UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

GLAUCIONOR LIMA DE OLIVEIRA

DISTRIBUIÇÃO QUANTUM-CAÓTICA DE CHAVES USANDO OSCILADORES OPTOELETRÔNICOS

FORTALEZA

2018

GLAUCIONOR LIMA DE OLIVEIRA

DISTRIBUIÇÃO QUANTUM-CAÓTICA DE CHAVES USANDO OSCILADORES OPTOELETRÔNICOS

Tese apresentada ao Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Doutor em Engenharia de Teleinformática. Área de concentração: Eletromagnetismo Aplicado e linha de pesquisa em Dispositivos e Sistemas Ópticos e de Micro-ondas.

Orientador: Prof. Dr. Rubens Viana Ramos.

FORTALEZA

2018

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

O47d Oliveira, Glaucionor Lima de.
Distribuição Quantum-Caótica de Chaves Usando Osciladores Optoeletrônicos / Glaucionor Lima de Oliveira. – 2018.
116 f. : il. color.

Tese (doutorado) – Universidade Federal do Ceará, Centro de Tecnologia, Programa de Pós-Graduação em Engenharia de Teleinformática, Fortaleza, 2018.
Orientação: Prof. Dr. Rubens Viana Ramos.

1. Osciladores Optoeletrônicos. 2. Distribuição de Chaves. 3. Quantum-Caótico. I. Título.
CDD 621.38

GLAUCIONOR LIMA DE OLIVEIRA

DISTRIBUIÇÃO QUANTUM-CAÓTICA DE CHAVES USANDO OSCILADORES OPTOELETRÔNICOS

Tese apresentada ao Programa de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Doutor em Engenharia de Teleinformática. Área de concentração: Eletromagnetismo Aplicado e linha de pesquisa em Dispositivos e Sistemas Ópticos e de Micro-ondas.

Aprovada em: 26/02/2018.

BANCA EXAMINADORA

_____

Prof. Dr. Rubens Viana Ramos (Orientador)
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. João Batista Rosa Silva
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. Glendo de Freitas Guimarães
Instituto Federal do Ceará (IFCE)

_____

Prof. Dr. Vitaly Félix Rodrígues Esquerre
Universidade Federal da Bahia (UFBA)

_____

Prof. Dr. Kleber Zuza Nóbrega
Instituto Federal do Maranhão (IFMA)

AGRADECIMENTOS

Ao meu Senhor Deus.

Aos meus pais (Salustiano e Mozarina), e filhos (Filipe e Raul).

À minha esposa (Ranara) pela força, correções e por compartilhar sua vida comigo.

Ao amigo e Prof. Rubens Viana Ramos pela confiança e ajuda incondicional na realização deste trabalho.

Aos meus amigos do GIQ e ao professor João Batista, pelos igualmente agradáveis momentos de estudos, pesquisa, trabalho e descontração.

Agradeço também ao apoio dos meus colegas do IFCE, em especial ao Prof. Glendo de Freitas.

Por fim, aos professores do PPGETI, pelos ensinamentos que completaram a minha formação, e ao funcionário Renato Barbosa, pelo trabalho competente na secretaria do PPGETI.

RESUMO

A primeira parte da presente tese apresenta sistemas ópticos baseados em osciladores optoeletrônicos para a realização de distribuição de chaves criptográficas, em redes ópticas, com segurança baseada em princípios da física quântica e de sistemas caóticos. Três sistemas são propostos: I) Sistema de distribuição caótica de chaves. II) Sistema de distribuição caótica de chaves com segurança quântica. III) Sistema de distribuição quantum-caótica de chaves, no qual os sistemas quânticos e caóticos estão integrados em um só. Em todos os casos a análise de segurança é realizada. Os três sistemas se mostraram viáveis sem o sistema quantum-caótico o mais seguro deles. Na segunda parte da tese são abordados aspectos experimentais da geração fotônica de sinais de micro-ondas utilizando ressonadores de fibra. Experimentos para geração de harmônicas com moduladores de amplitude e fase no loop do ressonador foram realizados. Pode-se constatar que os sistemas com moduladores de fase apresentam uma maior quantidade de harmônicas geradas.

Palavras chave: Osciladores optoeletrônicos, Distribuição de chaves, Quantum-Caótico.

ABSTRACT

The first part of the present thesis brings optical setups based on optoelectronic oscillators for realization of key distribution, in optical networks, with security based on quantum physics and chaotic systems principles. Three optical setups are proposed: I) A setup for chaotic key distribution. II) A setup for quantum secured chaotic key distribution. III) A setup for quantum-chaotic key distribution, in which quantum and chaotic systems are integrated. In all cases the security analysis is realized. All three systems proved to be viable without the safest quantum-chaotic system. In the second part of the thesis, experimental aspects of photonic generation of microwave signals using fiber optical resonator are considered. Experiments for harmonic generation using amplitude and phase modulators in the optical loop were realized. It can be verified that the systems with phase modulators present a greater amount of harmonics generated.

Keywords: Optoelectronic Oscillators, Key Distribution, Quantum-Caotic.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AMP	Amplificador
BER	Taxa de Erro de Bit (Bit Error Rate)
BS	Divisor de Feixe (Beam Splitter)
DCC	Distribuição Caótica de Chaves
DFB	Laser de Retroação Distribuída (Distributed Feedback Laser)
DPS-QKD	Distribuição Quântica de Chaves com Deslocamento Diferencial de Fase (Differential Phase-Shift Quantum Key Distribution)
DQC	Distribuição Quântica de Chaves
DQPS-QKD	Distribuição Quântica de Chaves com Deslocamento Diferencial de Fase em Quadratura (Differential Quadrature Phase-Shift Quantum Key Distribution)
EDFA	Amplificador a fibra dopada com érbio (Erbium-Doped Fiber Amplifier)
ESA	Analisador de Espetro (Spectrum Analyzer)
FWHM	Largura Total à Metade Máxima (Full Width at Half-Maximum)
FSR	Faixa Espectral Livre (Free Spectral Range)
GB	GigaBytes
GBps	GigaBytes por segundo
HEMT	Transistor de Alta Mobilidade de Elétron (High Electron Mobility Transistor)
IoT	Internet das Coisas (Internet Of Things)
IMPATT	Ionização por Impacto com Avalanche de Tempo Transitório (IMPact Ionization Avalanche Transit Time)
IP	Protocolo de Internet (Internet Protocol)
LD	Diodo Laser (Laser Diode)
MIT	Massachusetts Institute of Technology (Instituto de Tecnologia de Massachusetts)
MOD	Modulador
MZM	Modulador Mach-Zehnder (Mach-Zender Modulator)
ODL	Linha de atraso óptico (Optical Delay Line)
OEO	Oscilador Optoeletrônico (Opto-Electronic Oscillator)
OTP	Uso Único (One Time Pad)
PBS	Divisor de feixe de Polarização(Polarization Beam Splitter)
PD	Fotodetector (Photodetector)
PIN	Positivo Intrínseco Negativo (Positive Intrinsic Negative)
PLL	Laço de Travamento em Fase (Phase-Locked Loop)
PSD	Densidade Espectral de Potência (Power Spectral Density)
PRNG	Gerador de Números Pseudo-Aleatórios (Pseudorandom Number Generator)

QCM_CS	Máquina de Clonagem Quântica de Estados Coerentes (Quantum Cloning Machine of Coherent States)
QKD	Distribuição Quântica de Chaves (Quantum Key Distribution)
RF	Radiofrequência (Radio Frequency)
RIN	Intensidade Relativa de Ruído do Laser (Relative Intensity Noise)
RoF	Rádio sobre Fibra (Radio over Fiber)
SG	Gerador de Sinais (Signal Genarated)
SMF	Fibra Monomodo (Single Mode Fiber)
VCO	Oscilador Controlado por Tensão (Voltage Controlled Oscillator)
VNI	Índice Visual da Rede (Visual Networking Index)
ZB	ZettaBytes
WGM	Modo de Galeria Sussurrando (Whispering Gallery Mode)

SUMÁRIO

1 INTRODUÇÃO

Os dados estimados pela Cisco® Visual Networking Index (VNI) em seu relatório "previsão Cisco do tráfego global IP" [1] mostram que o crescimento de informações digitais levarão o tráfego de dados na Internet a superar o patamar dos zettabytes (ZB), unidade que representa o valor de um sextilhão de *bytes* trafegados. A previsão é que chegará a 2,3 ZB por ano até 2020. O tráfego IP no final de 2016 atingiu 1,1 ZB por ano, ou 88,7 exabytes/mês, e em 2020 será 194 exabytes/mês. Boa parte destes dados é confidencial, por exemplo, informações militares, segredos industriais, empresariais, financeiros, bancários ou médicos. Portanto, o uso de técnicas de segurança da informação é crucial.

Atualmente, a criptografia se divide em dois tipos: 1) Segurança baseada na intratabilidade de problemas matemáticos. 2) Segurança baseada em princípios físicos. Como nunca se sabe quando alguém vai descobrir um método de solução viável de um determinado problema matemático até então considerado intratável (em tempo razoável), tem havido um crescente interesse por sistemas de segurança da informação baseados em leis da natureza. No que diz respeito às redes ópticas, o uso de criptografia caótica e criptografia quântica são as opções. Nesta direção, o objetivo desse trabalho é apresentar três esquemas para implementação de segurança para distribuição de chaves que utilizam tecnologia quântica e caótica. A primeira parte da presente tese propõe os três sistemas de distribuição de chaves: I) Sistema de distribuição caótica de chaves com osciladores optoeletrônicos sincronizados. II) Sistema de distribuição caótica de chaves protegido por um protocolo quântico de transmissão de informações analógicas. III) Sistema de distribuição quantum-caótica de chaves. O uso integrado de criptografia caótica e quântica proporciona um aumento da segurança e um novo tipo de abordagem para a análise de segurança passa a ser requerido. A metodologia empregada nessa primeira parte foi a simulação numérica.

Na segunda parte da presente tese aborda-se a geração fotônica de sinais de micro-ondas com o uso de ressonador a fibra e moduladores de amplitude e fase. Diferente dos osciladores eletrônicos que apresentam limitações de frequência de operação e de pureza espectral, os geradores fotônicos podem trabalhar com sinais de micro-ondas, ondas milimétricas e até mesmo ondas em THz, pois esses sinais são uma fração da frequência da luz. Outra vantagem é que a utilização de elementos ópticos minimiza a perda com o aumento

da frequência [2]. Nesta direção, este trabalho apresenta os resultados alcançados com o uso de metodologia experimental para a geração de harmônicas de um sinal fundamental de RF, com um esquema de ressonador a fibra utilizando modulador de amplitude e/ou de fase.

Este trabalho está dividido em seis capítulos e dois apêndices descritos a seguir: no Capítulo 2 é apresentada uma revisão geral sobre os osciladores optoeletrônicos (OEO - *Opto-Electronic Oscillator*); o Capítulo 3 apresenta o estudo realizado através de simulação para distribuição caótica de chaves com o uso de OEOs sincronizados; no Capítulo 4 mostra-se uma modelagem de configuração para uso conjunto da criptografia caótica e quântica onde o protocolo quântico protege um sistema de distribuição caótica de chaves; o Capítulo 5 apresenta um esquema para distribuição quantum-caótica de chaves utilizando OEOs sincronizados e estados coerentes atenuados; o Capítulo 6 apresenta a realização de experimentos de geração fotônica de harmônicas de um sinal de RF por meio do uso de ressonador com laço de fibra e moduladores de amplitude e fase. Por fim, as conclusões e a perspectivas de trabalhos futuros são apresentadas no Capítulo 7. O Apêndice A apresenta uma introdução à teoria do caos enquanto que no Apêndice B encontra-se uma revisão sobre distribuição quântica de chaves.

2 OSCILADORES OPTOELETRÔNICOS

Neste capítulo são apresentadas as características, modo de operação e parâmetros de funcionamento dos osciladores optoeletrônicos (OEOs).

2.1 Osciladores optoeletrônicos para sistema de comunicação

Com o aumento da demanda por processamento de sinais em altas velocidades e desempenho, cresce a necessidade de desenvolvimento de circuitos osciladores de radiofrequência (RF) de alta precisão e baixo ruído de fase. A construção de circuitos osciladores de radiofrequência para altas frequências envolve o uso de técnicas que demandam o emprego de uma quantidade razoável de dispositivos para gerar, estabilizar e controlar o ruído presente nestes sinais. Os métodos para geração eletrônica de sinais de micro-ondas e ondas milimétricas utilizam, por exemplo, transistores HEMT (*High Electron Mobility Transistor*), diodos Gunn ou IMPATT (*Impact Ionization Avalanche Transit Time*) em cavidades ressonantes. A necessidade de distribuição dos sinais de micro-ondas através de cabos coaxiais introduz altas perdas devido ao efeito pelicular, tornando a distribuição impraticável para determinadas aplicações.

Como citado em [4] algumas dessas aplicações abrangem desde sistemas RF analógicos, como radares e ultrassonografia médica, bem como sistemas digitais para comunicações de longa distância e interconexões *on-chip* em computadores. Outras aplicações incluem amostragem para conversor analógico-digital, recuperação de relógio e as fontes de pulso.

Os osciladores de quartzo atualmente proporcionam alto desempenho e pureza espectral sem precedentes, mas apenas para frequências iguais ou inferiores a algumas centenas de MHz [2]. O uso desses osciladores nos sistemas de alta frequência muitas vezes exige a multiplicação da frequência de oscilação aumentando a complexidade do sistema, bem como a multiplicação do ruído do oscilador. Um fator importante na construção de osciladores é o elemento de alta figura de mérito Q, que em osciladores convencionais normalmente determina tanto a frequência de operação quanto a pureza espectral. Um

exemplo são os osciladores que utilizam ressonador, pois o tamanho do ressonador diminui com o aumento da frequência, resultando em um Q menor e aumento do ruído.

A geração de sinais de alta frequência no domínio óptico, por sua vez, traz vantagens quanto ao número de elementos empregados, e quanto a distribuição do sinal que faz uso das redes de fibras. Diferente da geração de sinais de RF utilizando circuitos eletrônicos, que podem exigir vários estágios de duplicação de frequência, elevando os custos, os sistemas ópticos se aproveitam de sua ampla largura de banda e baixas perdas para gerar RF com extrema simplicidade e pequena quantidade de dispositivos.

Outro fator a considerar no emprego de osciladores optoeletrônicos (OEO - *Opto-Electronic Oscillator*) é que os guias de onda ópticos e ressonadores podem ser produzidos com perda extremamente baixa, obtendo-se assim componentes com elevada figura de mérito Q [2]. Ressonadores ópticos com Q extremamente alto permitem o aparecimento de não linearidades e isso pode ser uma vantagem para a geração de sinais de referência em alta frequência.

2.2 O Oscilador optoeletrônico básico

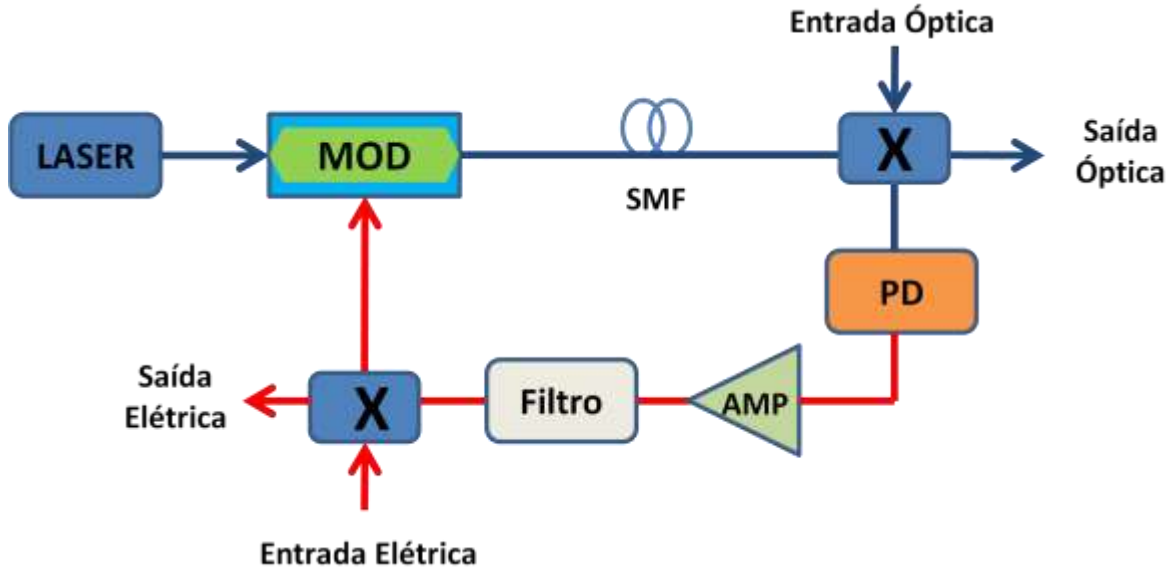
Amplamente utilizado hoje, o oscilador eletrônico foi inventado por L. de Forest em 1912 [5]. Os osciladores são basicamente dispositivos que convertem energia contínua em um sinal de variação periódica. Seu funcionamento está baseado em um princípio fundamental da física que é o oscilador harmônico. É sem dúvida o dispositivo mais utilizado nos diversos equipamentos eletrônicos modernos. A qualidade e precisão de um oscilador dependem fundamentalmente de seu grau de pureza espectral e estabilidade de oscilação, e essa medida está diretamente relacionada com a capacidade de armazenamento de energia do oscilador, determinada pela perda de resistência nos vários elementos que o compõem e que também vai depender da frequência de trabalho do oscilador.

Para conseguir reduzir o ruído nos osciladores eletrônicos utiliza-se ressonadores com elevado Q. A figura de mérito de um ressonador pode ser medida por $Q = 2\pi f\, \tau_d$, onde τ_d é o tempo de decaimento da energia que mede a capacidade de armazenamento de energia do ressonador e f é a frequência de ressonância. Os ressonadores a quartzo têm alguns modos de elevado Q de ressonância, mas em frequências baixas limitando a gama de frequências

sintonizáveis, impedindo seu uso para geração de altas frequências diretamente [4]. Em 1996 Yao e Maleki [3] propuseram o uso do OEO para a geração de sinal de RF de alta frequência e baixo ruído de fase.

O OEO básico é um circuito realimentado que converte a luz modulada de um laser em sinal de RF. É composto por um laser de onda contínua que alimenta um modulador. O sinal de saída do modulador óptico passa por uma longa linha de atraso de fibra óptica e é acoplado a um fotodiodo. O sinal elétrico detectado é amplificado e após passar por um filtro passa faixa eletrônico alimenta de volta o modulador completando a cavidade optoeletrônica. Quando o ganho do laço é maior do que as perdas, o OEO começa a oscilar. A figura de mérito Q alta no segmento óptico é proporcionada pelo circuito de atraso com uma fibra longa, neste caso, é a frequência central do filtro eletrônico que determina a frequência de operação do OEO. Pode-se utilizar como elemento de alto Q um ressonador óptico, caso em que a sua faixa espectral livre (FSR - *Free Spectral Range*) vai definir a frequência do oscilador [2,4]. O circuito fechado de realimentação consiste de componentes eletrônicos e ópticos, pois dependendo do tipo de aplicação estes componentes podem ser permutados entre si. Na sua configuração mais comum o amplificador, o filtro e o acoplador estão incluídos no segmento eletrônico. A Fig. 2.1 mostra o esquema básico de um OEO.

Fig. 2.1. Oscilador Optoeletrônico Básico. Laser, MOD: Modulador, SMF: Fibra Monomodo, PD: Fotodiodo, AMP: Amplificador, Filtro passa faixa, X: Acoplador.



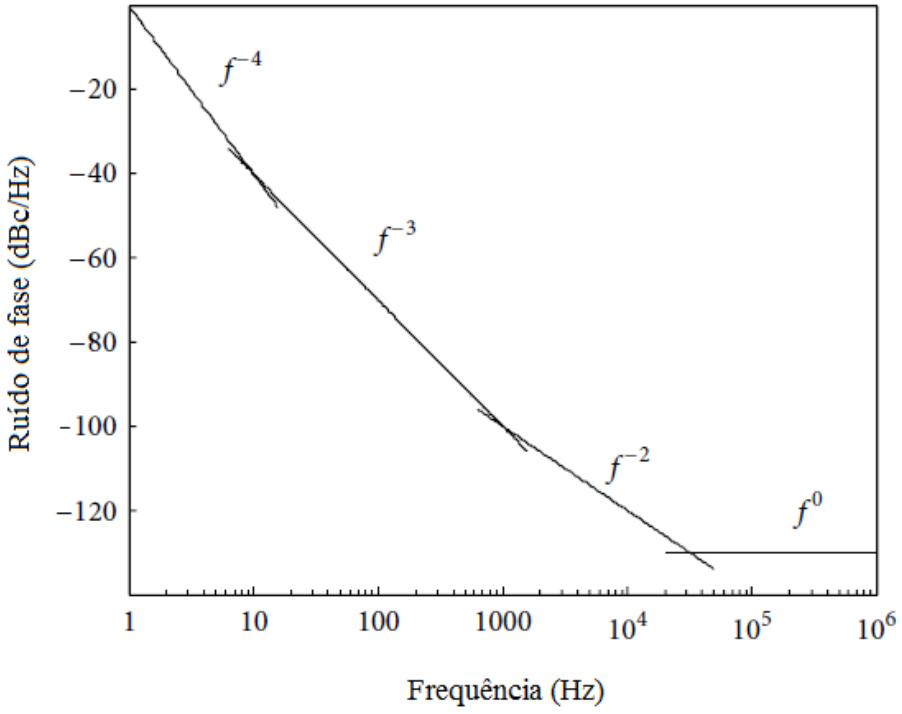
Fonte: referência [5].

O uso de componentes baratos e disponíveis comercialmente torna o OEO vantajoso, pois seu elevado desempenho para a geração de altas frequências tem custo baixo. Várias modificações tem sido apresentadas para melhorar o projeto inicial do primeiro OEO, bem como seu uso para outras aplicações que não a de geração do sinal RF de baixo ruído de fase [4].

Segundo [5], as condições para oscilações autossustentadas incluem coerência das ondas parciais em cada sentido em torno do laço e um ganho de *loop* superior às perdas para os sinais que circulam no circuito. A primeira condição implica que todos os sinais que diferem em fase por um múltiplo de 2π a partir do sinal fundamental podem ser sustentados. A frequência de oscilação é limitada apenas pela resposta de frequência característica do modulador e a atuação do filtro. A segunda condição implica que, com potência de luz adequada, oscilações autossustentadas podem ser obtidas sem a necessidade do amplificador de RF.

O ruído de fase é a medida que permite caracterizar osciladores de qualquer tipo. Como mostrado em [4], o ruído de fase £(f) do OEO é definido como a densidade espectral de potência (PSD - *Power Spectral Density*) da banda lateral única do sinal de RF gerado a partir do OEO. A PSD é normalizada para a energia do sinal de RF e tem unidade de dBc/Hz. O ruído de fase pode ser citado como um único valor medido a partir de um deslocamento da frequência da portadora. A Figura 2.2 apresenta uma curva teórica aara mostrar a forma geral do espectro de ruído de fase de um OEO. Segundo [4], na faixa de frequência entre 1 Hz a 10 Hz da curva teórica, a inclinação tem um declive de f^{-4}, pois o ruído dominante nela tem como fonte as flutuações ambientais, provocados pelas variações de temperatura e vibrações acústicas. No intervalo de 10 Hz a 1 kHz, o ruído é dominado pelo ruído de fase do estágio de amplificação RF, necessário para a maioria dos OEOs oscilarem e tem um declive de f^{-3}. A faixa seguinte de 1 kHz a 30 kHz é dominada pelo ruído de fase branco e tem um declive de f^{-2}. Por fim, para sinais acima de 30 kHz, o ruído de fase tem uma resposta de ruído plana que é devido ao próximo modo lateral não oscilante do OEO.

Fig. 2.2. Ruído de fase teórico mostrando as diferentes influências de ruído sobre a densidade de potência espectral para desvios de frequência de 1 Hz a 1 MHz a partir da portadora.



Fonte: referência [4].

2.3 Descrição da operação do OEO

O equacionamento dos sinais que circulam no OEO pode ser representado a partir do sinal $E(t)$ que sai do modulador, dado por [5]:

$$E(t) = (\alpha P_0 / 2)\left\{1 - \eta \sin \pi\left[V_{in}(t)/V_\pi + V_B/V_\pi\right]\right\}, \quad (1)$$

onde α é a perda de inserção fracionada do modulador, V_π é a tensão de meia onda, V_B é a tensão de polarização, P_0 é a potência óptica de entrada, e η determina a relação de extinção do modulador dada por $(1 + \eta) / (1 - \eta)$.

Como $E(t)$ é convertido num sinal elétrico no fotodiodo, o sinal elétrico na saída do amplificador de RF é:

$$E_{out}(t) = \rho E(t) R G_A, \tag{2}$$

onde ρ é a responsividade do detector, R é a sua impedância e G_A é o ganho de tensão do amplificador. Como a fotocorrente é $I_F \equiv \alpha P_0 \rho/2$, a fotovoltagem gerada é:

$$V_F \equiv (\alpha P_0 \rho/2) R G_A. \tag{3}$$

Substituindo V_F e Eq. (1) em Eq. (2) :

$$E_{out}(t) = (\alpha P_0 \rho / 2) R G_A \left\{1 - \eta \sin \pi \left[V_{in}(t) / V_\pi + V_B / V_\pi \right]\right\} \tag{4}$$

ou

$$E_{out}(t) = V_F \left\{1 - \eta \sin \pi \left[V_{in}(t) / V_\pi + V_B / V_\pi \right]\right\}. \tag{5}$$

O ganho G_{out} do sinal na condição do OEO em *loop* aberto, ou seja, sem a alimentação do sinal E_{out} na entrada de RF do modulador, é dada por:

$$G_{out} \equiv \frac{dE_{out}}{dE_{in}} \Big| E_{in} = 0 \tag{6}$$

$$G_{out} = -\frac{\eta \pi V_F}{V_\pi} \cos\left(\frac{\pi V_B}{V_\pi}\right). \tag{7}$$

Nessa condição, um maior ganho é conseguido quando o modulador é polarizado em quadratura, para isso V_B = 0 ou $V_B = V\pi$. G_{out} pode ter valor positivo ou negativo, dependendo da tensão de polarização. Se $G_{out} > 0$, o modulador está polarizado positivamente caso contrário, negativamente. Quando V_B = 0, o modulador está polarizado em quadratura negativa e quando $V_B = V\pi$, o modulador está polarizado em quadratura positiva. Para que o OEO entre em oscilação, a magnitude do ganho em *loop* aberto (G_{out}) deve ser maior do que 1 [5].

O limiar de oscilação do OEO obtido a partir da Eq. (7), e considerando G_{out} = 1, é:

$$V_F = V_\pi / \left[\eta\pi \left| \cos\left(\frac{\pi V_B}{V_\pi} \right) \right| \right]. \quad (8)$$

Sendo η = 1 e V_B = 0 ou $V_B = V_\pi$, resulta:

$$V_F = V_\pi / \pi. \quad (9)$$

Um fato importante analisando as Eqs. (3) e (6) é que o uso do amplificador não é uma condição necessária para oscilação. Desde que $I_F R \geq V_\pi/\pi$, sendo G_A = 1, o amplificador não será necessário, pois a potência óptica do laser vai fornecer energia suficiente para o funcionamento do OEO. Um benefício que a retirada do amplificador traz é a eliminação do ruído de amplificação, o que resulta em um oscilador mais estável.

2.4 Parâmetros de funcionamento do OEO

Realizando uma análise dos sinais presentes no OEO, a partir da Eq. (5), pode-se determinar os quatro mais importantes parâmetros do seu funcionamento: a frequência de oscilação f_{osc}, a amplitude de oscilação V_{osc}, a largura de linha Δf e a densidade espectral de oscilação $S_{RF}(f')$. A Eq. (5), que é a saída do modulador, é não linear. O sinal de entrada do modulador $E_{in}(t)$ é um sinal senoidal como na Eq. (10):

$$E_{in}(t) = V_0 \, sin\left(\omega t + \beta\right), \quad (10)$$

onde V_0 é a amplitude, ω é a frequência angular e β a fase inicial. A saída do fotodiodo pode ser determinada com a substituição da Eq. (10) na Eq. (5). Com a utilização das funções de Bessel na Eq. (5) é obtido a Eq. (11) que mostra a saída contendo as harmônicas do sinal $E_{in}(t)$.

$$E_{out}(t) = V_F \left\{ \begin{array}{l} 1 - \eta \sin\pi\left(\dfrac{\pi V_B}{V_\pi}\right)\left[J_0\left(\dfrac{\pi V_0}{V_\pi}\right) + 2\sum_{m=1}^{\infty} J_{2m}\left(\dfrac{\pi V_0}{V_\pi}\right)\cos\left(2m\omega t + 2m\beta\right)\right] \\ -2\eta\cos\left(\dfrac{\pi V_B}{V_\pi}\right)\sum_{m=0}^{\infty} J_{2m+1}\left(\dfrac{\pi V_0}{V_\pi}\right) x \sin\left[\left(2m+1\right)\omega t + \left(2m+1\right)\beta\right] \end{array} \right\}. \quad (11)$$

Para a linearização deste sinal, faz-se necessário sua passagem através de um filtro RF com reduzida largura de banda, o que vai permitir a eliminação de todas as harmônicas. A saída linearizada é obtida a partir da Eq. (12):

$$E_{out}(t) = G(V_0)\, E_{in}\left(t\right), \quad (12)$$

sendo V_0 a amplitude do sinal de entrada e $G(V_0)$ o coeficiente do ganho de tensão, que é definido como:

$$G(V_0) = Gs\,\frac{2V_\pi}{\pi V_0} J_1\left(\frac{\pi V_0}{V_\pi}\right). \quad (13)$$

A Eq.(13) pode ser a aproximada para a Eq. (14) considerando-se um sinal de entrada pequeno [$V_0 << V_\pi$ e $J_1(\pi V_0/V_\pi) = \pi V_0/2V_\pi$], pois pode-se recuperar a partir de Eq. (12) e (13) pequenos sinais de ganho de ciclo aberto com $G(V_0) = Gs$. Ao expandir o lado direito da Eq. (13) com série de Taylor, o coeficiente de ganho fica na forma de:

$$G(V_0) = Gs\left[1 - \frac{1}{2}\left(\frac{\pi V_0}{2V_\pi}\right)^2 + \frac{1}{12}\left(\frac{\pi V_0}{2V_\pi}\right)^4\right]. \quad (14)$$

Mesmo sendo a Eq. (12) a forma linearizada do OEO, o coeficiente de linearidade $G(V_0)$ é uma função não linear da amplitude de entrada e, por conseguinte, as propriedades não lineares do modulador são mantidas. Baseado nessa relação quase linear, o princípio de superposição se mantém, e pode-se usar o modelo *feedback*-regenerativo [6] para analisar o OEO e obter seus principais parâmetros.

Quando um único modo oscilante está presente, a frequência de oscilação é denominada de f_{osc} ou $\omega_{osc} = 2\pi f_{osc}$, a amplitude de oscilação é V_{osc} e a potência de oscilação é P_{osc}, onde $P_{osc} = V_{osc}^2 / (2R)$. Desta maneira, a amplitude V_0 na Eq. (14) é apenas V_{osc}. Se o filtro de RF tem o pico de transmissão na frequência de oscilação ω_{osc} e $F(\omega_{osc}) = 1$, a amplitude de oscilação pode ser determinada fazendo $| G(V_{osc}) | = 1$ na Eq. (14) [6].

As Eqs. (15) e (16) mostram como determinar a frequência de oscilação:

$$f_{osc} = (k + 1/2)/\tau, \quad \text{para } G(V_{osc}) < 0 \tag{15}$$

e

$$f_{osc} = k/\tau, \quad \text{para } G(V_{osc}) > 0, \tag{16}$$

onde k é um número inteiro que representa os diferentes modos oscilantes possíveis e τ é o atraso de grupo total do ciclo, incluindo o atraso físico do comprimento do *loop* e o atraso de grupo resultante de componentes dispersivos no *loop* [6].

Segundo [6], sob o ponto de vista prático, o sinal $G(V_{osc})$ é determinado pelo ganho de pequeno sinais de *Gs*. Além disso, observando as Eqs. (15) e (16) pode-se verificar que a frequência de oscilação depende da polaridade do modulador. Assim, quando $Gs < 0$ a polarização é negativa e a frequência fundamental será $1/(2\tau)$, mas quando $Gs > 0$ a polarização é positiva e a frequência fundamental é $1/\tau$.

Como dito anteriormente, colocando $| G(V_{osc}) | = 1$ pode-se determinar a amplitude de oscilação do OEO. Conforme se observa nas Eqs. (17) e (19), são três as maneiras de obter a amplitude [6]:

- usando a Eq. (13):

$$\left| J_1\left(\frac{\pi V_{osc}}{V_\pi}\right)\right| = \frac{1}{2|Gs|}\frac{\pi V_{osc}}{V_\pi}; \tag{17}$$

- usando o termo de segunda ordem da Eq. (14):

$$V_{osc} = \frac{2\sqrt{2}V_{\pi}}{\pi}\sqrt{1-\frac{1}{|Gs|}}; \tag{18}$$

- usando todos os termos da Eq. (14):

$$V_{osc} = \frac{2\sqrt{3}V_{\pi}}{\pi}\left(1-\frac{1}{\sqrt{3}}\sqrt{\frac{4}{|Gs|}-1}\right)^{1/2}. \tag{19}$$

A densidade espectral de oscilação do OEO é determinada através da Eq. (20) [6]:

$$S_{RF}\left(f^{'}\right) = \frac{\delta}{\left(\delta/2\tau\right)^2 + \left(2\pi\right)^2\left(\tau f^{'}\right)^2}, \tag{20}$$

onde $f^{'}$ é a frequência de deslocamento a partir da frequência de oscilação f_{osc} e δ é a relação sinal ruído do OEO que é definida na Eq. (21):

$$\delta \equiv \rho_N G_A^2 / P_{osc}, \tag{21}$$

aqui, ρ_N é a densidade de ruído total de entrada do oscilador, que é a soma do ruído térmico, do ruído *shot* e da intensidade relativa de ruído do laser (RIN - *Relative Intensity Noise*), respectivamente mostradas na Eq. (22), G_A é o ganho do amplificador e P_{osc} é a potência de oscilação dada por $P_{osc} = V^2_{osc} / (2R)$:

$$\rho_N = 4k_B T\left(NF\right) + 2eI_{ph}R + N_{RIN}I_{ph}^2 R, \tag{22}$$

sendo k_B a constante de Boltzmann, T a temperatura ambiente, NF o fator de ruído do amplificador de RF, e a carga do elétron, I_{ph} a fotocorrente através do resistor de carga do fotodiodo, N_{RIN} o RIN do laser [6] e $2\pi f^{'}\tau << 1$ na Eq. (20).

Pode ser visto a partir da Eq. (20) que a densidade espectral do modo oscilante é uma função lorentziana de frequência. A largura total a meia altura do máximo (FWHM - *Full Width at Half-Maximum*) é dada pela Eq.(23):

$$\Delta f_{FWHM} = \frac{1}{2\pi}\frac{\delta}{\tau^2} = \frac{1}{2\pi}\frac{G_A^2 \rho_N}{\tau^2 P_{osc}}. \qquad (23)$$

Analisando a Eq. (23) é possível verificar que Δf_{FWHM} é inversamente proporcional ao quadrado do tempo de atraso do *loop* e linearmente proporcional à relação sinal ruído de entrada δ [6]. Também se verifica que para um valor fixo de ρ_N e G_A, a largura espectral de um OEO é inversamente proporcional à potência de oscilação, mas como P_{osc} e ρ_N são funções da fotocorrente, a afirmação é válida apenas quando o ruído térmico predomina no oscilador em baixos níveis de fotocorrente [5].

Como afirma [6], se um oscilador tem flutuação de fase >> 1, a densidade espectral de potência é igual à soma da densidade do ruído de fase de banda lateral única e da densidade da amplitude do ruído desta mesma banda. Quando a variação de amplitude é muito menor que a flutuação de fase, a densidade espectral de potência é apenas o ruído de fase da banda lateral única. Assim, na Eq. (20) quando $|f'| >> \Delta f_{FWHM}/2$, o ruído de fase do OEO diminui de forma quadrática com o deslocamento de frequência f'. Com um valor de f' fixo o ruído de fase diminui de forma quadrática com o tempo de atraso do *loop*. Quanto maior for τ, menor é o ruído de fase. Mas, o ruído de fase não chega a zero porque mesmo com um valor enorme de τ, o pressuposto $2\pi f' \tau << 1$ não se sustenta mais.

Analisando as Eq. (20) e (21) pode-se ver que o ruído de fase do OEO é independente de f_{osc}. Isso significa que o OEO permite a geração de sinais de alta frequência e de baixo ruído de fase. Já o ruído de fase de um sinal gerado com o método de multiplicação de frequência aumenta quadraticamente com a frequência [5].

3 DISTRIBUIÇÃO CAÓTICA DE CHAVES

Este capítulo discute a sincronização de dois e três osciladores optoeletrônicos operando em regime caótico. São consideradas duas aplicações de OEOs sincronizados em comunicações seguras. No primeiro caso, o OEO é usado para produzir uma sequência pseudoaleatória de bits. Através de simulações numéricas, a taxa de erro de bit foi calculada na presença de erro paramétrico e ruído gaussiano na potência óptica de entrada. A segunda aplicação é uma configuração para transmissão óptica segura de sinais analógicos amostrados. Por fim, mostra-se o acoplamento de dois osciladores optoeletrônicos, operando em regime caótico, para realizar um protocolo de compromisso de imagem usando os parâmetros de Stokes.

3.1. Introdução

Sistemas não lineares operando em regime caótico foram observados em várias áreas. Nos sistemas ópticos, o comportamento caótico tem sido estudado, por exemplo, em lasers com injeção óptica [7,8], ressonadores ópticos não lineares com base no efeito Kerr [9-11] e OEOs [12], cuja não linearidade na linha de realimentação é obtida pela detecção de luz, pois a fotocorrente é proporcional à potência óptica incidente. Neste trabalho considera-se exclusivamente o comportamento caótico em OEOs produzindo estados de polarização de luz caóticos [13].

Uma aplicação importante de sistemas ópticos caóticos é a criptografia de mensagens para comunicação segura entre partes autorizadas distantes. Para implementar um sistema de comunicação seguro usando as propriedades dos sistemas caóticos (pseudoaleatoriedade e alta dependência dos valores dos parâmetros), dois ou mais sistemas caóticos devem ser sincronizados. A sincronização de sistemas caóticos foi abordada primeiramente em [14,15] e a realização de um sistema óptico seguro que emprega sistemas caóticos sincronizados tem sido relatada em diversos trabalhos [16-24].

Como citado anteriormente, nesse capítulo mostra-se numericamente a sincronização de dois e três OEOs operando em regime caótico, bem como seu uso em sistemas de comunicação seguros digitais e analógicos. No primeiro caso, cada sistema

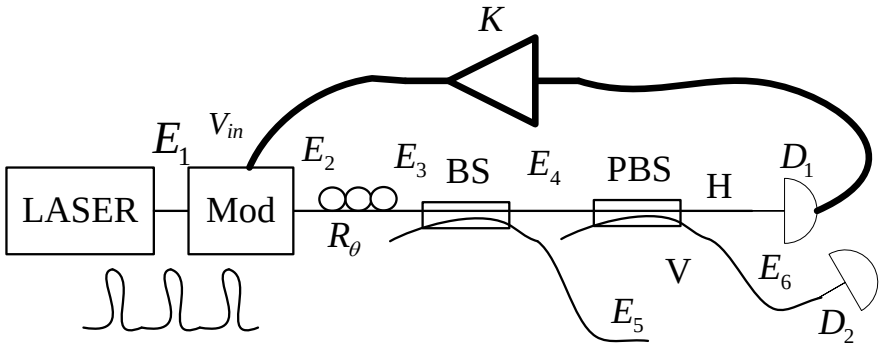
caótico sincronizado (um em Alice, o transmissor, e o outro em Bob, o receptor) gera uma chave binária a partir da quantização do parâmetro de Stokes S_1 do estado de polarização da luz na saída. Numa segunda etapa, a chave é usada para comunicação segura através de um protocolo de chave de uso único (OTP - *One-Time Pad*). Além disso, a taxa de erro na chave binária é calculada numericamente com e sem a presença de erro nos valores dos parâmetros. No que diz respeito ao sistema de comunicação analógica, é apresentada uma configuração para comunicação segura de sinais analógicos amostrados.

Por fim, é proposta uma configuração para o acoplamento de dois OEOs. Nesse esquema as saídas são dois campos elétricos com estados de polarização caóticos, em contraste com os dois OEOs sincronizados, as saídas dos OEOs acoplados são independentes. Usando esse regime caótico, é implementado um protocolo de compromisso de imagem no qual os parâmetros de Stokes dos campos de saída são usados como variáveis caóticas.

3.2. Oscilador optoeletrônico operando na geração de estados de polarização caótico

O oscilador optoeletrônico aqui considerado é semelhante ao que produz estados de polarização caóticos descritos em [13]. No entanto, diferentemente do explicado no Capítulo 2 e descrito em [13], aqui considera-se o regime pulsado, portanto, um filtro na linha de realimentação não é usado. A configuração é mostrada na Fig. 3.1.

Fig. 3.1 – Oscilador Optoeletrônico para geração de estados de polarização caóticos. Mod: Modulador de polarização eletro-óptico, R_θ - Rotacionador, BS: Acoplador, PBS: Divisor de feixe por polarização, $D_{1,2}$: Fotodetectores, K: Amplificador elétrico, E_1-E_6 são os campos elétricos nas posições marcadas.



Fonte: o autor.

Como pode ser observado na Fig. 3.1, o oscilador optoeletrônico é um esquema óptico onde a luz emitida pela fonte laser é modulada e detectada. A fotocorrente produzida é amplificada e utilizada para realimentar o modulador eletro-óptico. Além disso, o tempo necessário para a luz ser detectada em D_1 e produzir o sinal elétrico para alimentar o modulador eletro-óptico (Mod) é igual ao intervalo de tempo entre dois pulsos consecutivos gerados pelo laser. BS é um acoplador óptico (BS - *Beam Splitter*) balanceado, o PBS é um divisor de feixe de polarização (PBS - *Polarization Beam Spliter*), D_1 e D_2 são detectores ópticos e K é um amplificador elétrico.

Os estados de polarização na Fig. 2.1 e a equação de recorrência que descreve a dinâmica do OEO são [25]:

$$E_1 = \left|\alpha, \alpha\right\rangle_{HV} \tag{24}$$

$$E_2 = \left|\alpha \exp\left(j\left(\frac{\pi}{2}\frac{V_{in}(t)}{V_\pi} + \varphi\right)\right), \alpha \exp\left(-j\left(\frac{\pi}{2}\frac{V_{in}(t)}{V_\pi} + \varphi\right)\right)\right\rangle_{HV} \tag{25}$$

$$E_3 = \left|i\sqrt{2}\alpha \sin\left(\frac{\pi}{2}\frac{V_{in}(t)}{V_\pi} + \varphi\right), \sqrt{2}\alpha \cos\left(\frac{\pi}{2}\frac{V_{in}(t)}{V_\pi} + \varphi\right)\right\rangle_{HV} \tag{26}$$

$$E_4 = \left|i\alpha \sin\left(\frac{\pi}{2}\frac{V_{in}(t)}{V_\pi} + \varphi\right), \alpha \cos\left(\frac{\pi}{2}\frac{V_{in}(t)}{V_\pi} + \varphi\right)\right\rangle_{HV} \tag{27}$$

$$E_5 = \left|-\alpha \sin\left(\frac{\pi}{2}\frac{V_{in}(t)}{V_\pi} + \varphi\right), i\alpha \cos\left(\frac{\pi}{2}\frac{V_{in}(t)}{V_\pi} + \varphi\right)\right\rangle_{HV} \tag{28}$$

$$E_6 = \left|0, i\alpha \cos\left(\frac{\pi}{2}\frac{V_{in}(t)}{V_\pi} + \varphi\right)\right\rangle_{HV} \tag{29}$$

$$V_{in}(t+\tau) = K\left|\alpha\right|^2 \sin^2\left(\frac{\pi}{2}\frac{V_{in}(t)}{V_\pi} + \varphi\right). \tag{30}$$

Em Eqs. (24) - (29) a notação de Dirac $E = |\alpha_x, \alpha_y\rangle_{HV}$ corresponde ao vetor coluna do campo elétrico $E = [\alpha_x \ \alpha_y]^T$ e os índices H e V significam, respectivamente, os modos horizontal (α_x) e vertical (α_y). Em (30) τ é o intervalo de tempo entre dois pulsos de luz consecutivos. A luz gerada pelo laser é polarizada linearmente em $\pi/4$. O modulador óptico adiciona uma fase de $\pi V_{in}/(2V\pi)+\varphi$ na componente horizontal e $-\pi V_{in}/(2V\pi)-\varphi$ na componente

vertical. A tensão V_{in} é o sinal de modulação, V_π é a tensão necessária para adicionar uma fase $\pi/2$ e φ é o valor de *offset*. O rotacionador de polarização aplica uma rotação $\pi/4$ no estado de entrada. Após o rotacionador de polarização, o sinal óptico é dividido por um divisor de feixes balanceado. Uma metade é o estado de saída, E_5, e a outra metade tem as suas componentes horizontais e verticais separadas por um divisor de feixe por polarização. A parte horizontal é detectada em D_1 e a fotocorrente resultante é amplificada e utilizada como o sinal de modulação. A componente vertical é detectada em D_2 e o seu valor é usado para fins de sincronização.

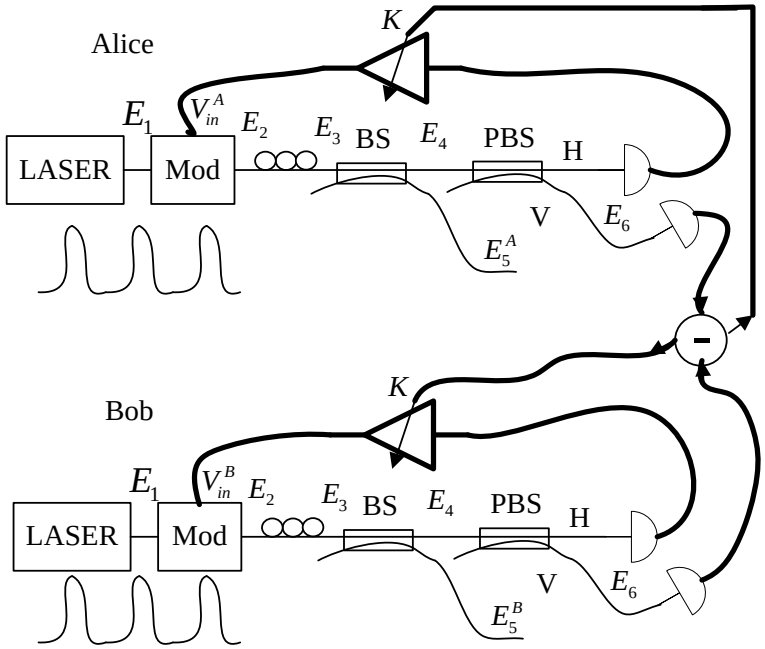
O comportamento caótico aparece para valores adequados de K, que modela o ganho do amplificador elétrico, as perdas ópticas e a eficiência do detector (D_1), a potência de entrada óptica ($|\alpha|^2$), φ e V_π. O valor inicial de V_{in} depende do ruído interno dos dispositivos eletrônicos. Devido à equação de recorrência Eq. (30), V_{in} apresenta um comportamento caótico que é traduzido para o estado de polarização de E_5.

3.3. Sincronização de dois e três OEOs operando no regime caótico

O uso de sistemas caóticos em esquemas de comunicação segura requer a sincronização entre dois ou mais sistemas caóticos. Manter esse sincronismo não é uma tarefa trivial, principalmente na presença de ruídos. A fim de manter o sincronismo, os sistemas caóticos têm que trocar informações. A sincronização de dois sistemas caóticos do tipo mostrado na Fig. 3.1 foi primeiramente apresentada em [25]. No entanto, naquela oportunidade o ruído não era considerado. Por isso, nesta seção, realiza-se uma análise mais profunda da sincronização de dois OEOs propostos em [25] e mostra-se a sincronização de três OEOs.

Como pode ser visto na Fig. 3.2, para obter a sincronização, informações sobre a potência óptica da saída vertical E_6 são enviadas de um sistema para o outro. A diferença entre esses valores é a variável de controle usada para manter os dois sistemas caóticos sincronizados e a variável controlada é o ganho do amplificador dK.

Fig. 3.2 – Dois sistemas sincronizados produzindo estados de polarização da luz caóticos.



Fonte: o autor.

A correção para ambos os sistemas é dada por:

$$dK_{A,B} = \delta \left|\alpha_{A,B}\right|^2 \left[\cos^2\left(\frac{\pi}{2} \frac{V_{in}^B(t)}{V_\pi} + \varphi \right) - \cos^2\left(\frac{\pi}{2} \frac{V_{in}^A(t)}{V_\pi} + \varphi \right) \right]. \tag{31}$$

Na Eq. (31), δ é uma constante relacionada com o detector óptico. As variáveis controladas V_{in}^A (+) e V_{in}^B (-) são:

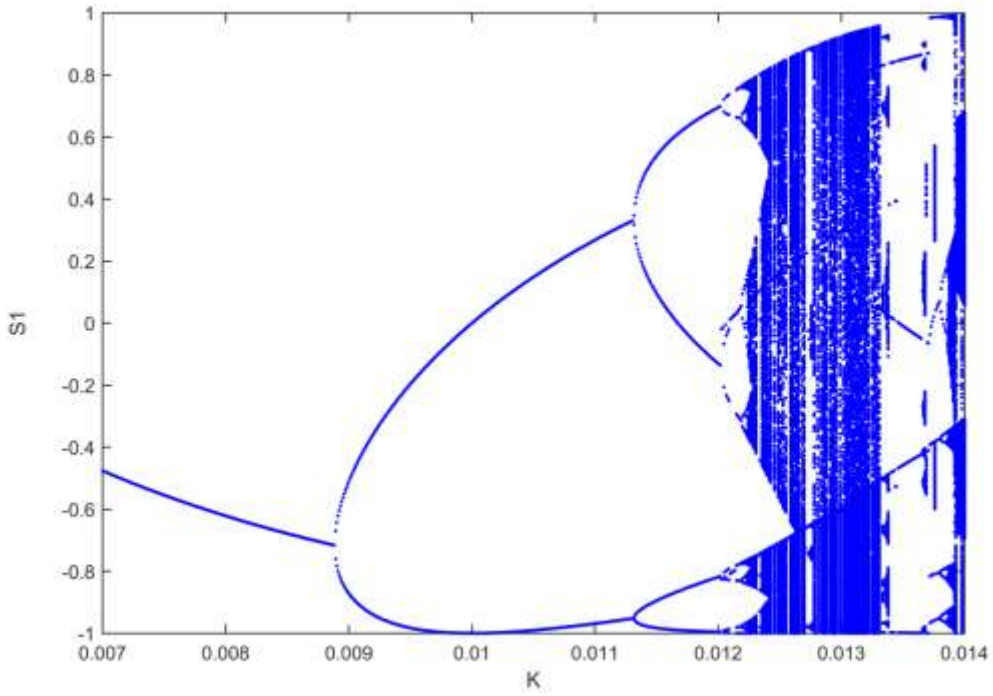
$$V_{in}^{A,B}(t+\tau) = K_{A,B} \left|\alpha_{A,B}\right|^2 \sin^2\left(\frac{\pi}{2} \frac{V_{in}^{A,B}(t)\left(1 \pm dK_{A,B}\right)}{V_\pi} + \varphi \right). \tag{32}$$

A Fig. 3.3 mostra o diagrama de bifurcação do parâmetro de Stokes S_1 de E_5. O valor de S_1 é dado por:

$$S_1^{A,B} = \varepsilon\left[\left|-\alpha_{A,B}\sin\left(\frac{\pi}{2}\frac{V_{in}^{A,B}}{V_\pi}+\varphi\right)\right|^2 - \left|i\alpha_{A,B}\cos\left(\frac{\pi}{2}\frac{V_{in}^{A,B}}{V_\pi}+\varphi\right)\right|^2\right] \quad (33)$$
$$= -\varepsilon\left|\alpha_{A,B}\right|^2\cos\left(\pi V_{in}^{A,B}/V_\pi + 2\varphi\right),$$

onde ε é uma constante que leva em conta os detalhes do polarímetro usado para medir S_1. Nesta simulação foram utilizados os seguintes valores de parâmetros: ε = 0,01, $|\alpha|^2$ = 100, φ = π/4, V_π = 1V, δ = 0,015, $K \in$ [0,007-0.014], $V_{in}^A = 0{,}1$ e $V_{in}^B = 0{,}2$ (os dois sistemas caóticos são iguais, mas eles começam com diferentes condições iniciais).

Fig. 3.3 - Diagrama de bifurcação dos sistemas sincronizados mostrados na Figura 2.2.

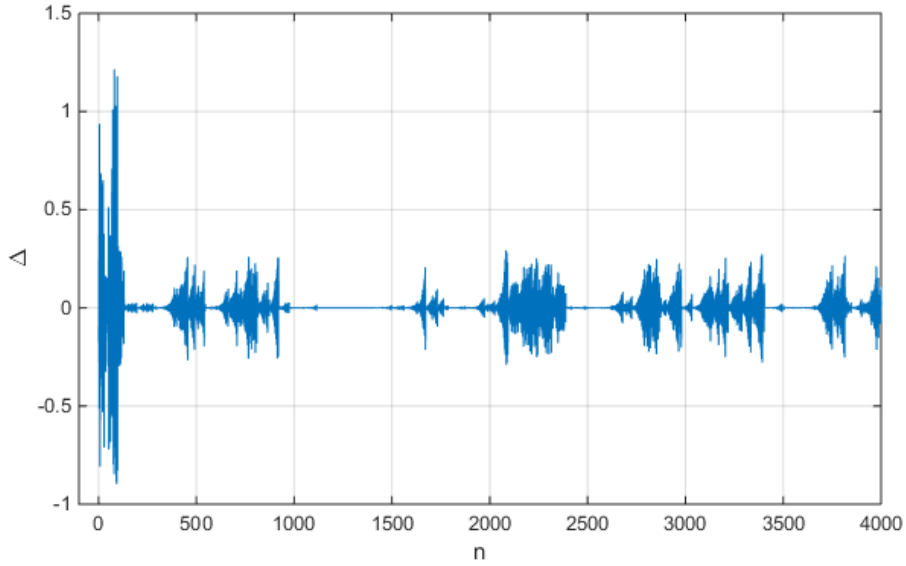


Fonte: o autor.

Utilizando os mesmos valores dos parâmetros descritos antes e $K_A = K_B$ = 0,0132, o resultado do sincronismo entre os dois sistemas pode ser visto nas Figs. 3.4 e 3.5. A Fig. 3.4 mostra $\Delta = V_{in}^A(t) - V_{in}^B(t)$ durante os primeiros 4.000 pulsos. A estratégia de sincronização é ativada somente após o pulso óptico n = 100. Como pode ser visto na Fig. 3.4, a dinâmica

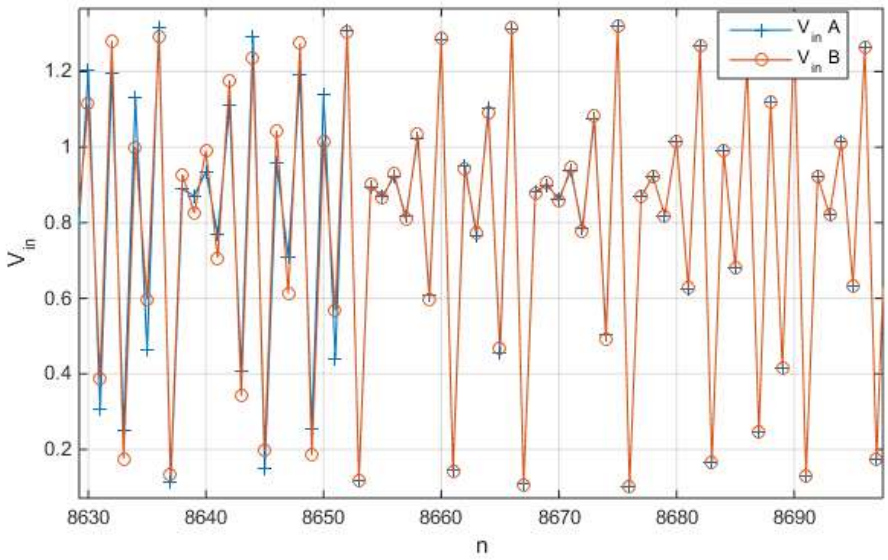
varia de sincronismo quase perfeito para perfeito várias vezes. Um exemplo desta transição é mostrado na Fig. 3.5.

Fig. 3.4 - Resultado da sincronização dos dois OEOs em regime caótico durante os primeiros 4.000 pulsos $\Delta = V_{in}^{A} - V_{in}^{B}$.



Fonte: o autor.

Fig. 3.5 - V_{in}^{A} e V_{in}^{B} durante a transição da sincronização não perfeita para a sincronização quase perfeita.



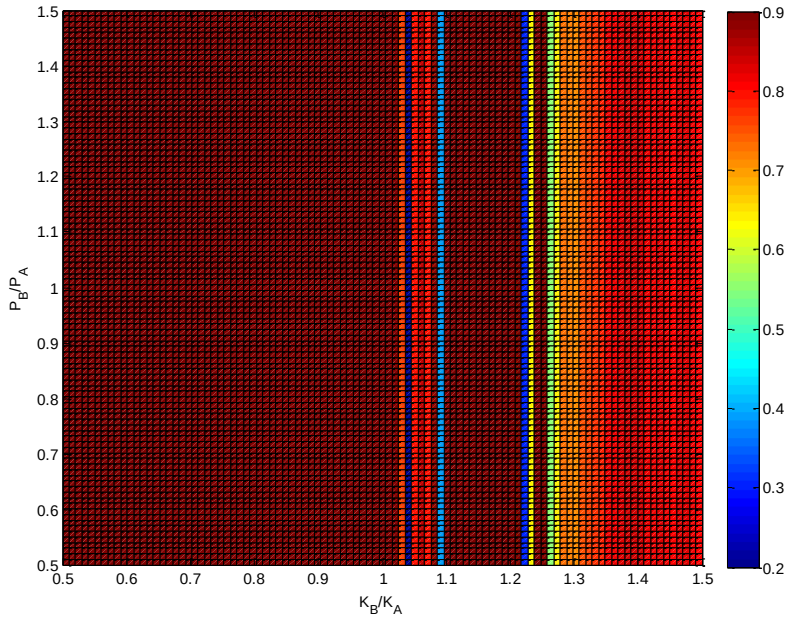
Fonte: o autor.

A desincronização mostrada nas Figs. 3.4 e 3.5 é devido ao erro paramétrico, ou seja, os dois sistemas não lineares não têm exatamente os mesmos valores de todos os parâmetros [26]. Nesse caso, os valores de $V_{in}^{A}(t=0)$ e $V_{in}^{B}(t=0)$ são intencionalmente diferentes. Para o resultado mostrado na Fig. 3.4 usa-se $V_{in}^{A}(t=0)=0{,}1$ e $V_{in}^{B}(t=0)=0{,}2$. Se for feito $V_{in}^{B}(t=0)=V_{in}^{A}(t=0)$, o erro paramétrico não existiria e a desincronização desapareceria. Por outro lado, se o erro paramétrico aumenta, $V_{in}^{B}(t=0)\gg V_{in}^{A}(t=0)$, por exemplo, a desincronização aumenta de duas maneiras: a amplitude de Δ aumenta e a duração dos intervalos de sincronização (quase) perfeita diminui. Para verificar a qualidade do sincronismo para diferentes valores de parâmetros, pode-se usar o coeficiente X_C dado por:

$$X_C=\sum_i\left(X_i^{AB}\right)^2\Big/\sqrt{\sum_i\left(X_i^{AA}\right)^2\sum_i\left(X_i^{BB}\right)^2}\,, \tag{34}$$

na qual X_i^{AB} é o *i*-ésimo elemento do vetor de correlação cruzada entre V_{in}^{A} e V_{in}^{B} enquanto X_i^{AA} (X_i^{BB}) é o *i*-ésimo elemento do vetor de autocorrelação de V_{in}^{A} (V_{in}^{B}). Uma boa (quase boa) sincronização implica em valores para X_C perto de 1 (0). Na Fig. 3.6 pode-se ver o gráfico de (34) para $P_A \equiv |\alpha_A|^2 = 100$, $\varphi = \pi/4$, $V_\pi = 1\text{V}$, $K_A = 0{,}0132$, $V_{in}^{A}(t=0)=0{,}1$, $V_{in}^{B}(t=0)=0{,}2$, $P_B \equiv |\alpha_B|^2 \in [P_A/2, 3P_A/2]$ e $K_B \in [K_A/2, 3K_A/2]$, portanto, há erro paramétrico na potência óptica de entrada e no parâmetro de ganho. Como pode ser observado na Fig. 2.6, mesmo com um descasamento dos parâmetros da ordem de até 50%, na maioria dos casos, um bom sincronismo é mantido.

Fig. 3.6 - Equação (34) versus P_B/P_A e K_B/K_A.



Fonte: o autor.

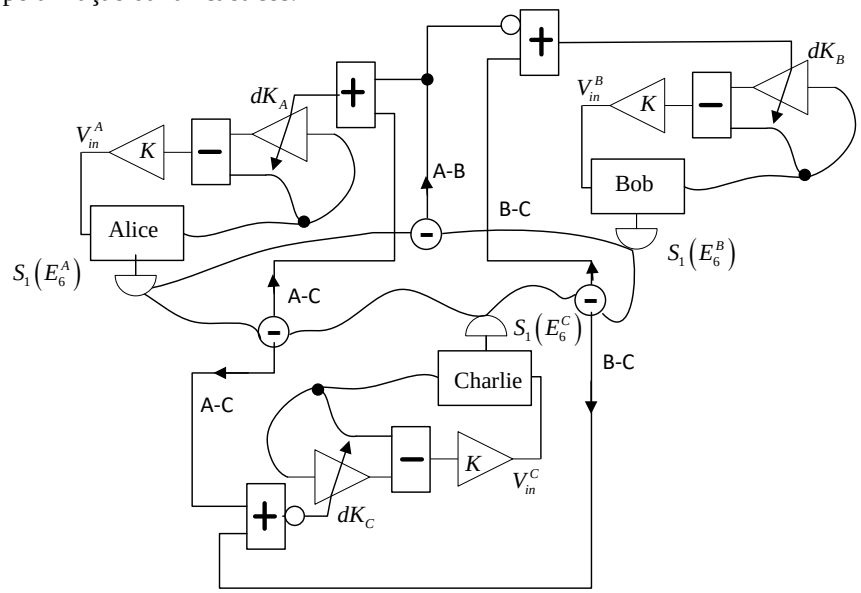
Trabalhando com Eq. (32) e usando a aproximação de pequenos sinais obtém-se que, se $\Delta_n = V_{in}^A(n\tau) - V_{in}^B(n\tau) = 0$, então

$$\Delta_{n+1} = \frac{\left(|\alpha_A|^2 K_A - |\alpha_B|^2 K_B\right)}{2}\left(1+\sin\left(\frac{V_{in}^A(n\tau)}{V_\pi}\pi\right)\right). \qquad (35)$$

Portanto, quanto mais perto de zero ($|\alpha_A|^2K_A$ - $|\alpha_B|^2K_B$) for, melhor é o sincronismo.

O próximo passo natural é a sincronização de três OEOs trabalhando no regime caótico. A Fig. 3.7 mostra o esquema para sincronizar três OEOs.

Fig. 3.7 – Esquema de sincronização de três OEOs produzindo estados de polarização da luz caóticos.



Fonte: o autor.

O esquema mostrado na Fig. 3.7 é uma extensão natural do sistema na Fig. 3.2. Os sinais modulantes são:

$$V_{in}^A(t+\tau) = K_A|\alpha_A|^2 \sin^2\left(\frac{\pi}{2}\frac{V_{in}^A(t)(1-dK_A)}{V_\pi} + \varphi\right) \tag{36}$$

$$V_{in}^B(t+\tau) = K_B|\alpha_B|^2 \sin^2\left(\frac{\pi}{2}\frac{V_{in}^B(t)(1-dK_B)}{V_\pi} + \varphi\right) \tag{37}$$

$$V_{in}^C(t+\tau) = K_C|\alpha_C|^2 \sin^2\left(\frac{\pi}{2}\frac{V_{in}^C(t)(1-dK_C)}{V_\pi} + \varphi\right), \tag{38}$$

sendo as correções são dadas por:

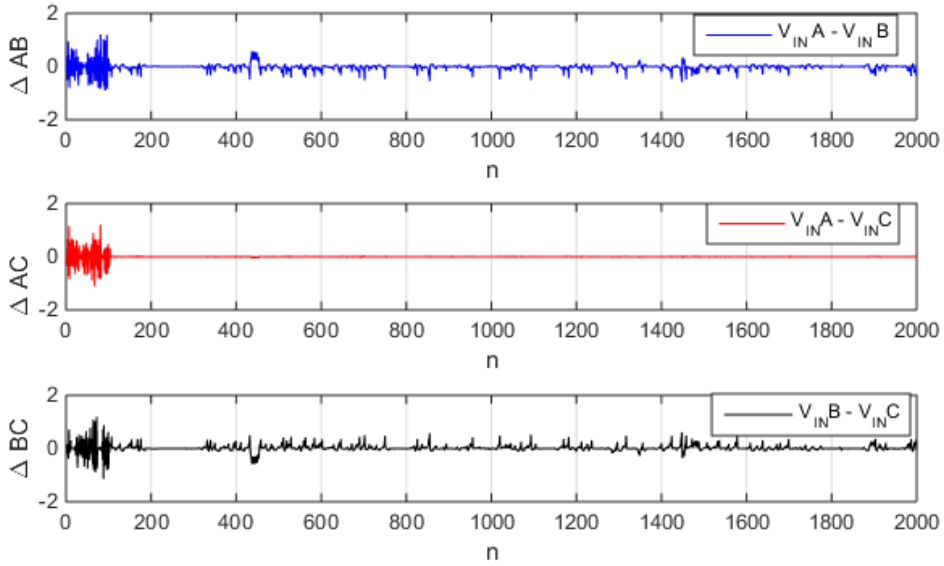
$$dK_A = \delta_A|\alpha_A|^2\left\{2\cos^2\left(\frac{\pi}{2}\frac{V_{in}^A}{V_\pi}+\varphi\right) - \cos^2\left(\frac{\pi}{2}\frac{V_{in}^B}{V_\pi}+\varphi\right) - \cos^2\left(\frac{\pi}{2}\frac{V_{in}^C}{V_\pi}+\varphi\right)\right\} \tag{39}$$

$$dK_B = \delta_B|\alpha_B|^2\left\{2\cos^2\left(\frac{\pi}{2}\frac{V_{in}^B}{V_\pi}+\varphi\right) - \cos^2\left(\frac{\pi}{2}\frac{V_{in}^A}{V_\pi}+\varphi\right) - \cos^2\left(\frac{\pi}{2}\frac{V_{in}^C}{V_\pi}+\varphi\right)\right\} \tag{40}$$

$$dK_C = \delta_C|\alpha_C|^2\left\{2\cos^2\left(\frac{\pi}{2}\frac{V_{in}^C}{V_\pi}+\varphi\right) - \cos^2\left(\frac{\pi}{2}\frac{V_{in}^A}{V_\pi}+\varphi\right) - \cos^2\left(\frac{\pi}{2}\frac{V_{in}^B}{V_\pi}+\varphi\right)\right\}. \tag{41}$$

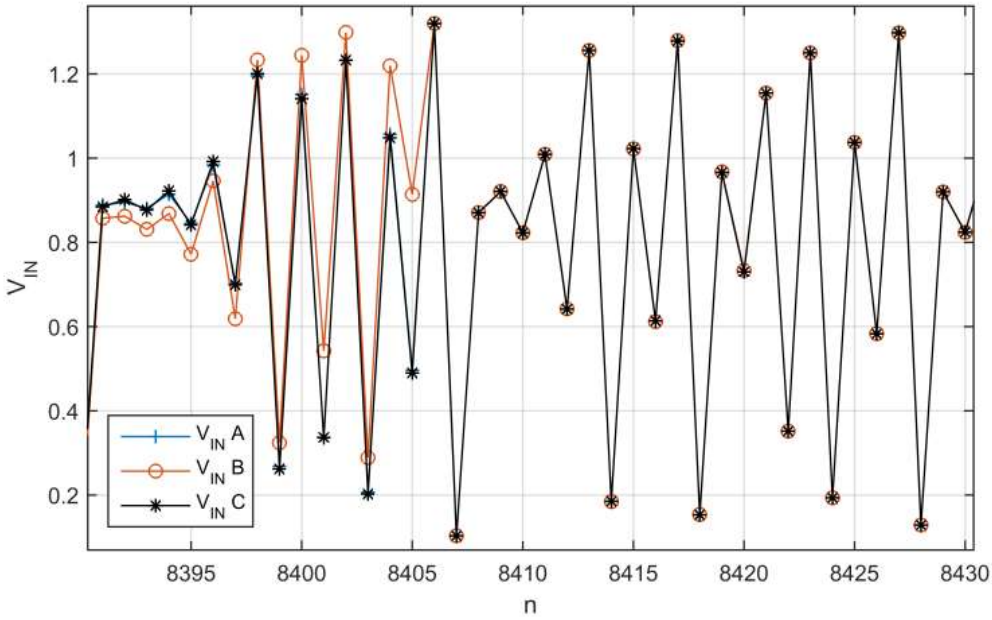
Os resultados da simulação com 10.000 pulsos de sincronização dos três OEOs operando no regime caótico podem ser vistos nas Figs. 3.8 e 3.9. Os valores dos parâmetros são $|\alpha_{A,B,C}|^2$ = 100, $\varphi = \pi/4$, V_π = 1V, δ_A = 0,0010, δ_B = 0,006, δ_C = 0,0013, $K_{A,B,C}$ = 0,0132, $V_{in}^A(t=0)$ = 0,1, $V_{in}^B(t=0)$ = 0,2 and $V_{in}^C(t=0)$ = 0,15 (os três OEOs são iguais, mas eles começam com uma condição inicial diferente). A Fig. 3.8 mostra $V_{in}^A - V_{in}^B$, $V_{in}^A - V_{in}^C$ e $V_{in}^B - V_{in}^C$ durante os primeiros 2.000 pulsos. Novamente a estratégia de sincronização é ativada somente após o centésimo pulso óptico. A partir da Fig. 3.8 pode-se observar que os osciladores OEO_A e OEO_C conseguem se manter bem sincronizados. A Fig. 3.9, por sua vez, mostra a transição da sincronização não perfeita para a sincronização quase perfeita.

Fig. 3.8 - Resultado da sincronização de três OEOs operando em regime caótico: $\Delta AB = V_{in}^A - V_{in}^B$, $\Delta AC = V_{in}^A - V_{in}^C$ *e* $\Delta BC = V_{in}^B - V_{in}^C$.



Fonte: o autor.

Fig. 3.9 - V_{in}^{A} , V_{in}^{B} e V_{in}^{C} versus número de iterações. Transição entre sincronismo não perfeito para sincronismo quase perfeito.



Fonte: o autor.

A muito boa sincronização entre OEO_A e OEO_C, quando comparada ao OEO_B, acontece porque, para o conjunto de parâmetros utilizados, o descasamento entre δ_A e δ_C é muito menor do que o descasamento entre qualquer um deles e δ_B: $|\delta_A - \delta_C| << \min(|\delta_A - \delta_B|, |\delta_B - \delta_C|)$. Trocando os valores de δ_B e δ_C e mantendo todos os outros parâmetros com os mesmos valores, resultaria em uma boa sincronização entre OEO_A e OEO_B. Por fim, usando, por exemplo, $\delta_A = \delta_B = \delta_C = 0{,}0013$, os três OEOs seriam muito bem sincronizados no entanto, em um regime periódico.

3.4. Aplicações de OEOs sincronizados em criptografia caótica

No sistema mais simples de comunicação segura, dois usuários autorizados, Alice e Bob, compartilham uma chave binária comum, X^k, normalmente gerada por um gerador de números pseudoaleatórios (PRNG - *PseudoRandom Number Generator*). Uma comunicação segura é alcançada se Alice envia para Bob a mensagem codificada $X^k \oplus M$, em que M é a mensagem secreta tendo o mesmo número de bits da chave. Além disso, a chave deve ser utilizada apenas uma vez. Uma vez que Bob tem a mesma chave, ele pode recuperar a

mensagem, fazendo $X^k \oplus (X^k \oplus M) = M$. Nesse sentido, o uso mais óbvio de sistemas caóticos em comunicação segura é usá-los como PRNGs. Cada sistema caótico (um em Alice e o outro em Bob) desempenha o papel do PRNG. Uma vez que eles estão sincronizados, espera-se que gerem a mesma chave em Alice e Bob. Quando Alice e Bob usam um PRNG algorítmico, eles devem usar a mesma semente (outra sequência binária compartilhada por Alice e Bob com antecedência), a fim de produzirem as mesmas sequências binárias que serão utilizadas como chave. Quando os sistemas caóticos são utilizados como PRNG, o segredo inicial corresponde aos parâmetros do sistema não linear.

Sistemas não lineares semelhantes, mas com valores de parâmetros diferentes, mostraram diferentes dinâmicas. A saída X^k é a sequência de bits formada pela discretização do parâmetro S_1 de Stokes do campo elétrico E_5 na saída, Eq. (33).

A fim de se obter uma sequência binária a partir dos valores contínuos de S_1, um valor de limiar S_{th} é definido. Quando $S_1 < S_{th}$ o bit "0" é obtido, de outro modo o resultado é o bit "1". Para o exemplo dado nas Figs. 3.4 e 3.5, usando em Eq.(33) ε = 0,01 e S_{th} = 0,7, obtém-se uma taxa de erro de bit (BER - *Bit Error Rate*) entre as sequências de bits obtidos por Alice e Bob de 4,78% em 10.000 bits gerados. Este erro é devido às regiões de sincronismo não perfeita como aquelas mostradas na Fig. 3.4. Na prática, um protocolo de correção de erro pode ser utilizado e uma correlação perfeita entre as sequências de bit, $X^k\left(V_{in}^A\right)$ obtida por Alice e $X^k(V_{in}^B)$ obtida por Bob pode ser alcançada.

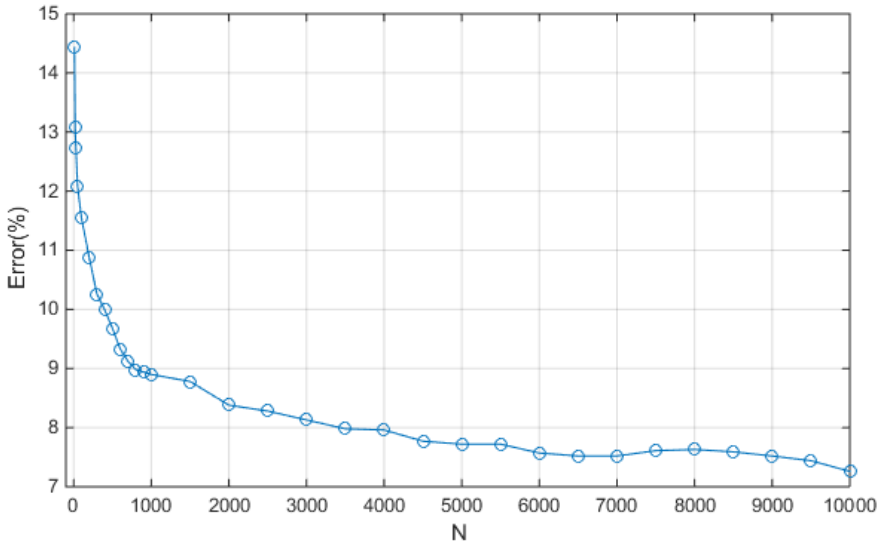
A fim de analisar a influência do ruído na taxa de erro das chaves brutas (antes da correção de erro) entre Alice e Bob, foi calculado numericamente a BER quando um ruído gaussiano é adicionado no ganho do amplificador de Bob. Neste caso, o sinal modulante de Bob é:

$$V_{in}^B\left(t+\tau\right) = K_B\left(1+\frac{x(t)}{N}\right)\left|\alpha_B\right|^2 \sin^2\left(\frac{\pi}{2}\frac{V_{in}^B(t)\left(1-dK_B\right)}{V_\pi}+\varphi\right). \tag{42}$$

Em (42), x é uma variável aleatória com distribuição normal, média zero e desvio padrão igual a 1. A variável N controla a intensidade do ruído. Com N variando na faixa de 10 a 10.000, pode-se ver na Fig. 3.10 a taxa de erro de bit (média). A taxa de erro de bit média

máxima é de 14,46% (N = 10), que é um valor que ainda permite a reconciliação entre as chaves de Alice e Bob através de um protocolo de correção de erros.

Fig. 3.10 - Taxa média de erro de bit versus força do ruído N.



Fonte: o autor.

O uso de três OEOs em comunicações seguras é uma extensão direta do que foi discutido. No entanto, neste caso, a chave final é compartilhada entre três usuários autorizados: Alice, Bob e Charlie. Simulando um sistema sem ruído externo (quando a BER é apenas devido ao sincronismo imperfeito) com ε = 0,01 e S_{th} = 0,7, consegue-se uma BER de 10,73% entre Alice e Bob, 10,63% entre Alice e Charlie e 1,08% entre Bob e Charlie para 10.000 bits.

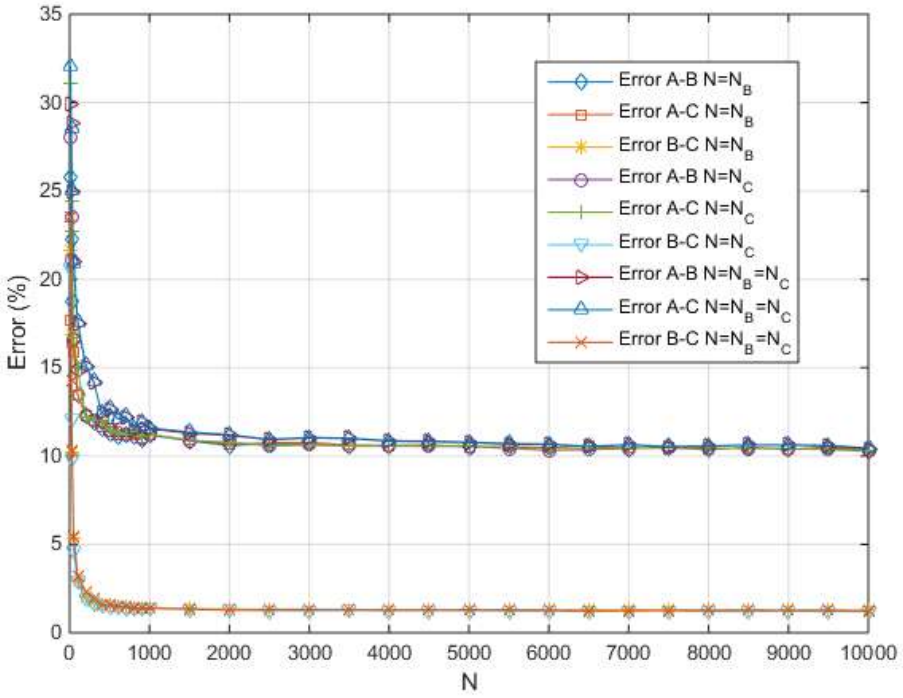
A fim de analisar a taxa de erro na presença de ruído, foi traçada a BER média versus a força do ruído em três situações: I) Ruído apenas em Bob; II) Ruído apenas em Charlie; III) Ruído em Bob e Charlie. As equações para Bob e Charlie na presença de ruído são:

$$V_{in}^{B} = K\left(1+\frac{x_B}{N_B}\right)|\alpha|^2 \sin^2\left(\frac{\pi}{2}\frac{V_{in}^{B}\left(1-dK_B\right)}{V_\pi}+\varphi\right) \tag{43}$$

$$V_{in}^{C} = K\left(1+\frac{x_C}{N_C}\right)|\alpha|^2 \sin^2\left(\frac{\pi}{2}\frac{V_{in}^{C}\left(1-dK_C\right)}{V_\pi}+\varphi\right). \tag{44}$$

Como anteriormente, nas Eqs. (43) e (44) x_B e x_C são variáveis aleatórias com desvio padrão igual a 1. As variáveis de N_B e N_C controlam a intensidade do ruído em Bob e Charlie, respectivamente. As curvas são mostradas na Fig. 3.11

Fig. 3.11 – Taxa de erro de bit entre as sequências de bits obtidas pela sincronização de três OEOs que operam no regime caótico versus o parâmetro N em (43) - (44) ($N = N_B$ quando há ruído em Bob e $N = N_C$ quando há ruído em Charlie).



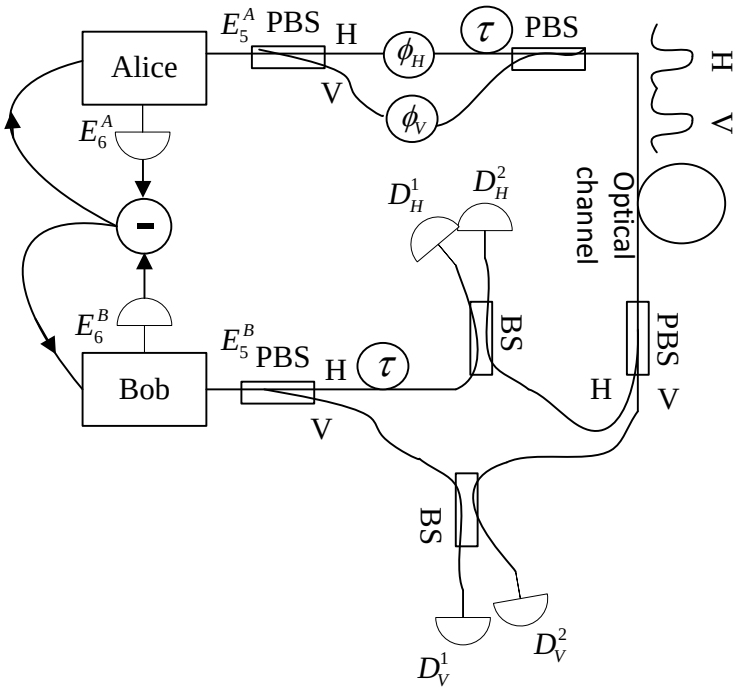
Fonte: o autor.

No procedimento de correção de erros mais simples, inicialmente Alice e Bob dividem suas sequências binárias em duas partes, $k_A = [k_{A1}\ k_{A2}]$ e $k_B = [k_{B1}\ k_{B2}]$. Eles comparam a paridade de cada parte. Se, por exemplo, PAR(k_{A1}) ≠ PAR(k_{B1}), onde PAR(X) dá a paridade do número de bits '1' em X, então sabe-se que ocorreu um erro. Nesse caso, k_{A1} e k_{B1} são divididos em dois subconjuntos e uma nova comparação de paridade é aplicada em ambos os subconjuntos. O processo é repetido até que os dois subconjuntos finais com paridades diferentes tenham apenas dois bits. Uma vez que um deles está errado, ambos são descartados

e nenhuma informação é vazada. As novas chaves são “embaralhadas” e todo o processo é repetido várias vezes. A ação de descartar um par de bits implica em uma diminuição do comprimento da chave. Em média, a fração de bits perdida durante a correção de erro, R_{ec}, é dada por $R_{ec} = (7/2)BER\text{-}BER\log_2(BER)$ [27]. Assim, na prática, a taxa máxima de erro aceitável é de cerca de 15% (R_{ec}~0,935). Assim, de acordo com os resultados numéricos mostrados nas Figs. 3.10 e 3.11, mesmo na presença de algum ruído externo, pode ser obtida uma chave útil. No entanto, o sistema com três OEOs sincronizados é mais suscetível ao ruído.

Outra possível aplicação de dois OEOs sincronizados é mostrada na Fig. 3.12. Essa implementação visa a transmissão segura de sinais analógicos amostrados.

Fig. 3.12 – Esquema para transmissão óptica segura de sinais analógicos amostrados empregando estados de polarização caótica.



Fonte: o autor.

Basicamente, o estado de polarização caótico produzido pelo OEO de Alice, E_5^A, tem seus componentes de polarização separadas por um divisor de feixe de polarização. A componente horizontal tem sua fase modulada por ($\emptyset_H$) e a vertical por ($\emptyset_V$). Além disso, a componente horizontal é atrasada no tempo de τ. Deste modo, as componentes verticais e

horizontais são lançadas no canal óptico em tempos diferentes. Quando eles chegam a Bob, eles vão sofrer interferência nos divisores de feixe BS com as componentes horizontais e verticais de E_5^B. Se os OEOs estão bem sincronizados então $E_5^A \approx E_5^B$ e os resultados das interferências dependerão apenas de $\emptyset_H$ e $\emptyset_V$.

Considerando a ação dos divisores de feixe balanceados como:

$$U_{BS}\left|\xi,\lambda\right\rangle = \left|\left(\xi+\lambda\right)/\sqrt{2},\left(-\xi+\lambda\right)/\sqrt{2}\right\rangle, \tag{45}$$

as equações que explicam o funcionamento da configuração da Fig. 3.12 são as seguintes:

- na entrada do canal óptico:

$$\left|-\alpha\sin\left(\frac{\pi}{2}\frac{V_{in}}{V_\pi}+\varphi\right)e^{i\phi_H}, i\alpha\cos\left(\frac{\pi}{2}\frac{V_{in}}{V_\pi}+\varphi\right)e^{i\phi_V}\right\rangle_{HV}; \tag{46}$$

- nas entradas dos divisores de feixe de Bob:

$$\left|-\alpha\sin\left(\frac{\pi}{2}\frac{V_{in}^A}{V_\pi}+\varphi\right)e^{i\phi_H}, -\alpha\sin\left(\frac{\pi}{2}\frac{V_{in}^B}{V_\pi}+\varphi\right)\right\rangle, \tag{47}$$

$$\left|i\alpha\cos\left(\frac{\pi}{2}\frac{V_{in}^A}{V_\pi}+\varphi\right)e^{i\phi_V}, i\alpha\cos\left(\frac{\pi}{2}\frac{V_{in}^B}{V_\pi}+\varphi\right)\right\rangle; \tag{48}$$

- nos divisores de feixe de saídas de Bob:

$$\left|\begin{array}{l}\frac{-\alpha}{\sqrt{2}}\left[\sin\left(\frac{\pi}{2}\frac{V_{in}^A}{V_\pi}+\varphi\right)e^{i\phi_H}+\sin\left(\frac{\pi}{2}\frac{V_{in}^B}{V_\pi}+\varphi\right)\right], \\ \qquad \frac{-\alpha}{\sqrt{2}}\left[-\sin\left(\frac{\pi}{2}\frac{V_{in}^A}{V_\pi}+\varphi\right)e^{i\phi_H}+\sin\left(\frac{\pi}{2}\frac{V_{in}^B}{V_\pi}+\varphi\right)\right]\end{array}\right\rangle \tag{49}$$

$$\left|\begin{array}{l}i\frac{\alpha}{\sqrt{2}}\left[\cos\left(\frac{\pi}{2}\frac{V_{in}^A}{V_\pi}+\varphi\right)e^{i\phi_V}+\cos\left(\frac{\pi}{2}\frac{V_{in}^B}{V_\pi}+\varphi\right)\right], \\ \qquad i\frac{\alpha}{\sqrt{2}}\left[-\cos\left(\frac{\pi}{2}\frac{V_{in}^A}{V_\pi}+\varphi\right)e^{i\phi_V}+\cos\left(\frac{\pi}{2}\frac{V_{in}^B}{V_\pi}+\varphi\right)\right]\end{array}\right\rangle. \tag{50}$$

A fotocorrente produzida nos detectores para os quatro campos Eqs. (49) e (50) são:

$$I_{1,2} = R\frac{|\alpha|^2}{2}\left[\begin{array}{c}\sin^2\left(\frac{\pi}{2}\frac{V_{in}^A}{V_\pi}+\varphi\right)+\sin^2\left(\frac{\pi}{2}\frac{V_{in}^B}{V_\pi}+\varphi\right)\pm \\ 2\sin\left(\frac{\pi}{2}\frac{V_{in}^A}{V_\pi}+\varphi\right)\sin\left(\frac{\pi}{2}\frac{V_{in}^B}{V_\pi}+\varphi\right)\cos\left(\phi_H\right)\end{array}\right] \tag{51}$$

$$I_{3,4} = R\frac{|\alpha|^2}{2}\left[\begin{array}{c}\cos^2\left(\frac{\pi}{2}\frac{V_{in}^A}{V_\pi}+\varphi\right)+\cos^2\left(\frac{\pi}{2}\frac{V_{in}^B}{V_\pi}+\varphi\right)\pm \\ 2\cos\left(\frac{\pi}{2}\frac{V_{in}^A}{V_\pi}+\varphi\right)\cos\left(\frac{\pi}{2}\frac{V_{in}^B}{V_\pi}+\varphi\right)\cos\left(\phi_V\right)\end{array}\right]. \tag{52}$$

Em Eqs. (51) - (52) R é a responsividade dos detectores. Agora, para $\emptyset_H = \emptyset_V = \emptyset$, tem-se:

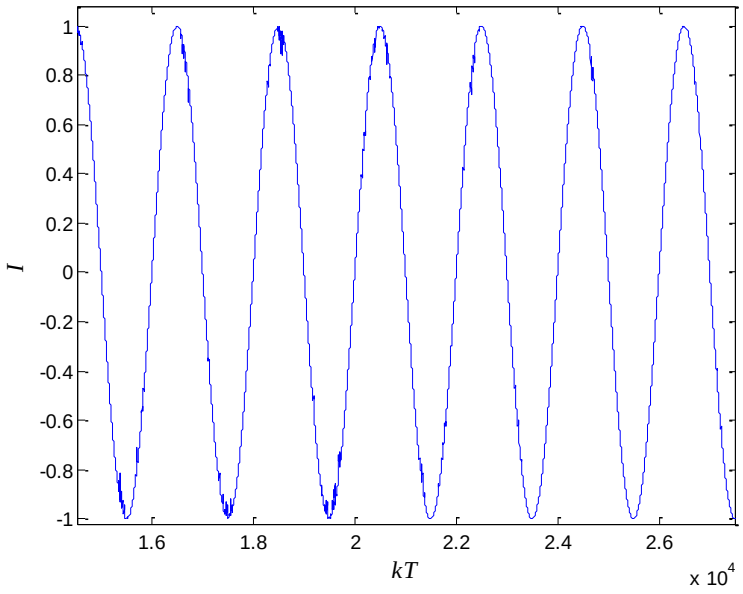
$$I = \left(I_1 - I_2\right) + \left(I_3 - I_4\right) = R\frac{|\alpha|^2}{2}\cos\left(\phi\right)\cos\left(\frac{\pi}{2}\frac{V_{in}^A - V_{in}^B}{V_\pi}\right). \tag{53}$$

Aqui assume-se que em um sinal de modulação sinusoidal amostrado, $\phi = mA\sin(\omega kT)$, m é o índice de modulação, k é um número inteiro e T é o intervalo de tempo igual à separação entre pulsos ópticos consecutivos gerados pelo laser. Para um pequeno valor de m tem-se $\cos(\phi) \sim 1-\phi = 1-mA\sin(\omega kT)$. Substituindo em Eq. (53), finalmente consegue-se:

$$I = R\frac{|\alpha|^2}{2}\left[1 - mA\sin\left(\omega kT\right)\right]\cos\left(\frac{\pi}{2}\frac{V_{in}^A - V_{in}^B}{V_\pi}\right). \tag{54}$$

Se o sincronismo entre os OEOs é perfeito, então $V_{in}^A = V_{in}^B$ e o sinal de modulação amostrado estará totalmente recuperado em Bob. Como mostrado nas Figs. 3.4 e 3.5 o sincronismo não é perfeito o tempo todo, no entanto, é bom o suficiente para fazer o cosseno em Eq. (54) próximo de um. Pode ser visto na Fig. 3.13 o resultado de uma simulação da transmissão de $\sin(kT/1000)$ ($R|\alpha|^2mA/2 = 1$) com a presença de ruído devido ao sincronismo não perfeito.

Fig. 3.13 – *I* versus *kT*.



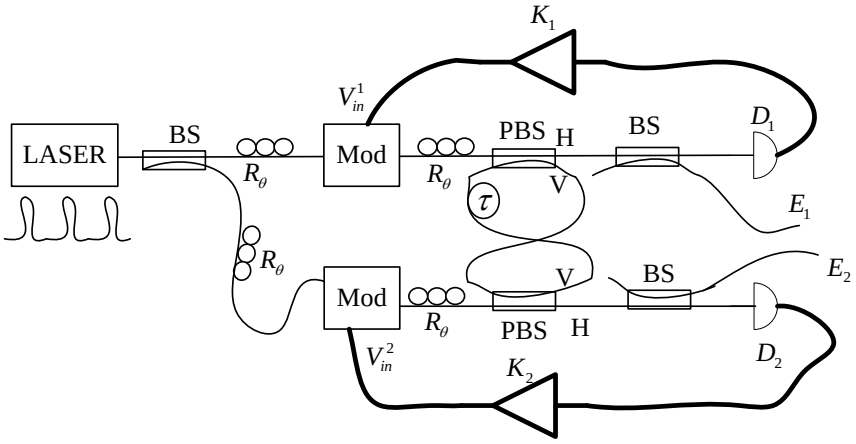
Fonte: o autor.

Assim, é o suficiente passar a corrente *I* por um filtro passa-baixa, a fim de recuperar o sinal de modulação.

3.5. Osciladores optoeletrônicos acoplados

O esquema óptico na Fig. 3.1 tem apenas uma saída caótica, no entanto, é possível combinar dois OEOs para ter dois campos de saída mostrando polarização caótica. O esquema proposto para fazer isso é mostrado na Fig. 3.14.

Fig. 3.14 – Dois OEOs acoplados produzindo duas saídas com estados de polarização caóticos.



Fonte: o autor.

Após alguns cálculos semelhantes aos mostrados em Eqs. (24) - (30), pode-se obter o conjunto de equações que descrevem a dinâmica dos OEOs acoplados na Fig. 3.14:

$$V_{in}^1(t+\tau) = K_1|\alpha|^2\left[\sin^2\left(\frac{\pi}{2}\frac{V_{in}^1(t)}{V_\pi}+\frac{\varphi_0^1+\varphi_1^1}{2}\right)+\sin^2\left(\frac{\pi}{2}\frac{V_{in}^2(t-\tau)}{V_\pi}+\frac{\varphi_0^2+\varphi_1^2}{2}\right)\right] \quad (55)$$

$$V_{in}^2(t+\tau) = K_2|\alpha|^2\left[\cos^2\left(\frac{\pi}{2}\frac{V_{in}^2(t)}{V_\pi}+\frac{\varphi_0^2+\varphi_1^2}{2}\right)+\cos^2\left(\frac{\pi}{2}\frac{V_{in}^1(t)}{V_\pi}+\frac{\varphi_0^1+\varphi_1^1}{2}\right)\right]. \quad (56)$$

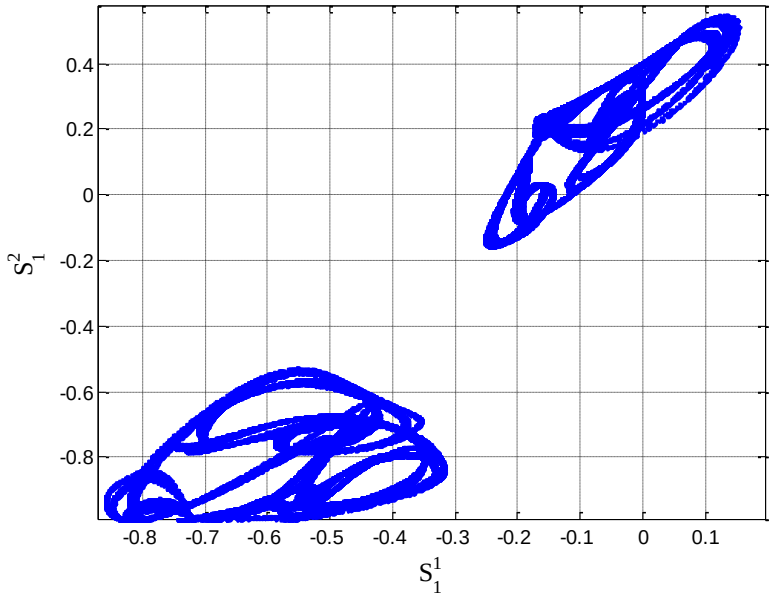
Em Eqs. (55) - (56), φ_0^1 (φ_1^1) é o valor do deslocamento de fase experimentado pelo campo horizontal (vertical) no modulador de polarização superior enquanto φ_0^2 (φ_1^2) são iguais para o modulador de polarização inferior. Os dois campos elétricos de saída são:

$$E_1 = \left| i\alpha e^{i\frac{\varphi_0^1-\varphi_1^1}{2}}\sin\left(\frac{\pi}{2}\frac{V_{in}^1(t)}{V_\pi}+\frac{\varphi_0^1+\varphi_1^1}{2}\right), \alpha e^{i\frac{\varphi_0^2-\varphi_1^2}{2}}\sin\left(\frac{\pi}{2}\frac{V_{in}^2(t-\tau)}{V_\pi}+\frac{\varphi_0^2+\varphi_1^2}{2}\right)\right\rangle_{HV} \quad (57)$$

$$E_2 = \left| -i\alpha e^{i\frac{\varphi_0^2-\varphi_1^2}{2}}\cos\left(\frac{\pi}{2}\frac{V_{in}^2(t)}{V_\pi}+\frac{\varphi_0^2+\varphi_1^2}{2}\right), \alpha e^{i\frac{\varphi_0^1-\varphi_1^1}{2}}\cos\left(\frac{\pi}{2}\frac{V_{in}^1(t)}{V_\pi}+\frac{\varphi_0^1+\varphi_1^1}{2}\right)\right\rangle_{HV}. \quad (58)$$

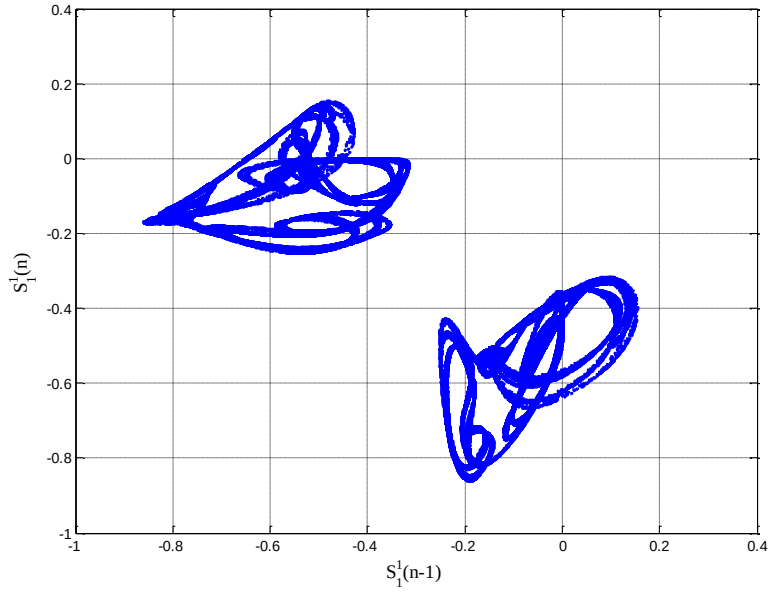
Duas coisas importantes devem ser enfatizadas: 1) O atraso de tempo τ (tempo necessário para uma volta completa da luz) é crucial para alcançar o comportamento caótico; 2) Os estados de polarização caóticos de E_1 e E_2 não estão sincronizados. Por exemplo, na Fig. 3.15 pode-se ver o parâmetro S_1 de Stokes de E_1, S_1^1, em relação aos parâmetros S_1 de Stokes de E_2, S_1^2, enquanto a Fig. 3.16 mostra $S_1^1(t)$ versus $S_1^1(t-\tau)$. Os valores de parâmetros utilizados são: $|\alpha|^2$ = 70, $\varphi_0^1 = \varphi_1^1 = \varphi_0^2 = \varphi_1^2 = \pi/4$, V_π = 1V, K_1 = 0,0132, K_2 = 0,0133, $V_{in}^1(t=0) = 0{,}1$ e $V_{in}^2(t=0) = 0{,}2$.

Fig. 3.15 – $S_1^1(t)$ versus $S_1^2(t)$.



Fonte: o Autor.

Fig. 3.16 – $S_1^1(t)$ versus $S_1^1(t-\tau)$.



Fonte: o Autor.

Na Fig. 3.15, pode-se ver que as dinâmicas caóticas das polarizações de E_1 e E_2 não estão sincronizadas. Na Fig. 3.16, observando o diagrama de fase de S_1^1, pode-se notar sua dinâmica rica. Por fim, uma vez que o sistema é pulsado, tem-se $t = k\tau$ onde k é um número inteiro. Assim, as variáveis de saída e os parâmetros de Stokes, são discretos no tempo.

O uso de sinal caótico para criptografia de imagens é um tópico quente que tem sido intensamente estudado na última década. Pode-se ver, por exemplo, em [28-30] e suas referências.

Assim, o objetivo é mostrar como o esquema óptico na Fig. 3.14, trabalhando em regime caótico, pode ser usado para produzir um protocolo de compromisso de imagem: inicialmente, no estágio de compromisso, Alice envia uma imagem colorida criptografada para Bob e uma informação extra. Na fase de revelação, Alice conta a Bob qual era a imagem criptografada e como ele pode usar essa informação para obter a imagem anunciada a partir da imagem criptografada compromissada no início do protocolo.

Antes de começar a descrever o protocolo, é importante lembrar que, para a luz totalmente polarizada os parâmetros de Stokes obedecem à relação $(s_1)^2+(s_2)^2+(s_3)^2 = 1$, onde $s_i = S_i/S_0$ e S_0 é a potência óptica total. Escolhe-se os valores dos parâmetros dos sistemas de

modo que $s_2 = 0$, portanto, tem-se $(s_1)^2+(s_3)^2 = 1$. O protocolo de compromisso de imagem N x N proposto é descrito da seguinte maneira.

Etapa de Compromisso:

1) Os parâmetros de Stokes s_1 e s_3 dos campos de saída E_1 (s_1^1, s_3^1) e E_2 (s_1^2, s_3^2), são medidos. Uma sequência de valores N^2 deles é gravada por Alice e as matrizes N x N s_{11}, s_{31}, s_{12}, s_{32} são formadas, onde:

$$s_{ij} = \begin{bmatrix} s_i^j(1) & \text{K} & s_i^j(N) \\ \text{M} & \text{O} & \text{M} \\ s_i^j(N^2 - N + 1) & \text{K} & s_i^j(N^2) \end{bmatrix}. \tag{59}$$

2) Alice escolhe aleatoriamente três operações R_p, G_p e B_p que fornecerão uma permutação dos valores das matrizes de cores R, G e B, respectivamente: $R_2=R_p(R)$, $G_2=G_p(G)$ e $B_2=B_p(B)$.

3) As matrizes permutadas são então criptografadas da seguinte maneira: $R_3 = [R_2\cdot(s_{11})^2]^{1/2}$, $G_3 = [G_2\cdot(s_{12})^2]^{1/2}$ e $B_3 = \{B_2\cdot[(s_{11})^2+(s_{12})^2]/2\}^{1/2}$. O produto e a potência das operações são feitos elemento por elemento, por exemplo, $R_3(i,j) = [R_2(i,j)$ x $(s_{11}(i,j))^2]^{1/2}$. Pode-se notar que as matrizes de imagens R, G e B utilizadas aqui possuem valores de entrada entre 0 e 1, em vez de números inteiros. A imagem criptografada (R_3,G_3,B_3) e a informação $S = p([s_3^1\ s_3^2])$, uma permutação da concatenação de s_3^1 e s_3^2, são enviadas para Bob.

Etapa de revelação:

No estágio de revelação, Alice envia para Bob as matrizes R, G e B, bem como todas as regras de permutações usadas: Rp, Gp, Bp e p. Agora, Bob pode tentar recuperar R, G e B, de R_3, G_3 e B_3 da seguinte maneira: A) Inicialmente, Bob obtém s_3^1 e s_3^2 de S usando o inverso de p e ele constrói as matrizes s_{31} e s_{32}; B) Como foi feito por Alice, Bob usa Rp, Gp e Bp em R, G e B, respectivamente, para obter R_2, G_2 e B_2; C) Bob faz $R_4 = [R_2\cdot(s_{31})^2]^{1/2}$, $G_4 = [G_2\cdot(s_{32})^2]^{1/2}$ e

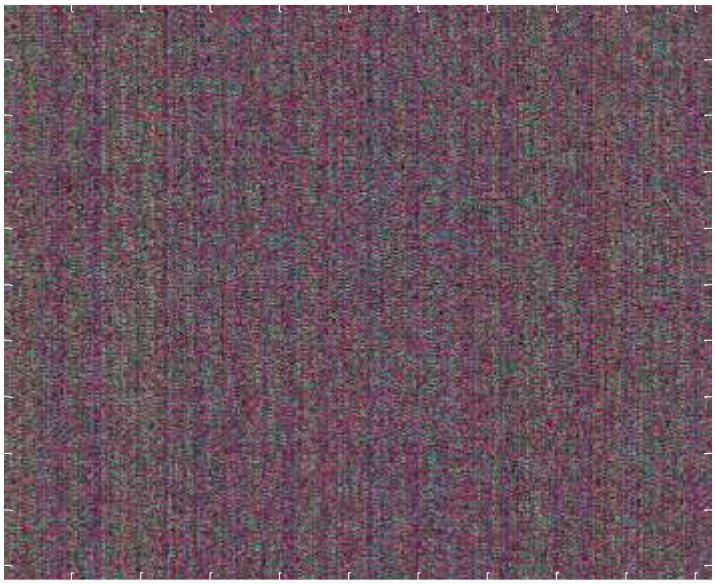
$B_4 = \{B_2 \cdot [(s_{31})^2 + (s_{32})^2]/2\}^{1/2}$; D) Bob verifica se $R_p^{-1}[R_3^2 + R_4^2] = R$, $G_p^{-1}[G_3^2 + G_4^2] = G$ e $B_p^{-1}[B_3^2 + B_4^2] = B$. Se todas as condições estiverem satisfeitas, ele acredita que Alice foi honesta.

Para a simulação do protocolo foram usados $|\alpha|^2 = 100$, $\varphi_0^1 = \varphi_1^1 = \varphi_0^2 = \varphi_1^2 = \pi/4$, $V_\pi = 1\text{V}$, $K_1 = 0{,}0132$, $K_2 = 0{,}0133$, $V_{in}^1(t = 0) = 0{,}1$ e $V_{in}^2(t = 0) = 0{,}2$. A imagem utilizada (Lena) e sua versão criptografada são mostradas nas Figs. 3.17 e 3.18.

Fig. 3.17 – Imagem da Lena antes da criptografia usando permutação aleatória e parâmetros de Stokes caóticos.

Fonte: o Autor.

Fig. 3.18 – Imagem de Lena depois da criptografia usando permutação aleatória e parâmetros de Stokes caóticos.



Fonte: o Autor.

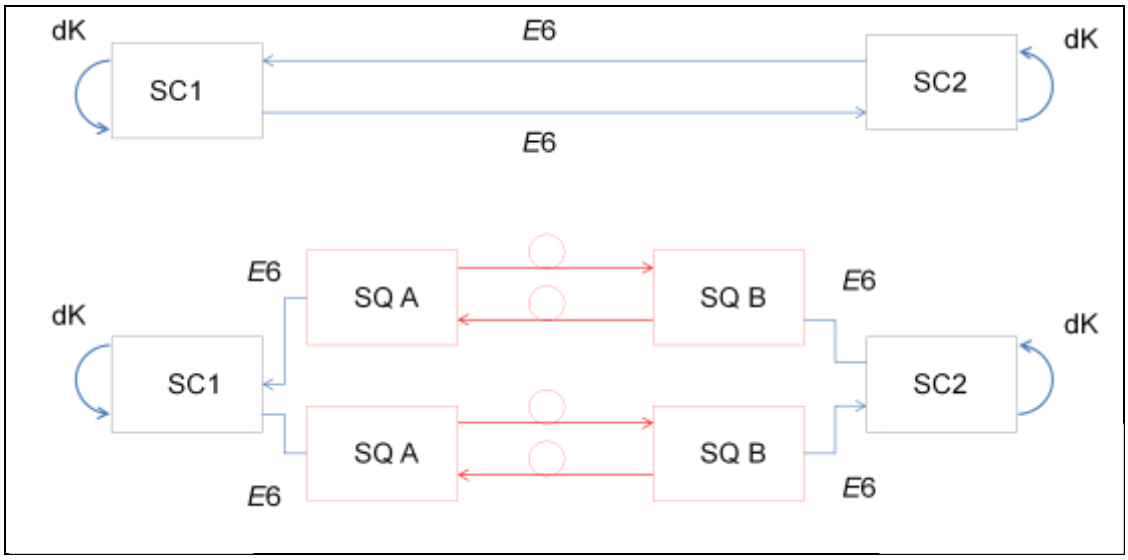
3.6. Conclusão

A sincronização de sistemas caóticos pode implementar segurança a partir da transmissão de informação entre os dois ou três OEOs. A segurança pode ser realizada através da geração de chaves para ser utilizada na transmissão segura de sinais digitais, nessa configuração os OEOs são utilizados como PRNG. Outra possibilidade é a transmissão da informação analógica embaralhada com uma variável caótica. Nos dois casos a garantia da recepção da informação está associada a realização da perfeita sincronização, que por sua vez depende da transmissão segura dos sinais de sincronismo.

Supondo que o espião possa construir um OEO idêntico aos de Alice e Bob e que tenha acesso aos variáveis iniciais, tudo o que ele precisaria fazer para ter acesso a informação transmitida entre Alice e Bob era atacar os sinais de sincronismo que são enviados de um sistema caótico para o outro. Desse que os sinais de sincronismo trafegam em uma rede de telecomunicação comum, existiria uma vulnerabilidade no sistema. Para garantir que a troca dos sinais de sincronismo possam ser feitas com segurança, pode-se pensar na utilização de

um sistema de comunicação quântico associado ao sistema caótico. A Fig. 3.19 mostra a modificação do sistema de distribuição caótica de chaves sem segurança para um sistema de distribuição caótica de chaves com segurança quântica na transmissão dos sinais de sincronismo.

Fig. 3.19 – Diferença entre um sistema de distribuição caótica de chaves sem segurança na transmissão dos sinais de sincronismo para um sistema de transmissão com segurança quântica.



Fonte: o Autor.

Como pode ser visto na Fig.3.19 o método de correção do sincronismo na nova configuração proposta continua a ser realizada através da variável *dK*.

4 DISTRIBUIÇÃO CAÓTICA DE CHAVES COM SEGURANÇA QUÂNTICA

Duas soluções para segurança de dados em redes ópticas baseadas em sistemas físicos são a criptografia quântica e a criptografia caótica. Enquanto o primeiro promete segurança incondicional, o último oferece taxas de transmissão mais elevadas, entretanto, sem segurança incondicional. Esse capítulo mostra uma configuração para o uso conjunto das duas soluções. Nesse esquema um protocolo quântico protege o sistema de distribuição caótica de chaves descrito no capítulo 3, tornando-o incondicionalmente seguro devido a proteção dada aos sinais de sincronismo trocados entre os dois sistemas caóticos.

4.1. Introdução

Se dois sistemas caóticos distantes, um em Bob e outro em Alice, estiverem sincronizados, eles podem gerar a mesma sequência de bits, que pode ser usada como chave em protocolos criptográficos. Para estarem sincronizados, Alice e Bob, como foi visto anteriormente, devem trocar informações. Neste caso, apenas os dados de sincronização viajam ao longo do canal óptico. Se um espião, Eve, quiser espionar, tudo o que ela pode fazer é detectar os sinais de sincronização para tentar usá-los na sincronização de seu próprio sistema caótico. Por isso, para tornar a distribuição de chave caótica incondicionalmente segura, os sinais de sincronização devem ser protegidos. Assim, a proposta é usar um sistema de comunicação quântica para proteger os sinais de sincronização (que, em geral, é um sinal analógico).

O oscilador optoeletrônico aqui considerado possui a mesma estrutura do oscilador que produz estados de polarização de luz caóticos descritos no capítulo 3. A configuração utilizada é a mesma mostrada na Fig. 3.1. Da mesma forma, os estados de polarização e a equação de recorrência que descrevem a dinâmica do OEO são as mesmas mostradas em Eqs. (24) - (30). Relembrando que o parâmetro de Stokes S_1 de E_5 na Fig. 3.1 é dado por:

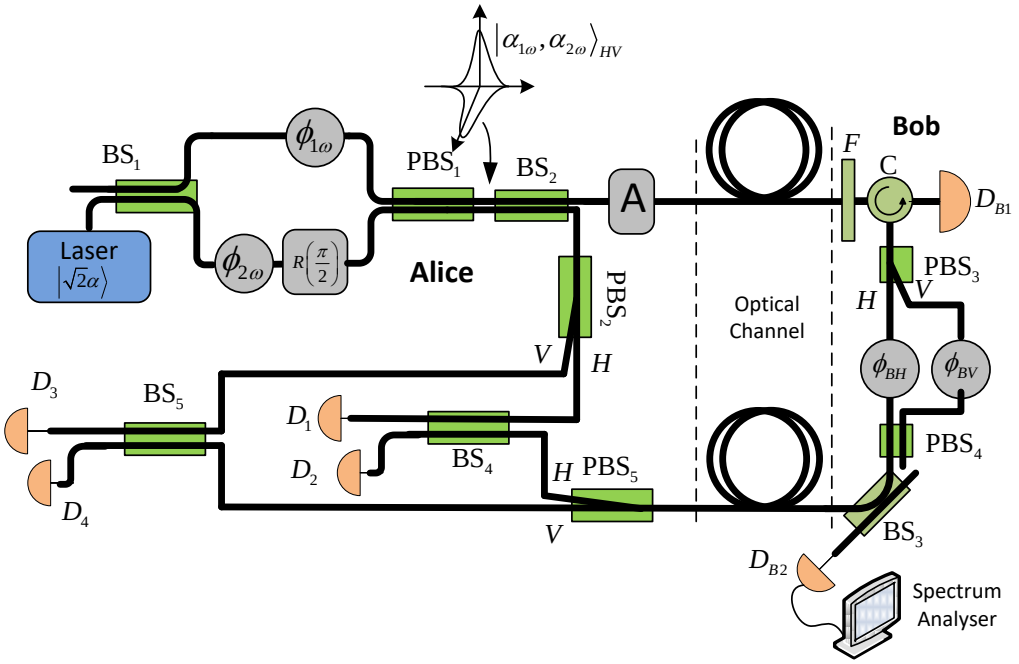
$$S_1 = -\varepsilon \left|\alpha\right|^2 \cos\left(\pi V_{in}/V_\pi + 2\varphi\right), \tag{60}$$

onde ε é uma constante que leva em consideração detalhes do polarímetro usado para medir S_1.

4.2. Distribuição de chaves caóticas com segurança quântica

A fim de tornar os sistemas de distribuição de chave caóticos discutidos no capítulo anterior incondicionalmente seguro, os sinais de sincronização trocados por Alice e Bob (e Charlie quando há três partes) devem ser protegidos contra espionagem. Para implementar um esquema de comunicação quântica que proteja os sinais de sincronização, o esquema escolhido é o proposto em [31] e mostrado na Fig. 4.1.

Fig. 4.1 - Configuração óptica para transmissão segura de sinais analógicos amostrados. BS - divisor de feixe, PBS - divisor de feixe polarizado, C - circulador óptico R - rotacionador de polarização, F - filtro óptico, D - detector, A - atenuador óptico, ϕ - modulador de fase e ϕ_ω - modulador de fase dependente da frequência.



Fonte: referência [31].

Este esquema é adequado porque pode transmitir de forma segura um sinal elétrico analógico. Na Fig. 4.1, $\phi_{1\omega}$ e $\phi_{2\omega}$ são moduladores de fase dependentes da frequência (como elementos dispersivos), enquanto ϕ_{BH} e ϕ_{BV} são moduladores de fase comuns e A é um

atenuador óptico. O filtro *F* evita que um espião use sinais ópticos em uma frequência que os detectores de Bob não podem "ver". O circulador *C* e o detector D_{B1} tornam a configuração unidirecional. A luz detectada na D_{B1} anuncia um ataque. O grupo formado pelo BS_3, D_{B2} e o analisador de espectro funciona como um cão de guarda, evitando que Eve envie sinais ópticos fortes para Bob, visando lê-los em sua saída [32,33]. Como pode ser observado, Alice usa a modulação de fase dependente da frequência, apenas conhecida por ela, para ocultar as informações da modulação de fase de Bob. Caso o pulso usado por Alice tenha um número médio de fótons menor que 1, Eve não pode determinar as funções $\phi_{1\omega}$ e $\phi_{2\omega}$. Agora, considerando a operação unitária realizada pelos divisores de feixe dado por:

$$U_{BS}\left|x,y\right\rangle = \left|\left(x+y\right)/\sqrt{2},\left(-x+y\right)/\sqrt{2}\right\rangle, \tag{61}$$

o funcionamento da configuração na Fig. 4.1 pode ser explicado da seguinte maneira [31]: os estados quânticos em PBS_2 e nas entradas do canal são, respectivamente,

$$\left|\alpha_1 e^{i\phi_1(\omega)}, \alpha_1 e^{i\phi_2(\omega)}\right\rangle_{HV} \tag{62}$$

$$\left|\alpha_2 e^{i\phi_1(\omega)}, \alpha_2 e^{i\phi_2(\omega)}\right\rangle_{HV} \tag{63}$$

$$\alpha_2 = \alpha_1 10^{-\frac{\sigma[dB]}{10}}. \tag{64}$$

Em Eq. (64), σ (em dB) é a perda do atenuador *A*. O estado total na saída de Bob é:

$$\left|\alpha_3 e^{i\left[\phi_1(\omega)+\phi_{BH}\right]}, \alpha_3 e^{i\left[\phi_2(\omega)+\phi_{BV}\right]}\right\rangle_{HV} \tag{65}$$

$$\alpha_3 = t_B t_{ab} \alpha_2. \tag{66}$$

Em Eq. (66) t_B é a transmissividade do BS_3 e t_{ab} é a transmissividade do canal óptico entre Alice e Bob. Retornando a Alice, os estados quânticos nas entradas dos divisores de feixe BS_4 e BS_5 são:

$$\left|\alpha_1 e^{i\phi_1(\omega)}, \alpha_4 e^{i\left[\phi_1(\omega)+\phi_{BH}\right]}\right\rangle \tag{67}$$

$$\left|\alpha_1 e^{i\phi_2(\omega)}, \alpha_4 e^{i\left[\phi_2(\omega)+\phi_{BV}\right]}\right\rangle \tag{68}$$

$$\alpha_4 = \alpha_3 t_{ba}. \tag{69}$$

Em Eq. (69) t_{ba} é a transmissividade do canal óptico entre Bob e Alice. Agora, usando Eq. (61), os estados nas saídas dos divisores de feixe BS_4 e BS_5 são:

$$\left|\frac{\alpha_1 e^{i\phi_1(\omega)} + \alpha_4 e^{i\left[\phi_1(\omega)+\phi_{BH}\right]}}{\sqrt{2}}, \frac{-\alpha_1 e^{i\phi_1(\omega)} + \alpha_4 e^{i\left[\phi_1(\omega)+\phi_{BH}\right]}}{\sqrt{2}}\right\rangle_{12} \tag{70}$$

$$\left|\frac{\alpha_1 e^{i\phi_2(\omega)} + \alpha_4 e^{i\left[\phi_2(\omega)+\phi_{BV}\right]}}{\sqrt{2}}, \frac{-\alpha_1 e^{i\phi_2(\omega)} + \alpha_4 e^{i\left[\phi_2(\omega)+\phi_{BV}\right]}}{\sqrt{2}}\right\rangle_{34}. \tag{71}$$

Assim, as fotocorrentes em D_1, D_2, D_3 e D_4 são dadas por:

$$I_{1,2} = R\left[\frac{\alpha_1^2 + \alpha_4^2}{2} \pm \alpha_1\alpha_4 \cos\left(\phi_{BH}\right)\right] \tag{72}$$

$$I_{3,4} = R\left[\frac{\alpha_1^2 + \alpha_4^2}{2} \pm \alpha_1\alpha_4 \cos\left(\phi_{BV}\right)\right]. \tag{73}$$

Em Eqs. (72) e (73) R é a responsividade dos detectores, assumida como sendo o mesmo valor para todos eles. Agora, fazendo $I = (I_1\text{-}I_2) + (I_3\text{-}I_4)$ resulta em:

$$I = 2R\alpha_1\alpha_4\left[\cos\left(\phi_{BH}\right) + \cos\left(\phi_{BV}\right)\right]. \tag{74}$$

O sinal modulante analógico $V(t)$ tem $\phi_{BH} = mV_H(kT)$ e $\phi_{BV} = mV_V(kT)$, onde m (<< 1) é o índice de modulação, k é um número inteiro e T é o passo de tempo, igual à separação de tempo entre pulsos ópticos consecutivos gerados pelo laser. Para um pequeno valor de m

tem $\cos(\phi_{BH}) \sim 1-\phi_{BH} = 1 - mV_H(kT)$ e, de forma semelhante, $\cos(\phi_{BV}) \sim 1 - mV_V(kT)$. Substituindo estas expressões em (74), resulta:

$$I \approx 2R\alpha_1\alpha_4\left\{2-m\left[V_H\left(kT\right)+V_V\left(kT\right)\right]\right\}. \tag{75}$$

Observando Eq. (75), pode-se notar que $V(t) = V_H(t) + V_V(t)$ enviado de forma segura por Bob pode ser recuperado por Alice.

No que diz respeito à distribuição de chave caótica usando dois OEOs sincronizados, são necessárias duas configurações de comunicação quântica do tipo mostrado na Fig. 4.1 (uma vez que a sincronização é bidirecional). Para o sistema de comunicação quântica usado por Alice (Bob) para receber o sinal de sincronização de Bob (Alice) de forma segura, Bob (Alice) usa o sinal proveniente da detecção de E_6 para modular ϕ_{BH} e ϕ_{BV} (ϕ_{AH} e ϕ_{AV}).

Uma vez que Eve não consegue descobrir os valores de $\phi_{1\omega}$ e $\phi_{2\omega}$, o melhor que ela pode fazer é usar um divisor de feixe com refletividade igual à perda total entre Alice e Bob e mudar a fibra entre Alice e Bob por um fibra sem perdas. Na saída de Bob, Eve usa o mesmo aparelho de Alice. Nesse caso, Eve teria:

$$I \approx 2R\alpha_2\alpha_4\left\{2+m\left[V_H\left(kT\right)+V_V\left(kT\right)\right]\right\}. \tag{76}$$

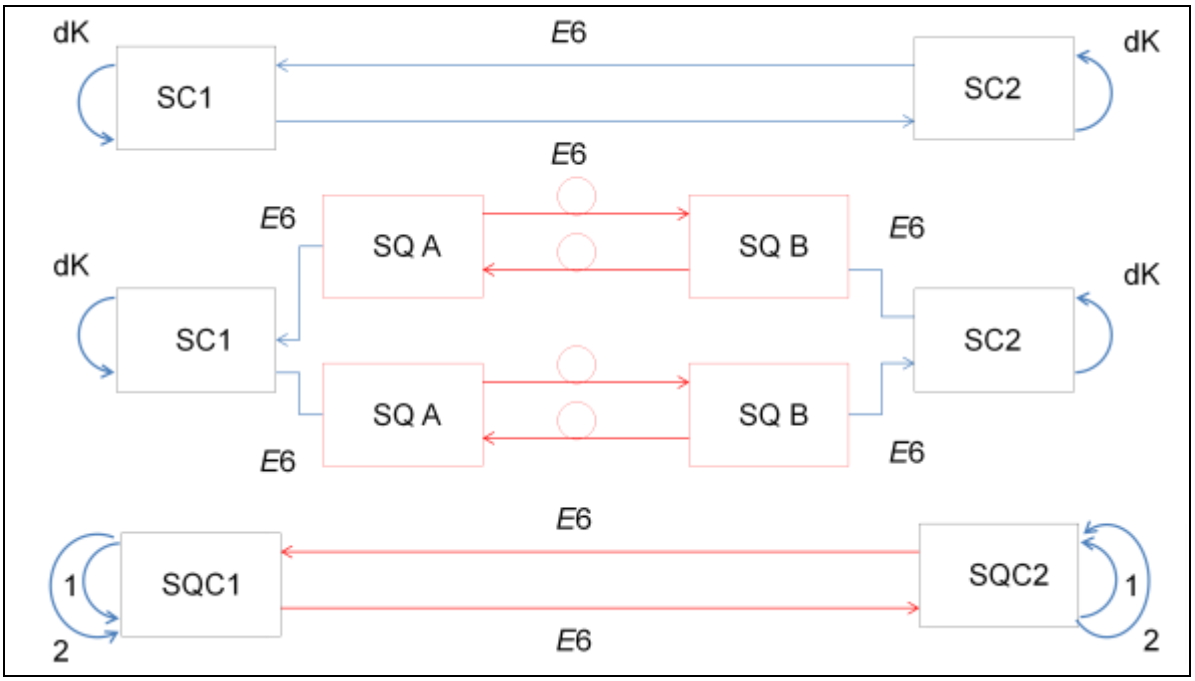
Uma vez que $\alpha_2 << \alpha_1$, o sinal obtido por Eve seria muito fraco e não detectável (é uma detecção homódina em que o sinal e o oscilador local são muito fracos). Por fim, a extensão para o caso com as três partes autorizadas é trivial.

4.3. Conclusão

O sistema de distribuição caótico de chaves com segurança quântica pode garantir uma segurança incondicional na transmissão dos sinais de sincronismo, porém os sistemas caótico e quântico nessa configuração trabalham de forma separada, ou seja, são totalmente independentes.

Pensando em reduzir a complexidade do sistema proposto, pode-se elaborar uma configuração que realize a integração total entre os sistemas caótico e quântico. Isso irá permitir que a chave produzida dependa tanto da dinâmica caótica quanto da sincronização enviada por estados quânticos. A Fig. 4.2 mostra a diferença da configuração do sistema de distribuição caótico de chaves com segurança quântica para o sistema integrado de distribuição quantum-caótica de chaves.

Fig. 4.2 – Diferença entre um sistema de distribuição caótica de chaves com segurança quântica para o sistema integrado de distribuição quntum-caótico de chaves.



Fonte: o Autor.

A integração dos sistema também exige uma alteração no método de correção do sincronismo, enquanto nas duas configurações anteriores a variável *dK* é a responsável pela manutenção do sincronismo, no sistema quantum-caótico haverá duas condições de manutenção do sincronismo (1 e 2) como visto na Fig. 4.2

5 DISTRIBUIÇÃO QUANTUM-CAÓTICA DE CHAVES

Neste capítulo, é apresentado um esquema óptico para distribuição quantum-caótica de chaves. A chave produzida depende da dinâmica caótica e a sincronização entre o OEO de Alice e o de Bob usa estados quânticos. Um ataque nos sinais de sincronização irá perturbar a sincronização dos sistemas caóticos aumentando a taxa de erro na chave final, indicando assim a presença da espiã.

5.1. Introdução

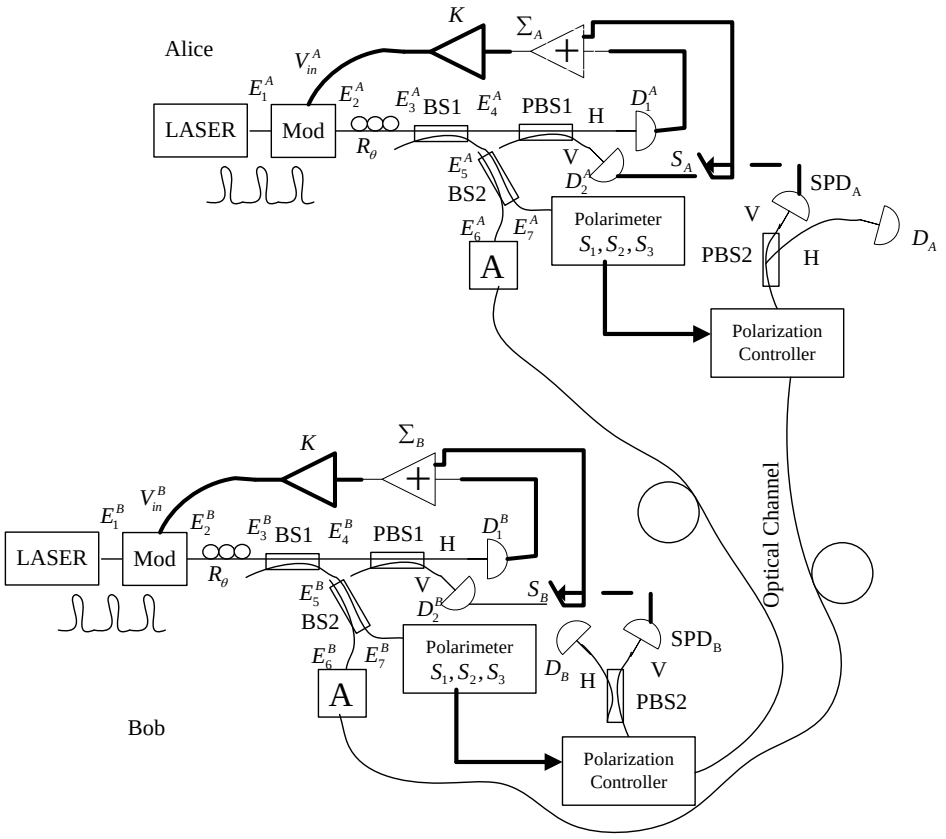
Como visto anteriormente, a distribuição caótica de chaves (DCC) requer, pelo menos, dois sistemas caóticos sincronizados e aproveita a pseudoaleatoriedade e alta dependência dos valores dos parâmetros para proteger a informação [12,18-21,24]. A distribuição quântica de chaves (DQC), por sua vez, usa escolhas aleatórias de estados quânticos (não ortogonais) e/ou bases de medição, bem como o teorema de não clonagem, para garantir a segurança da informação [34-37]. As propostas de colocar DCC e DQC para trabalharem em conjunto [17,25], como a mostrada no capítulo 4, possuem os sistemas quântico e caótico claramente distintos. São como módulos conectados. Nesse capítulo, é proposta uma configuração para a distribuição quantum-caótica na qual os sistemas quântico e caótico são integrados em apenas um sistema: a chave produzida depende da dinâmica caótica e a sincronização entre os OEOs de Alice e Bob usa estados quânticos. Como será mostrado a seguir, este é um tipo muito diferente de distribuição quântica de chaves, uma vez que os estados quânticos não carregam os bits da chave, eles são responsáveis por manter a sincronização dos sistemas caóticos.

Mais uma vez o oscilador optoeletrônico aqui considerado é o mesmo descrito no capítulo 3. A configuração utilizada para cada OEO individual é a mesma mostrada na Fig. 3.1.

5.2. Distribuição quantum-caótica usando OEOs sincronizados

A configuração óptica para criptografia quantum- caótica é mostrada na Fig. 5.1.

Fig. 5.1. Esquema para distribuição quantum-caótica de chaves. $SPD_{A,B}$ – Detector de fótons únicos, A – Atenuador óptico, $S_{A,B}$ – Chave elétrica e $\Sigma_{A,B}$ - Somador elétrico.



Fonte: o Autor.

O sistema na Fig. 5.1 funciona da seguinte forma:

1. Em Alice (Bob), o campo de saída E_5^A (E_5^B) é dividido por um divisor de feixe. Uma parte é fortemente atenuada pelo atenuador óptico *A* e enviada para Bob (Alice) através do canal óptico. A segunda parte tem sua polarização medida por um polarímetro. Esta informação é usada para controlar um controlador de polarização de tal forma que, se a luz proveniente de Bob (Alice) tiver o mesmo estado de polarização medido por Alice (Bob), ela é guiada para o detector $D_{A(B)}$. Por exemplo, se o estado de polarização medido pelo polarímetro é o estado de polarização linear $|\phi\rangle = \cos(\phi)|H\rangle + \sin(\phi)|V\rangle$, então o controlador de polarização é configurado para $R(-\phi)$, uma vez que $R(-\phi)|\phi\rangle = |H\rangle$ (R é um rotacionador de polarização). Portanto, Alice (Bob) escolhe a base de medição (controlador de polarização e PBS) de

acordo com o estado de polarização da luz de saída (dele). A detecção no $SPD_{A(B)}$ fecha o interruptor elétrico $S_{A(B)}$. Neste caso, a equação de recorrência (30) torna-se apenas

$$V_{in}^{A,B}\left(t+\tau\right)=K_{A,B}\left|\alpha_{A,B}\right|^2. \tag{78}$$

2. A sequência de bits (chave) de Alice (Bob) é formada pela discretização do parâmetro de Stokes S_1 do campo óptico de saída $E_7^A(E_7^B)$. Para obter uma sequência binária a partir dos valores contínuos de $S_1^{A,B}$, um valor de limiar S_{th} é definido e, quando $S_1^{A,B} < S_{\text{th}}$ o bit '0' é obtido de outra forma, o bit '1 ' é obtido.

No cenário de sincronização perfeita, ambos os sistemas caóticos produzirão os mesmos estados de polarização da luz nas saídas, $E_7^A = E_7^B$, e a chave formada será a mesma, pois $S_1^A = S_1^B$, implicando em um taxa de erro de bit zero. Por outro lado, uma sincronização não perfeita resultará em uma taxa de erro diferente de zero: quanto menor a sincronização, maior será a taxa de erro. Na falta de sincronização, a taxa de erro é de cerca de 50%. Por isso, neste esquema, os sinais de sincronização (estados fracos e coerentes) são cruciais para a análise de segurança.

Como discutido anteriormente, a sincronização consiste em mudar a equação de recorrência de Eq. (30) para Eq. (78), o que acontece quando um pulso de luz proveniente de Bob (Alice) é detectado por Alice (Bob). As probabilidades de detecção em SPD_A (q_A) e SPD_B (q_B) são dadas por:

$$q_A=\min\left\{p_A t_c\left|\alpha_b\right|^2\sin^2\left(\frac{\pi}{2}\frac{\left[V_{in}^A(t)-V_{in}^B(t)\right]}{V_\pi}\right),1\right\} \tag{79}$$

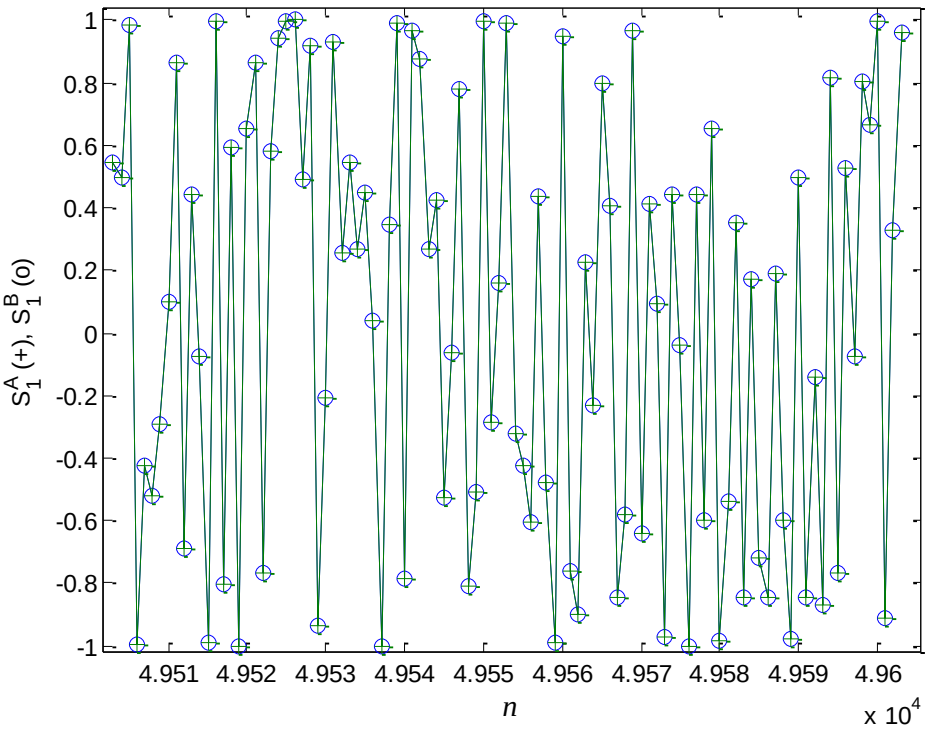
$$q_B=\min\left\{p_B t_c\left|\alpha_a\right|^2\sin^2\left(\frac{\pi}{2}\frac{\left[V_{in}^A(t)-V_{in}^B(t)\right]}{V_\pi}\right),1\right\}. \tag{80}$$

Em Eqs. (79) - (80), p_A (p_B) é a probabilidade do detector de fótons único de Alice (Bob) produzir um sinal elétrico detectável quando um fóton chega, $|\alpha_a|^2$ ($|\alpha_b|^2$) é o número médio de fótons (inferior a 1) do pulso que sai de Alice (Bob), isto é, após a atenuação, e t_c é o coeficiente de transmissão do canal. Quanto menor os valores de q_A e q_B, pior é a

sincronização e grande é a taxa de erro de bits. Assim como no QKD (*Quantum Key Distribution*) tradicional, existe uma distância máxima para a qual a taxa de erro ainda é aceitável.

Foi realizada uma simulação com 49.603 pontos e com os seguintes valores de parâmetros: $|\alpha_A|^2 = |\alpha_B|^2 = 2.500$, $\varepsilon_A = \varepsilon_B = 1/2.500$, $\varphi = \pi/4$, $V_\pi = 1\text{V}$, $K_A = K_B = 0{,}0133$, $p_A t_c |\alpha_b|^2 = p_B t_c |\alpha_a|^2 = 0{,}04$, $V_{in}^A(t=0) = 0{,}1$ e $V_{in}^B(t=0) = 0{,}2$ (os dois sistemas caóticos são iguais, mas eles começam com diferentes condições iniciais para V_{in}). Além disso, os OEOs funcionam sem sincronismo durante os primeiros 100 intervalos de tempo. Pode-se ver os cem últimos valores de S_1 para Alice e Bob na Fig. 5.2, onde o sincronismo quase perfeito entre os parâmetros de Stokes S_1^A (+) e S_1^B (o) (n é o número do intervalo tempo) é mostrado. A taxa de erro foi de 0,54% em uma sequência de 49.603 bits.

Fig. 5.2 - S_1^A e S_1^B versus n (sincronismo quase perfeito).



Fonte: o Autor.

Uma segunda simulação com $V_{in}^A(t=0) = 0.1$ e $V_{in}^B(t=0) = 1$ (e os outros parâmetros com os mesmos valores) produz uma taxa de erro em torno de 1%. Pode-se

também aumentar o erro paramétrico [26] fazendo $K_A \neq K_B$, no entanto, de acordo com Eq. (30) e Eq. (78) uma boa sincronização requer $K_A|\alpha_A|^2 = K_B|\alpha_B|^2$, portanto, pode-se alterar a potência do laser para compensar um descasamento dos valores de ganho.

5.3. Análise de segurança

Para obter os bits da chave, um espião deve ter um OEO sincronizado com o OEO de Alice e Bob. Assim, o espião terá que atacar os sinais quânticos utilizados na sincronização e adivinhar corretamente (dentro de uma faixa estreita) os valores dos parâmetros dos OEOs usados por Alice e Bob, caso contrário, o erro paramétrico não permitirá uma boa sincronização e a taxa de erro de bit aumentará. Assim, como esperado, a segurança da distribuição quantum-caótica é garantida por regras da física quântica e do caos.

Durante um ataque, o espião não pode diminuir o número médio de fótons dos pulsos de luz que chegam a Alice e Bob (por exemplo, aumentando a perda do canal inserindo um divisor de feixe), uma vez que isso piora a sincronização, aumentando a taxa de erro de bit. Por outro lado, o espião pode fazer um ataque que aumentaria a detecção nos detectores de fótons únicos de Alice e Bob. Por exemplo, fortes pulsos de luz podem ser enviados para Alice e Bob. Para evitar este tipo de cavalo de Tróia, o detector óptico D_A (D_B) está conectado à saída horizontal do PBS_2 em Alice (Bob) para verificar se os pulsos de luz fortes estão sendo enviados por um espião.

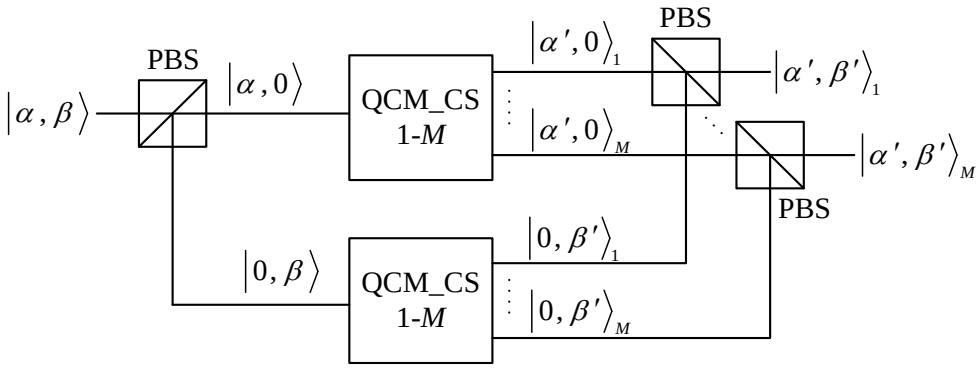
Por fim, o espião pode apenas medir os sinais de sincronização e enviar estados coerentes fracos para Alice e Bob em estados de polarização que estejam de acordo com os resultados da medição. Sem saber em que base medir (a polarização da luz dos pulsos enviados por Alice e Bob segue uma dinâmica caótica, portanto, é uma variável contínua), o espião irá introduzir um ruído que aqui é modelado por uma variável aleatória uniforme. As simulações numéricas mostraram um erro em torno de 50% neste caso.

Pode-se considerar também um ataque por máquina de clonagem quântica, no qual Eve usa uma máquina de clonagem quântica de estados coerentes (QCM_CS - *Quantum Cloning Machine of Coherent States*) [38-44] para produzir *M* cópias dos estados de polarização enviados por Alice e Bob. Para fazer a clonagem, Eve primeiro separa as componentes horizontal e vertical usando um PBS, em seguida ela clona cada componente

separadamente. Por fim, ela junta os componentes novamente para obter os clones do estado de polarização.

O processo para a máquina de clonagem de $1 \rightarrow M$, é mostrado na Fig. 5.3 [45]. A fidelidade da clonagem gaussiana de estados coerentes não depende do número médio de fótons e é dada por $F_c = M/(2M\text{-}1)$ [38]. Uma vez que a clonagem da polarização requer a clonagem dos dois componentes, a fidelidade da clonagem de polarização é dada por $F = [M/(2M\text{-}1)]^2$.

Fig. 5.3 – Clonagem quântica da polarização de estados coerentes de dois modos.



Fonte: referência [45].

Com o objetivo de simplificar a análise, é considerada a situação mais favorável para Eve. Supõe-se que seja suficiente para ela clonar apenas os estados de polarização que vão de Alice a Bob (ou vice-versa). Além disso, assume-se que a Eve pode sincronizar seu sistema caótico (com os de Alice e Bob) usando o estado de polarização clonado (esta é uma situação muito pouco realista). Eve usa $M = 2$, isto é, ela mantém um estado e manda o outro para Bob. Nessas circunstâncias, a probabilidade de detecção em Bob é

$$q_B = \min\left\{ p_B t_c |\alpha_a|^2 (1-F), 1 \right\} = \min\left\{ p_B t_c |\alpha_a|^2 \frac{5}{9}, 1 \right\}. \quad (81)$$

Considerando (80), isso é equivalente a $V_{in}^A(t) - V_{in}^B(t) \sim 0{,}5$, o que significa um sincronismo fraco entre Alice e Bob. De fato, simular o protocolo criptográfico quântico

caótico sob o ataque da máquina de clonagem quântica de Eve produz uma taxa de erro de ~ 48%, denunciando o ataque.

6 GERAÇÃO DE HARMÔNICOS COM RESSONADORES ÓPTICOS A FIBRA

Este capítulo apresenta um conjunto de esquemas utilizando ressonadores e moduladores ópticos para a geração de harmônicas. São apresentadas três configurações experimentais para geração fotônica de harmônicos de um sinal RF. As configurações são baseadas em um ressonador com laço de fibra. A vantagem das configurações propostas, além da simplicidade de sua implementação, é o grande número de harmônicas produzidas.

6.1. Introdução

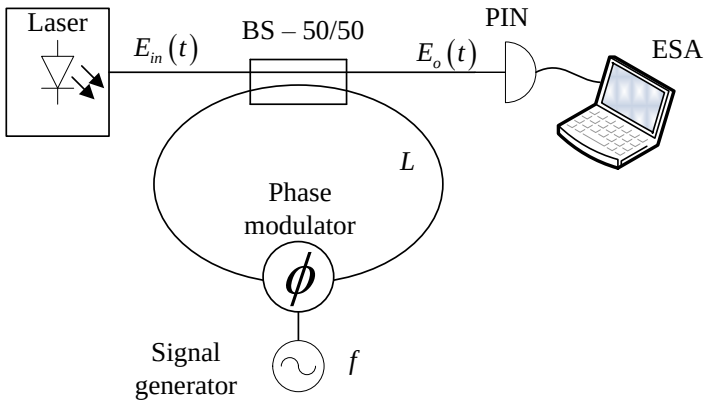
A transmissão de sinais de RF através de fibras ópticas permite a integração de redes ópticas e sem fio formando um sistema chamado redes de Rádio sobre Fibra (RoF-*Radio over Fiber*) [46-48]. Um subsistema importante das redes RoF é a geração fotônica de micro-ondas e ondas milimétricas [49,50]. Uma forma interessante de produzir tais sinais de RF é através da geração fotônica de harmônicos [51-53]. Há um grande número de configurações ópticas que podem ser usadas para a geração fotônica de sinais de RF, vários deles são apresentados em [49]. Moduladores eletro-ópticos, interferômetros de Mach-Zehnder e Sagnac, lasers de fibra, grades de fibra e amplificadores ópticos são comumente encontrados nessas configurações. Aqui são apresentadas três montagens experimentais para a geração fotônica de harmônicas usando um ressonador óptico sem amplificador e sem filtro elétrico utilizando moduladores de fase e de amplitude no laço de fibra.

No regime linear, esse ressonador com laço de fibra funciona como um filtro [54]. No entanto, no regime linear com um modulador inserido dentro do laço, a geração de harmônicas é conseguida. Os experimentos desenvolvidos mostraram que, utilizando um modulador no laço de fibra, várias harmônicas são produzidas.

6.2. Ressonador com laço de fibra e modulador de fase

A primeira configuração óptica é mostrada na Fig. 6.1. Basicamente é um ressonador a fibra com um modulador de fase inserido no anel.

Fig. 6.1. Geração fotônica de micro-ondas usando laço de fibra com modulador de fase. ESA – Analisador de Espectro, BS – Acoplador, PIN – Fotodetector.



Fonte: o autor.

No esquema apresentado na Fig. 6.1 sendo $E_{in}(t) = Ee^{j\omega t}$, onde ω é a frequência do sinal óptico, tem-se para o campo elétrico de saída $E_0(t)$ a seguinte equação de sinal RF.

$$E_o(t) = \frac{Ee^{i\omega t}}{\sqrt{2}} - \sum_k \frac{Ee^{i\omega t}}{\left(\sqrt{2}\right)^{k+1}} e^{ik(\beta L - \omega\tau)} \, \mathrm{e}^{\left\{ im\left[\begin{array}{l} \cos(\Omega t+\Phi)\sum_{l=0}^{k-1}\cos(l\Omega\tau)+ \\ \sin(\Omega t+\Phi)\sum_{l=0}^{k-1}\sin(l\Omega\tau) \end{array} \right] \right\}}. \quad (82)$$

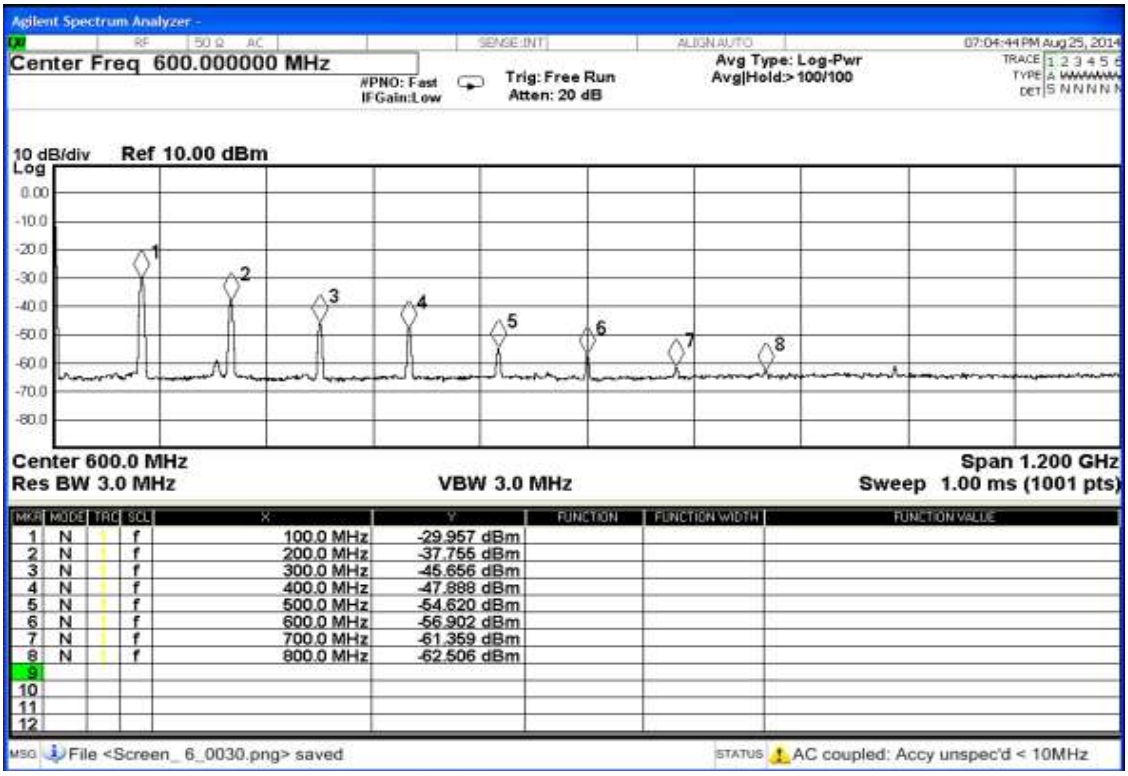
Em Eq. (82), m é o índice de modulação, Ω (Φ) é a frequência (fase) do sinal de RF modulante e τ é o tempo que a luz leva para dar uma volta no laço. A última exponencial em Eq. (82) é o termo responsável pela geração das harmônicas.

A configuração do ressonador para a geração fotônica da Fig. 6.1 foi implementada usando um laser com potência de 70mW (DFB - *Distributed Feedback*), modelo CQF915/408-19330, de fabricação da JDS Uniphase, que gera uma portadora óptica CW com comprimento de onda em 1.550,75 nm, possui banda passante de 3 GHz e suporta taxa de transmissão de até 2,5 Gbps. O receptor óptico (PIN - *Positive Intrinsic Negative*) SIR5 da ThorLabs, com largura de banda de 5 GHz, que trabalha com comprimentos de onda entre 900 e 1.650 nm com potência máxima de entrada de 20 mW e tempo de resposta menor

que 70 ps. O modulador de fase modelo JDS Uniphase 10023874 trabalha na faixa de 1.550 nm, com taxa de transmissão de até 10 Gbps e perda de inserção de 4,5 dB. O *beam spliter* da ThorLabs com perda de 3,13 dB. O gerador de RF com uma frequência de 0,1 GHz, um SLM 03 da Rohde&Schwarz, que trabalha na faixa de 9 kHz a 3,3 GHz. Este gerador possui vários formatos de modulação e alta confiabilidade do sinal gerado. O tamanho do laço é de 4,30m.

O espectro do sinal de saída pode ser visto na Fig. 6.2. Os valores utilizados para o sinal óptico e o sinal modulante estão descritos no quadro 6.4.

Fig. 6.2. Espectro do sinal detectado no analisador de espectro que foi produzido com o esquema mostrado na Figura 6.1. Eixo (x) frequência em Hertz e eixo (y) potência em dBm.



Fonte: o autor.

Os valores dos picos das harmônicas na Fig. 6.2 são mostrados no Quadro 4.1.

Quadro 6.1. Potência elétrica da fundamental e harmônicas produzida pelo esquema ótico mostrado na Figura 6.1.

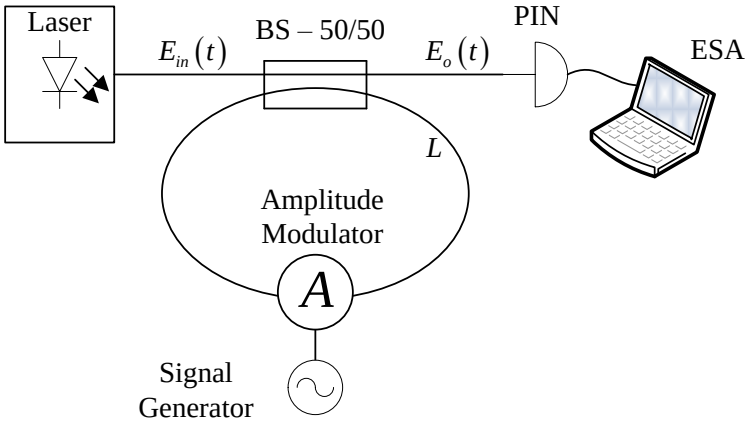
Frequência (GHz) Eixo X	Potência (dBm) Eixo Y
0.1	-29,95
0.2	-37,75
0.3	-45,65
0.4	-47,88
0.5	-54,62
0.6	-56,90
0.7	-61,35
0.8	-62,50

Fonte: o autor.

6.3. Ressonador com laço de fibra e modulador de amplitude

A segunda configuração óptica é mostrada na Fig. 6.3. Basicamente, o ressonador com laço de fibra tem agora um modulador de amplitude modelo MACH-10 da Covega que trabalha na faixa de 1.525 a 1.605 nm, com taxa de bits de até 12,5 Gbps e perda de inserção de 4 dB. O modulador possui arquitetura baseada em interferômetro de Mach-Zehnder com geração de *chirp* nulo e conta com atenuador integrado.

Fig. 6.3. Geração fotônica de micro-ondas usando laço de fibra com modulador de amplitude. ESA – Analisador de Espetro, BS – Acoplador, PIN - Fotodetector.



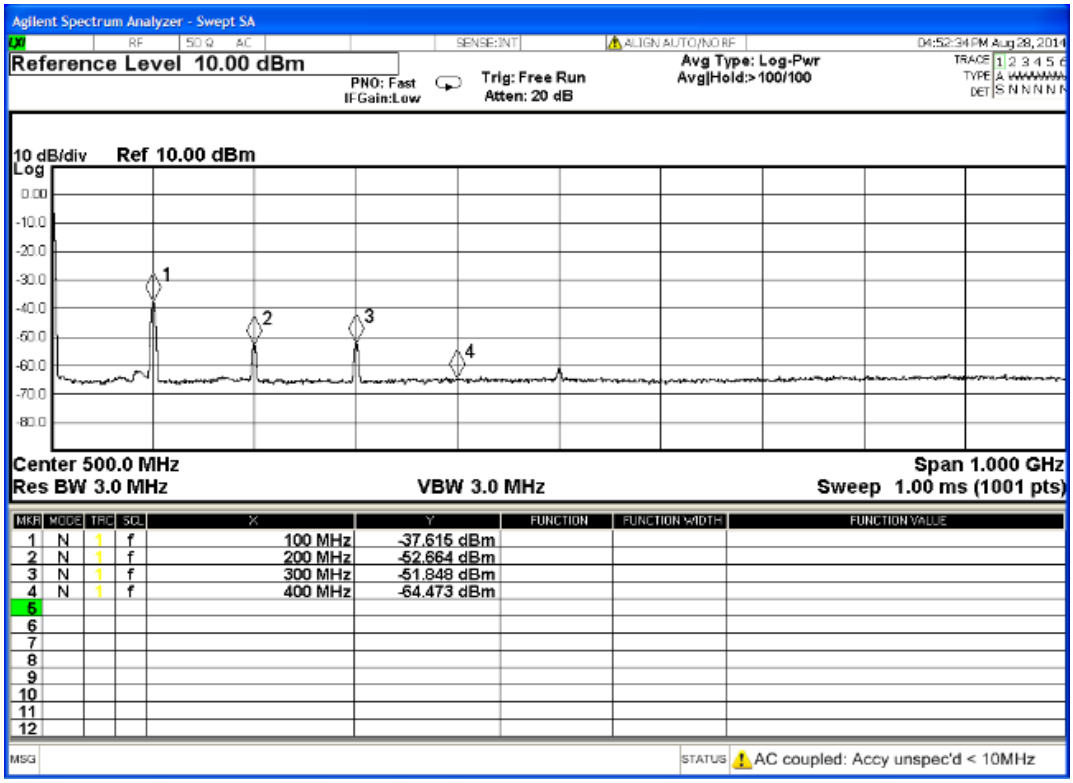
Fonte: o autor.

Sendo, novamente, $E_{in}(t) = Ee^{j\omega t}$, tem-se para o campo elétrico de saída $E_0(t)$ a seguinte equação:

$$E_o(t) = \frac{Ee^{i\omega t}}{\sqrt{2}}\left[1 - \sum_k \frac{1}{\left(\sqrt{2}\right)^k} e^{ik(\beta L - \omega\tau)} \prod_{l=0}^{k-1} \sqrt{1 + m\cos\left(\Omega(t - l\tau) + \Phi\right).}\right] \quad (83)$$

Nesse esquema, uma vez que o índice de modulação não está dentro de uma exponencial, é esperado um menor número de harmônicas a ser produzido, quando comparado com a configuração da Fig. 6.1. A configuração de geração fotônica da Fig. 6.3 foi implementado utilizando o mesmo laser e detector óptico do primeiro esquema. O espectro do sinal de saída pode ser visto na Fig. 6.4. Os valores dos picos da fundamental e suas harmônicas da Fig. 6.4 são mostrados no Quadro 6.2. Os valores utilizados para o sinal óptico e o sinal modulante estão descritos no Quadro 6.4.

Fig. 6.4. Espectro do sinal detectado no analisador de espectro que foi produzido com o esquema mostrado na Figura 6.3. Eixo (x) frequência em Hertz e eixo (y) potência em dBm.



Fonte: o autor.

Quadro 6.2. Potência elétrica da fundamental e harmônicas produzida pelo esquema ótico mostrado na Figura 6.3.

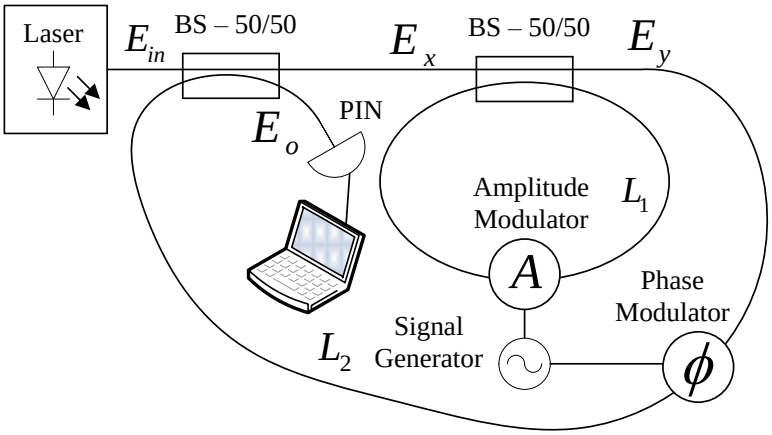
Frequência (GHz) Eixo X	Potência (dBm) Eixo Y
0.1	-37,61
0.2	-52,66
0.3	-51,84
0.4	-64,47

Fonte: o autor.

6.4. Ressonador com laço de fibra duplo e moduladores de amplitude e fase

A terceira configuração para a geração fotônica de harmônicas é mostrada na Fig. 6.5. Trata-se de um ressonador com duplo laço de fibra. Um modulador de amplitude é inserido dentro do anel interno e um modulador de fase no anel externo. O laço interno tem comprimento de 4,30m e o externo de 5,57m.

Fig. 6.5. Geração fotônica de micro-ondas usando duplo laço de fibra com modulador de amplitude e fase. BS – Acoplador, PIN - Fotodetector.



Fonte: o autor.

As equações de modelagem do sistema na Fig. 6.5, para $L1 = L2$, são:

$$E_x(t) = \frac{E_{in}(t)}{\sqrt{2}} + \frac{ie^{i\beta L}e^{im\cos(\Omega t+\Upsilon)}E_y(t-\tau)}{\sqrt{2}} \tag{84}$$

$$E_y(t) = \frac{E_x(t)}{\sqrt{2}} - \sum_k \frac{E_x(t-k\tau)}{\left(\sqrt{2}\right)^{k+1}} e^{ik\beta L} \times \prod_{l=0}^{k-1} \sqrt{1+m\cos\left(\Omega\left(t-l\tau\right)+\Phi\right)} \tag{85}$$

$$E_o(t) = \frac{iE_{in}(t)}{\sqrt{2}} + \frac{e^{i\beta L} e^{im\cos\left(\Omega t+\Upsilon\right)} E_y(t-\tau)}{\sqrt{2}} \tag{86}$$

As equações Eqs. (84) a (86) são complexas para resolver, no entanto, pode-se ver que aparecem termos do tipo:

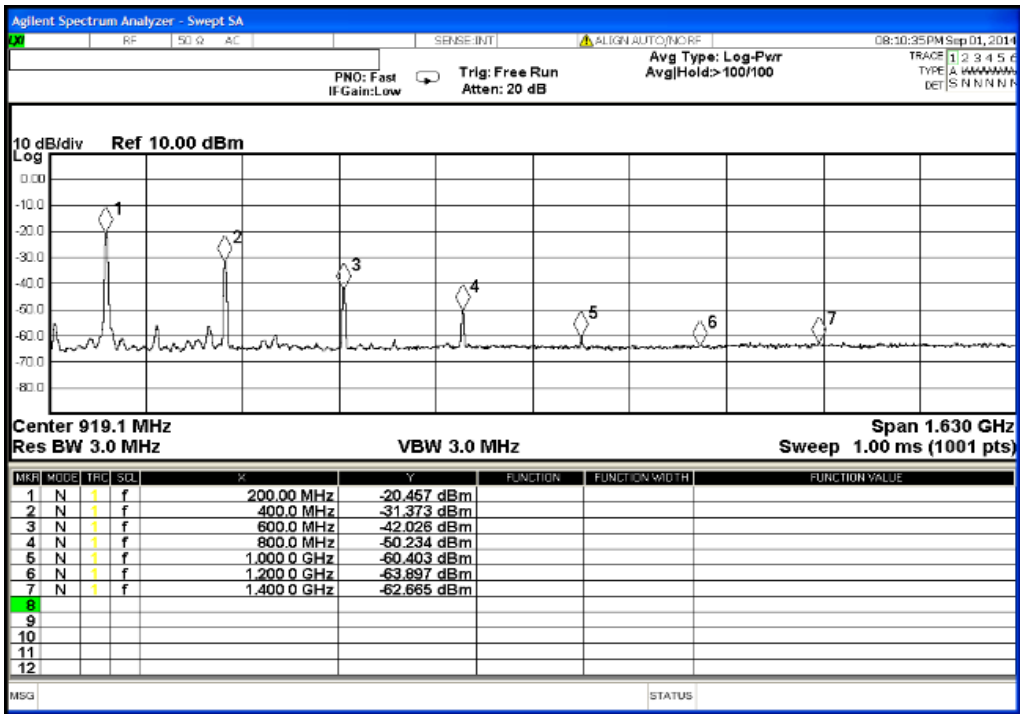
$$e^{im\cos\left(\Omega\left(t-j\tau\right)+\Upsilon\right)},\ \sqrt{1+m\cos\left(\Omega\left(t-l\tau\right)+\Phi\right)}, \tag{87}$$

implicando em uma combinação de modulação de fase e de amplitude. Em tal caso, pode-se esperar como resultado uma infinidade de raias no espectro.

No entanto, uma vez que ambos os moduladores na Fig. 6.5 são alimentados pelo mesmo gerador de sinal, apenas harmônicas de Ω são produzidas.

A configuração de geração fotônica da Fig. 6.5 foi implementada e o espectro do sinal de saída pode ser visto na Fig. 6.6. Diferentemente das duas primeiras configurações, aqui foi utilizado um sinal de modulação com uma frequência de 0,2 MHz. Os valores dos picos dos sinais resultantes da Fig. 6.6 estão apresentados no Quadro 6.3. Os valores utilizados para o sinal óptico e o sinal modulante estão descritos no Quadro 6.4.

Fig. 6.6. Espectro do sinal detectado no analisador de espectro produzido com o esquema óptico mostrado na Figura 6.5. Sinal de modulação com frequência igual a 0,2 GHz. Eixo (x) frequência em Hertz e eixo (y) potência em dBm.



Fonte: o autor.

Quadro 6.3. Potência elétrica da fundamental e harmônicas produzida pelo esquema ótico mostrado na Figura 6.5. Fonte: o autor.

Frequência (GHz) Eixo X	Potência (dBm) Eixo Y
0.2	-20,45
0.4	-31,37
0.6	-42,02
0.8	-50,23
1	-60,40
1.2	-63,89
1.4	-62,66

Fonte: o autor.

A Fig. 6.7 mostra a montagem realizada no LATIQ (Laboratório de Informação Quântica) da Universidade Federal do Ceará para implementar o ressonador e executar a geração fotônica de harmônicas através da utilização de laço duplo.

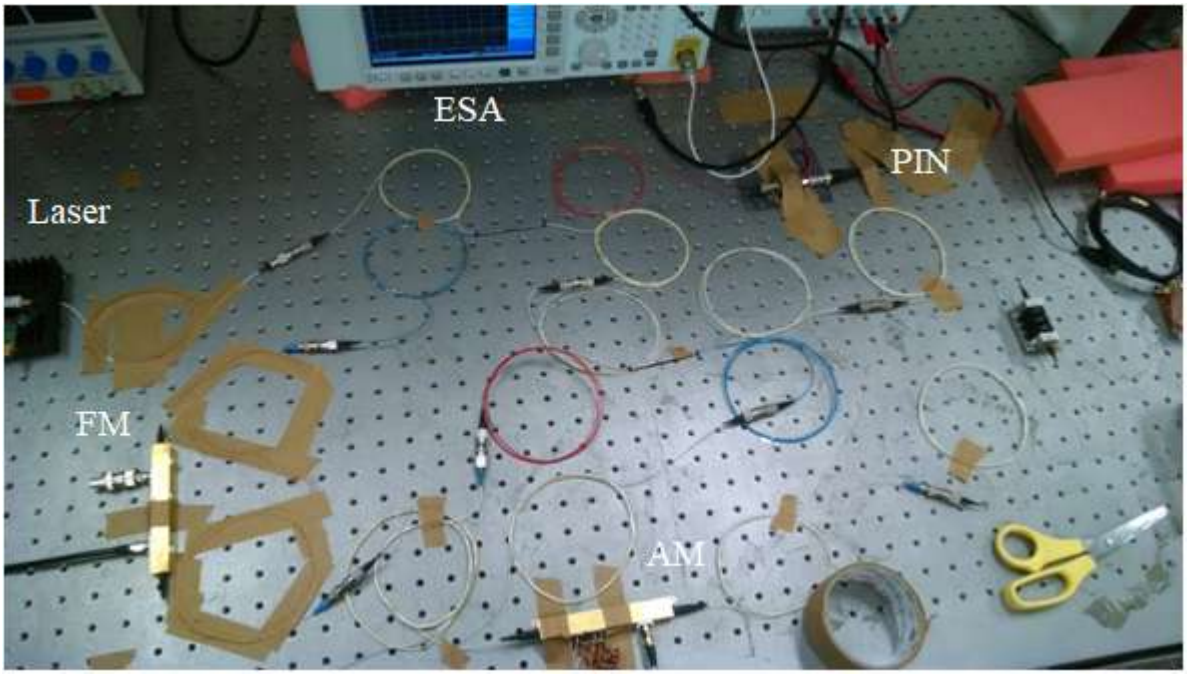
Para realizar uma comparação entre os três sistemas de ressonadores propostos o Quadro 6.4 mostra as diferenças de cada esquema.

Quadro 6.4. Comparação entre os três ressonadores.

Esquema	P (μW) Laser	Λ (nm) Laser	A (mV) *fm*	F (MHz) *fm*	Harmônicas geradas	Potência da maior harmônica	Potência da menor harmônica	Complexidade
Com modulador de Fase	1.383	1.550,75	2.283	100	8	-29,95	-62,50	Baixa
Com modulador de Amplitude	1.819	1.550,75	2.283	100	4	-37,61	-54,47	Baixa
Com modulador de Fase e Amplitude	1.819	1.550,75	2.283	200	7	-20,45	-62,66	Média

Fonte: o autor.

Fig. 6.7. Esquema do ressonador montado para a geração fotônica de micro-ondas usando duplo laço de fibra com modulador de amplitude e fase.



Fonte: o Autor.

7 CONCLUSÕES E PERSPECTIVAS DE TRABALHOS FUTUROS

7.1 Conclusões

A partir dos resultados mostrados nesta tese, as seguintes conclusões se apresentam:

I) É possível fazer um sistema de distribuição caótica de chaves com osciladores optoeletrônicos sincronizados. Entretanto, quanto maior o número de OEOs maior a taxa de erro de bits devido aos erros paramétricos dos OEOs. Além disso, uma vez que a sincronização de OEOs no regime caótico requer comunicação bidirecional, a principal desvantagem da comunicação segura usando o OEO sincronizado é o fato de que a taxa de transmissão depende da distância entre o OEOs. Em outras palavras, a separação do tempo entre os pulsos consecutivos emitidos pelo laser, τ, é igual ao tempo requerido para as informações produzidas em um OEO chegar ao outro, L/V_g, onde L é a distância entre dois OEOs e V_g é a velocidade do grupo. Portanto, altas taxas só são possíveis para curtas distâncias.

II) No que diz respeito à configuração óptica com dois OEOs acoplados, como exemplo de uma aplicação, foi descrito um protocolo de compromisso de imagem usando os valores caóticos dos parâmetros de Stokes dos campos de saída. Existem várias questões relacionadas a este protocolo (como a análise estatística e sensibilidade da chave) que merecem um trabalho completo e não puderam ser discutidos aqui, pois o objetivo foi apenas fornecer uma aplicação para os dois OEOs acoplados.

III) Foi proposto pela primeira vez um esquema óptico para distribuição caótica de chaves com segurança quântica. Portanto, este é o primeiro sistema de distribuição caótica de chaves com segurança incondicional. Embora todos os dispositivos ópticos e optoeletrônicos utilizados na proposta estejam disponíveis com a tecnologia atual, o que o torna passível de implementação prática em um futuro próximo, o sistema possui um de grau de complexidade de implementação considerável. Neste esquema, as partes caótica e

quântica são completamente independentes: o sistema quântico é utilizado para transportar a informação de sincronismo de forma segura entre os dois sistemas caóticos sincronizados. Isto também indica que tanto o sistema caótico quanto o sistema quântico podem ser alterados individualmente visando à redução da complexidade de implementação.

IV) Foi proposto pela primeira vez um esquema óptico para distribuição quantum-caótica de chaves. Neste caso, um único sistema realiza a dinâmica caótica e o sincronismo usando estados quânticos. Ou seja, as partes quântica e caótica estão integradas em um sistema só. Desta forma, a segurança é garantida por regras quânticas e caóticas. Além disso, não existe o estágio de reconciliação de base. A segurança é aumentada pois o conjunto de estados quânticos (estado de polarização da luz) usados é contínuo, já que a variável caótica é uma variável contínua. Uma vez que o sinal de sincronização nem sempre está presente (devido ao baixo número médio de fótons utilizado para eles), a taxa de erro de bit é muito sensível ao erro paramétrico, ou seja, quando os valores dos parâmetros não são exatamente os mesmos. Na falta de sincronismo, o erro paramétrico torna impossível operar os dois OEOs no regime caótico sincronizados. Em outras palavras, quanto maior o erro paramétrico, maiores devem ser os valores de $p_B t_c|\alpha_{a,}|^2$ e $p_A t_c|\alpha_b|^2$ para se obter uma taxa de erro aceitável.

V) Os esquemas implementados de ressonadores com laço de fibra são bastante promissores para a geração de harmônicas de ordem superior, pois o modulador introduzido no laço permite realizar a multiplicação da frequência do sinal portador facilmente. A configuração com o modulador de fase gera mais raias que com o uso do modulador de amplitude. A configuração com laço duplo pode apresentar um espectro rico quando geradores de sinais com frequências diferentes são usados para alimentar o modulador de fase e o modulador de amplitude.

7.2 Perspectivas de trabalhos futuros

Como perspectivas de trabalhos futuros, pode-se citar:

I) A proposição de novos sistemas ópticos mais rápidos e menos complexos para distribuição quantum-caótica de chaves.

II) A realização experimental de um sistema de distribuição quantum-caótica de chaves.

III) Realizar a análise teórica e experimental da dinâmica do ressonador com laço de fibra duplo e modulador de amplitude e fase quando sinais de frequências diferentes alimentam os dois moduladores.

REFERÊNCIAS

[1] CISCO. **VNI Forecast and Methodology, 2015-2020**. Disponível em <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html>. Acesso em: 03/04/2017.

[2] MALEKI, L. High Performance Optical Oscillators for Microwave and mm-wave Applications, **Microwave Journal**. v.56, n.10 p. 106-118, 2013.

[3] WU, B.; SHASTRI, B. J.; PRUCNAL, P. R. **Secure communication in fiber-optic networks, in emerging trends in information and communication technologies security**. Disponível em < http://ee.princeton.edu/research/prucnal/sites/default/files/chap11_0.pdf>. Acesso em: 20/06/2016.

[4] PAUL, D. A review of optoelectronic oscillators for high speed signal processing applications, **Hindawi Publishing Corporation ISRN Electronics,** Optical Sciences, NRL, Washington, DC 20032, v. 2013, p.1-16, 2013.

[5] YAO, X. S.; MALEKI, L. Optoelectronic microwave oscillator, **Journal Optical Society of America**, v.13, n. 8, p.1725-1735, 1996.

[6] YAO, X. S.; MALEKI, L. Optoelectronic oscillator for photonic systems**, IEEE Journal of Quantum Electronics**, v.32, n.7, p.1141-1149, 1996.

[7] BONATTO, C.; FEYEREISEN, M.; BARLAND, S.; GIUDICI, M.; MASOLLER, C.; LEITE, J. R. R.; TREDICCE, J. R. Deterministic rogue wave, **Physical Review Letters**, v. 107, p. 1-5, 2011.

[8] ZAMORA-MUNT, J.; GARBIN, B.; BARLAND, S.; GIUDICI, M.; LEITE, J. R. R.; MASOLLER, C.; TREDICCE, J. R. Rogue waves in optically injected lasers: origin, predictability, and suppression, **Physical Review A**, v. 87, p. 2-5, 2013.

[9] NAKATSUKA H.; ASAKA, S.; ITOH, H.; IKEDA, K.; MATSUOKA, M. Observation of bifurcation to chaos in an all-optical bistable system, **Physical Review Letters**, v. 50, n.2, p. 109-112, 1983.

[10] STEINMEYER, G.; MITSCHK, F.; BUCHHOLZ, A.; HANSEL, M.; HEUER, M.; SCHWACHE, A. Dynamical pulse shaping in a nonlinear resonator, **Physical Review A**, v. 52, n.1, p.830-838, 1995.

[11] BLOW, K. J.; DORAN N.J. Global and local chaos in the pumped nonlinear Schrödinger equation, **Physical Review Letters**, v. 52, n.7, p. 526-529, 1984.

[12] GOEDGEBUER, J. P.; LEVY, P.; LARGER, L.; CHEN, C.-C.; RHODES, W. T. Optical communication with synchronized hyperchaos generated electrooptically, **IEEE Journal Quantum Electronics**, v. 38, n. 9, p. 1178–1183, 2002.

[13] LIU, X.; PAN, W. Investigation on tunable modulation in the polarization-modulator-based optoelectronic oscilattor**, IEEE Journal Quantum Electronics**, v. 50, n. 2, p. 68-73, 2014.

[14] PECORA, L. M.; CARROLL, T.L. Synchronization in chaotic systems, **Physical Review Letters**, v. 64, n. 8, p. 821–824, 1990.

[15] PECORA, L. M.; CARROLL, T.L. Synchronization of chaotic systems, **Chaos**, v. 25, p. 1 - 11, 2015.

[16] DAISY, R.; FISCHER, B. Synchronization of chaotic nonlinearoptical ring oscillators, **Optics Communications**, v. 133, p. 282-286, 1997.

[17] RAMOS, R. V.; SOUZA, R. F. Controlling a quantum communication system with synchronized nonlinear fiber ring resonator, **Microwave and Optical Technologies Letters**, v. 27, n. 5, p. 302-304, 2000.

[18] ANNOVAZZI-LODI, V.; DONATI, S.; SCIRE, A. Synchronization of chaotic lasers by optical feedback for cryptographic applications, **IEEE Journal Quantum Electronics**, v. 33, n. 9, p. 1449–1454, 1997.

[19] ARGYRIS, A.; SYVRIDS, D.; LARGER, L.; ANNOVAZZI-LODI, V.; COLET, P.; FISCHER, I.; GARCIA-OJALVO, J.; MIRASSO, C. R.; PESQUERA, L.; SHORE, K. A. Chaos-based communications at high bit rates using commercial fibre-optic links, **Nature**, v. 437, n. 17, p. 343–346, 2005.

[20] FISCHER, I.; LIU, Y.; DAVIS, P. Synchronization of chaotic semiconductor laser dynamics on sub-nanosecond time scales and its potential for chaos communication, **Physical Review A**, v. 62, n. 1, p. 110–115, 2000.

[21] JIANG, N.; PAN, W.; YAN, L.; LUO, B.; ZHANG, W.; XIANG, S.; YANG, L.; ZHENG, D. Chaos synchronization and communication in mutually coupled semiconductor lasers driven by a third laser, **Journal of Lightwave Technology**, v. 28, n. 18, p. 1978–1986, 2010.

[22] SPENCER, P. S.; MIRASSO, C. R.; COLET, P.; SHORE, K. A. Modeling of optical synchronization of chaotic external-cavity VCSEL's, **IEEE Journal Quantum Electronics**, v. 9, n. 4, p. 1673-1679, 1998.

[23] FUJIWARA, N.; TAKIGUCHI, Y.; OHTSUBO, J. Observation of the synchronization of chaos in mutually injected vertical-cavity surface-emitting semiconductor lasers, **Optical Letters**, v. 18, n. 28, p. 1677-1679, 2003.

[24] VAN WIGGEREN, G. D.; ROY ,R. Communication with chaotic lasers, **Science**, v. 20, n. 279, p. 1198-1200, 1998.

[25] STOJANOVIC, A. D.; RAMOS, R. V.; MATAVULJ, P. S. Authenticated B92 QKD protocol employing synchronized optical chaotic systems, **Optical and Quantum Electronics**, v. 285, n. 48, p. 285-291, 2016.

[26] KOUOMOU, Y. C.; COLET, P.; LARGER, L.; GASTAUD, N. Mismatch-induced bit error rate in optical chaos communications using semiconductor lasers with electrooptical feedback, **IEEE Journal Quantum Electronics**, v. 2, n. 41, p. 156-163, 2005.

[27] RIBORDY, G.; J. GAUTIER, D.; GISIN, N.; GUINNARD, O.; ZBINDEN, H. Fast and user-friendly quantum key distribution, **Journal of Modern Optics**, v. 2, n. 47, p. 517-531, 2000.

[28] ZHANG, Y.; XIAO, D. Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform, **Optics and Lasers in Engineering**, v.51, p. 472–480, 2013.

[29] NIYAT, A. Y.; MOATTAR, M. H.; TORSHIZ, M. N. Color image encryption based on hybrid hyper-chaotic system and cellular automata, **Optics and Lasers in Engineering**, v.90, p. 225–237, 2017.

[30] LI, Y.; WANG, C.; CHEN, H. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation, **Optics and Lasers in Engineering**, v.90, p. 238–246, 2017.

[31] RIOS, F. F. S.; GUERRA, A. G. de A. H.; RAMOS, R. V. Quantum communication with continuum single-photon, two-photons and coherent states, **Journal Quantum Information and Computation**, v.17, p. 1277-1291, 2017.

[32] PINHEIRO, P. V. P.; RAMOS, R. V. Two-layer quantum key distribution, **Quantum Information Processing**, v.14, n.6, p. 2111-2124, 2015.

[33] MENDONCA, F. A.; DE BRITO, D. B.; RAMOS, R. V. An optical scheme for quantum multi-service network, **Journal Quantum Information and Computation**, v.12, n.7, p. 620-629, 2012.

[34] BENNETT, C. H.; BRASSARD, G. Quantum cryptography: public key distribution and coin tossing, **Theoretical Computer Science**, v.560, p. 7-11, 2014.

[35] EKERT, A. K. Quantum cryptography based on Bell's theorem, **Physical Review Letters**, v.67, n.6, p. 661-663, 1991.

[36] NAMEKATA, N.; FUJI, G.; INOUE, S.; HONJO, T.; TAKESUE, H. Differential phase shift quantum key distribution using single-photon detectors based on a sinusoidally gated InGaAs/InP avalanche photodiode, **Physical Letters Applied**, v.91, n.1, p. 1- 3, 2007.

[37] LO, H.-K.; ZHAO, Y. Quantum cryptography, **Quantum Physics**, v.1, p. 1- 51, 2008.

[38] CERF, N. J.; IBLISDIR, S. Optimal N-to-M cloning of quantum coherent states, **Quantum Physics**, v.62, p. 1-3, 2000.

[39] ANDERSEN, U. L.; JOSSE, V.; LEUCHS, G. Unconditional quantum cloning of coherent states with linear optics, **Physical Review Letters**, v.94, p. 1-4, 2005.

[40] CERF, N. J.; KRÜGER, O.; NAVEZ, P.; WERNER, R. F.; WOLF, M. M. Non-Gaussian cloning of quantum coherent states is optimal, **Physical Review Letters,** v.95, p. 1- 4, 2005.

[41] JOSSE, V.; SABUNCU, M.; CERF, N. J.; LEUCHS, G.; ANDERSEN, U. L. Universal optical amplification without nonlinearity, **Physical Review Letters**., v.96, p. 1-4, 2006.

[42] OLIVARES, S.; PARIS, M. G. A.; ANDERSEN, U. L. Cloning of Gaussian states by linear optics, **Physical Review A**, v.73, p. 1-8, 2006.

[43] ZHAI, Z.; GUO, J.; GAO, J. Generalization of continuous-variable quantum cloning with linear optics, **Physical Review A**, v.73, p. 1-5, 2006.

[44] OLIVARES, S.; PARIS, M. G. A.; ANDERSEN, U. L. Optimal cloning of coherent states by linear optics, **Quantum Electronics**, v.26, n.3–4, p. 293–299, 2006.

[45] MENDONÇA, F. A.; RAMOS, R. V. Quantum bit string commitment protocol using polarization of mesoscopic coherent states**, Physical Letters Applied**, v.372, n.8, p. 1190-1193, 2008.

[46] JIA, Z.; YU, J.; HSUEH, Y.-T.; CHIEN, H.-C.; CHOWDHURY, A.; CHANG, G.-K. Wireless high-definition services over optical fiber networks, **Journal of Optical Networking**, v.8, n.2, p. 235-243, 2009.

[47] GOMES, N. J.; NKANSAH, A.; WAKE, D. Radio-over-MMF techniques – Part I: RF to microwave frequency systems, **Journal of Lightwave Technology**, v.26, n.15, p. 2388-2395, 2008.

[48] KOONEN, A. M. J.; LARRODÉ, M. G. Radio-over-MMF techniques – Part II: Microwave to millimeter-wave systems, **Journal of Lightwave Technology**, v.26, n.15, p. 2396-2408, 2008.

[49] YAO, J. Microwave photonics, **Journal of Lightwave Technology**, v.27, n.3, p. 314-335, 2009.

[50] YAO, J; ZEN, F.; WANG, Q. Photonic generation of ultrawideband signals, **Journal of Lightwave Technology**, v.25, n.11, p. 3219-3235, 2007.

[51] CHI, H.; YAO, J. Frequency quadrupling and upconversion in a radio over fiber link**, Journal of Lightwave Technology**, v.26, n.15, p. 2706-2711, 2008.

[52] DE OLIVEIRA, G. L.; GIRAUDO, E. C.; RAMOS, R. V. Setups for harmonics generation using optical modulators, **Microwave and Optical Technology Letters**, v.54, n.2, p. 519-521, 2012.

[53] INSUA, I. G.; SCHÄFFER, C. G. Optical microwave signal generation using a fiber loop, **Journal of Lightwave Technology**, v.25, n.11, p. 3341-3349, 2007.

[54] ZHANG, J.; LIT, J. W. Y. All-Fiber Compound Ring Resonator with a Ring Filter**, Journal of Lightwave Technology**, v.12, n.7, p. 1256-1262, 1994.

[55] BLOW, K. J.; DORAN, N. J. Global and local chaos in the pumped nonlinear Schrödinger equation, **Physical Review Letters**, v.52, p. 526-529, 1984.

[56] MARIETTO, M. L.; SANCHES, C.; MEIRELES, M. Teoria do caos: Uma contribuição para formação de estratégias, **Revista Ibero-Americana de Estratégias - RIAE**, vol. 10, n.3, p. 66-93, set./dez. 2011.

[57] GLEICK, J. **Chaos: making a new science**, 1. ed. New York: Viking, 1987.

[58] WOOD JR, T. Caos: A criação de uma nova ciência, **Revista de Administração de Empresas/ EAESP/ FGV**, vol. 33, n.4, p. 94-105, jul./ago. 1993.

[59] KATZ, F. J. **Contribuições metodológicas da teoria do caos para o pensamento Econômico**. Campinas: Neal - Núcleo de Estudos para América Latina, UNICAMP, 2010. Disponível em <http://www.unicap.br/neal/artigos/Texto10ProfFred.pdf>. Acesso em: 06/07/2017.

[60] MARTINS, A. C. N. **Uma abordagem sobre caos e sistemas não-lineares**, 2016, 114 f. (Monografia de Graduação) - Centro de Ciência Exatas e da Terra. Departamento de Física Teórica e Experimental. Universidade Federal do Rio Grande do Norte. Natal, 2016.

[61] NUSSENZVEIG, H. M. **Complexidade e caos**. 2. ed. Rio de Janeiro: Editora UFRJ/COPEA, 1991.

[62] SAVI, M. A. **Dinâmica não-linear e caos**. 1. ed. Rio de Janeiro: Editora UFRJ, 2006.

[63] STEWART, I. **Será que Deus joga dados? A nova matemática do caos**. 1. ed. Rio de Janeiro: Editora Zahar, 1991.

[64] ONIAS, H. H. S. **Bifurcações dinâmicas em circuitos eletrônicos**, 2012, 69f. (Dissertação de Mestrado) - Centro de Ciência Exatas e da Natureza. Departamento de Física. Universidade Federal de Pernambuco. Recife, 2012.

[65] STROGATZ, S. H. **Nonlinear dynamics and chaos with applications to physics, biology, chemistry and engineering.** 1. ed. New York: Perseus Books, 2014.

[66] Santos, F. O. **Dinâmica caótica em um circuito eletrônico**, 2007, 87f. (Dissertação de Mestrado) - Centro de Ciência Exatas e da Natureza. Departamento de Física. Universidade Federal de Pernambuco. Recife, 2007.

[67] ARAÚJO, S. B. **Sistemas caóticos simples**. 2009, 15f. (Monografia de Graduação) - Centro de Ciência Exatas. Departamento de Física. PUC-RIO. Rio de Janeiro, 2009.

[68] MANNEVILLE, P.; POMEAU, Y. Intermittency and the Lorenz model, **Physics Letters**, v.75A, p.1-2, 1979.

[69] MENDONÇA, F. A. **Análise teórica e resultados experimentais de sistemas de distribuição quântica de chaves usando fótons isolados e estados coerentes mesoscópicos**, 2006, 99f. (Dissertação de Mestrado) – Centro de Tecnologia. Departamento de Engenharia de Teleinformática, Universidade Federal do Ceará, Fortaleza, 2006.

[70] WU, B.; SHASTRI, B. J.; PRUCNAL, P. R. **Emerging Trends in ICT Security**. 1. ed. Waltham: Morgan Kaufmann, 2013.

[71] DAMASCENO, R.L.C. **Comunicação quântica segura direta usando distribuição quântica de chaves**. 2016, 54f (Dissertação de Mestrado) – Programa de pós Graduação em Engenharia de Telecomunicações - PPGET. Instituto Federal do Ceará. Fortaleza, 2016.

[72] LO, H.-K.; ZHAO, Y. **Encyclopedia of Complexity and Systems Science**, 1. ed. New York: Springer, 2009.

[73] CAMARGO, A.L.P.; PEREIRA, L.O.; BALTHAZAR, W.F.; HUGUENIN, J.A.O. Simulação do protocolo BB84 de criptografia quântica utilizando um feixe laser intenso, **Revista Brasileira de Ensino de Física**, v. 39, n. 2, p. 1-12, 2017.

[74] BENNETT, C.H.; BRASSARD, G. Quantum cryptography: public key distribution and coin tossing. *In:* PROCEEDINGS OF THE IEEE INTERNATIONAL CONFERENCE ON

COMPUTERS, SYSTEMS, AND SIGNAL PROCESSING, Bangalore, India IEEE Computer Society Press, p. 175–179, 1984.

[75] BENNETT, C.H. Quantum cryptography using any two nonorthogonal states, **Physical Review Letters**, v. 68, n. 21, p. 3121 – 3124, 1992.

[76] SCULLY, M. O.; ZUBAIRY, M. S. **Quantum Optics**. 1. ed. Cambridge: Cambridge University Press, 1997.

APÊNDICE A - INTRODUÇÃO À TEORIA DO CAOS

Este apêndice apresenta uma introdução à teoria do caos, seus conceitos e fundamentos.

A.1 Introdução ao caos

A Teoria do Caos é um campo da ciência que surgiu apenas no início dos anos 60 quando o meteorologista Edward Lorenz no MIT (*Massachusetts Institute of Technology*) desenvolveu modelos computacionais dos padrões do tempo. Surgiu a partir da perspectiva da busca da ordem determinística da natureza, e passou a ser o estudo daquilo que era considerado apenas "ruído". Na Teoria do Caos a ideia principal reside no fato de que, em determinados sistemas, pequenas variações nas condições iniciais podem gerar grandes variações nos resultados finais, também chamado pelo nome famoso de "efeito borboleta" [56], [57]. Essa ideia surgiu inicialmente em estudos e modelações matemáticas ligadas à meteorologia, à biologia, à física e à química. Se popularizou através de divulgação científica principalmente por sua característica de transdisciplinaridade, sua capacidade de explicar eventos como: fenômenos meteorológicos, crescimento de populações, variações do mercado financeiro, movimento de placas tectônicas e outros [58].

Para [59] a Teoria do Caos estuda comportamentos irregulares de certa natureza. Em um sistema determinístico, em que se tem uma situação muito bem definida, o comportamento dos agentes é previsível. Assim, o resultado da ação combinada dos agentes no tempo deve ser sempre possível de antecipar, pelo menos, sua direção. No entanto, quando o caos se manifesta em um sistema, em certas circunstâncias, surgem comportamentos inesperados e o resultado são posições inusitadas. Quando isso acontece, para se conhecer a posição do resultado do sistema em um determinado momento, deve-se efetivamente realizar seu cálculo.

A Teoria do Caos avançou em várias áreas da ciência, mas inicialmente evoluiu a partir do trabalho de cientistas que lidavam com sistemas dinâmicos. Hoje, a teoria do caos é uma área científica em desenvolvimento, focada no estudo dos sistemas dinâmicos não lineares complexos. Para um melhor entendimento do caos faz-se necessário o conhecimento

destes três termos básicos que estão intrinsecamente relacionados: sistemas dinâmicos, não linearidade e complexidade [56].

O termo sistema dinâmico pressupõe primeiro que existe uma relação de interdependência e inter-relacionamento entre as partes. Em um sistema dinâmico representa-se cada agente como uma variável e a inter-relação entre os mesmos por relações funcionais, ou seja, equações. É este conjunto de equações que recebe o nome de sistema, indicando que existe um relacionamento entre elas e que podem ser tratadas como um todo. O termo dinâmico advém do fato de que o sistema se destina a estudar os processos de mudança dos agentes, sendo o tempo incluído como um componente do sistema. Outra característica do sistema dinâmico é sua dimensão que é determinada pelo número de variáveis que possui [56].

A não linearidade está relacionada à estrutura matemática utilizada para representar o comportamento do sistema real [56]. Em um sistema com dinâmica linear existe uma relação de proporcionalidade constante entre variáveis, ou seja, quando acontece uma mudança em uma variável, há uma alteração proporcional em outra e essa alteração pode ser representada por uma linha reta. Quando o sistema apresenta não linearidade deixa de haver a proporcionalidade constante entre as variáveis. Assim, a mudança em uma variável produz alterações não proporcionais em outra. Diferente da dinâmica linear, o relacionamento entre as variáveis não é mais representado por uma linha reta, mas sim, por formas curvilíneas.

A complexidade corresponde à dificuldade de se estruturar um modelo para predizer o comportamento de um sistema real. Em um sistema pouco complexo pode-se predizer o resultado de seu comportamento com facilidade. É o caso por exemplo, da necessidade de determinar o tempo para se deslocar da cidade (A) para a cidade (B). O resultado é dado pela razão entre a distância e a velocidade de deslocamento ($t = d/v$). Mesmo com algumas paradas no caminho a distorção entre o tempo estimado e o tempo real será pouco diferente. A complexidade relacionada ao caos resulta da imprevisibilidade do resultado do comportamento do sistema, pois existe uma dependência sensitiva às condições iniciais. O comportamento caótico não está relacionado com as influências de fatores externos, mas tem origem interna ao próprio sistema [56].

Para [58] a Teoria do Caos está ligada à descoberta de padrões e leis razoavelmente simples governando uma série de fenômenos complexos. Porém, o fato da

existência de padrões não pode ser associado à condição de previsão, pois uma característica dos sistemas caóticos é que qualquer mínima alteração em uma das suas condições iniciais pode provocar profundas mudanças de trajetória ou comportamento.

A trajetória de um sistema dinâmico pode ser estudada a partir da verificação do estado do sistema. O estado de um sistema dinâmico em um determinado momento é dado pelo valor de cada uma de suas variáveis naquele momento. A representação de cada estado do sistema pode ser vista como um ponto em um gráfico denominado Espaço de Fase. Com o passar do tempo, este ponto descreve uma trajetória que é chamada de Linha de Fase e que representa a evolução do estado no sistema [59].

O termo atrator é utilizado para representar uma região restrita do espaço de fase onde se concentra a linha de fase após o sistema dinâmico realizar alguns movimentos. Pode existir mais de um atrator para onde a linha de fase do sistema dinâmico se dirige, e neste caso as condições iniciais definirão de qual deles o sistema irá se aproximar [59].

A.2 Caos

O estudo do caos em sistemas determinísticos não lineares tomou-se relevante nas recentes décadas [60]. Sistemas simples e modelados por equações determinísticas podem ter comportamento imprevisível em determinas condições. A imprevisibilidade do comportamento não vem da falta de determinismo, ela aparece devido à complexidade da dinâmica do sistema que requer uma precisão impossível de calcular. Existe caos na ordem e ordem no caos [61], ou seja, a dinâmica caótica aparece na evolução temporal de sistemas sem nenhum componente aleatório como uma forma ruidosa.

Poincaré foi o primeiro a esbarrar com o que ele chamou de "fenômeno do acaso" [62]. Em um ensaio premiado e chamado "Sobre o problema dos três corpos e as equações da dinâmica", que foi publicado em 1890, ele concluiu que era imprevisível determinar o comportamento de um corpo sob a influência gravitacional de outros dois muito mais pesados. A imprevisibilidade de Poincaré não despertou interesse na época, mesmo com todos os resultados por ele apresentados. Mas, as ideias de Poincaré ganharam força quando em 1963 os estudos de Edward Norton Lorenz sobre problemas atmosféricos foram divulgados no *Journal of the Atmospheric Sciences* [63]. Lorenz trabalhava com modelos para a previsão

do tempo e, como conta [57], quando alterou o valor de uma variável de 0,506127 para 0,506 certo de que a diferença não teria consequências, se deparou com uma mudança no comportamento do sistema. O resultado leva Lorenz a concluir que pequenas mudanças podem ter grandes consequências à longo prazo. Atualmente esta ideia é denominada de efeito borboleta.

Hoje o caos é definido como um comportamento aperiódico em um sistema determinístico que tem alta sensibilidade às condições iniciais, com longa duração, e torna impossível a previsão do estado do sistema mesmo sendo este determinístico.

Pode-se ver em Eqs. (A1-A3) as equações diferencias que Lorenz utilizou para descrever seu problema:

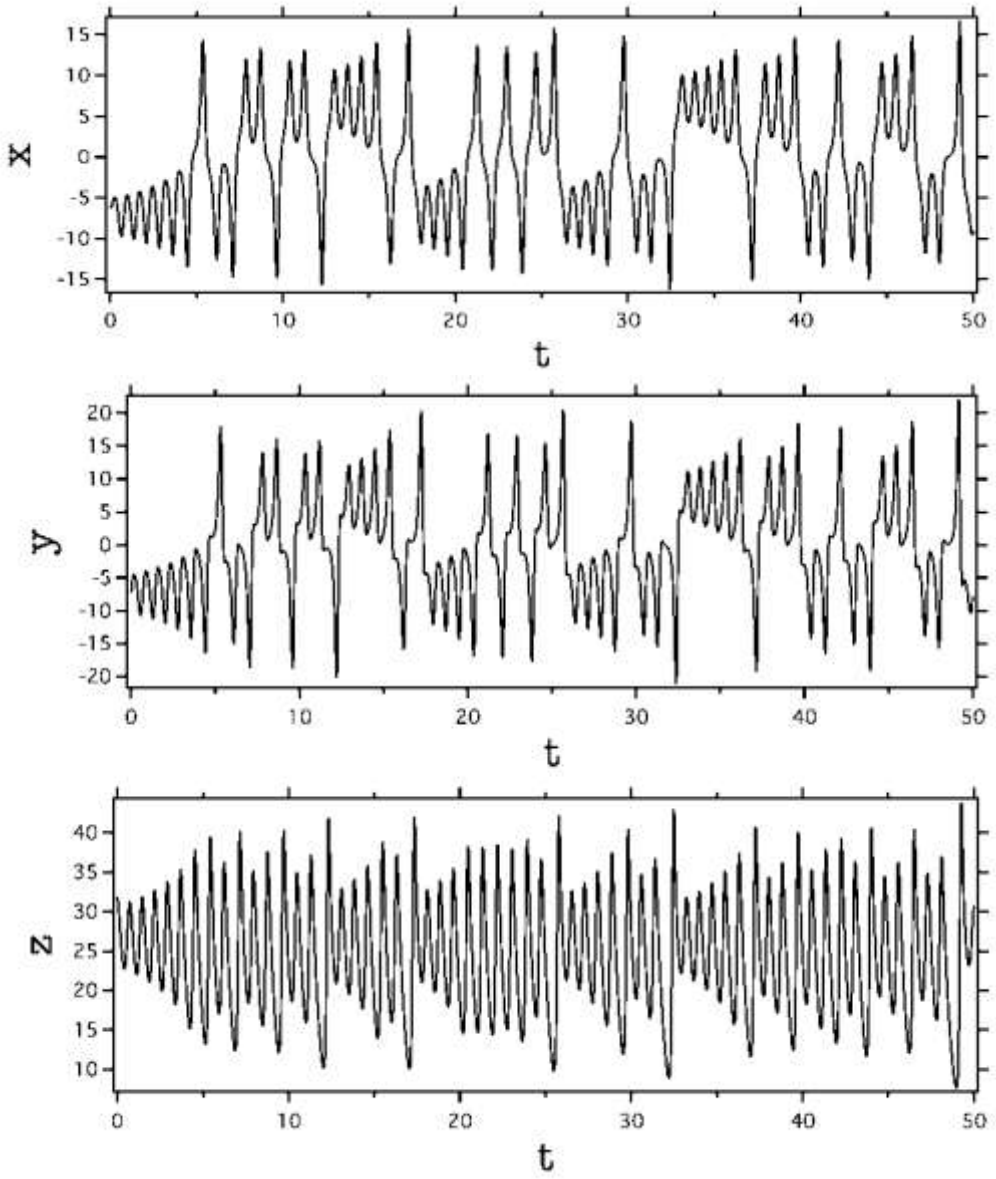
$$\dot{x} = \sigma(y - x) \tag{A1}$$

$$\dot{y} = rx - y - xz \tag{A2}$$

$$\dot{z} = xy - bz \tag{A3}$$

A Fig. A.1 mostra as séries temporais quando os parâmetros de controle têm os valores: $\sigma = 10$, $b = 8/3$ e $r = 28$.

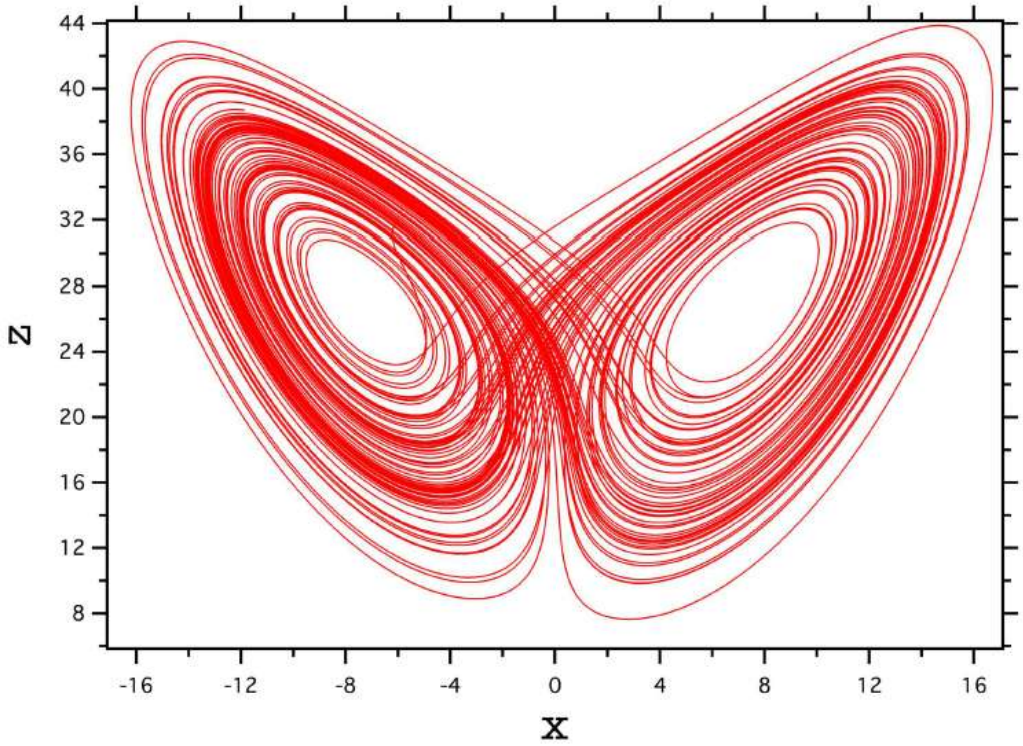
Fig. A.1. Séries temporais de Lorenz que mostram a oscilação irregular.



Fonte: referência [61,62].

A Fig. A.2 mostra as trajetórias do mapa de Lorenz que é o gráfico de *z* verso *x*. A trajetória caótica espiralada de um lado para o outro é uma projeção de uma trajetória tridimensional. No atrator de Lorenz não é possível prever o número de voltas dadas em cada uma das espirais [64,65].

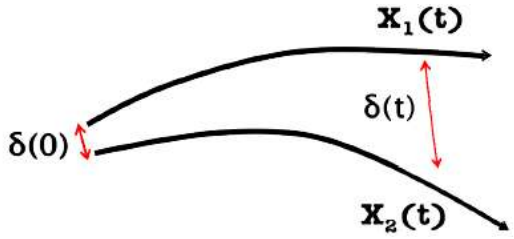
Fig. A.2. Atrator de Lorenz em plano bidimensional.



Fonte: referência [64,65].

Um sistema caótico tem como característica ser altamente sensível às condições iniciais. Essa sensibilidade pode ser medida através do expoente de Lyapunov [60]. Se duas trajetórias do mapa de Lorenz são próximas, devido às condições iniciais muito próximas, elas se afastaram rapidamente e estarão em diferentes posições no futuro. Ou seja, sendo $x_1(0)$ e $x_2(0) = x_1(0) + \delta(0)$ as condições iniciais, depois de um tempo a separação entre eles será $\delta(t)$. Resultando em $x_1(t)$ e $x_2(t) = x_1(t) + \delta(t)$ como mostra a Fig. A.3.

Fig. A.3. Evolução de duas condições iniciais próximas.



Fonte: referência [64,65].

A velocidade com que as trajetórias do mapa de Lorenz se separam pode ser obtida através do expoente de Lyapunov λ, que é definido para qualquer ponto do espaço de fase como [66]:

$$\left|\delta(t)\right| \approx \left|\delta(0)\right| \mathrm{e}^{\lambda t}. \tag{A4}$$

Se o expoente de Lyapunov $\lambda < 0$, a distância entre os pontos x_1 e x_2 diminui exponencialmente, se $\lambda > 0$ a distância entre os pontos x_1 e x_2 aumenta exponencialmente. É necessária a existência de pelo menos um expoente de Lyapunov positivo para que o sistema apresente caos [64,65].

Uma forma simples de obter o expoente de Lyapunov λ é considerar δ_{n} como a separação depois de n iterações. Assim, tem-se que $|\delta_n| \sim |\delta_0|\ e^{nt}$ que pode ser reescrito como [60]:

$$\delta n = f^n(x_0 + \delta_0) - f^n(x_0). \tag{A5}$$

Como o logaritmo da Eq. (A4) é:

$$\lambda \approx \frac{1}{n} \ln \left| \frac{\delta_n}{\delta_0} \right| \tag{A6}$$

Substituindo Eq. (A5) em Eq. (A6) resulta que:

$$\lambda \approx \frac{1}{n} \ln \left| \frac{f^n(x_0 + \delta_0) - f^n(x_0)}{\delta_0} \right| \tag{A7}$$

Assim,

$$\lambda \approx \frac{1}{n} \ln \left| (f^n)' \ (x_0) \right| \tag{A8}$$

Sendo o limite $\delta_0 \rightarrow 0$ e expandindo o logaritmo usando a regra da cadeia, resulta em:

$$(f^n)' \ (x_0) = \prod_{i=0}^{n-1} f'(x_i) \tag{A9}$$

Como:

$$\lambda \approx \frac{1}{n} \ln |\prod_{i=0}^{n-1} f'(x_i)| = \frac{1}{n} \sum_{i=0}^{n-1} \ln |(f^n)' \ (x_i)| \tag{A10}$$

A Eq. (A10) tem limite finito quando $n \rightarrow \infty$ e o expoente de Lyapunov λ começando no ponto x_0 é:

$$\lambda = \lim_{n \rightarrow \infty} \{ \frac{1}{n} \sum_{i=0}^{n-1} \ln |(f^n)' \ (x_i)| \} \tag{A11}$$

Em um sistema *n*-dimensional existe um expoente de Lyapunov associado a cada dimensão. Não é possível comportamento caótico em sistemas não lineares com menos três dimensões. O teorema de Poincaré Bendixson limita as possibilidades da dinâmica e impossibilita a existência do caos em duas dimensões [64]. A inexistência de caos em sistemas com duas dimensões deve-se ao fato de que se uma trajetória está confinada em uma região fechada, limitada e que não contém pontos fixos em seu interior, então essa trajetória ou é uma órbita fechada ou tende para uma órbita fechada [65].

A.3 Caos em mapas

Os mapas, diferentes dos fluxos, não possuem restrições de continuidade e possibilitam a obtenção de caos em sistema de uma dimensão desde que este não seja inversível. Nos mapas inversíveis o caos só é possível em sistemas com duas dimensões [66].

No estudo do caos em mapas unidimensionais, o mapa logístico é um sistema utilizado frequentemente, e por isso tornou-se um clássico. Além de ter matemática simples, ele apresenta uma grande riqueza na sua dinâmica. Segundo [66] o mapa logístico surgiu como um modelo para estudo demográfico sendo posteriormente usado para explicar a dinâmica populacional de insetos que convivam com falta de alimentos e doenças. Se uma população cresce a uma taxa proporcional à quantidade de indivíduos atuais, ou seja, se a geração sucessiva é diretamente proporcional à geração atual, matematicamente o sistema será:

$$x_{n+1} = ax_n \tag{A12}$$

O parâmetro *a* representa a taxa de crescimento da espécie. Sendo x_0 a população inicial, as gerações futuras serão determinadas por:

$$x_n = a^n x_0 \tag{A13}$$

Analisando a Eq. (A13) pode-se verificar que se o parâmetro *a* for positivo e *n* crescer, o resultado é um crescimento populacional para o infinito. Mas, se *a* for negativo, com o crescimento de *n* a população tende à extinção. No caso de a = 1 a população não muda com o passar do tempo. Para solucionar o problema do crescimento da população para infinito é introduzido um fator limitador que diminui a população numa taxa proporcional à diferença entre a capacidade do meio e a população atual, ou seja, a espécie morre por falta de alimento. Assim, o mapa logístico matematicamente será [60]:

$$x_{n+1} = ax_n(1- x_n) \tag{A14}$$

Em Eq. (A14) x_n representa a população na geração *n*. Já sua taxa de crescimento é representada em *a*. Assim, x_n deve estar no intervalo entre (0,1), pois com outro valor vai divergir para - ∞, o que extingue a população. Também se verifica que o parâmetro *a* deve ficar no intervalo entre (1-4), pois se $a < 1$ a órbita é atraída para 0. E se $a > 4$ x_n diverge para - ∞, e nos dois casos acontecerá a extinção [66].

Pode-se analisar o comportamento do ponto fixo em função de *a*. Para isso, desde que: $x_{n+1} = x_n = x^*$ o ponto fixo deve satisfazer a equação:

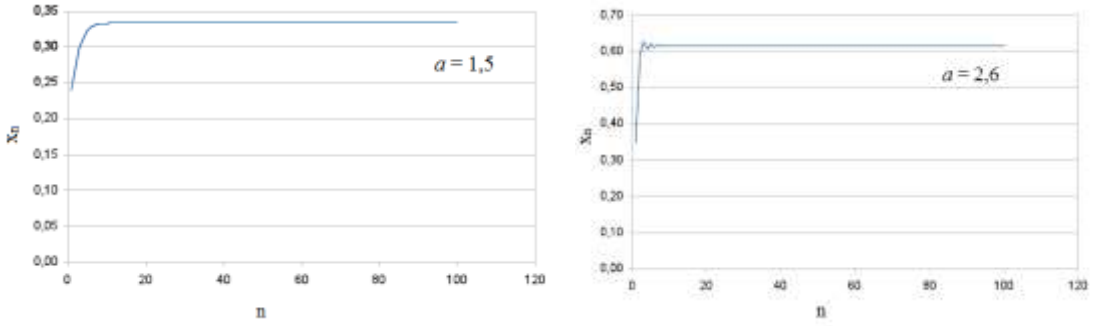
$$x^* = M(x^*) = ax^*(1-x^*), \tag{A15}$$

e como resultado os pontos fixos são as raízes da Eq. (A15): $x_1^* = 0$ e $x_2^* = 1 - \frac{1}{a}$. Observando x_1^*, verifica-se que ele é estável para $0 \leq a < 1$ e instável quando $a > 1$. O ponto fixo x_2^* é estável apenas no intervalo $1 < a < 3$. Para $a = 1$ as duas raízes são iguais e o sistema sofre uma bifurcação transcrítica [64,60]. O aumento de *a* faz as órbitas convergirem para o ponto atrator $(1 - 1/a)$. Os pontos fixos podem ser analisados através de gráficos pelas interseções da função *M (x)* com a função identidade, e a estabilidade vai depender da inclinação de *M (x)* em x^* dada por:

$$\lambda_1 \equiv \frac{dM(x^*)}{dx} = 2 - a \tag{A16}$$

As Figs. A.4 e A.5 mostram as duas séries temporais e o diagrama *stair-step* para os valores de $a = 1{,}5$ e 2,6. Pode-se verificar nas figuras que a partir de uma condição inicial, depois de algumas iterações, o sistema converge suavemente para um ponto fixo.

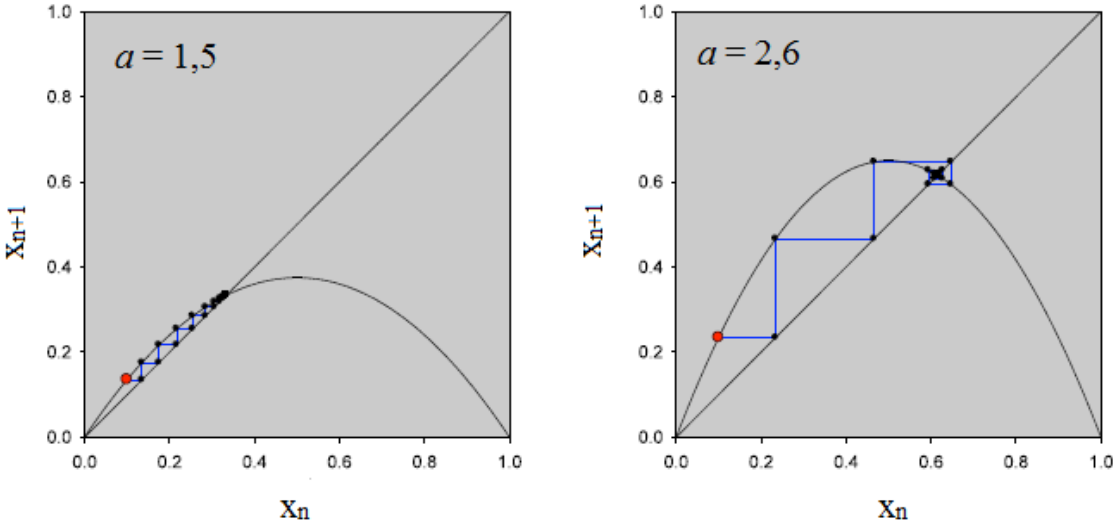
Fig. A.4. Séries temporais de período 1 do mapa logístico. (a) a = 1,5 e (b) a = 2,6.



(a) (b)

Fonte: referência [67].

Fig. A.5. Diagramas *stair-step* do mapa logístico. (a) a = 1,5 e (b) a = 2,6.



(a) (b)

Fonte: referência [67].

Aumentando o valor de a acima de três, o ponto atrator tem comportamento diferente, pois a órbita passa a alternar entre dois valores, ou seja, o sistema passa a ter um ciclo atrator de período dois. Quando aparece um ciclo atrator de período m, após uma determinada quantidade de iterações, as órbitas do mapa alternam entre m valores [60]. No caso do ciclo atrator de período dois, os pontos fixos de período dois são dados por:

$$x_2^* = M^2(x^*_2) \qquad \text{(A17)}$$

Para esse caso a inclinação de $M(x)$ em x^* será dada por:

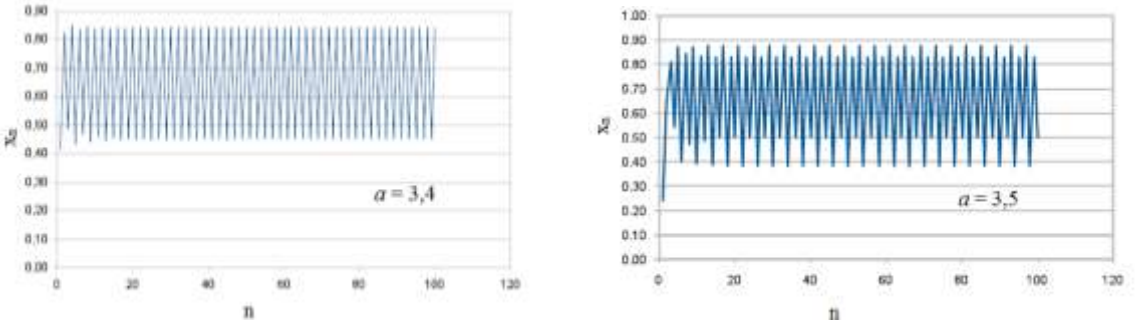
$$\lambda_1 = \lambda_1^2 \tag{A18}$$

Assim, quando $\lambda_1 < -1$, x^* se torna instável. Com $\lambda_2 > 1$ M^2 forma um laço e com isso aparece dois pontos fixos estáveis de período dois. A inclinação λ_2 segue diminuindo até chegar em -1 tornando-se instável. A duplicação de período irá acontecer para outros valores de *a*. Com $a = 3,5$ nasce um ciclo de período quatro e o mapa M^4 mostra quatro pontos fixos estáveis. Com o incremento de *a*, bifurcações de ciclos continuam a acontece para 8,16, 32... ciclos. A distância entre as bifurcações diminui e irão convergir para um ponto de acumulação de ciclos de período 2^n em torno de $a = 3,5699$. Após esse valor crítico, infinitas órbitas de diferentes períodos coexistem [64,66].

Nesse ponto, as trajetórias são aperiódicas e extremamente sensíveis às condições iniciais, ou seja, o sistema passa a apresentar um comportamento caótico.

A Fig. A.6 mostra a série temporal do mapa logístico para o valor de $a = 3,4$ e $a = 3,5$ com ciclo de período dois e quatro respectivamente.

Fig. A.6. Séries temporais de período 2 e 4 do mapa logístico. (a) $a = 3,4$ e (b) $a = 3,5$.

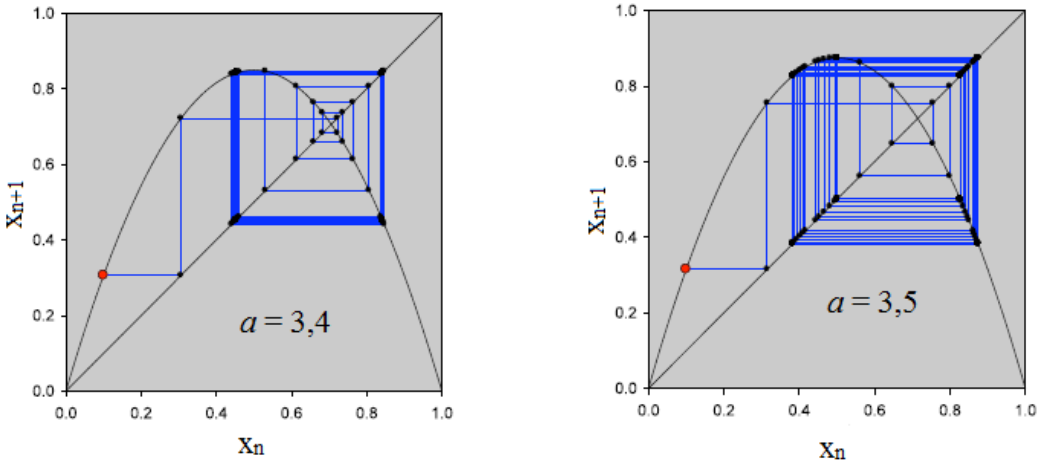


(a) (b)

Fonte: referência [67].

A Fig. A.7 mostra o diagrama *stair-step* do mapa logístico para o valor de $a = 3,4$ e $a = 3,5$. Verifica-se que em $a = 3,4$ aparece o ciclo de período dois. Em $a = 3,5$ há uma nova duplicação e os valores oscilam entre quatro valores.

Fig. A.7. Diagramas *stair-step* do mapa logístico. (a) a = 3,4 e (b) a = 3,5.

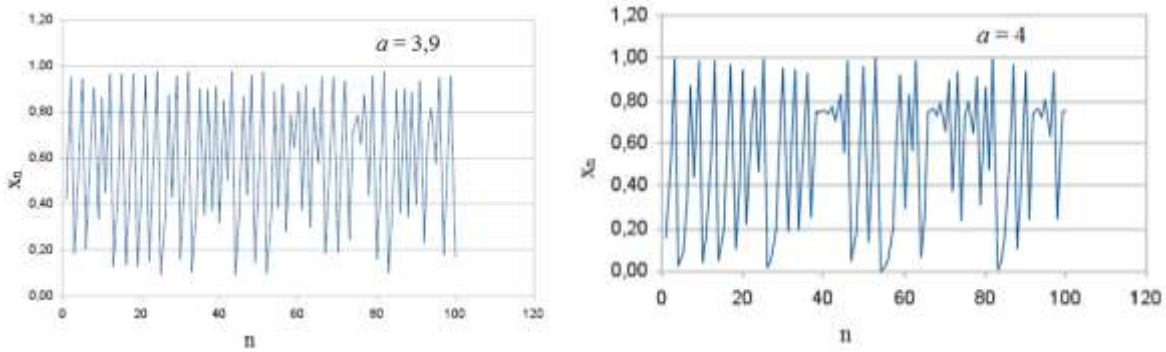


(a) (b)

Fonte: referência [67].

Na Fig. A8 pode-se ver a série temporal para a = 3,9 e a = 4. Nota-se que o número de ciclos se torna infinito e o caos aparece, pois não é possível prever o valor para o qual a função se aproxima, mesmo após um número infinito de iterações.

Fig. A.8. Séries temporais do aparecimento do caos. (a) a = 3,9 e (b) a = 4.

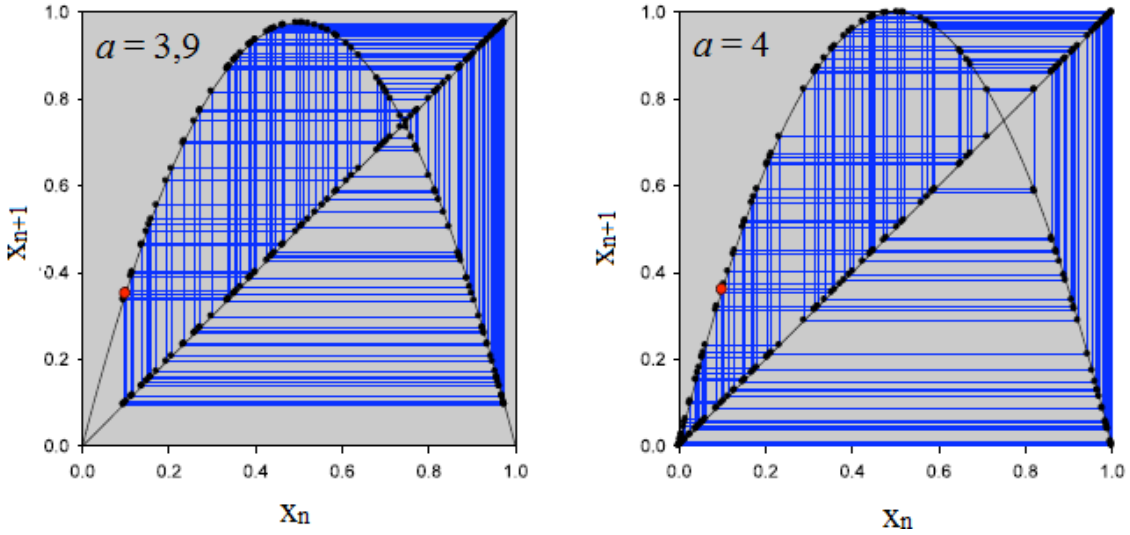


(a) (b)

Fonte: referência [67].

Os diagramas *stair-step* do mapa logístico para os valores de a = 3,9 e a = 4 são mostrados na Fig. A.9. No caos, como se verifica na Figura A.9, a parábola toda é percorrida pelos ciclos, porém com uma probabilidade não uniforme de taxa de visitação [66].

Fig. A.9. Diagramas *stair-step* do caos. (a) a = 3,9 e (b) a = 4.

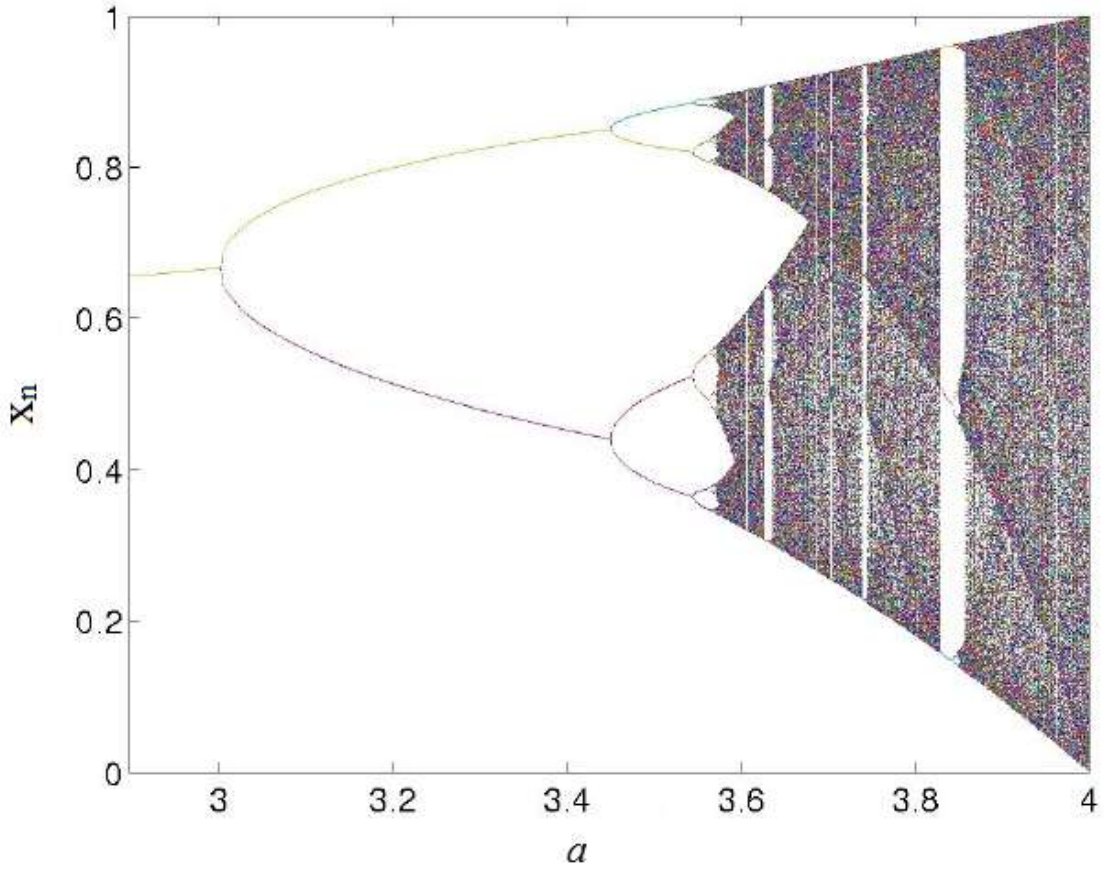


(a) (b)

Fonte: referência [67].

O diagrama de bifurcação para o mapa logístico é uma ferramenta muito utilizada para representar o caos. A Fig. A.10 mostra o diagrama de bifurcação para o mapa logístico, onde é possível visualizar as janelas de bifurcações para o caos.

Fig. A.10. Diagramas de bifurcação do mapa logístico.



Fonte: referência [67].

O diagrama de bifurcação mostra a alternância entre regiões de ordem e caos, onde janelas periódicas são intercaladas entre nuvens caóticas [60]. Como analisado anteriormente verificam-se bifurcações primeiramente em a = 1, depois em a = 3, em seguida em a = 3,45 e a partir deste ponto os ramos se dividem simultaneamente aparecendo ciclo de período 4, 8, 16, 32... Em a = 3,57 o comportamento caótico tem início e o atrator muda para um conjunto infinito de pontos.

A.4 Rota para o caos

Para [66], uma ampla variedade de sistemas não lineares apresenta transições para o caos. Esses sistemas apresentam propriedade qualitativas para o caos que podem ser estimadas quantitativamente. Para [64] as rotas para o caos estão associadas a uma sequência de bifurcações que fazem o sistema alternar do regime periódico para o caótico. As rotas para

o caos dividem-se em duas classes de bifurcações: global e local. Dentre as rotas via bifurcação local as mais estudadas são: o cenário de Feigenbaum via cascata de duplicação de período e o cenário de Pomeau-Manneville via intermitência.

O cenário de Feigenbaum via cascata de duplicação de período, visualizado no mapa logístico e estudado anteriormente, é caracterizado pela ocorrência seguida de bifurcação por duplicação de período, até o ponto de acumulação $a \rightarrow \infty$ onde o sistema apresenta o comportamento caótico. Essa rota para o caos apresenta propriedades universais que são as leis de escala e sequências universais [64]. O número de Feigenbaum é uma das leis e está ligada à velocidade com que o sistema atinge o caos. Os intervalos Δn entre os valores dos parâmetros para o qual acontece uma bifurcação para órbita de período 2^n vão diminuindo à taxa geométrica δn que converge para o número de Feigenbaum δ.

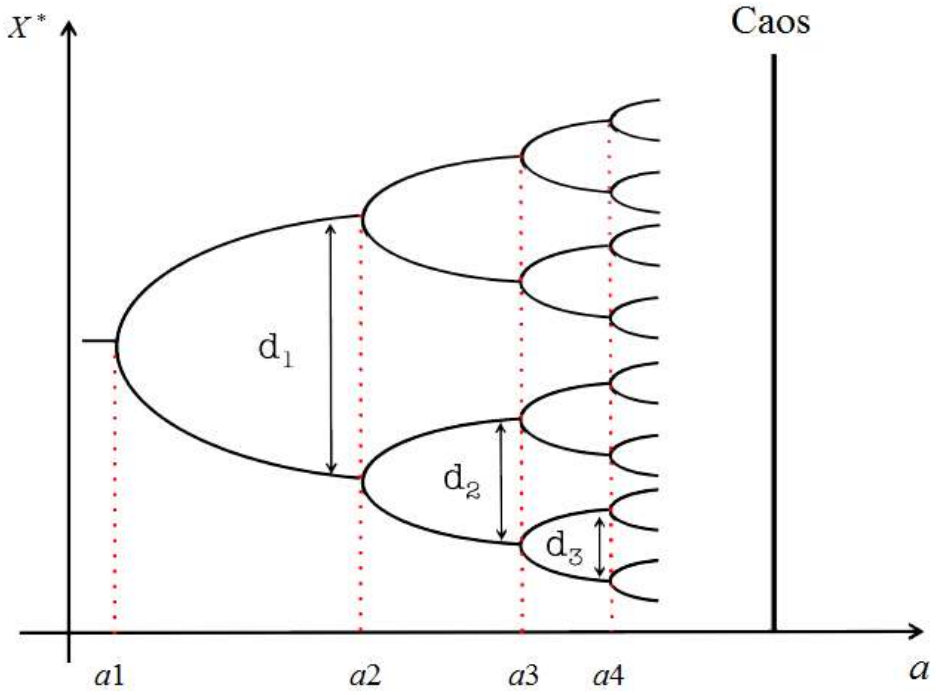
$$\delta \equiv \lim_{n\to\infty} \delta_n = \lim_{n\to\infty} \frac{\Delta_n}{\Delta_{n+1}} = 4,66920161... \tag{A19}$$

Outra lei observada por Feigenbaum é que a escala relativa de sucessivas bifurcações tende para um número universal, ou seja, as distâncias *dn* dos pontos fixos valem:

$$\frac{d_n}{d_{n+1}} = -\alpha \tag{A20}$$
$$\alpha = 2.5029078... \quad , n >> 1.$$

A Fig. A.11 mostra a rota para o caos com o cenário de Feigenbaum via cascata de duplicação de período. A cascata culmina numa órbita de período infinito e o nascimento do caos [66].

Fig. A.11. Cascata de duplicação de período.



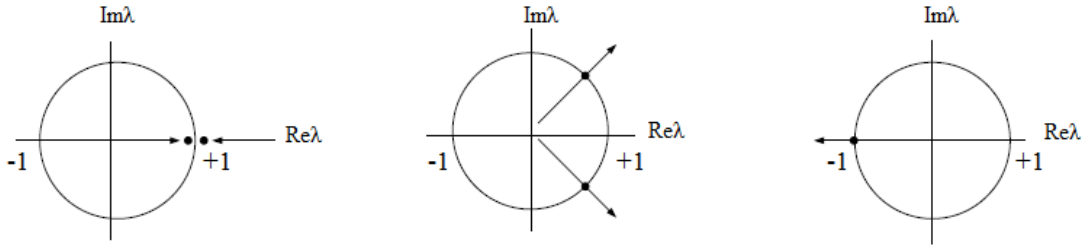
Fonte: referência [64].

O caos não aumenta com o aumento do parâmetro de controle. Assim como para o caos, existem infinitas regiões em que o sistema apresenta comportamento periódico [66]. Como comenta [66], nas chamadas "janelas periódicas" uma órbita periódica estável, e outra instável, nascem por bifurcação tangente e com o aumento do parâmetro se bifurca por dobramento de período de acordo com os mesmos números de Feigenbaum.

A rota para o caos no cenário de Pomeau-Manneville via intermitência também tem comportamento universal e é caracterizado por um comportamento periódico interrompido por regiões de comportamento caótico. Quando o sistema está em um comportamento periódico e o parâmetro de controle ultrapassa o valor crítico começam a surgir os saltos abruptos de comportamento caótico em meio a um comportamento aparentemente periódico. Com o aumento do parâmetro além do valor crítico, o sistema passa a ter períodos de irregularidade cada vez mais frequentes e com uma maior duração, até o ponto que se torna completamente caótico. Esse intervalo de aparente regularidade é chamado de "fase laminar" e sua duração é aparentemente aleatória [66].

As três formas de intermitência apresentadas por Pomeau e Manneville [68], tem para cada uma delas uma bifurcação associada e uma passagem de pelo menos um multiplicador de Floquet pelo círculo de raio unitário no plano complexo [64]: o tipo I está associada à bifurcação tangente (sela-nó) e os autovalores cruzam o ponto real +1; o tipo II está associada à bifurcação de Hopf subcrítica e dois autovalores complexos conjugados cruzam o círculo unitário simultaneamente; já o tipo III está associada à bifurcação por dobramento de período inversa e os autovalores cruzam o ponto real -1. A Fig. A.12 mostra os três tipos de intermitência.

Fig. A.12. Três tipos de intermitências. (a) tipo I, (b) tipo II e (c) tipo III.



(a) (b) (c)

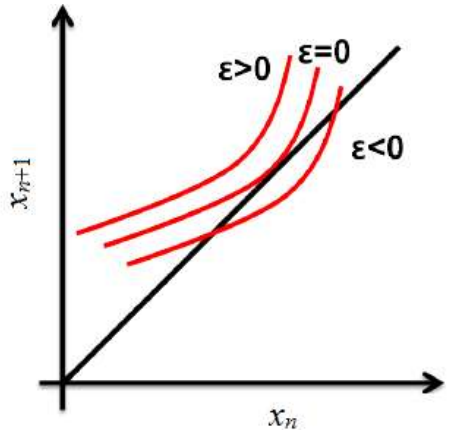
Fonte: referência [66].

A intermitência tipo I se caracteriza pela presença de um ciclo limite instável devido ao crescimento de uma perturbação que ocorre no cruzamento do autovalor pelo círculo unitário em +1. Esse tipo de intermitência está presente no mapa logístico [64]. A intermitência tipo I tem a forma normal dada por:

$$x_{n+1} = \varepsilon + x_n + x_n^2. \qquad \text{(A19)}$$

Assim, os pontos fixos são: $x_{1,2}^2 = \pm\sqrt{-\varepsilon}$. E como pode ser visto na Fig. A.13, quando $\varepsilon < 0$ o sistema possui dois pontos fixos, em $\varepsilon = 0$ existe apenas um ponto fixo e quando $\varepsilon > 0$ o sistema não apresenta pontos fixos, ou seja, os pontos fixos dependem do valor de ε [64].

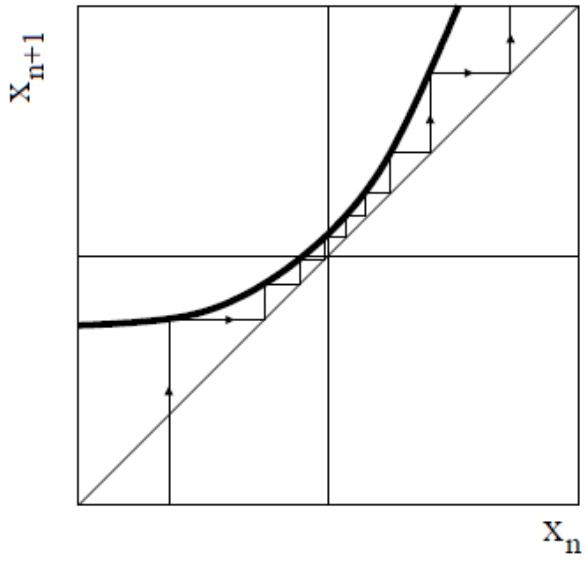
Fig. A.13. Mapas próximos a bifurcação tangente conforme o valor de ε.



Fonte: referência [64].

Como citado anteriormente, a fase laminar é um intervalo de aparente regularidade e pode-se verificar seu acontecimento quando ε é ligeiramente maior do que zero. Na Fig. A.14 verifica-se que a existência de um canal estreito entre o mapa e a diagonal. No canal os valores de x_n são muito próximos dando a impressão de comportamento periódico. Na fase laminar o comportamento do sistema é considerado como quasi-periódico. Após essa região o comportamento é caótico, até ser reinjetado novamente no canal e voltar a ser quasi-periódico [64,66].

Fig. A.14. Canal formado entre o mapa e a diagonal na fase laminar.



Fonte: referência [66].

O comprimento médio das fases laminares $\langle l \rangle$ pode ser deduzido a partir do número médio de iteradas que a órbita permanece no canal para determinado *a*, e é dado por:

$$\langle l \rangle = \varepsilon^{-1/2}. \tag{A22}$$

Como cita [66] a Eq. (A22) é válida para mapas parabólicos, mas pode ser generalizada para:

$$\langle l \rangle(\varepsilon) \propto \varepsilon^{-(1-1/z)}. \tag{A23}$$

Sendo a forma normal da bifurcação tangente igual a:

$$x_{n+1} = \varepsilon + x_n + |x_n|^{z}, \; z > 1. \tag{A24}$$

O valor denominado expoente crítico para intermitência tipo I é $V \equiv (1 - 1/z)$, que é ligado à classe de universalidade do sistema e representa a média da variável, sendo seu valor mais comum $V = 1/2$ [64].

No mapa logístico a média pode ser calculada por [64]:

$$\langle x \rangle = \lim_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N-1} x_n \qquad \text{(A25)}$$

As intermitências tipo II e III possuem forma normal semelhante e que é obtida por:

$$x_{n+1} = \pm(1+\varepsilon)x_n \pm a x_n^3 \ . \qquad \text{(A26)}$$

Na Eq. (A26) a variável a tem valor positivo sendo seu sinal alterado para representar quando + a intermitência tipo II e – a intermitência tipo III. O comprimento médio da fase laminar pode ser obtido com a Eq. (A27) para a intermitência tipo II e $\varepsilon > 0$ [64].

$$\langle l \rangle = \int_{c_1}^{c_2} P(x_{in}) l(x_{in}) dx_{in}. \qquad \text{(A27)}$$

O valor de P representa a probabilidade de reinjeção, c_2 - c_1 a largura do canal e x_{in} o ponto de reinjeção.

APÊNDICE B - DISTRIBUIÇÃO QUÂNTICA DE CHAVES

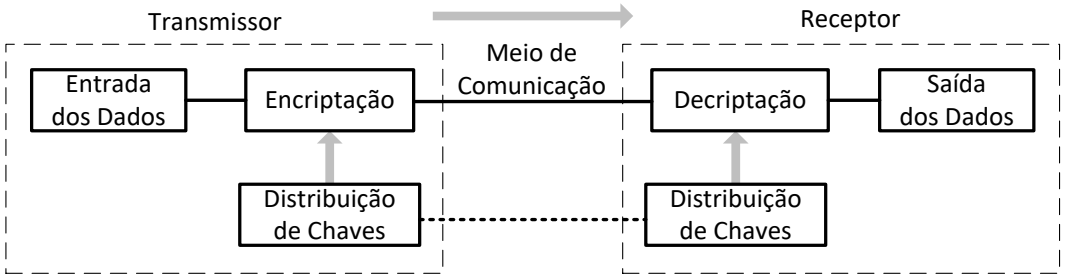
Nesse apêndice são discutidos os princípios da distribuição quântica de chaves (QKD - *Quantum Key Distribution*) e seus primeiros protocolos, o BB84 e B92.

B.1 Introdução

Segundo [69], a criptografia permite a troca de mensagens secretas somente entre os usuários legítimos da comunicação, pois apenas eles são capazes de decifrá-la. Para isso eles devem conhecer a chave criptográfica, sem a qual é impossível para um espião ter acesso a mensagem original.

Os processos envolvidos na técnica da criptografia são: encriptação dos dados que serão enviados; decriptação dos dados recebidos e a distribuição da chave criptográfica entre o transmissor e o receptor, necessária para realizar a encriptação e decriptação. A Fig. B1 mostra o conjunto de processos envolvidos na criptografia [70].

Fig. B.1. Diagrama esquemático da criptografia.



Fonte: referência [70]

Os métodos de criptografia são [69]:

a) assimétrico - no método assimétrico, uma chave pública, criada a partir de uma chave secreta que apenas Bob, o receptor, detém, é divulgada para um outro usuário que deseja lhe transmitir mensagens, por exemplo, Alice. Quando Alice enviar uma mensagem codificada fazendo uso da chave pública que Bob lhe enviou, apenas ele conseguirá decodifica-la, pois ele é o detentor da chave secreta correta;

b) simétrico - aqui Alice e Bob compartilham uma chave secreta escolhida aleatoriamente que será utilizada para codificar a mensagem através de uma operação de adição módulo dois entre a mensagem e a chave.

Em relação à segurança, o método assimétrico fundamenta-se na complexidade matemática e computacional para decifrar o código. Mas hoje essa complexidade vem sendo ameaçada pelo surgimento dos computador quântico e algoritmos de fatoração mais rápidos. No método simétrico a segurança é decorrência da operação *XOR*, nesse caso é necessário garantir que a chave secreta é conhecida apenas por Alice e Bob. Assim, o principal desafio é garantir que a chave seja distribuída seguramente entre os usuários legítimos da comunicação.

Diante dessa realidade faz-se necessário a introdução da criptografia quântica, que tem como objetivo a execução de tarefas que são impossíveis com a criptografia convencional, pois ela faz uso das propriedades da mecânica quântica como o teorema da não clonagem, que afirma não ser possível obter informação de um estado quântico genérico, do qual não se tenha conhecimento a priori, sem que se perturbe o sistema e o princípio da incerteza de Heisenberg [71].

Com a distribuição quântica de chaves os dois entes distantes, Alice e Bob, podem compartilhar uma chave aleatória mesmo na presença de uma espiã, Eva, e a chave vai permitir realizar tanto comunicação quanto autenticação seguras. Para realizar a distribuição quântica de chaves, é necessário que Alice e Bob tenham sido previamente autenticados, ou seja, eles devem compartilhar de uma mesma chave secreta que os identificará quando da primeira comunicação [72].

O BB84 e o B92, são dois dos primeiros protocolos de distribuição quântica de chaves, mas hoje existem novos protocolos de QKD como: Distribuição Quântica de Chaves com Deslocamento Diferencial de Fase – DPS-QKD (*Differential Phase-Shift Quantum Key Distribution*) e o Distribuição Quântica de Chaves com Deslocamento Diferencial de Fase em Quadratura – DQPS-QKD (*Differential Quadrature Phase-Shift Quantum Key Distribution*).

B.2 Protocolo BB84

Charles Henry Bennet e Gilles Brassard propuseram o BB84 em 1984. O protocolo consiste de um esquema de quatro estados quânticos que constituem duas bases ortogonais com a polarização da luz: a base linear (↑→) e a base diagonal (↖↗). O protocolo BB84 acontece em quatro fases [72-74]:

I) Fase de comunicação quântica - Alice envia para Bob uma sequência de bits através de fótons, cada um polarizado aleatoriamente em um dos quatro estados quânticos (↑,→,↖,↗). Para cada fóton recebido, Bob escolhe, aleatoriamente, uma das duas bases (linear ou diagonal) para realizar a medição. Bob registra a base usada para a medição bem como o resultado medido;

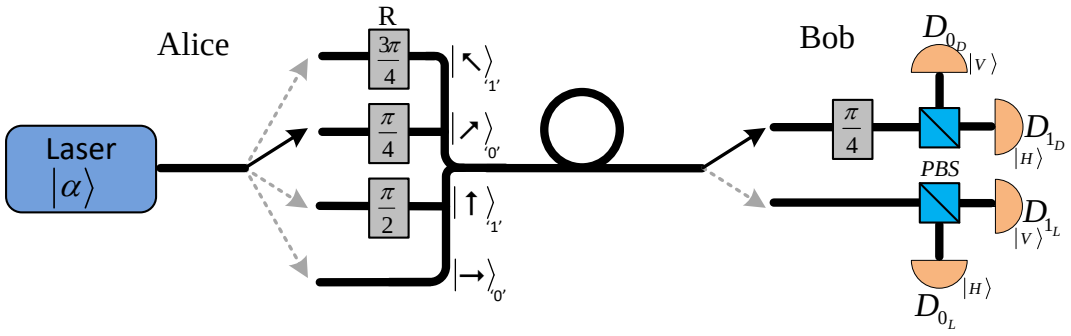
II) Fase de discussão pública - Após o envio de um grande número de bits, Alice informa publicamente as suas bases de preparação sem informar o qubit que foi transmitido, Bob compara com as suas bases de medição. Alice e Bob descartam todos os eventos em que eles usaram bases diferentes;

III) Para verificar se a distribuição foi segura, Alice e Bob escolhe aleatoriamente uma fração dos bits não descartado e transmitem publicamente. Alice e Bob computam a taxa de erro dos bits testados e se ela for maior do que um valor limite preestabelecido eles descartam toda a chave, caso contrário eles procedem para o próximo passo;

IV) Na próxima etapa, Alice e Bob convertem a polarização dos eventos restantes numa sequência binária (por exemplo, mapeando um fóton vertical ou diagonal a direita como o bit ‘0’ e um horizontal ou diagonal a esquerda como o bit ‘1’) chamada de chave bruta. Daí por diante eles podem efetuar um processo clássico de correção de erro e de amplificação de privacidade para gerar uma chave final.

Um esquema para implementação do BB84 é mostrado na Fig. B.2. Pode-se ver que Alice pode utilizar um dos estado quântico (↑,→,↖,↗) para enviar o bit para Bob. Já Bob pode escolhe aleatoriamente se realizará a medição de cada fóton com a base linear (sem rotação de $\pi/4$) ou se com a base diagonal (com rotação de $\pi/4$).

Fig. B.2. Esquema de implementação do protocolo BB84.



Fonte: referência [72].

Como exemplo de utilização do protocolo BB84 o Quadro B.1 mostra uma distribuição entre Alice e Bob.

Quadro B.1 – Procedimento do BB84. (+) Base Linear, (×) Base Diagonal.

Bits de Alice	0	1	1	1	0	1	0	0	0	1
Bases de Alice	+	×	+	+	×	×	+	×	+	×
Polarização dos fótons de Alice	→	↖	↑	↑	↗	↖	→	↗	→	↖
Bases de Bob	+	+	×	+	+	×	×	+	+	×
Polarização medida por Bob	→	↑	↖	↑	→	↖	↗	↑	→	↖
Polarização coincidente de Bob com Alice	→	?	?	↑	?	↖	?	?	→	↖
Bits de Bob	0	-	-	1	-	1	-	-	0	1

Fonte: referência [72].

B.3 Protocolo B92

Diferente do BB84 o protocolo B92 que foi criado em 1992 por Charles Henry Bennett utiliza apenas dois estados quânticos não ortogonais (→,↗ ou ↑,↖ ou →,↖ ou ↑,↗). Assim, o bit ‘0’ pode representar um fóton polarizado horizontalmente e o bit ‘1’ um fóton com polarização diagonal à direita [75].

Na primeira fase do B92, Alice envia para Bob uma sequência de bits (fótons), cada um polarizado aleatoriamente em um dos dois estados quânticos escolhidos (→ e ↗).

Para cada fóton, Bob escolhe aleatoriamente se rotaciona ou não de $\pi/4$ a polarização do fóton que chega ao seu aparato óptico de medição.

Como mostra [69,72] supondo que Alice envie o estado $|\rightarrow\rangle$ para o bit '0' e Bob escolha rotacionar o estado, quando Bob fizer a medição haverá detecção em D_0 ou em D_x com 50% de probabilidade cada, pois após a rotação o estado será $|\nearrow\rangle = 1/\sqrt{2}|\rightarrow\rangle + 1/\sqrt{2}|\uparrow\rangle$. Isso pode ser visto na Fig. B3, entretanto, se Bob decidir não rotacionar o estado, então poderá haver detecção apenas em D_y.

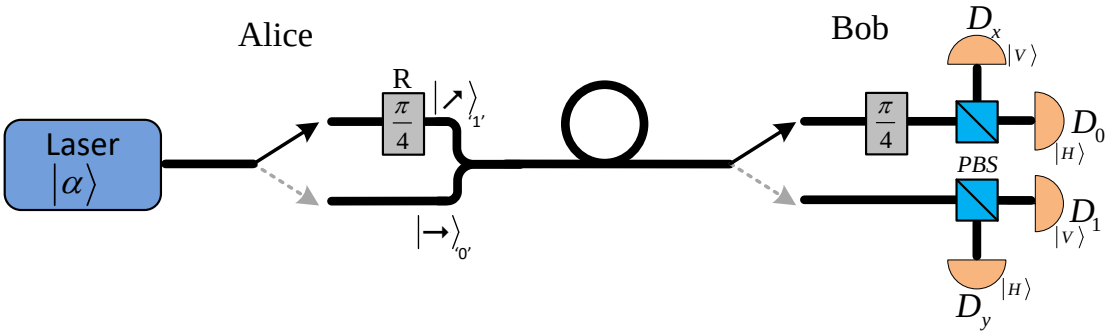
Quando Alice enviar o estado $|\nearrow\rangle$ para o bit '1' e Bob escolher rotacioná-lo poderá haver detecção somente em D_x, mas se Bob não rotacioná-lo poderá haver detecção em D_1 ou em D_y com 50% de probabilidade cada, pois o estado será $|\nearrow\rangle = 1/\sqrt{2}|\rightarrow\rangle + 1/\sqrt{2}|\uparrow\rangle$.

Como pode-se perceber, tanto o estado $|\rightarrow\rangle$ como o estado $|\nearrow\rangle$ enviados por Alice podem produzir uma contagem em D_x ou em D_y dependendo da escolha de rotação de Bob, mas apenas o estado $|\rightarrow\rangle$ pode produzir uma contagem em D_0 e apenas o estado $|\nearrow\rangle$ pode produzir uma contagem em D_1.

Na segunda fase do B92 ao contrário do BB84, não é necessário passar pela fase de discussão pública de divulgação das bases. Nessa fase final da comunicação, Bob anuncia as posições dos bits que foram detectados e eles passam a formar a chave.

Como no protocolo BB84, a chave final no B92 será obtida após a estimativa da taxa de erro da transmissão, inferência do máximo de informação roubada, correção de erros e amplificação de privacidade.

Fig.B.3. Esquema de implementação do protocolo B92.



Fonte: referência [72].

O Quadro B.2 mostra um exemplo de distribuição usando o protocolo B92.

Quadro B.2 – Procedimento do B92.

Bits de Alice	0	1	1	1	0	1	0	0	0	1
Polarização dos fótons de Alice	→	↗	↗	↗	→	↗	→	→	→	↗
Rotação realizada por Bob	$\frac{\pi}{4}$	0	0	0	$\frac{\pi}{4}$	$\frac{\pi}{4}$	$\frac{\pi}{4}$	$\frac{\pi}{4}$	0	0
Possibilidades de detecção em Bob	$D_{0,x}$	$D_{1,y}$	$D_{1,y}$	$D_{1,y}$	$D_{0,x}$	D_x	$D_{0,x}$	$D_{0,x}$	D_y	$D_{1,y}$
Contagem de Bob	D_0	D_1	D_1	D_1	D_0	D_x	D_0	D_0	D_y	D_1
Polarização coincidente de Bob com Alice	→	↗	↗	↗	→	-	→	→	-	↗
Bits de Bob	0	1	1	1	0	-	0	0	-	1

Fonte: referência [72].

B.4 Estados coerentes

Alguns protocolos de distribuição quântica de chaves enviam um trem de pulsos coerentes altamente atenuados sendo que cada pulso tem a sua fase aleatoriamente modulada por $\{0, \pi\}$. A potência do sinal transmitido é muito baixa, de forma que o número médio de fótons por pulso é menor do que um, por exemplo 0,1, de modo que a probabilidade de haver dois fótons no pulso seja muito pequena [69].

Os estados que possuem distribuição Poissoniana do número de fótons são chamados de estados coerentes. Ao contrário dos estados número, que possuem fase totalmente aleatória, os estados coerentes possuem fase mais bem definida, devido à característica de possuir distribuição Poissoniana do número de fótons, além do produto de incerteza ser o mínimo permitido pelo princípio da incerteza de Heisenberg [76].

$$\Delta p \Delta q = \frac{\hbar}{2}. \tag{B.1}$$

Como cita [69], a expressão do estado coerente em função dos estados números é definida como sendo:

$$|\alpha\rangle = e^{\left(\alpha a^{\dagger} - \alpha^{*} a\right)}|0\rangle = e^{\alpha a^{\dagger}} e^{-\alpha^{*} a} e^{-|\alpha|^{2}/2}|0\rangle = e^{-\frac{|\alpha|^{2}}{2}} \sum_{n=0}^{\infty} \frac{\alpha^{n}}{\sqrt{n!}}|n\rangle, \tag{B.2}$$

em que $a^{\dagger}$ é o operador criação e a é o operador aniquilação.

As propriedades mais importantes do estados coerentes podem ser verificadas a partir da Eq. (B.2):

(a) Número médio de fótons do estado $|\alpha\rangle$ é dado por:

$$\langle n\rangle = \langle \alpha | a^{\dagger} a | \alpha \rangle = |\alpha|^{2}; \tag{B.3}$$

(b) Probabilidade de encontrar *n* fótons no estado $|\alpha\rangle$:

$$p(n) = \langle n | \alpha \rangle \langle \alpha | n \rangle = \frac{\langle n \rangle^{n} e^{-\langle n \rangle}}{n!}; \tag{B.4}$$

(c) Relação de completude para o conjunto supercompleto de todos os estados coerentes $|\alpha\rangle$:

$$\frac{1}{\pi} \int |\alpha\rangle\langle\alpha| d^{2}\alpha = 1. \tag{B.5}$$

APÊNDICE C -ALGORITMO PARA SINCRONIZAÇÃO DE DOIS OEOs

```
Clear
home
Km=0.0132;
Ks=Km;
P0=100;
Vp=1;
VinM(1)=0.1;
VinS(1)=0.2;
dK=0;r=2;DP(1)=0.1;
for cr=1:1,
   %Km=0.01+cr/10000;
   KM(cr)=Km;
   for ct=1:40000,
      if (ct<100)
         VinM(ct+1)=Km*P0*(sin(pi/4+(pi/2)*VinM(ct)/Vp)^2);
         VinS(ct+1)=Km*P0*(sin(pi/4+(pi/2)*VinS(ct)/Vp)^2);
      else
         p1=P0*(cos(pi/4+(pi/2)*VinM(ct)/Vp)^2);
         p2=P0*(cos(pi/4+(pi/2)*VinS(ct)/Vp)^2);
         DP(r)=(p1-p2);
         dK=(0.0015*(p2-p1));
         VinM(ct+1)=Km*P0*(sin(pi/4+(pi/2)*VinM(ct)*(1+dK)/Vp)^2);
         VinS(ct+1)=Km*P0*(sin(pi/4+(pi/2)*(VinS(ct)*(1-dK))/Vp)^2);
         r=r+1;
      end
   end
V(cr,:)=VinM;
cr
end
BitM=zeros(size(VinM));
```

```
BitS=zeros(size(VinS));
BitM(find(-0.01*P0*cos(pi*VinS)<=0.7))=1;2
BitS(find(-0.01*P0*cos(pi*VinM)<=0.7))=1;

plot([1:length(VinM)],VinM,'+-',[1:length(VinS)],VinS,'o-')
figure
plot(VinM(100:length(VinM)-1),VinM(101:length(VinM)),'.')
```