 3.3.2. Uma diferença de $1\%$ será permitida na tolerância entre os componentes dos dois sistemas, para retratar uma implementação experimental.

### 3.3.1 Acoplamento via $V_1$

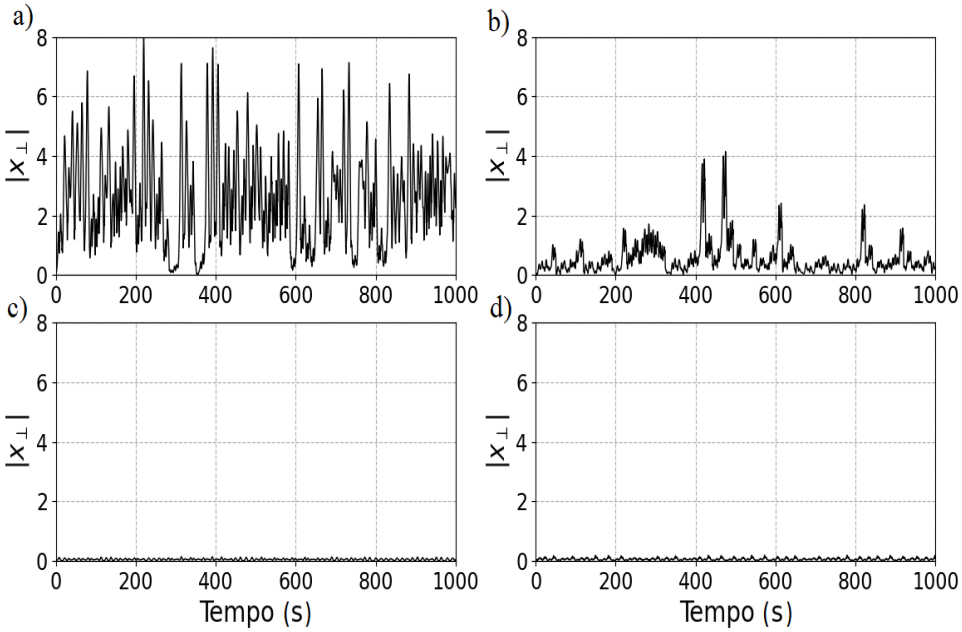
Considere dois sistemas de Gauthier-Bienfang oscilando acoplados através de $V_1$ ($E_{11} = 1{,}0$ e $E_{ij} = 0{,}0$ de outra forma) e partindo de condições iniciais arbitrárias (ver Eqs. 3.31 e 3.32). Acoplar através de $V_1$ significa fazer a diferença $V_{1m}$ - $V_{1e}$ e reinjetá-la em $V_{1e}$ do sistema escravo. Em seguida, faça $\alpha$ na Eq. 3.32 assumir os valores ($0{,}00$, $0{,}25$, $0{,}50$, $1{,}00$). Por fim, resolva numericamente a Eq. 3.34, para obter o resultado apresentado na Fig. 15.

Nas Figs. 15(a-b), nota-se que a força de acoplamento $\alpha$ foi insuficiente para fazer os osciladores sincronizarem, por isso a amplitude de $|x_\perp|$ é diferente de zero na maior parte do tempo. Nas Figs. 15(c-d), observa-se que $\alpha$ agora foi suficiente para sincronizar os osciladores, haja vista que a amplitude de $|x_\perp|$ é zero ou muito próxima a zero. Em suma, verifica-se que $|x_\perp| \to 0$ quando $t \to \infty$ para valores de $\alpha$ acima de um $\alpha$ crítico.

Para analisar a qualidade (estabilidade ou instabilidade) da sincronização de $V_1$, mede-se $|\mathbf{x}_\perp|_{med}$ e $|\mathbf{x}_\perp|_{max}$ como função da força de acoplamento ($\alpha$). O resultado numérico está apresentado na Fig. 16.

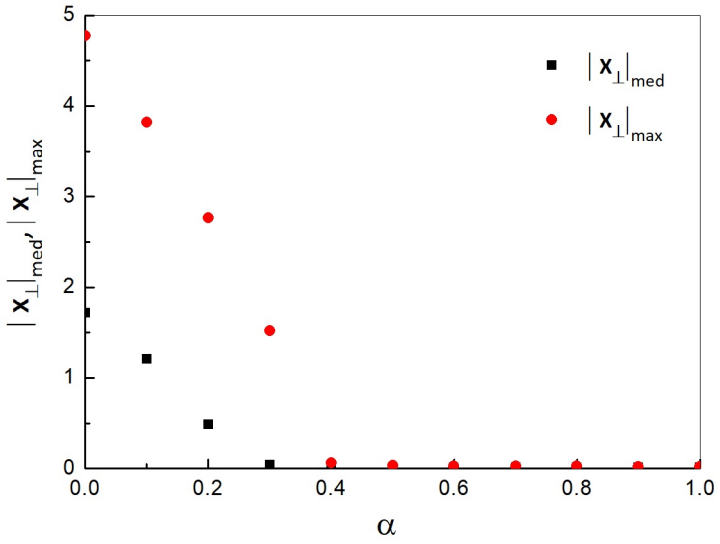
Na Fig. 16, mostra-se que $|x_\perp|_{max}$ e $|x_\perp|_{med}$ convergem rapidamente para zero

Figura 15 – Séries temporais mostrando a distância escalar entre as trajetórias dos dois osciladores acoplados através $V_1$ para (a) $\alpha = 0{,}00$; (b) $\alpha = 0{,}25$; (c) $\alpha = 0{,}50$; e (d) $\alpha = 1{,}00$.




Fonte: Autor.

Figura 16 – Medida de convergência entre os osciladores, mestre e escravo, acoplados através $V_1$. Gráfico dos $|x_\perp|_{max}$, quadrado preto, e $|x_\perp|_{med}$, bola vermelha, em função do coeficiente de acoplamento, $\alpha$, variando entre 0,0 e 1,0.



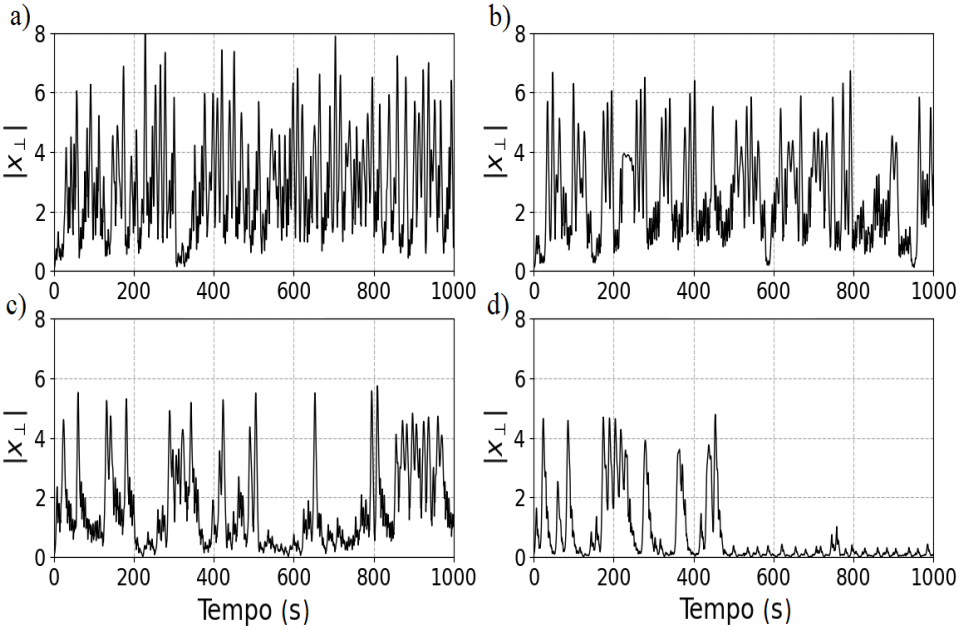

Fonte: Autor.

à medida que a força de acoplamento, $\alpha$, aumenta no acoplamento por meio de $V_1$. Este comportamento evidencia a sincronização de alta qualidade ($|x_\perp|$ perto do nível de ruído) observada na série temporal $|x_\perp|$ da Fig. 15(c-d).

### 3.3.2 Acoplamento via $V_2$

Considere dois sistemas Gauthier-Bienfang oscilando acoplados através de $V_2$ ($E_{22} = 1{,}0$ e $E_{ij} = 0{,}0$ de outra forma) e partindo de condições iniciais arbitrárias (ver Eqs. 3.31 e 3.32). Acoplar através de $V_2$ significa fazer a diferença $V_{2m}$ - $V_{2e}$ e reinjetá-la em $V_{2e}$ do sistema escravo. Em seguida, faça $\alpha$ na Eq. 3.32 assumir os valores ($0{,}00$, $0{,}25$, $0{,}50$, $1{,}00$). Por fim, resolva numericamente a Eq. 3.34, para obter o resultado apresentado na Fig. 17.

Figura 17 – Séries temporais mostrando a distância escalar entre as trajetórias dos dois osciladores acoplados através $V_2$ para (a) $\alpha = 0{,}00$; (b) $\alpha = 0{,}25$; (c) $\alpha = 0{,}50$; e (d) $\alpha = 1{,}00$.



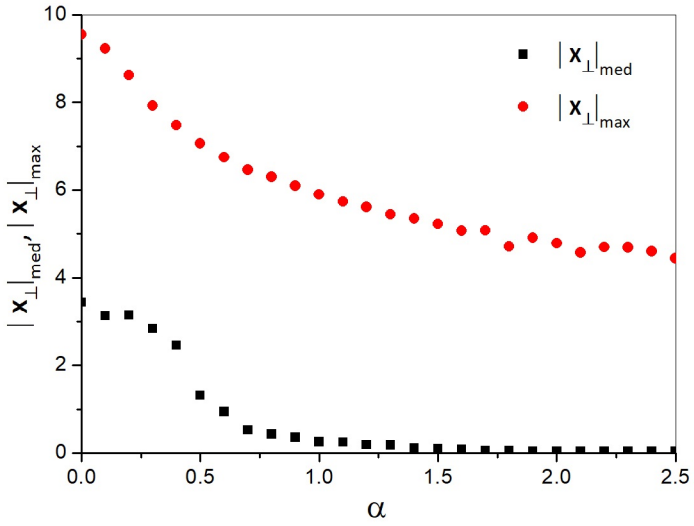

Fonte: Autor.

Na Fig. 17(a), nota-se que a força de acoplamento $\alpha$ foi insuficiente para fazer os osciladores sincronizarem, por isso a amplitude de $|x_\perp|$ é diferente de zero na maior parte do tempo. A medida que $\alpha$ aumenta, o número de ocorrências e a amplitude de $|x_\perp|$ diminuem, mas não desaparecem, conforme se observa nas Figs. 17(b-d). Observa-se indefinidamente breves eventos de dessincronização intermitente em grande escala na evolução temporal experimentalmente de $|x_\perp|$, independente do valor de $\alpha$.

Para analisar a qualidade (estabilidade ou instabilidade) da sincronização de $V_2$, mede-se $|\mathbf{x}_\perp|_{med}$ e $|\mathbf{x}_\perp|_{max}$ como função da força de acoplamento ($\alpha$). O resultado numérico está apresentado na Fig. 18.

Na Fig. 18, evidencia-se que $|x_\perp|_{med}$ converge rapidamente para zero e $|x_\perp|_{max}$ sequer vai a zero à medida que a força de acoplamento, $\alpha$, aumenta no acoplamento por meio de $V_2$. Isso significa que os osciladores sincronizam globalmente, mas não localmente. Este comportamento evidencia a sincronização de alta qualidade ($|x_\perp|$

Figura 18 – Medida de convergência entre os osciladores, mestre e escravo, acoplados através $V_2$. Gráfico dos $|x_\perp|_{max}$ (quadrado preto) e $|x_\perp|_{med}$ (bola vermelha) em função da força de acoplamento, $\alpha$, variando de 0,0 a 2,5.




Fonte: Autor.

perto do nível de ruído), intercalada por breves eventos de dessincronização, observada na série temporal $|x_\perp|$ da Fig. 17(d).

Esses longos períodos de sincronização de alta qualidade intercalados por breves eventos de dessincronização, em que $|x_\perp|$ assume um grande valor, são denominadas borbulhamento, em que a bolha - um evento extremo - corresponde a uma grande excursão temporária do estado do sistema para regiões do espaço de fase distantes da variedade de sincronização.

No sistema Gauthier-Bienfang, os eventos extremos são consequências do borbulhamento do atrator, que é um fenômeno em que a trajetória do sistema, de forma irregular e breve, deixa a vizinhança de uma variedade de sincronização, contendo um atrator caótico, como resultado de um salto induzido por ruído ocasional para uma região onde as órbitas são repelidas localmente da variedade de sincronização. O estado do sistema segue então uma órbita que se afasta da variedade de sincronização, mas que eventualmente retorna ao atrator (CAVALCANTE et al., 2013).

Lembre-se que o sistema Gauthier-Bienfang possui um ponto fixo instável ($E_0$) e dois estáveis ($E_1$ e $E_2$) no atrator caótico. Quando o acoplamento é realizado por meio de $V_1$, ele é forte o suficiente para manter o sincronismo entre os osciladores, mesmo quando as trajetórias passam por regiões instáveis (origem) no espaço de fase. Logo, eventos de dessincronização não são observados. Já quando o acoplamento é realizado por meio de $V_2$, a instabilidade da origem interfere na sincronização, separando brevemente as trajetórias dos osciladores acoplados que passam próximas a ela. Quanto mais próxima essas trajetórias passam da origem, maior é a separação entre elas, ou seja, maior será $|x_\perp|$.

Um fato interessante dos eventos extremos é que a distribuição estatística da amplitude dos eventos segue uma lei de potência, cuja principal característica é que os mecanismos dinâmicos que regulam a amplitude (pequena, intermediária e grande) do evento são os mesmos, o que implica na impossibilidade de previsão (CAVALCANTE et al., 2013). Essa imprevisibilidade é explorada na geração e distribuição de chaves criptográficas simétricas do sistema proposto na próxima seção.

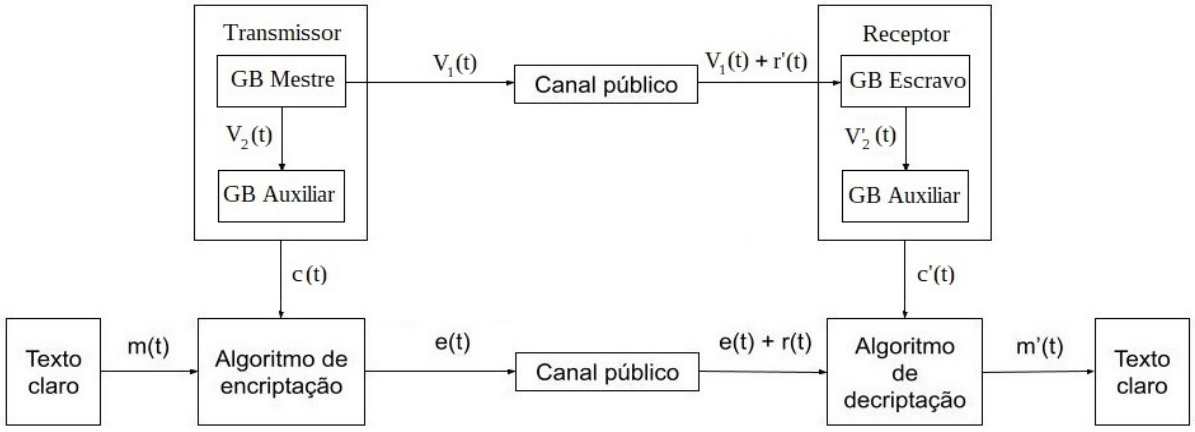
# 4 SISTEMA PROPOSTO DE GERAÇÃO E DISTRIBUIÇÃO DE CHAVES CRIPTOGRÁFICA SIMÉTRICAS

As seções anteriores foram dedicadas ao referencial teórico necessário para o desenvolvimento desta seção. Na seção 1 foi apresentada a proposta do presente trabalho, na seção 2 foram tratados dos conceitos básicos de criptografia e na seção 3 foi abordado o estudo da sincronização de sistemas caóticos, do sistema Gauthier-Bienfang e do acoplamento unidirecional de dois sistemas Gauthier-Bienfang quase-idênticos.

Nesta seção, propõe-se um sistema de geração e distribuição de chaves criptográficas simétricas, baseado em hardware, que utiliza a sincronização intermitente de circuitos eletrônicos caóticos acoplados para produzir chaves que atendam às premissas do *one-time pad*. Esta seção é o cerne do presente trabalho.

No sistema proposto, tanto o transmissor quanto o receptor são compostos por dois osciladores Gauthier-Bienfang quase-idênticos acoplados por meio da variável $V_2$. Por outro lado, a sincronização entre o transmissor e o receptor é feita por meio de $V_1$, conforme apresentado na Fig. 19. Dessa forma, a mesma chave criptográfica aleatória pode ser gerada no transmissor e no receptor por amostragem da evolução caótica temporal de $|x_\perp|$ - evento extremo. Essas chaves são então usadas para criptografar a mensagem no lado do remetente e decifrá-la no lado do destinatário. O sistema criptográfico proposto está mostrado na Fig. 19, com o módulo transmissor à esquerda e o módulo receptor à direita.

Figura 19 – Diagrama esquemático simplificado do sistema de geração e distribuição de chaves criptográficas simétricas, em que m(t) é o texto claro original, c(t) é a chave gerada no transmissor, e(t) é o texto encriptado, r(t) é o ruído gerado no canal que trafega a mensagem, c'(t) é a chave gerada no receptor, r'(t) é o ruído gerado no canal que trafega $V_1$(t) e m'(t) é o texto claro recuperado.




Fonte: Autor.

Um ponto fundamental a ser observado no sistema proposto é que as chaves não necessitam serem compartilhadas por meio do canal de comunicação privado, como geralmente ocorre nos esquemas de criptografia simétrica (STALLINGS, 2015).

As chaves são geradas de forma independente e simultaneamente no transmissor e no receptor, sem compartilhamento algum por qualquer meio de comunicação.

Como a chave binária é obtida a partir da variável $|x_\perp|$ e não é compartilhada no meio público de comunicação, os quatro requisitos do *one-time pad* estão atendidos, haja vista que o $|x_\perp|$ (eventos de dessincronização) ocorre indefinidamente, possui uma distribuição estatística de amplitude que segue uma lei de potências e, por fim, não guarda correlação alguma com a variável de sincronização ($V_1$) e com o texto claro. Observe que, devido ao fato de a variável $|x_\perp|$ não ser transmitida pelo meio de comunicação, qualquer tentativa de ataque que utiliza o texto cifrado ou a variável de sincronização para reconstruir o texto claro (SHORT, 1994) ou a chave, será frustrada, pelo simples fato de o texto cifrado ou a variável de sincronização não carregarem consigo qualquer tipo de informação relevante.

Vale destacar que o sistema proposto não apenas difere completamente dos métodos de mascaramento caótico aditivo (CUOMO; OPPENHEIM; STROGATZ, 1993) e de modulação caótica (ARGYRIS et al., 2005), mas também possui uma segurança mais robusta quando comparado com tais métodos, pois não se tem conhecimento de que o método do sistema proposto já tenha sido quebrado (YANG; WU; CHUA, 1997), ao passo que Short demonstrou a fragilidade dos métodos de mascaramento caótico aditivo em (SHORT, 1994) e de modulação caótica em (SHORT, 1996).

Em seguida, na subseção 4.1, a concepção do sistema é implementada numericamente e, na subseção 4.2, realiza-se a implementação experimental.

## 4.1 SIMULAÇÃO E RESULTADOS NUMÉRICOS

As equações de estado dos osciladores do transmissor do sistema proposto na Fig. 19 são dadas por

$$\dot{\mathbf{x}}_m = \mathbf{F}(\mathbf{x}_m) \quad e \tag{4.1}$$

$$\dot{\mathbf{x}}_A = \mathbf{F}(\mathbf{x}_A) + \alpha_2 \hat{E}_2(\mathbf{x}_m - \mathbf{x}_A), \tag{4.2}$$

e as do receptor por

$$\dot{\mathbf{x}}_e = \mathbf{F}(\mathbf{x}_e) + \alpha_1 \hat{E}_1(\mathbf{x}_m - \mathbf{x}_e) \quad e \tag{4.3}$$

$$\dot{\mathbf{x}}_B = \mathbf{F}(\mathbf{x}_B) + \alpha_2 \hat{E}_2(\mathbf{x}_e - \mathbf{x}_B), \tag{4.4}$$

em que $\mathbf{x}_i^T = (V_{1i}, V_{2i}, I_i)$, com $i = m, e, A, B$, denota a posição no espaço de fase *n*-dimensional dos osciladores mestre ($m$) e auxiliar do mestre ($A$), que compõem o transmissor, e escravo ($e$) e auxiliar do escravo ($B$), que compõem o receptor, **F**

representa o fluxo dos osciladores, $\alpha_i$, com $i = 1, 2$, é a força de acoplamento e $\hat{E}_i$, com $i = 1, 2$, é uma matriz de acoplamento $3$ x $3$.

A evolução dinâmica do sistema de Eqs. 4.1 - 4.4 foi obtida aplicando-se o método de Runge-Kutta de quarta ordem, com passo $dt = 0{,}1$, e impondo-se as seguintes condições: $\alpha_1 = 2{,}0$ e $E_{11} = 1{,}0$ e $E_{22} = E_{33} = E_{ij} = 0{,}0$, com $i \neq j$, para o acoplamento através de $V_1$; e $\alpha_2 = 1{,}0$ e $E_{22} = 1{,}0$ e $E_{11} = E_{33} = E_{ij} = 0{,}0$, com $i \neq j$, para o acoplamento através de $V_2$. Por oportuno, destaca-se que todo desenvolvimento numérico realizado neste trabalho utilizou a linguagem de programação python.

Consoante discutido na subseção 3.2, é sabido que o oscilador de Gauthier-Bienfang pode operar tanto caótica quanto periodicamente, a depender do resistor $R_2$, já que ele é o parâmetro do elemento não-linear e, consequentemente, possui grande influência no comportamento dinâmico do sistema, levando em consideração que todos os demais componentes são mantidos fixos.

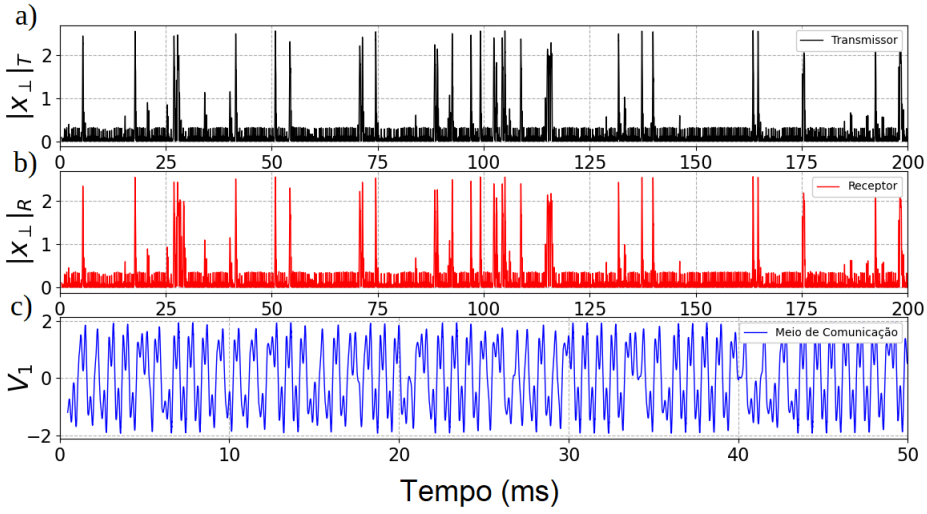
A fim de obter um $R_2$ que permita os quatro osciladores Gauthier-Bienfang operarem no regime caótico e gerarem séries temporais de $|x_\perp|$, no lado do transmissor e no lado do receptor, com a maior similaridade possível, adotou-se os seguintes valores adimensionais: $R_1 = 1{,}2$, $R_3 = 0{,}042$, $R_{dc} = 0{,}15$, $R_4 = R_3 + R_{dc} = 0{,}192$ e $R_2$ foi variado de $1{,}52$ a $4{,}00$, com passo de $0{,}04$. Além disso, foi permitido que os componentes de um oscilador em relação aos outros três possuíssem uma incompatibilidade de, no máximo, $1\%$, uma vez que na prática eles não são iguais. Vale salientar que os valores dos resistores aqui mencionados foram normalizados, conforme apresentado na subseção 3.2. Logo, na parte experimental, tais valores foram utilizados para encontrar os valores reais dos componentes que foram empregados no circuito experimental.

É fundamental para a geração de chaves de criptografia aleatórias, a partir da amostragem do traço de tempo caótico, o sistema trabalhar numa região caótica. Logo, a fim de se obter uma combinação de resistores tal que o sistema funcionasse em tal tipo de região, foram desenvolvidos quatro programas com as seguintes finalidades: 1) o primeiro programa foi implementado para gerar todas as combinações de resistores possíveis ao variar $R_2$ de $1{,}52$ a $4{,}00$, com passo de $0{,}04$; 2) o segundo programa executou a filtragem dessas combinações de resistores para obter apenas aquelas combinações em que a correlação cruzada tivesse valor superior a $90\%$; 3) o terceiro programa fez a filtragem para excluir aquelas combinações de resistores em que fazia o sistema trabalhar em regiões periódicas, a exemplo da Fig. 11(a), ficando apenas com resultados em que o sistema opera caoticamente (vide Fig. 11(b)). Nesta seção, utiliza-se o mesmo conjunto de valores de parâmetros utilizados na Fig. 11; e 4) o quarto programa testou a sensibilidade da combinação de resistores em relação a pequenas diferenças entre os parâmetros utilizados e às condições iniciais. Após isso, chegou-se a um conjunto com $15$ combinações de resistores, dentre as quais uma das combinações (a melhor, naturalmente) foi selecionada para implementar o sistema da

Fig. 19. A melhor combinação de resistores foi selecionada com base na correlação cruzada entre os sinais do transmissor e do receptor, ou seja, aquela combinação de resistores que forneceu a maior correlação cruzada foi a escolhida. A geração de dados numéricos requereu alto custo computacional e, em algumas ocasiões, foram necessárias vários dias para gerar esses dados. Apenas a título de exemplo, a geração do $|x_\perp|_T$ levou 6 dias e 18 horas.

Na Fig. 20, apresentam-se as séries temporais dos eventos de dessincronização do transmissor, $|x_\perp|_T$, e do receptor, $|x_\perp|_R$, bem como o sinal caótico transmitido pelo meio de comunicação público, $V_1$, para realizar a sincronização entre o transmissor e o receptor. Observe que, por meio de um sinal caótico (Fig. 20(c)), o transmissor e o receptor estão sincronizados, conforme demonstrado no retrato de fase da Fig. 21. É oportuno deixar claro que o retrato de fase é uma representação geométrica que mostra todas as diferenças qualitativas das trajetórias de um sistema dinâmico (STROGATZ, 2018). A reta diagonal com inclinação igual a 1, na Fig. 21, deixa claro que as trajetórias do transmissor e do receptor estão seguindo a mesma dinâmica, indicando que o transmissor e o receptor estão sincronizados.

Figura 20 – Séries temporais de: a) $|x_\perp|_T$ (sinal da chave do transmissor); b) $|x_\perp|_R$ (sinal da chave do receptor); e c) $V_1$ (sinal caótico de sincronização do transmissor e do receptor).




Fonte: Autor.

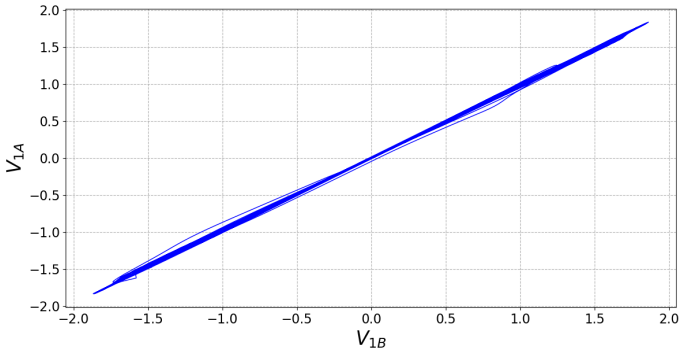
Observe que os sinais do transmissor e do receptor possuem boa similaridade, mostrando que as chaves geradas a partir de tais sinais devem possuir baixíssima taxa de erro, ao passo que o sinal do transmissor (ou receptor) possui série temporal completamente diversa da série temporal do sinal $V_1$. Destaca-se que os sinais do transmissor e do receptor que geram as chaves criptográficas são frutos do processo de perda de sincronização dos osciladores principais (mestre e escravo) e seus respectivos auxiliares. Além disso, vale ressaltar que todos os três sinais são caóticos, garantindo que as chaves geradas são imprevisíveis.

Para quantificar a qualidade da sincronização e, consequentemente, o grau de similaridade entre os sinais caóticos do transmissor e do receptor, calcula-se numericamente o valor absoluto da correlação cruzada entre $s_T(t) \equiv |x_\perp|_T$ e $s_R(t) \equiv |x_\perp|_R$,

$$C_{s_T,s_R}(\tau) = \left| \frac{< s_T(t) s_R(t+\tau) >}{\sigma_{s_T} \sigma_{s_R}} \right|, \tag{4.5}$$

em que $\sigma$ é o desvio padrão dos sinais e $\tau$ é o atraso temporal.

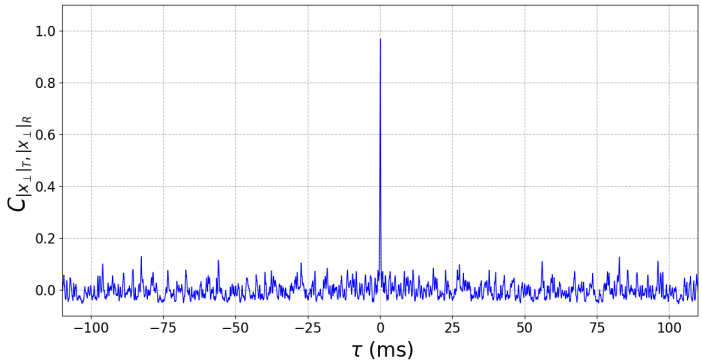
Figura 21 – Retrato de fase $V_{1A}$ x $V_{1B}$ da sincronização caótica entre o transmissor e o receptor.




Fonte: Autor.

Na Fig. 22, apresenta-se a $C_{|x_\perp|_T,|x_\perp|_R}(\tau) \equiv C_{s_T,s_R}(\tau)$ como uma função do atraso de tempo $\tau$. Para $\tau = 0$, a correlação cruzada encontra seu máximo valor $C_{|x_\perp|_T,|x_\perp|_R}(0) \approx 0{,}97$, o que indica alto grau de similaridade e a possibilidade de extrair sequências de bits idênticos da série temporal do emissor e do receptor, como é mostrado mais adiante. Para $\tau \neq 0$, a correlação cruzada vai ao nível de ruído, indicando claramente que os sinais se aproximam de dois sinais aleatórios.

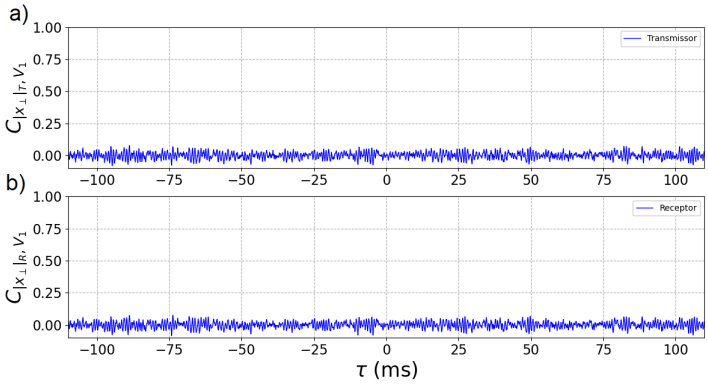
Figura 22 – Correlação cruzada entre o transmissor e o receptor, $C_{|x_\perp|_T,|x_\perp|_R}(\tau)$.




Fonte: Autor.

Ao mesmo tempo, conforme Fig. 23, a correlação cruzada entre transmissor (ou receptor) e o sinal $V_1$, que trafega pelo meio público, permanece no nível de ruído independente de $\tau$. Logo, é impossível se extrair alguma informação da chave do transmissor (ou receptor) a partir do sinal de $V_1$.

Figura 23 – Correlação cruzada: a) entre $C_{|x_\perp|_T,V_1}(\tau)$; e b) entre $C_{|x_\perp|_R,V_1}(\tau)$.




Fonte: Autor.

Do gráfico da Fig. 23, veja que não há picos visíveis na correlação cruzada, indicando que a informação compartilhada entre transmissor e o sinal $V_1$ é comparável a de dois sinais completamente aleatórios, garantindo assim a segurança da chave.

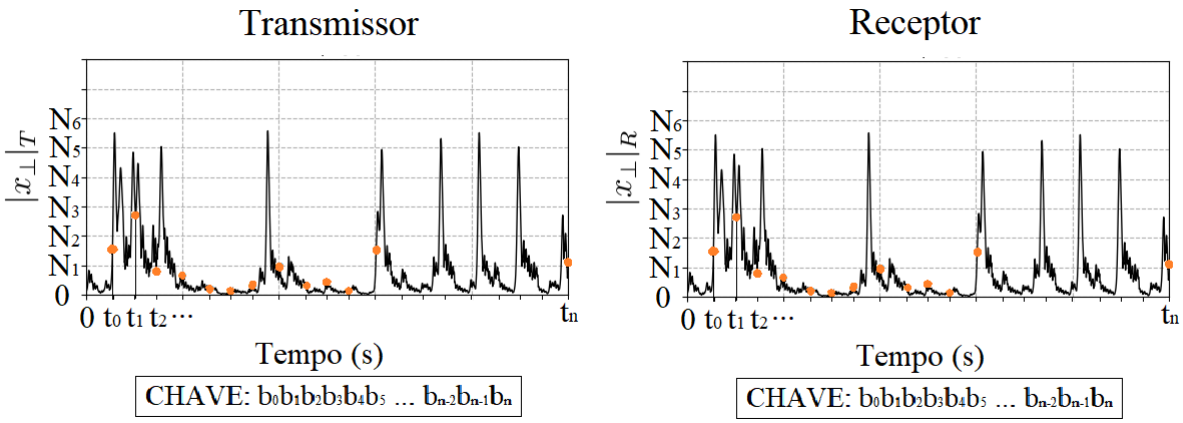
O próximo passo é gerar as chaves criptográficas a partir dos sinais caóticos, o que pode ser realizado de diversas formas, a exemplo de (ITO et al., 2017) e (KEUNINCKX et al., 2017). No presente trabalho, no entanto, optou-se por desenvolver um programa que implementasse o seguinte processo: a partir da amostragem da amplitude dos sinais de $|x_\perp|_T$ e $|x_\perp|_R$ em intervalos de tempo iguais, uma sequência de três bits é gerada para cada ponto amostrado. O transmissor comanda o início do processo de amostragem através de um pulso enviado ao receptor. Para entender a ideia de geração da chave, é necessário analisar a Fig. 24 em conjunto com a Tabela 1. Observando a Fig. 24, no instante $t_0$, quando realizada a primeira amostragem, a amplitude de $|x_\perp|$ está entre os níveis $N_1$ e $N_2$, indicado pelo ponto vermelho. Ao consultar a Tabela 1, verifica-se que os bits $b_0b_1b_2$ estão entre os níveis $N_1$ e $N_2$. Logo, a sequência de bits $b_0b_1b_2$ é gerada. Em $t_1$, a amplitude de $|x_\perp|$ está entre os níveis $N_2$ e $N_3$, o que dá origem a sequência $b_3b_4b_5$, já que esses são os bits que estão entre os níveis $N_2$ e $N_3$ na Tabela 1. O processo segue assim sucessivamente e indefinidamente, gerando fluxos de bits e, por consequência, chaves de tamanho infinito e sem repetição, haja vista que os bits da chave são gerados de uma série temporal caótica.

Destaca-se que esse processo de gerar chave pode ser tão complexo quanto se queira, mas, obviamente, isso tem implicações na velocidade de geração da chave, além de exigir um maior custo computacional.

Na parte numérica, a Tabela 2 foi utilizada para converter as amplitudes de $|x_\perp|_T$ e $|x_\perp|_R$ na chave binária do transmissor e do receptor, respectivamente. Isto quer dizer que, se a amplitude amostrada de $|x_\perp|$ for maior ou igual a $1{,}5$ e menor que $2{,}0$, a sequência de bits gerada será $100$.

Para aumentar a segurança, antes de ser utilizada, a chave foi submetida a dois

Figura 24 – Diagrama esquemático do processo de geração de chave a partir dos sinais caóticos de $|x_\perp|_T$ e $|x_\perp|_R$. Os pontos vermelhos indicam onde os sinais foram amostrados.




Fonte: Autor.

Tabela 1 – Conversão de amplitude de $|x_\perp|$ em chave binária

| Níveis | Sequência de bits |
|---|---|
| $N_1 \leq \|x_\perp\| < N_2$ | $b_0 b_1 b_2$ |
| $N_2 \leq \|x_\perp\| < N_3$ | $b_3 b_4 b_5$ |
| $N_3 \leq \|x_\perp\| < N_4$ | $b_6 b_7 b_8$ |
| $N_4 \leq \|x_\perp\| < N_5$ | $b_9 b_{10} b_{11}$ |
| $N_5 \leq \|x_\perp\| < N_6$ | $b_{12} b_{13} b_{14}$ |
| $N_6 \leq \|x_\perp\| < N_7$ | $b_{15} b_{16} b_{17}$ |

Fonte: Autor.

Tabela 2 – Conversão de amplitude de $|x_\perp|$ em chave binária da parte numérica

| Níveis | Sequência de bits |
|---|---|
| $0{,}0 \leq \|x_\perp\| < 0{,}5$ | 011 |
| $0{,}5 \leq \|x_\perp\| < 1{,}0$ | 110 |
| $1{,}0 \leq \|x_\perp\| < 1{,}5$ | 001 |
| $1{,}5 \leq \|x_\perp\| < 2{,}0$ | 100 |
| $2{,}0 \leq \|x_\perp\| < 2{,}5$ | 010 |
| $2{,}5 \leq \|x_\perp\| < 3{,}0$ | 101 |

Fonte: Autor.

estágios de rotação de bits e operação ou-exclusivo bit a bit. No primeiro estágio, uma cópia da chave original foi realizada e, em seguida, os primeiros $113$ bits dessa cópia foram rotacionados. Por fim, essa nova sequência de bits foi submetida a uma operação ou-exclusivo com a chave original. No segundo estágio, uma cópia da sequência de bits resultante do primeiro estágio foi realizada e, em seguida, foi feita uma rotação de $547$ bits. Por fim, essa nova sequência de bits foi submetida a uma operação ou-exclusivo com a sequência de bits resultante do primeiro estágio. A escolha do número de bits rotacionados foi arbitrária e pode ser um dos segredos para tornar o

sistema mais seguro. Esse tipo de operação de pós-processamento é muito comum em propostas de geradores de números aleatórios (BÖHM et al., 2020). Isso aumentou consideravelmente a segurança da chave sem impactar na eficiência de sua geração.

Para avaliar o grau de similaridade entre as chaves do transmissor e do receptor, foi calculada a taxa de erro de bit (Bit Error Rate - BER), que corresponde ao número de bits incompatíveis em uma sequência de 56 milhões de bits, aproximadamente. Em média, o BER encontrado foi de aproximadamente 0,0096 ± 0,0001, demonstrando que a probabilidade de os bits serem similares é próximo de 99,9%. Da mesma forma, foi calculada também a taxa de erro de bit entre as chaves do transmissor e do meio de comunicação, cujo o BER obtido foi de aproximadamente 0,500005 ± 0,000001 em média, demonstrando que a probabilidade de os bits serem similares é praticamente a mesma de eles serem diferentes. Vale ressaltar que tais resultados estão de acordo com as correlações cruzadas apresentadas nas Fig. 22 e Fig. 23, respectivamente.

Todo sistema criptográfico que se preze deve gerar chaves criptográficas preferencialmente aleatórias. Logo, para avaliar a aleatoriedade da chave gerada pelo sistema proposto, a suíte de testes estatísticos do *National Institute of Standards and Technology* (NIST) (BASSHAM et al., 2010) foi utilizada. A suíte do NIST é uma bateria de 15 (quinze) testes estatísticos consolidados que aponta o quanto a chave gerada se desviou da aleatoriedade de uma chave genuinamente aleatória.

Sabe-se que o sistema criptográfico proposto não é Gerador de Números Aleatórios (ou *Random Numbers Genarator* - RNG, em inglês), e sim um Geradores de Números Pseudoaleatórios (ou *Pseudo-Random Numbers Genarator* - PRNG, em inglês), pois os sistemas caóticos são por natureza determinísticos. Ainda assim, dado a imprevisibilidade de seu comportamento dinâmico, eles podem gerar chaves criptográficas bastante próximas de chaves intrinsecamente aleatórias, consoante demonstra os resultados apresentados na Tabela 3.

O teste do NIST foi realizado a partir de uma sequência de 56 milhões de bits. Para cada teste, foi adotado um comprimento da sequência de bits (n) específico, consoante Tabela 3. Cada um dos 15 testes foi executado 55 vezes para que pudesse possuir relevância estatística, conforme preconizado em (BASSHAM et al., 2010). A taxa de aprovação mínima para cada teste estatístico é de aproximadamente 52 para um tamanho de amostra de 55 sequências binárias, com exceção do teste de excursão aleatória e variante de excursão aleatória, cuja taxa de aprovação mínima é de aproximadamente 32 para um tamanho de amostra de 35 sequências binárias. Além disso, o *Valor-p* para cada teste estatístico deve ser maior que 0,01. Um teste com *Valor-p* < 0,01 é considerado reprovado e, consequentemente, a sequência binária em teste deve ser considerada como não aleatória. Nos casos em que várias instâncias de um único teste foram realizadas (por exemplo, somas cumulativas), apenas o pior resultado foi apresentado na Tabela 3. Os testes que exigem parâmetros de entrada

Tabela 3 – Resultados numéricos obtidos a partir do conjunto de testes de aleatoriedade do NIST

| Teste | Valor-p | Aprovação | n |
|---|---|---|---|
| Frequência (Monobit) | 0,102526 | 55/55 | $10^4$ |
| Frequência dentro de um bloco (M = 128) | 0,249284 | 54/55 | $10^4$ |
| Corrida | 0,162606 | 55/55 | $10^4$ |
| A corrida mais longa de 1's em um bloco | 0,129620 | 55/55 | $10^4$ |
| Classificação da matriz binária | 0,678686 | 55/55 | $10^5$ |
| Transformada discreta de Fourier (espectral) | 0,021999 | 55/55 | $10^5$ |
| Não-sobreposição de modelo (m = 9) | 0,048716 | 52/55 | $10^5$ |
| Sobreposição de de modelo (m = 9) | 0,719747 | 55/55 | $10^5$ |
| "Estatístico Universal" de Maurer | 0,401199 | 55/55 | $10^6$ |
| Complexidade linear (M = 500) | 0,595549 | 55/55 | $10^5$ |
| Serial (m = 16) | 0,162606 | 55/55 | $10^5$ |
| Entropia aproximada (m = 5) | 0,129620 | 55/55 | $10^4$ |
| Somas cumulativas (Cusum) | 0,401199 | 55/55 | $10^4$ |
| Excursões aleatórias | 0,500934 | 34/35 | $10^6$ |
| Variante de excursões aleatórias | 0,090936 | 34/35 | $10^6$ |

Fonte: Autor.

estão com os respectivos valores dos parâmetros entre parênteses ao lado do seu nome. Diante dos resultados apresentados na Tabela 3, conclui-se que os bits gerados pelo sistema proposto não mostram sinais de desvio da aleatoriedade.

Por fim, é imprescindível que o sistema proposto garanta que a distribuição das chaves seja totalmente segura contra espionagem. Nesse esquema de distribuição, a única informação compartilhada entre o emissor e o receptor por meio do canal público é $V_1$. Um invasor ouvindo o canal público pode então capturar o sinal de $V_1$ e gerar sua própria chave por amostragem do sinal de $V_1$. Portanto, é importante que nenhuma informação sobre a chave esteja contida em $V_1$. Da Fig. 23, verifica-se de imediato que há pouca correlação entre o sinal do transmissor, $|x_\perp|_T$, e o sinal compartilhado no canal público, $V_1$, no caso sincronizado. Para determinar quanta informação sobre a chave do remetente, $C_T(t)$, pode ser obtida da chave extraída do sinal de $V_1$, $C_{V_1}(t)$, calcula-se a informação mútua

$$I(C_T,C_{V_1}) = \sum_{y\in C_{V_1}} \sum_{x\in C_T} p(x,y) \log \frac{p(x,y)}{p(x)p(y)}, \tag{4.6}$$

em que $p(x,y)$ é a distribuição de probabilidade conjunta de $C_T$ e $C_{V_1}$, e $p(x)$ e $p(y)$ são funções de probabilidade de distribuição marginal de $C_T$ e $C_{V_1}$, respectivamente. A informação mútua é igual a $0$ para duas chaves não correlacionadas e igual a $1$ para duas chaves idênticas. A partir de cálculos numéricos, a distribuição de probabilidade

conjunta $p_{C_T,C_{V_1}}(x,y) = p(C_T = x|C_{V_1} = y)$, com $x, y \in 0, 1$, obtida foi

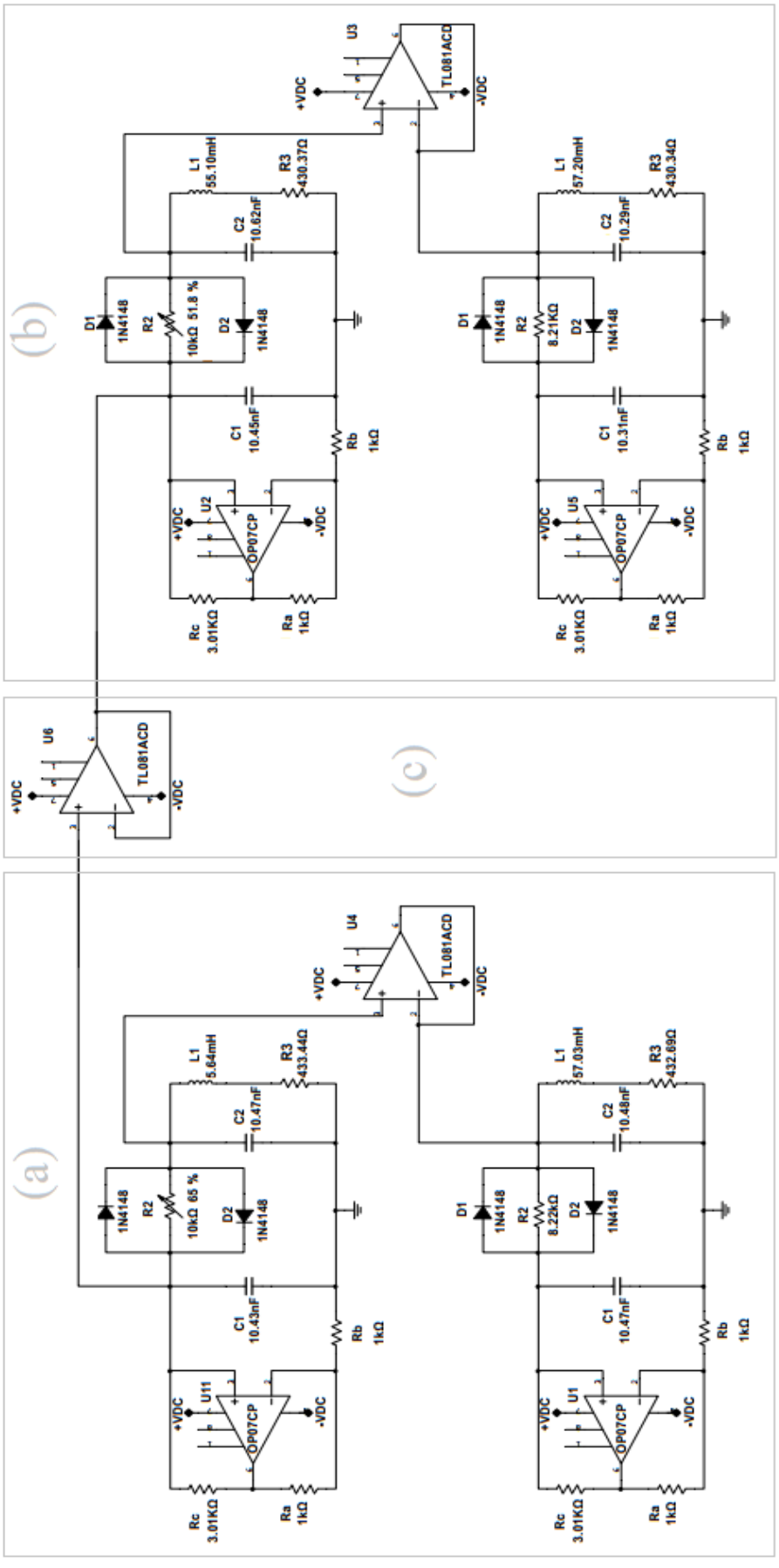
$$p_{C_T,C_{V_1}}(x,y) = \begin{pmatrix} 0{,}2382 & 0{,}2379 \\ 0{,}2621 & 0{,}2617 \end{pmatrix}. \tag{4.7}$$

Da distribuição de probabilidade conjunta, verifica-se que a probabilidade de haver similaridade entre $C_T(t)$ e $C_{V_1}(t)$ é exatamente a mesma de não haver o que é esperado para duas variáveis aleatórias independentes. A informação mútua entre $C_T$ e $C_{V_1}$ é $I_{C_T,C_{V_1}} = 2{,}99$ x $10^{-10}$, mostrando que, mesmo no caso de um atacante ser capaz de obter alguma chave do meio de comunicação a partir do sinal de $V_1$, ainda assim, quase nenhuma informação ele obterá da chave do remetente.

Na próxima subseção, implementa-se experimentalmente o sistema de geração e distribuição de chaves criptográficas simétrica proposto na Fig. 19 para que se possa verificar experimentalmente a validade dos resultados numéricos.

## 4.2 IMPLEMENTAÇÃO E RESULTADOS EXPERIMENTAIS

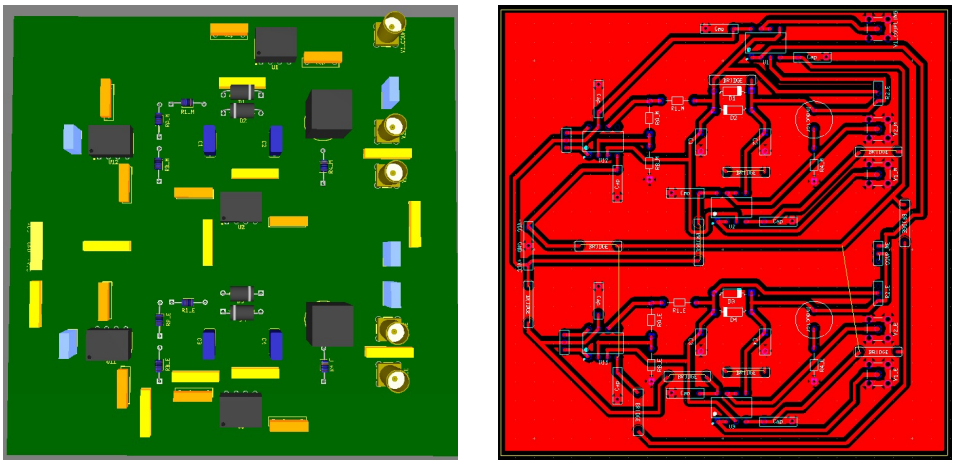
Os excelentes resultados numéricos encorajaram a implementação experimental do sistema proposto na Fig. 19, a fim de verificar seu funcionamento na prática. No entanto, destaca-se que, antes de as placas do transmissor e do receptor serem construídas, o diagrama elétrico do sistema proposto (Fig. 25) foi projetado e o funcionamento do sistema foi simulado utilizando o programa Multisim 14.1, da *National Instruments*. No transmissor (Fig. 25(a)), o oscilador mestre é o circuito mostrado na parte superior do diagrama e seu auxiliar é o apresentado na parte inferior (vide Fig. 25(a)). No receptor (Fig. 25(b)), o oscilador escravo é o circuito mostrado na parte superior do diagrama e seu auxiliar é o apresentado na parte inferior (vide Fig. 25(b)). O transmissor e o receptor estão acoplados através de uma *buffer* (Fig. 25(c)), que representa o meio de comunicação no diagrama elétrico. Diante dos resultados animadores da simulação no Multisim, ainda utilizando o citado programa, a placa da Fig. 26 foi desenhada para, em seguida, ser usinada com a máquina de prototipagem ProtoMat S63, da LPKF Laser $\&$ Electronics. Na Fig. 27, a placa usinada é apresentada. Por fim, os componentes eletrônicos (capacitores, indutores e resistores) foram testados, selecionados e soldados na placa. Optou-se por não montar os conectores BNC para minimizar o custo do projeto. Na Fig. 28, mostram-se as placas do transmissor e do receptor construídas especificamente para o desenvolvimento do presente trabalho, bem como o retrato de fase $V_{1A}$ x $V_{1B}$, cujo plote na tela do osciloscópio mostra claramente um reta diagonal de inclinação igual a $1$, típica de sistemas sincronizados.




Fonte: Autor.

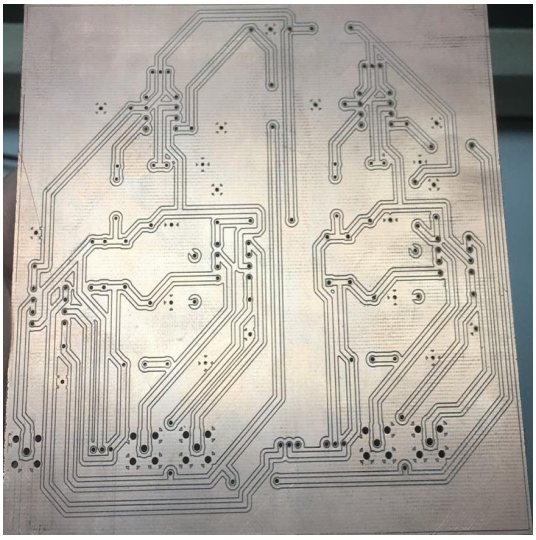
Figura 25 – Diagrama elétrico do sistema de geração e distribuição de chaves criptográficas simétricas, com os circuitos: (a) do transmissor; (b) do receptor; e (c) do meio de comunicação.

Figura 26 – Visão dos componentes em 3D e das trilhas na placa desenhada no Multisim 14.1.



Fonte: Autor.

Figura 27 – Placa usinada na máquina de prototipagem ProtoMat S63, da LPKF Laser & Electronics.

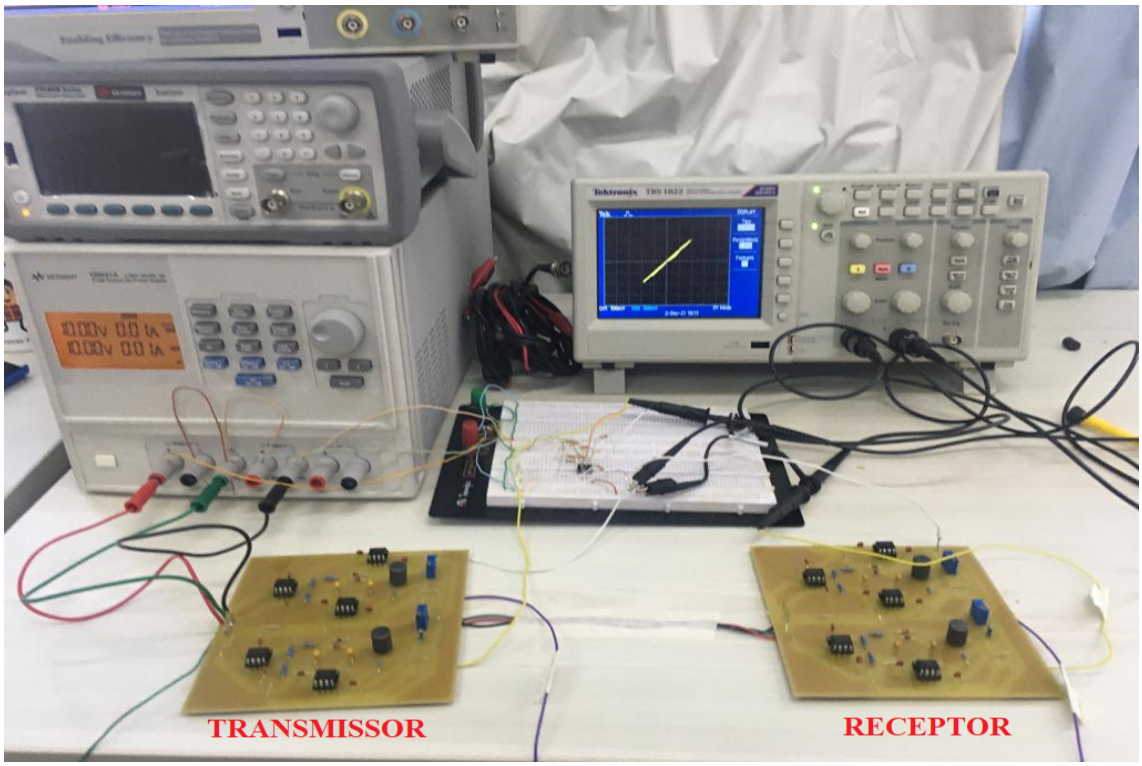


Fonte: Autor.

Na montagem experimental, todos os componentes do sistema foram mantidos fixos, exceto os resistores $R_2$ dos osciladores mestre e escravo, que foram utilizados para realizar um ajuste fino na operação do sistema, de tal forma que passasse a operar numa região caótica e gerasse chaves com a maior similaridade possível. Na Tabela 4, são apresentados os componentes utilizados na construção do sistema. Os componentes foram selecionados de forma que não possuíssem mais do que $1\%$ de tolerância entre eles, exceto naturalmente $R_2$, que foi utilizado para ajustar a operação do sistema.

A aquisição dos dados foi obtida através da placa NI USB-6211 (16 Inputs, 16-bit, 250 kS/s, Multifunction I/O), da National Instruments, com uma frequência de amostragem de f = 40 kS/s, do programa LabVieW e do osciloscópio TBS 1072B (70 MHz, 1 GS/s), da Tektronix.

Figura 28 – Placas do transmissor e do receptor sincronizadas por meio de $V_1$, conforme demonstra o retrato de fase apresentado na tela do osciloscópio.




Fonte: Autor.

Tabela 4 – Componentes utilizados na montagem dos circuitos

| | **Transmissor** | | **Receptor** | |
|---|---|---|---|---|
| | **Pricipal** | **Auxiliar** | **Pricipal** | **Auxiliar** |
| $C_1$ | 10,43 nF | 10,47 nF | 10,45 nF | 10,31 nF |
| $C_2$ | 10,47 nF | 10,48 nF | 10,62 nF | 10,29 nF |
| $L$ | 56,64 mH | 57,03 mH | 55,10 mH | 57,20 mH |
| $R_{dc}$ | 44,28 Ω | 44,00 Ω | 42,82 Ω | 42,91 Ω |
| $R_1$ | 3,01 kΩ | 3,01 kΩ | 3,01 kΩ | 3,01 kΩ |
| $R_2$ | 6,50 kΩ | 8,22 kΩ | 5,18 kΩ | 8,21 kΩ |
| $R_3$ | 389,16 Ω | 388,69 Ω | 387,55 Ω | 387,43 Ω |

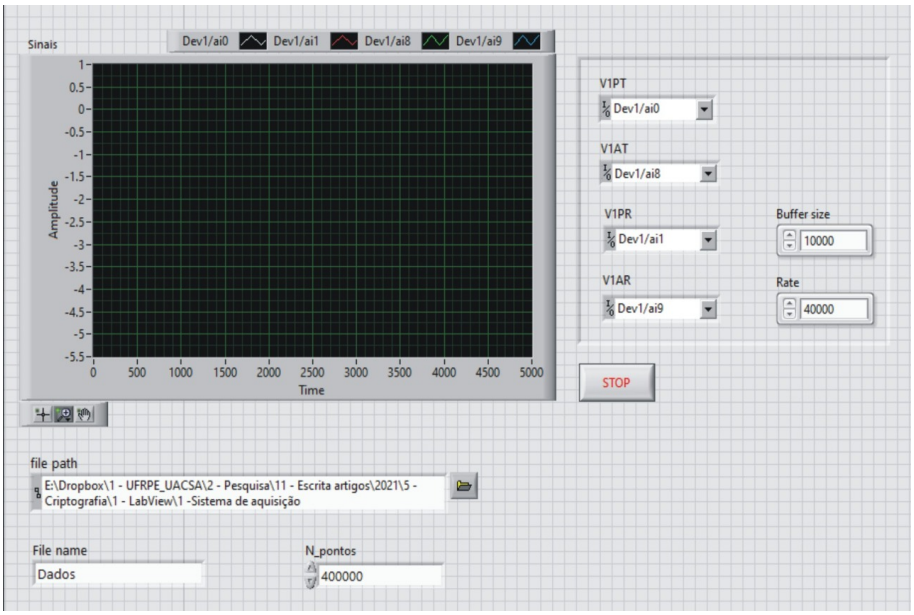
Fonte: Autor.

O LabView é um programa baseado em uma linguagem de programação gráfica, denominada de linguagem G, e na interconexão de blocos, denominados de VIs. Tais blocos possuem desde funções básicas, como simples operações algébricas ou booleanas, até funções mais complexas como métodos de integração, comunicação serial, dentre outras.

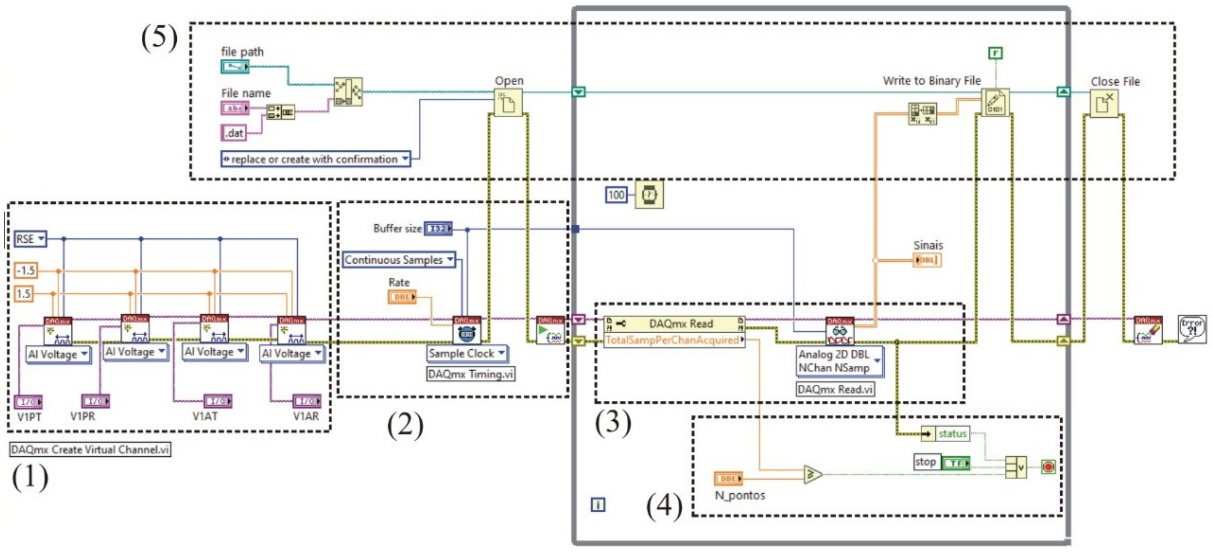
Na Fig. 29(a), apresenta-se a interface por meio da qual o usuário pode visualizar os dados adquiridos, configurar os canais da placa de aquisição que serão utilizados e definir o nome do arquivo a ser salvo e o local de armazenamento. Na Fig. 29(b), traz-se o diagrama em blocos do programa. Nela, tem-se: em (1) são alocados e configurados os canais a serem usados, definindo-se um intervalo máximo e mínimo de tensão a

Figura 29 – (a) Interface Homem-Máquina do LabView; e (b) Diagrama em blocos do programa desenvolvido para adquirir e salvar os dados.

(a)




(b)



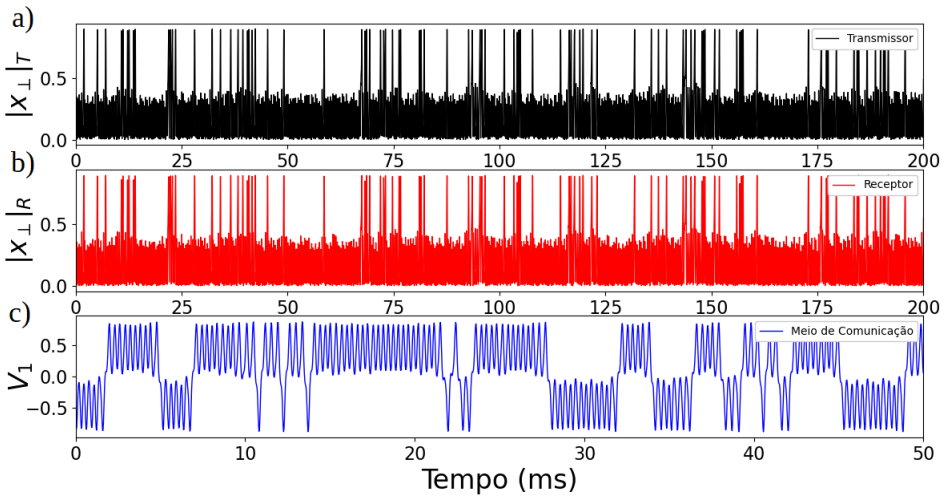

Fonte: Autor.

ser adquirida. Em (2) são configurados a taxa de aquisição, o tamanho do *buffer* e o ponto onde inicia o processo de aquisição de dados. As etapas (3) e (4) são inseridas dentro de um laço condicional que irá atuar até que a condição estabelecida em (4) seja satisfeita, ou seja, até que o número de pontos adquirido por canal seja igual ao da variável **N_ponto** estabelecida pelo usuário na interface. (3) é o bloco responsável por adquirir os dados e contar o número de pontos adquiridos. Já (5) corresponde a etapa de salvar os dados. Inicialmente é criado um arquivo e os dados adquiridos em (4) são enviados para o bloco Write to Binary File, sendo salvos no formado binário

possibilitando manter uma alta taxa de aquisição.

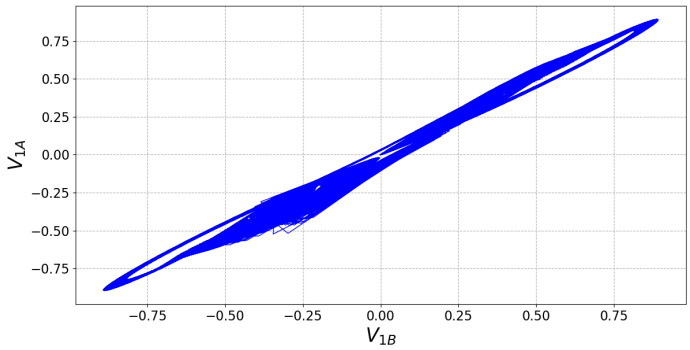
Na Fig. 30, apresentam-se as séries temporais dos eventos de dessincronização do transmissor, $|x_\perp|_T$, e do receptor, $|x_\perp|_R$, e o sinal $V_1$ (caótico). Ressalta-se que, para o resultado obtido, foi verificado que o sistema de fato estava operando no regime caótico. A partir daí, foi observado que o transmissor e o receptor estavam sincronizados caoticamente, consoante apresentado no retrato de fase da Fig. 31.

Figura 30 – Séries temporais: a) de $|x_\perp|_T$ (sinal da chave do transmissor); b) de $|x_\perp|_R$ (sinal da chave do receptor); e c) de $V_1$.




Fonte: Autor.

Figura 31 – Retrato de fase $V_{1A}$ x $V_{1B}$ da sincronização caótica entre o transmissor e o receptor.



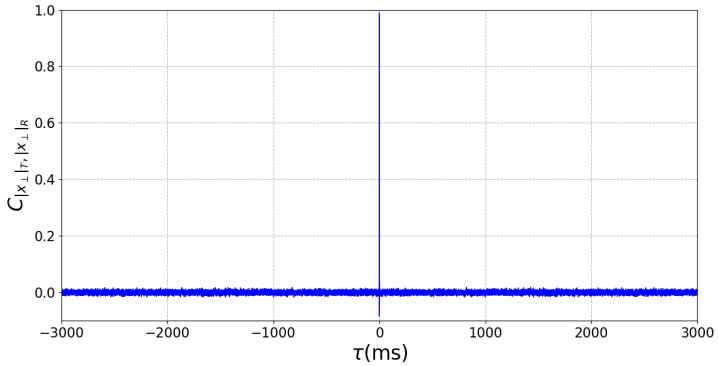

Fonte: Autor.

Verifica-se que os sinais do transmissor e do receptor na parte experimental possuem boa similaridade, ao passo que o sinal do transmissor (ou receptor) possui série temporal completamente diversa da série temporal do sinal $V_1$.

Para colocar em números essa similaridade, da Fig. 32, extrai-se que, para $\tau = 0$, a correlação cruzada entre o transmissor e o receptor encontra seu máximo valor em $0{,}99$, ou seja, $C_{|x_\perp|_T,|x_\perp|_R}(0) \approx 0{,}99$. Para $\tau \neq 0$, $C_{|x_\perp|_T,|x_\perp|_R}(\tau)$ está no nível de ruído. Da Fig. 33, verifica-se que, seja para $\tau = 0$ ou $\tau \neq 0$, a correlação cruzada

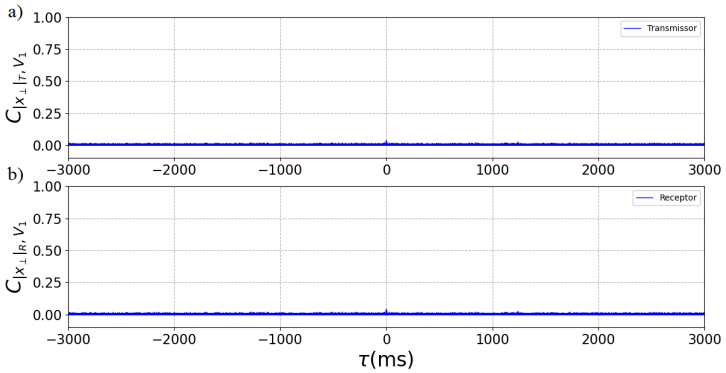
entre transmissor (ou receptor) e o sinal $V_1$ está no nível de ruído como esperado. Com isso, conclui-se que é possível extrair sequências de bits idênticos da série temporal do emissor e do receptor, ao passo que é muito baixa a probabilidade de se conseguir extrair algum tipo de informação relevante da sequência de bits da chave a partir do sinal de $V_1$.

Figura 32 – Correlação cruzada entre o transmissor e o receptor, $C_{|x_\perp|_T,|x_\perp|_R}(\tau)$.




Fonte: Autor.

Figura 33 – Correlação cruzada: a) entre $C_{|x_\perp|_T,V_1}(\tau)$; e b) entre $C_{|x_\perp|_R,V_1}(\tau)$.

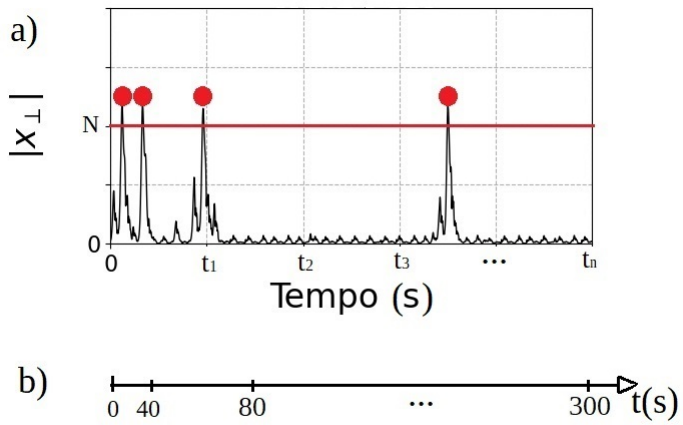



Fonte: Autor.

Na parte experimental, foi utilizado um processo diferente para converter as amplitudes de $|x_\perp|_T$ e $|x_\perp|_R$ na chave binária do transmissor e do receptor, respectivamente, dado ao processo utilizado na parte numérica não ter se mostrado eficaz na geração das chaves a partir dos dados experimentais. As chaves geradas apresentaram elevada taxa de erro e não passaram no teste de aleatoriedade do NIST. Logo, repensar o processo da parte numérica foi necessário. A forma encontrada para resolver os problemas supracitados foi implementar um novo programa que executasse o seguinte processo: acima do nível de corte (N) (vide Fig. 34(a)), detecta-se todas as amplitudes e mede-se a distância temporal entre uma determinada amplitude e a amplitude seguinte, da primeira à última. Em seguida, enquadra-se essa distância na escala exponencial da Fig. 34(b), que possui 40 subintervalos no intervalo de 0 a 300 s. Esses subintervalos serão utilizados para converter o valor decimal da distância temporal das amplitudes

numa sequência binária de 8 bits. Por fim, com base no subintervalo que acomodou a distância temporal das amplitudes, transforma-se o valor superior desse subintervalo no número binário correspondente. Por exemplo, se o tempo medido entre duas amplitudes consecutivas for de 56 s, esse valor está no subintervalo entre 40 s e 80 s, logo o valor superior do subintervalo (80) deve ser convertido no número binário 01010000. A escala exponencial foi necessária porque os valores das distâncias das amplitudes dos eventos de dessincronização não possuem uma distribuição uniforme no caso concreto. Além disso, foi observado que as distâncias temporais das amplitudes dos eventos de dessincronização acima de 300 s são raras. Assim, elas foram enquadradas no último subintervalo, que tem como valor superior 300, em binário 100101100. Além disso, assim como foi realizado na parte numérica, a chave foi submetida a dois estágios de rotação de bits e operação ou-exclusivo bit a bit para aumentar a segurança.

Figura 34 – Diagrama esquemático do processo de geração de chave a partir dos sinais caóticos de $|x_\perp|_T$ e $|x_\perp|_R$. Os pontos vermelhos indicam as amplitudes acima do nível de corte (N) detectadas.




Fonte: Autor.

Quanto à similaridade das chaves do transmissor e do receptor, em média, o BER encontrado foi de 0,106 ± 0,001. Embora o BER esteja um pouco alto, ainda assim a geração de chave síncrona é possível, usando códigos de correção de erro. Já o BER entre as chaves do transmissor e do meio de comunicação foi de aproximadamente 0,500 ± 0,001 em média, demonstrando que a probabilidade de os bits serem similares é praticamente a mesma de eles serem diferentes, conforme explicado na subseção 4.1. Vale ressaltar que tais resultados estão de acordo com as correlações cruzadas apresentadas nas Fig. 32 e Fig. 33, respectivamente.

O teste do NIST também foi aplicado a partir de uma amostra de 56 milhões de bits e o resultado está apresentado na Tabela 5. As condições do teste com os dados experimentais são exatamente as mesmas do teste com os dados numéricos.

Diante dos resultados apresentados na Tabela 5, conclui-se que os bits gerados pelo sistema proposto não mostram sinais de desvio da aleatoriedade significativos.

Tabela 5 – Resultados experimentais obtidos a partir do conjunto de testes de aleatoriedade do NIST

| Teste | Valor-p | Aprovação | n |
|---|---|---|---|
| Frequência (Monobit) | 0,678686 | 54/55 | $10^4$ |
| Frequência dentro de um bloco (M = 128) | 0,048716 | 55/55 | $10^4$ |
| Corrida | 0,678686 | 53/55 | $10^4$ |
| A corrida mais longa de 1's em um bloco | 0,759756 | 54/55 | $10^4$ |
| Classificação da matriz binária | 0,987896 | 55/55 | $10^5$ |
| Transformada discreta de Fourier (espectral) | 0,249284 | 54/55 | $10^5$ |
| Não-sobreposição de modelo (m = 9) | 0,102526 | 52/55 | $10^5$ |
| Sobreposição de de modelo (m = 9) | 0,202268 | 55/55 | $10^5$ |
| "Estatístico Universal" de Maurer | 0,080519 | 55/55 | $10^6$ |
| Complexidade linear (M = 500) | 0,798139 | 53/55 | $10^5$ |
| Serial (m = 16) | 0,145326 | 54/55 | $10^5$ |
| Entropia aproximada (m = 5) | 0,249284 | 54/55 | $10^4$ |
| Somas cumulativas (Cusum) | 0,401199 | 55/55 | $10^4$ |
| Excursões aleatórias | 0,162606 | 12/13 | $10^6$ |
| Variante de excursões aleatórias | 0,012650 | 13/13 | $10^6$ |

Fonte: Autor.

A distribuição de probabilidade conjunta $p_{C_T,C_{V_1}}(x,y) = p(C_T = x|C_{V_1} = y)$, com $x, y \in 0, 1$, das chaves obtidas experimentalmente foi

$$p_{C_T,C_{V_1}}(x,y) = \begin{pmatrix} 0{,}2584 & 0{,}2429 \\ 0{,}2572 & 0{,}2415 \end{pmatrix}. \tag{4.8}$$

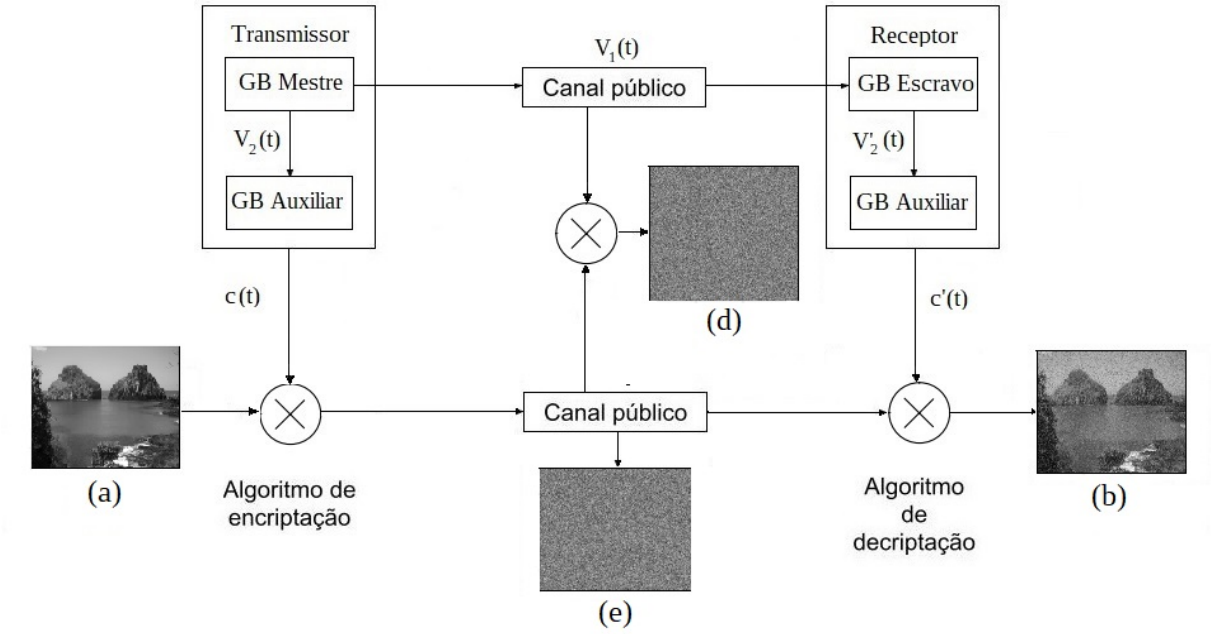
Logo, verifica-se que a probabilidade de haver similaridade entre $C_T(t)$ e $C_{V_1}(t)$ é exatamente a mesma de não haver, o que é esperado para duas variáveis aleatórias independentes. Para a informação mútua entre $C_T$ e $C_{V_1}$, obteve-se $I_{C_T,C_{V_1}} = 1{,}11$ x $10^{-7}$, mostrando que, mesmo no caso de um espião ser capaz de obter alguma chave do meio de comunicação a partir do sinal de $V_1$, ainda assim, muito pouca informação ele obterá da chave do remetente.

Agora, utilizando a chave obtida experimentalmente e a imagem de uma paisagem em branco e preto, o funcionamento do sistema de encriptação e decriptação está demonstrado na Fig. 35. A versão em tons de cinza da imagem consiste em 512 × 512 pixels de 8 bits, logo, demanda uma chave de criptografia de 2.097.152 bits.

Com a mensagem (a) e a chave de encriptação c(t) como entradas, o algoritmo de encriptação, operação XOR, produz o texto encriptado (e). O destinatário, de posse do texto encriptado (e) e da chave c'(t), é capaz de inverter a transformação e obter (b). Um atacante, acessando (e) e gerando uma chave a partir de $V_1$, após realizar uma operação XOR, obterá (d).

Outro detalhe importante: um atacante, acessando (e), mas não tendo acesso a c(t) ou (a), pode tentar recuperar (a) ou c(t), ou ambos. Contudo, não terá sucesso, mesmo considerando que ele tenha conhecimento dos algoritmos de encriptação e

Figura 35 – Demonstração do esquema de criptografia e descriptografia a partir da imagem de uma paisagem utilizada como mensagem.




Fonte: Autor.

decriptação.

Observe que a qualidade da imagem não está muito boa (porém ainda inteligível), o que já era esperado devido a taxa de erro apresentada pelas chaves do transmissor e do receptor na parte experimental. A mensagem recuperada será tão fidedigna à mensagem original quanto menor for a incompatibilidade entre as chaves do transmissor e do receptor. Supõe-se que o ruído esteja contribuindo de maneira decisiva para esse resultado, já que, na intenção de estudar o sistema em um cenário de adversidade, nenhum tipo de blindagem foi colocada no transmissor e no receptor para mitigar os efeitos do ruído no sistema.

Baseado nas evidências dos resultados numéricos e experimentais, realiza-se uma ampla discussão de tais resultados na próxima seção.

# 5 DISCUSSÃO DOS RESULTADOS NUMÉRICOS E EXPERIMENTAIS

Foi demonstrado numérica e experimentalmente que é possível gerar sinais de dessincronização com alta correlação (> 90%) tanto no circuito transmissor quanto no circuito receptor do sistema proposto na Fig. 19. Esse não é um resultado trivial, pois não se sabia como se comportariam as trajetórias dos sistemas sincronizados a partir da quebra da sincronização. No entanto, a partir dos resultados obtidos, verificou-se que, embora as trajetórias excursionem para longe uma da outra quando há a dessincronização, elas voltam a se aproximar rapidamente e os sistemas passam a apresentar uma dinâmica caótica sincronizada novamente até que outro evento de dessincronização ocorra. Tais eventos de dessincronização são consequências da aproximação da trajetórias da origem (ponto de equilíbrio instável) do sistema. Como os sistemas estão sincronizados, as trajetórias de ambos se aproximam da origem e divergem da mesma forma. Destaca-se que não é para qualquer conjunto de parâmetro que a correlação dos sinais é alta, por isso foi realizado uma minuciosa investigação numérica para se obter parâmetros adequados.

Uma vez alcançado o mesmo sinal de dessincronização no transmissor e no receptor, esses sinais foram utilizados para gerar as chaves criptográficas. Os resultados numérico e experimental demonstraram que as chaves geradas no transmissor e no receptor possuem boa similaridade e, por conseguinte, taxa de erro dentro de níveis aceitáveis (< 11%). Observe que é possível utilizar códigos corretores de erro para diminuir ainda mais esse nível de taxa de erro. Os resultados mostraram também que tais chaves possuem baixa similaridade e alta taxa de erro ($\approx$ 50%) com uma possível chave gerada por um atacante a partir do sinal de $V_1$, o que é altamente desejável e importante para a segurança do sistema. Ficou evidente que a chave experimental teve uma taxa de erro maior que a chave numérica. É provável que o desempenho inferior da chave experimental tenha sido ocasionado, principalmente, pelos ruídos do ambiente e do próprio sistema, haja vista que, propositalmente, nenhuma ação foi tomada para mitigá-lo no momento da realização experimental.

Vale salientar que uma melhora no algoritmo de geração de chave pode levar a uma redução da taxa de erro, conforme se verificou quando da mudança do algoritmo de geração de chave na parte experimental. Empregando o algoritmo inicial (o mesmo utilizado na parte numérica), obteve-se um BER de 0,262 ± 0,001, ao passo que, com o novo algoritmo, o BER foi de 0,106 ± 0,001. O algoritmo influencia também na aleatoriedade da chave. Lembre-se que foi necessário implementar um algoritmo na parte experimental diferente do algoritmo utilizado na parte numérica para que a chave experimental passasse no teste do NIST. Assim sendo, com vistas a uma implementação prática do sistema proposto, é fundamental investigar e implementar o melhor método de geração de chave digital a partir do sinal analógico.

No que diz respeito ao teste de aleatoriedade, tanto a chave numérica quanto a experimental apresentaram desempenho satisfatórios, segundo os testes do NIST. Esse resultado era esperado em virtude do comportamento caótico do sistema, que, apesar de ser determinístico, é imprevisível ao longo do tempo. Sob o aspecto da informação mútua, a chave experimental apresentou um resultado três ordens de grandeza pior do que a chave numérica. Uma das hipóteses para explicar essa diferença é a presença do ruído ambiente na parte experimental. Supõe-se que, dado ao fato de o transmissor, o receptor e o meio de comunicação estarem dispostos espacialmente no mesmo ambiente, de alguma forma, o ruído do ambiente interferiu nos três igualmente, o que gerou essa informação a mais entre o transmissor e o meio de comunicação retratado no calculo da informação mútua da parte experimental. Isso é algo que pode ser melhor explorado em trabalhos futuros.

Em virtude de o sistema proposto poder gerar séries temporais caóticas indefinidamente, pode-se obter chaves criptográficas tão grandes quanto se queira, logo, as chaves geradas podem possuir o mesmo comprimento das mensagens (1º requisito do *one-time pad*). A imprevisibilidade do comportamento dinâmico dos eventos de dessincronização evidencia que tais chaves nunca serão repetidas, ou seja, serão usadas uma única vez (2º requisito do *one-time pad*). A partir do resultado dos testes do NIST, foi possível verificar que as chaves não mostraram nenhuma desvio significativo de uma chave verdadeiramente aleatória (3º requisito do *one-time pad*). O fato de as chaves não serem compartilhadas pelo meio de comunicação, seja ele público ou privado, por si só já garante o fato de as chaves terem de ser compartilhadas de maneira segura entre o remetente e o destinatário (4º requisito do *one-time pad*). Portanto, o esquema de criptografia / descriptografia atende a todos requisitos do *one-time pad*) e, consequentemente, mostra-se incondicionalmente segura.

Outro fato importante a ser destacado é que a segurança do sistema está intimamente ligada a complexidade do circuito utilizado como plataforma do sistema e do algoritmo utilizado para transformar o sinal analógico na chave binária. Ou seja, quanto maior a complexidade do oscilador empregado e do método de geração da chave, maior será a segurança do sistema, pois mais difícil se torna para um atacante reproduzir o oscilador e descobrir o algoritmo.

Um ataque óbvio seria construir um sistema exatamente igual ao receptor, acoplá-lo à rede e fazê-lo sincronizar através de $V_1$. No entanto, isso não é trivial, uma vez que a sincronização só pode ser alcançada quando o sistema é construído com parâmetros dentro de tolerâncias muito rígidas (um por cento ou menos, por exemplo). Consequentemente, um ataque de força bruta por compatibilidade de parâmetros seria excessivamente demorado. Como dito acima, quanto mais complexo o sistema, ou seja, quanto mais parâmetros tiver o sistema, mais difícil se torna tal tipo de ataque.

Contudo, suponha que o atacante tenha tido sucesso em desenvolver um

sistema exatamente igual ao proposto e tenha conseguido sincronizá-lo à rede através de $V_1$ (obviamente que ele precisa ter acesso a $V_1$), ainda assim ele não terá sucesso em decifrar o texto claro, pois ele não terá conhecimento do algoritmo (taxa de amostragem, tipo de conversão analógico-digital, etc.) e do número de bits das operações de rotação ou-exclusivo para transformar o sinal analógico numa chave binária adequada.

A prova de conceito foi demonstrada utilizando osciladores caóticos eletrônicos analógicos devido a sua simplicidade e baixo custo, haja vista que o maior interesse do presente trabalho era demonstrar a viabilidade do conceito de gerar e distribuir chaves criptográficas simétricas a partir dos eventos de dessincronização e, certamente, isso foi plenamente conseguido. Outros tipos de osciladores, a exemplo de osciladores optoeletrônicos ou fotônicos, poderiam ser utilizados para conseguir taxas de transmissão de dados superior as conseguidas no presente trabalho.

Por último, vale frisar que o ruído influenciou de alguma forma no desempenho do sistema experimental, consoante se observa na pequena perda de qualidade da imagem recuperada da Fig. 35. Logo, mitigar o efeito do ruído é imperativo para se ter um sistema confiável.

# 6 CONCLUSÕES E PERSPECTIVAS

A presente dissertação explorou o fenômeno da sincronização intermitente de circuitos eletrônicos caóticos acoplados para propor um sistema inovador de geração e distribuição de chaves criptográficas simétricas, sistema extremamente prático e útil.

Foi demonstrado numérica e experimentalmente a viabilidade de gerar e distribuir chaves de criptografia, tanto no transmissor quanto no receptor, a partir da amostragem do sinal dos eventos de dessincronização de dois osciladores eletrônicos caóticos acoplados.

Sob o ponto de vista de segurança, as chaves geradas são incondicionalmente seguras, uma vez que podem ser geradas do mesmo tamanho da mensagem, não necessitam serem reutilizadas, não demonstram desvios relevantes da aleatoriedade e não são compartilhadas pelo meio de comunicação, ou seja, atendem às premissas do *one-time pad*.

Utilizando a chave criptográfica obtida experimentalmente e a imagem de uma paisagem, foi possível criptografar a mensagem (imagem) no transmissor, transmiti-la de forma segura pelo meio de comunicação e descriptografá-la no receptor, demonstrando cabalmente o funcionamento do sistema.

Obviamente que o sistema proposto no presente trabalho pode ser aprimorado para: 1) trabalhar em bandas de frequência maiores, a fim de atingir maiores taxas de geração de bits; 2) mitigar o ruído, para diminuir a taxa de incompatibilidade entre a sequência de bits do transmissor e do receptor; e 3) tornar o circuito mais complexo, com vistas a aumentar a segurança do sistema. Logo, ficam essas três sugestões para trabalhos futuros. Recomenda-se fortemente o desenvolvimento de um novo oscilador caótico para melhorar o binômio velocidade-segurança.

Por fim, espera-se que o sistema proposto seja uma alternativa à criptografia clássica, que é facilmente quebrada por algorítimos quânticos, e à criptografia quântica, que ainda não pode ser aplicada por falta de infraestrutura de telecomunicações adequada, no tocante a garantir segurança da informação de pessoas, instituições e governos na Internet.

# REFERÊNCIAS

ARGYRIS, A.; SYVRIDIS, D.; LARGER, L.; LODI-ANNOVAZZI, V.; COLET, P.; FISCHER, I.; GARCIA-OJALVO, J.; MIRASSO, C. R.; PESQUERA, L.; SHORE, A. Chaos-based communications at high bit rates using commercial fibre-optic links. **Nature**, [*s. l.*], v. 438, n. 7066, p. 343–346, 2005. Disponível em: https://www.nature.com/articles/nature04275. Acesso em: 6 dez. 2020.

BASSHAM, L.; RUKHIN, A.; SOTO, J.; NECHVATAL, J.; SMID, M.; LEIGH, S.; LEVENSON, M.; VANGEL, M.; HECKERT, N.; BANKS, D. **A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications**. Maryland: National Institute of Standards & Technology, 2010. Disponível em: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762. Acesso em: 10 ago. 2021.

BELYKH, I.; LANGE, E. de; HASLER, M. Synchronization of bursting neurons: What matters in the network topology. **Phys. Rev. Lett.**, [Maryland], v. 94, n. 18, p. 188101, 2005. Disponível em: https://link.aps.org/doi/10.1103/PhysRevLett.94.188101. Acesso em: 10 abr. 2021.

BOCCALETTI, S.; KURTHS, J.; OSIPOV, G.; VALLADARES, D.; ZHOU, C. The synchronization of chaotic systems. **Physics Reports**, [*s. l.*], v. 366, n. 1, p. 1–101, 2002. Disponível em: https://www.sciencedirect.com/science/article/pii/S0370157302001370. Acesso em: 13 de mar. 2021.

BÖHM, F.; SAHAKIAN, S.; DOOMS, A.; VERSCHAFFELT, G.; SANDE, G. Van der. Stable high-speed encryption key distribution via synchronization of chaotic optoelectronic oscillators. **Phys. Rev. Applied**, [Maryland], v. 13, n. 6, p. 064014, 2020. Disponível em: https://link.aps.org/doi/10.1103/PhysRevApplied.13.064014. Acesso em: 7 dez. 2020.

CAVALCANTE, H. L. D. S.; ORIÁ, M.; SORNETTE, D.; OTT, E.; GAUTHIER, D. J. Predictability and suppression of extreme events in a chaotic system. **Phys. Rev. Lett.**, [Maryland], v. 111, n. 19, p. 198701, 2013. Disponível em: https://link.aps.org/doi/10.1103/PhysRevLett.111.198701. Acesso em: 29 jan. 2021.

CUOMO, K.; OPPENHEIM, A.; STROGATZ, S. Synchronization of lorenz-based chaotic circuits with applications to communications. **IEEE Transactions on Circuits and Systems II**: Analog and Digital Signal Processing, [*s. l.*], v. 40, n. 10, p. 626–633, 1993. Disponível em: https://ieeexplore.ieee.org/document/246163. Acesso em: 10 de jan. 2021.

FALCO, A. D.; MAZZONE, V.; CRUZ, A.; FRATALOCCHI, A. Perfect secrecy cryptography via mixing of chaotic waves in irreversible time-varying silicon chips. **Nature communications**, [*s. l.*], v. 10, n. 1, p. 1–10, 2019. Disponível em: https://www.nature.com/articles/s41467-019-13740-y. Acesso em: 7 dez. 2020.

FUJISAKA, H.; YAMADA, T. Stability theory of synchronized motion in coupled-oscillator systems. **Progress of Theoretical Physics**, [*s. l.*], v. 69, n. 1, p. 32–47, 1983. Disponível em: https://doi.org/10.1143/PTP.69.32. Acesso em: 14 abr. 2021.

GAUTHIER, D. J.; BIENFANG, J. C. Intermittent loss of synchronization in coupled chaotic oscillators: Toward a new criterion for high-quality synchronization. **Phys. Rev. Lett.**, [Maryland], v. 77, n. 9, p. 1751–1754, 1996. Disponível em: https://link.aps.org/doi/10.1103/PhysRevLett.77.1751. Acesso em: 12 de fev. 2021.

ITO, T.; KOIZUMI, H.; SUZUKI, N.; KAKESU, I.; IWAKAWA, K.; UCHIDA, A.; KOSHIBA, T.; MURAMATSU, J.; YOSHIMURA, K.; INUBUSHI, M. et al. Physical implementation of oblivious transfer using optical correlated randomness. **Scientific reports**, [*s. l.*], v. 7, n. 1, p. 1–12, 2017. Disponível em: https://www.nature.com/articles/s41598-017-08229-x. Acesso em: 10 dez. 2020.

KAHN, D. **The Codebreakers**: The comprehensive history of secret communication from ancient times to the internet. New York: Simon and Schuster, 1996.

KEUNINCKX, L.; SPRIANO, M. C.; FISCHER, I.; MIRASSO, C. R.; NGUIMDO, R. M.; SANDE, G. V. Encryption key distribution via chaos synchronization. **Scientific reports**, [*s. l.*], v. 7, n. 1, p. 1–14, 2017. Disponível em: https://www.nature.com/articles/srep43428. Acesso em: 7 dez. 2020.

KOCAREV, L.; PARLITZ, U. Generalized synchronization, predictability, and equivalence of unidirectionally coupled dynamical systems. **Phys. Rev. Lett.**, [Maryland], v. 76, p. 1816–1819, 1996. Disponível em: https://link.aps.org/doi/10.1103/PhysRevLett.76.1816. Acesso em: 4 mai. 2021.

PAAR, C.; PELZL, J. **Understanding cryptography**: a textbook for students and practitioners. Berlin Heidelberg: Springer Science, 2010.

PECORA, L. M.; CARROLL, T. L. Synchronization in chaotic systems. **Phys. Rev. Lett.**, [Maryland], v. 64, n. 8, p. 821–824, 1990. Disponível em: https://link.aps.org/doi/10.1103/PhysRevLett.64.821. Acesso em: 7 dez. 2020.

PECORA, L. M.; CARROLL, T. L.; JOHNSON, G. A.; MAR, D. J.; HEAGY, J. F. Fundamentals of synchronization in chaotic systems, concepts, and applications. **Chaos**: An Interdisciplinary Journal of Nonlinear Science, [*s. l.*], v. 7, n. 4, p. 520–543, 1997. Disponível em: https://doi.org/10.1063/1.166278. Acesso em: 21 dez. 2020.

PIKOVSKY, A.; ROSENBLUM, M. G.; KURTHS, J. Synchronization: A universal concept in nonlinear science. **American Journal of Physics**, [*s. l.*], v. 70, n. 6, p. 655–655, 2002. Disponível em: https://doi.org/10.1119/1.1475332. Acesso em: 21 dez. 2020.

ROSENBLUM, M. G.; PIKOVSKY, A. S.; KURTHS, J. Phase synchronization of chaotic oscillators. **Phys. Rev. Lett.**, [Maryland], v. 76, n. 11, p. 1804–1807, 1996. Disponível em: https://link.aps.org/doi/10.1103/PhysRevLett.76.1804. Acesso em: 4 mai. 2021.

ROSENBLUM, M. G.; PIKOVSKY, A. S.; KURTHS, J. From phase to lag synchronization in coupled chaotic oscillators. **Phys. Rev. Lett.**, [Maryland], v. 78, n. 22, p. 4193–4215, 1997. Disponível em: https://link.aps.org/doi/10.1103/PhysRevLett.78.4193. Acesso em: 6 mai. 2021.

ROY, R.; THORNBURG, K. S. Experimental synchronization of chaotic lasers. **Phys. Rev. Lett.**, [Maryland], v. 72, n. 13, p. 2009–2012, 1994. Disponível em: https://link.aps.org/doi/10.1103/PhysRevLett.72.2009. Acesso em: 12 de mar. 2021.

SEDRA, A. S.; SEDRA, D. E. A. S.; SMITH, K. C. et al. **Microelectronic circuits**. New York: Oxford University Press, 1998.

SHORT, K. M. Steps toward unmasking secure communications. **International Journal of Bifurcation and Chaos**, [*s. l.*], v. 04, n. 04, p. 959–977, 1994. Disponível em: https://doi.org/10.1142/S021812749400068X. Acesso em: 5 jul. 2021.

SHORT, K. M. Unmasking a modulated chaotic communications scheme. **International Journal of Bifurcation and Chaos**, [*s. l.*], v. 06, n. 02, p. 367–375, 1996. Disponível em: https://doi.org/10.1142/S0218127496000114. Acesso em: 5 jul. 2021.

STALLINGS, W. **Criptografia e segurança de redes**: princípios e práticas. São Paulo: Pearson Education do Brasil, 2015.

STROGATZ, S. H. **Nonlinear dynamics and chaos**: with applications to physics, biology, chemistry, and engineering. Boca Raton: CRC press, 2018.

VOSS, H. U. Anticipating chaotic synchronization. **Phys. Rev. E**, [Maryland], v. 61, n. 5, p. 5115–5119, 2000. Disponível em: https://link.aps.org/doi/10.1103/PhysRevE.61.5115. Acesso em: 6 mai. 2021.

YANG, T. A survey of chaotic secure communication systems. **International journal of computational cognition**, [*s. l.*], v. 2, n. 2, p. 81–130, 2004. Disponível em: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.14.9724. Acesso em: 14 jun. 2021.

YANG, T.; WU, C. W.; CHUA, L. O. Cryptography based on chaotic systems. **IEEE Transactions on Circuits and Systems I**: Fundamental Theory and Applications, [*s. l.*], v. 44, n. 5, p. 469–472, 1997. Disponível em: https://ieeexplore.ieee.org/document/572346. Acesso em: 14 jun. 2021.