



UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
**DEPARTAMENTO DE TELEINFORMÁTICA PROGRAMA DE PÓS-
GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA**

RANARA LOUISE CAMPOS DAMASCENO

ANÁLISE DE SISTEMAS DE DISTRIBUIÇÃO QUANTUM-CAÓTICA DE CHAVES

FORTALEZA

2022

RANARA LOUISE CAMPOS DAMASCENO

ANÁLISE DE SISTEMAS DE DISTRIBUIÇÃO QUANTUM-CAÓTICA DE
CHAVES

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.

Orientador: Prof. Dr. Rubens Viana Ramos.

FORTALEZA

2022

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas

Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

- D162a Damasceno, Ranara Louise Campos.
Análise de sistemas de distribuição Quantum-caótica de Chaves / Ranara Louise Campos Damasceno. –
2022.
80 f. : il. color.
- Tese (doutorado) – Universidade Federal do Ceará, Centro de Tecnologia, Programa de Pós-Graduação
em Engenharia de Teleinformática, Fortaleza, 2022. Orientação: Prof. Dr. Rubens Viana Ramos. .
1. mapa logístico . 2. pulsos multifótons. 3. tomografia quântica;. 4. função wq lambert-tsallis . I. Título.
CDD 621.38
-



ATA DA SESSÃO DE DEFESA DE TESE DE DOUTORADO

UNIVERSIDADE FEDERAL DO CEARÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

Como parte das exigências para concessão do grau de doutora, às 14:00 horas do dia 06 de Dezembro de 2022, realizou-se a sessão pública da defesa de tese de doutorado da aluna RANARA LOUISE CAMPOS DAMASCENO. O trabalho tinha como título: "ANÁLISE DE SISTEMAS DE DISTRIBUIÇÃO QUANTUM-CAÓTICA DE CHAVES".

Compunham a banca examinadora os professores(as) doutores(as) RUBENS VIANA RAMOS, orientador, JOAO BATISTA ROSA SILVA, ANTONIO VIDIELLA BARRANCO, JOSÉ AUGUSTO OLIVEIRA HUGUENIN e PAULO ALEXANDRE CARREIRA MATEUS. A candidata expôs oralmente a tese, em seguida os membros da banca procederam à arguição, e a sessão foi finalizada com a APROVAÇÃO, por parte da banca examinadora, do trabalho sem ressalvas.

Foi lavrada a presente ata que é abaixo assinada pelos membros da referida banca:

RUBENS VIANA RAMOS
UFC - Orientador

JOAO BATISTA ROSA SILVA
UFC - Examinador Interno

ANTONIO VIDIELLA BARRANCO
UNICAMP - Examinador Externo à Instituição

JOSÉ AUGUSTO OLIVEIRA HUGUENIN
UFF - Examinador Externo à Instituição

PAULO ALEXANDRE CARREIRA MATEUS
ULISBOA - Examinador Externo à Instituição

A Deus, que me sustentou e sustenta diariamente.

Aos meus pais, Juciara e Júnior, que sempre entenderam, apoiaram e vibraram pelas minhas conquistas acadêmicas.

Aos meus filhos Ivy e Gael que nasceram no decurso deste doutorado e me tornaram mais resiliente.

Aos meus irmãos Luigi, Ana, Gabriel e Dara), cunhada Jéssica), sobrinha Maya), tia Raquel) e prima Beatriz).

Aos amigos alunos e professores) que conquistei no DETI durante todos esses anos de mestrado e doutorado.

Dedico!

AGRADECIMENTOS

A Deus, porque a caminhada foi longa, árdua, por vezes tenebrosa, mas Ele me sustentou com Seu amor e me deu ânimo para continuar.

Ao Prof. Dr. Rubens Viana Ramos, não só pela excelente orientação, mas também pela amizade, paciência, por todos os ensinamentos acadêmicos e de vida), por não ter “soltado a minha mão”, por acreditar em mim e por todos os momentos de descontração. Você tem, de longe, a mente mais brilhante que eu conheço.

Aos meus filhos Ivy e Gael, que em nada ajudaram de forma prática para que esta tese fosse concluída, mas que me deram um incentivo valioso: o de mostrar para eles que uma menina vinda do interior do Ceará para a capital, pobre, conseguiu conquistar o título de DOUTORA.

Aos professores do Grupo de Informação Quântica GIQ), que estão sempre próximo aos alunos para nos ajudar a ir mais longe, nos mostrar outras possibilidades e contribuir para a que alcancemos a excelência. Ao Renato Barbosa, secretário do PPGETI, por toda a ajuda administrativa ao longo de todos esses anos.

Aos meus amigos do doutorado, em especial Joacir e Gisele, meus companheiros de laboratório, com quem dividi tantas horas de experimentos, as alegrias de vê-los funcionando, de entender os fenômenos que estavam a acontecer e os lamentos quando nada dava certo.

Aos professores participantes da banca examinadora pelo tempo, pelas valiosas colaborações e sugestões.

“A mente que se abre a uma nova ideia jamais voltará ao seu tamanho original.” – Albert Einstein.

RESUMO

A presente tese trata da distribuição quântica de chaves, da distribuição caótica de chaves e da distribuição quantum-caótica de chaves onde faz uma revisão bibliográfica de alguns protocolos existentes. Propõe um protocolo inédito de distribuição quantum-caótica de chaves usando mapa-logístico e outro protocolo inédito de distribuição quantum-caótica de chaves usando pulsos multifótons e mapa-logístico. Discute ainda a coexistência de dados clássicos e quânticos na mesma rede óptica, propondo uma fórmula analítica inédita para a obtenção do comprimento do canal óptico através do uso da função de LambertTsallis.

Palavras-chave: caos; quântica; distribuição de chaves; distribuição quântica de chaves; distribuição quantum-caótica de chaves; mapa logístico; tomografia quântica; pulsos multifótons; função wq lambert-tsallis.

ABSTRACT

This thesis deals with quantum key distribution, chaotic key distribution and quantumchaotic key distribution where it makes a literature review of some existing protocols. It proposes an inedited quantum-chaotic key distribution protocol using logistic-map and another inedited quantum-chaotic key distribution protocol using multiphoton pulses and logistic-map. It also discusses the coexistence of classical and quantum data in the same optical network, proposing an inedited analytical formula to obtain the optical channel length using the Lambert-Tsallis function.

Keywords: chaos; quantum; key distribution; quantum key distribution; quantumchaotic key distribution; logistic map; quantum tomography; multiphoton pulses; wq lambert-tsallis function.

LISTA DE FIGURAS

Figura 1 – Diagrama esquemático da criptografia	16
Figura 2 – Esquema óptico para o protocolo BB84	18
Figura 3 – Esquema óptico para o protocolo B92	19
Figura 4 – Diagrama de estado representando as probabilidades de transição nos ensaios de Markov-Bernoulli sem correlação	25
Figura 5 – Coeficiente de correlação versus variância	27
Figura 6 – Taxa de entropia <i>versus</i> coeficiente de correlação	28
Figura 7 – Distribuição de frequências de símbolos ‘1’ em palavras de 100 símbolos. A curva CM representa a distribuição de frequência do mapa caótico sozinho ($x_A = x_B = 1$ em (3.5) e (3.6)) e a curva QCC representa a distribuição de frequência da criptografia quantum-caótica (3.5) – (3.8).....	30
Figura 8 – Distribuição de frequências de símbolos ‘1’ em palavras de 100 símbolos quando há um espião no canal.....	31
Figura 9 – Esquema em blocos para a sincronização de dois mapas logísticos escravos/secundários.....	32
Figura 10 – Sincronização dos sistemas caóticos $X(o)$ e $(Y+)$. Apenas os últimos 100 valores de uma simulação com 50.000 execuções são mostrados. A parte de baixo é a transformada de Fourier da saída x_n completa.	33
Figura 11 – Esquema óptico para QCKD usando interferômetro de Sagnac. ESA – analisador de espectro elétrico.	33
Figura 12 – Sincronização dos sistemas caóticos (Xo) e $Y+)$. Apenas os últimos 100 valores de uma simulação com 50.000 execuções são mostrados. A parte de baixo é a transformada de Fourier da saída x_n	36
Figura 13 – Esquema óptico para QCKD usando pulsos multifótons com interferômetro Mach-Zehnder. A_1 e A_2 são atenuadores ópticos, D_0 e D_1 são detectores de fótons únicos, PBS é um divisor de feixe por polarização e H e V representam os modos horizontal e vertical.	39
Figura 14– Esquema homodino usando divisor de feixe balanceado e contadores de fótons D_1 e D_2	41
Figura 15 – Distribuições real e estimada para N tendo $ \beta = 1$ e $\phi = \pi/3$	42
Figura 16 – Sincronização do sistema caótico (Xo) e $Y+)$. Apenas os últimos 100 valores de uma simulação com 50.000 execuções são mostrados. Na parte inferior observa-se a transformada de Fourier da saída x_n	43
Figura 17 – Esquema óptico para QCKD usando polarização da luz. A_1 e A_2 são atenuadores ópticos, D_0 e D_1 são detectores de fótons únicos, R é um rotacionador de polarização, PBS é um divisor de feixe por polarização e H e V representam os modos horizontal e vertical.....	43
Figura 18 – $W_q(z)$ versus z para $q = 3/4$ (linha pontilhada) e $q = 5/4$ (linha contínua).....	49
Figura 19 – QKD em redes ópticas passivas na configuração de downstream	50
Figura 20 – p_R versus L . $\alpha_c = 0.48$ dB/km (1310 nm), $\alpha_q = 0.35$ dB/km (1550nm).....	52
Figura 21 – R versus L . $\alpha_c = 0.48$ dB/km (1310 nm), $\alpha_q = 0.35$ dB/km (1550nm)	53
Figura 22 – $QBER$ versus L . $\alpha_c = 0.48$ dB/km (1310 nm), $\alpha_q = 0.35$ dB/km (1550nm)	54
Figura 23 – L versus p_R . $\alpha_c = 0.38$ dB/km (1480 nm), $\alpha_q = 0.35$ dB/km (1550nm)	54
Figura 24 – R versus L . $\alpha_c = 0.38$ dB/km (1480 nm), $\alpha_q = 0.35$ dB/km (1550nm)	55
Figura 25 – $QBER$ versus L . $\alpha_c = 0.38$ dB/km (1480 nm), $\alpha_q = 0.35$ dB/km (1550nm)	56

LISTA DE QUADROS

Quadro 1 – Procedimento do BB84. +) Base Linear, ×) Base Diagonal	18
Quadro 2 – Procedimento do B92	20

SUMÁRIO

1	INTRODUÇÃO	12
2	DISTRIBUIÇÃO QUÂNTICA DE CHAVES	15
2.1	Distribuição Quântica de Chaves QKD)	15
2.1.1	<i>Protocolo BB84</i>	17
2.1.2	<i>Protocolo B92</i>	19
2.2	Distribuição Caótica de Chaves CKD)	20
2.3	Distribuição Quantum-Caótica de Chaves QCKD)	21
3	DISTRIBUIÇÃO QUANTUM-CAÓTICA DE CHAVES EM REDES ÓPTICAS: DO SEGREDO À IMPLEMENTAÇÃO COM MAPA LOGÍSTICO	24
3.1	QCKD usando o modelo de geração de chave de Markov-Bernoulli	24
3.2	Taxa de entropia	27
3.3	QCKD usando mapas logísticos	31
4	PULSOS MULTIFÓTONS E ATAQUE POR TOMOGRAFIA QUÂNTICA EM DISTRIBUIÇÃO QUANTUM-CAÓTICA DE CHAVES COM MAPA LOGÍSTICO	37
4.1	QCKD usando pulsos multifóton e mapa logístico	37
5	USO DA FUNÇÃO DE LAMBERT-TSALLIS NA ANÁLISE DO IMPACTO DO ESPALHAMENTO RAMAN ESPONTÂNEO NA DISTRIBUIÇÃO QUÂNTICA DE CHAVES EM REDES ÓPTICAS PASSIVAS	45
5.1	Coexistência da rede quântica com a rede de acesso clássica numa mesma rede óptica passiva	45
5.2	Análise do impacto do espalhamento Raman espontâneo na QKD em redes ópticas passivas usando a função W_q de Lambert-Tsallis	47
6	CONCLUSÕES E PERSPECTIVAS DE TRABALHOS FUTUROS	56
6.1	Conclusões	56
6.2	Perspectivas de trabalhos futuros	58
	REFERÊNCIAS	59
	APÊNDICE A – CAOS	62
	APÊNDICE B – FUNÇÃO W_q DE LAMBERT-TSALLIS	72
	APÊNDICE C – ARTIGOS DECORRENTES DA TESE	78

1 INTRODUÇÃO

Um dos pontos mais relevantes para o crescimento contínuo do uso das redes de comunicações, nas quais a internet está inserida, é a garantia do sigilo dos dados que trafegam por elas, ou seja, elas devem garantir que mesmo sofrendo tentativas de espionagem de usuários não autorizados, os dados permanecerão invioláveis. Isso é crucial para aplicações como comércio eletrônico, aplicações bancárias, votação eletrônica, dentre outras. A segurança da informação que é armazenada ou trafega nas redes de comunicações é garantida por protocolos criptográficos.

Tradicionalmente, tais protocolos são baseados na intratabilidade de certos problemas matemáticos, como a fatoração de números primos muito grandes. Entretanto, nas últimas décadas esses protocolos foram se movendo do campo da matemática pura para o campo da física. Inicialmente protocolos criptográficos baseados em sistemas caóticos foram propostos.

Nesses, a pseudo-aleatoriedade de uma variável caótica é utilizada para esconder a informação útil. Apesar de ser uma abordagem interessante, não há prova teórica de que os protocolos criptográficos baseados em sistemas caóticos sejam incondicionalmente seguros (Ott; Grebogi; Yorke, 1990; Nascimento *et al.*, 2018).

Outra abordagem de segurança de dados baseada em sistemas físicos é a criptografia quântica que, provavelmente, teve seu primeiro passo em 1983 com o trabalho “*Conjugate Coding*”, escrito por Stephen Wiesner, mostrando para a sociedade científica que as propriedades da física quântica poderiam ser usadas em criptografia (Brassard, 2005). Em 1984 Bennet e Brassard propuseram o primeiro protocolo de distribuição quântica de chaves, atualmente chamado de BB84 (Bennett; Brassard, 2014). Em seguida, em 1991, Arthur Ekert demonstrou que o entrelaçamento quântico também pode ser usado para realizar distribuição quântica de chaves e o protocolo por ele proposto passou a ser chamado Ekert-91 (Ekert, 1991). Em 1992, Bennet apresentou outro protocolo que era mais simples que o BB84 e tal protocolo ganhou o nome de B92 (Bennett, 1992).

Esses três protocolos de distribuição quântica de chaves são considerados incondicionalmente seguros, o que atraiu bastante a atenção de físicos, engenheiros e matemáticos. Embora na teoria eles fossem incondicionalmente seguros, limitações práticas de dispositivos reais como o ruído de detectores de fótons e fontes que emitiam luz com mais de um fóton abriam possibilidades de ataques.

Assim, durante a década de 1990 e a primeira década do século XXI, o desafio passou a ser a implementação prática desses protocolos. Nesse período surgiram o protocolo de distribuição quântica de chaves com estados-isca (MA *et al.*, 2005), que garante a segurança de implementações que utilizam fontes de estado coerente, e os protocolos COW *Coherent One-Way* e DPS *Differential Phase-Shift* (Namekata *et al.*, 2007) que possuem implementações mais simples.

Com o sucesso dessas implementações em laboratório, os desafios na segunda década do século XXI passaram a ser: I) A realização de redes de distribuição quântica de chaves de multiusuários, com integração de redes com fibra e redes ópticas no espaço livre, incluindo enlaces entre terra-satélite-terra. II) A coexistência de dados quânticos e clássicos na mesma infraestrutura óptica. III) O aumento da distância entre os usuários. IV) A diminuição da dependência da segurança dos protocolos nos parâmetros dos dispositivos reais (Patel, 2012; Wang *et al.*, 2021; Fröhlich *et al.*, 2016).

Nestas direções surgiram os protocolos de variáveis contínuas que usam detecção homodina ou heterodina ao invés de detectores de fótons CV-QKD) (Fröhlich *et al.*, 2018), a distribuição quântica de chaves com segurança independente dos parâmetros dos detectores MDIQKD), o protocolo *Twin-Field* QKD para distâncias maiores entre transmissor e receptor, bem como verificou-se que, em redes ópticas passivas, o principal responsável por aumentar a taxa de erro é o espalhamento Raman espontâneo causado pelos sinais clássicos (Cai; Sun, 2020).

Neste sentido, a presente tese atua em duas vertentes da distribuição quântica de chaves. Primeiramente, discute-se a segurança e a implementação de um protocolo de distribuição quantum-caótica de chaves. Neste tipo de sistema, a segurança da distribuição da chave depende tanto das propriedades do sistema caótico quanto do sistema quântico utilizados.

A segunda parte da tese trata da coexistência de dados clássicos e quânticos na mesma rede óptica. Partindo do nível de ruído aceitável nos detectores do receptor devido ao espalhamento Raman espontâneo, uma fórmula analítica para a obtenção do comprimento do canal óptico é obtida através do uso da função W_q de Lambert-Tsallis. Simulações numéricas são então utilizadas para a obtenção das taxas de erro e de transmissão de bits da chave.

Assim, além desta introdução, a presente tese está dividida em mais cinco capítulos. O Capítulo 2 traz uma revisão da distribuição quântica de chaves e da distribuição quantum-caótica de chaves, o Capítulo 3 apresenta um esquema óptico inédito para realizar distribuição quantum-caótica de chaves usando o mapa logístico, o Capítulo 4 trata da realização da distribuição quantum-caótica de chaves usando pulsos multifótons, o Capítulo 5

apresenta uma fórmula analítica inédita para encontrar o comprimento do canal óptico que produzirá o nível de ruído causado pelo espalhamento Raman espontâneo desejado nos detectores do receptor e o Capítulo 6 encerra esta tese com as conclusões e perspectivas de trabalhos futuros.

2 DISTRIBUIÇÃO QUÂNTICA DE CHAVES

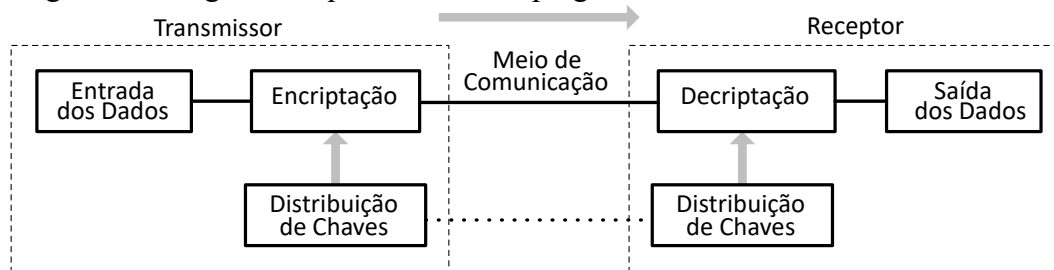
Duas das soluções empregadas para comunicação segura em redes ópticas baseadas em sistemas físicos são a Distribuição Caótica de Chaves CKD – *Chaotic Key Distribution*) e a Distribuição Quântica de Chaves QKD – *Quantum Key Distribution*). A primeira oferece taxas de transmissão bem mais elevadas que a segunda, entretanto, não se pode esperar segurança incondicional da mesma. A segunda, por sua vez, promete segurança incondicional, mas apresenta taxas de transmissão bem inferiores à primeira. Uma questão imediata que surge é a possibilidade de implementação de um protocolo quantum-caótico de distribuição de chaves que permita aproveitar o melhor de cada sistema. Neste sentido, este capítulo apresenta uma revisão sobre QKD e Distribuição Quantum-Caótica de Chaves QCKD – *Quantum-Chaotic Key Distribution*).

2.1 Distribuição Quântica de Chaves QKD)

A chave utilizada por algoritmos de criptografia precisa ser segura sigilosa e criptograficamente forte) para garantir que a informação trocada entre transmissor e receptor não seja descoberta por um espião ou espiã. A técnica que permite, teoricamente, a troca perfeitamente segura de uma sequência aleatória de bits chave) é a distribuição quântica de chaves mais especificamente o protocolo de QKD independente de dispositivos, DI-QKD – *Device Independent QKD*), cuja segurança dos protocolos utilizados é garantida pelos postulados da física quântica.

Basicamente, a criptografia é a técnica de troca de mensagens secretas que garante que somente os usuários legítimos da comunicação sejam capazes de decifrá-la, pois apenas estes detêm a chave criptográfica, sem a qual é muito difícil, senão impossível, para um espião recuperar a mensagem original (Mendonça, 2006). A criptografia inclui o processo de encriptação dos dados que serão enviados, a decríptação dos dados que foram recebidos e o processo de distribuição da chave criptográfica entre o transmissor e o receptor com a qual realizam-se os processos de encriptação e decríptação, conforme pode ser visto na Figura 1 (Wu; Shastri; Prucnal, 2013).

Figura 1 – Diagrama esquemático da criptografia



Fonte: Wu; Shastri; Prucnal (2013).

Podemos classificar os métodos de criptografia em: assimétrico e simétrico. No método assimétrico, uma chave pública, criada a partir de uma chave secreta que apenas um usuário receptor, chamado de Bob (detém, é divulgada para um outro usuário que deseja lhe transmitir mensagens transmissor, chamado de Alice). Quando Alice enviar uma mensagem codificada fazendo uso da chave pública que Bob lhe enviou, apenas ele conseguirá decodificá-la, pois ele é o único detentor da chave secreta correta. No método simétrico, Alice e Bob compartilham uma chave secreta escolhida aleatoriamente que será utilizada para codificar a mensagem através de uma operação adição módulo 2 entre a mensagem e a chave (Mendonça, 2006).

A segurança do método assimétrico fundamenta-se na complexidade matemática e computacional para decifrar o código e, por isso, ela é ameaçada pelo avanço tecnológico computadores quânticos e algoritmos de fatoração mais rápidos). Já a segurança do método simétrico é em decorrência da operação XOR ou operação de adição módulo 2 bit a bit), mas é necessário garantir que a chave secreta que codifica a mensagem seja conhecida apenas por Alice e Bob, que ela tenha o mesmo tamanho da mensagem e que só seja usada uma vez. Assim, o principal desafio dos sistemas criptográficos simétricos é garantir que a chave seja distribuída de forma segura entre os usuários legítimos da comunicação.

É nesse contexto que se insere a distribuição quântica de chaves, pois ela garante a segurança da distribuição da chave através do uso de propriedades da mecânica quântica como o teorema da não clonagem e o princípio da incerteza de Heisenberg. A distribuição quântica de chaves já foi provada ser segura sob determinadas condições experimentais (Lo; Zhao, 2009). Atualmente, sistemas de distribuição quântica de chaves estão comercialmente disponíveis e há sistemas implementados com centenas de quilômetros que utilizam fibra óptica ou o espaço livre como canal de comunicação.

A distribuição quântica de chaves permite que dois entes distantes, Alice e Bob, compartilhem uma chave aleatória na presença de uma espiã, Eva, e com ela possam 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 (Lo; Zhao, 2009). Por isso, a distribuição quântica de chaves as vezes também é chamada de protocolo de crescimento de chave.

Embora atualmente existam protocolos de QKD mais complexos como os protocolos de variáveis contínuas, *twin-field* QKD e MDI-QKD, nesta seção são discutidos apenas dois dos primeiros protocolos de QKD propostos, o BB84 e o B92.

2.1.1 Protocolo BB84

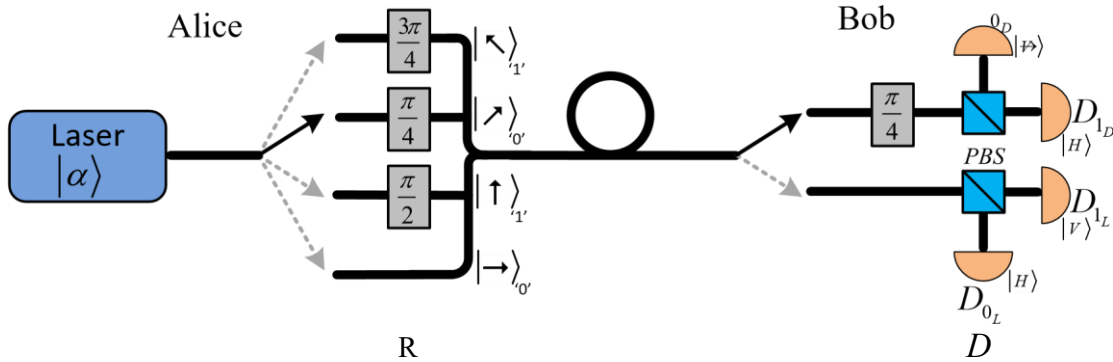
Proposto em 1984 por Charles Henry Bennet e Gilles Brassard, o BB84 consiste em um esquema de quatro estados quânticos que constituem duas bases ortogonais: usando-se a polarização da luz tem-se, por exemplo, a base linear ($\uparrow \rightarrow$) e a base diagonal ($\nearrow \nwarrow$). O protocolo BB84 pode ser dividido em duas fases: I) comunicação quântica e II) discussão pública (Bennett; Brassard, 2014).

- I) Na fase de comunicação quântica, Alice envia para Bob uma sequência de fótons, cada um polarizado aleatoriamente em um dos quatro estados quânticos ($\uparrow, \rightarrow, \nearrow, \nwarrow$). 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 e informa publicamente que recebeu o sinal.
- II) Na segunda fase, a fase de discussão pública, Alice informa as suas bases de preparação e Bob informa as suas bases de medição. Alice e Bob descartam todos os eventos em que eles usaram bases diferentes. Para verificar a presença de um espião na comunicação, Alice escolhe aleatoriamente uma fração dos eventos remanescentes (aqueles nos quais as bases de Alice e Bob coincidiram) e transmite publicamente as polarizações dos fótons usadas para estes eventos. Em seguida, Bob transmite os resultados de suas medições naqueles eventos. Alice e Bob computam a taxa de erro dos eventos 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. 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 (Mendonça, 2006).

A Figura 2 mostra o esquema óptico que implementa o protocolo BB84. Alice envia para Bob uma sequência de fótons polarizados aleatoriamente num estado quântico

($\uparrow, \rightarrow, \nearrow, \nwarrow$). Bob 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 $\pi/4$).

Figura 2 – Esquema óptico para o protocolo BB84



Fonte: Elaborada pela autora.

No Quadro 1 abaixo pode-se verificar um exemplo do procedimento do protocolo BB84 descrito acima.

Quadro 1 – Procedimento do BB84, (+) Base Linear, (x) Base Diagonal

Bits de Alice	0	1	1	1	0	1	0	0	0	1
Bases de Alice	+	x	+	+	x	x	+	x	+	x
Polarização dos fótons de Alice	\blacklozenge	\nwarrow	\uparrow	\uparrow	\nearrow	\nwarrow	\blacklozenge	\nearrow	\blacklozenge	\nwarrow
Bases de Bob	+	+	x	+	+	x	x	+	+	x
Polarização medida por Bob	\blacklozenge	\uparrow	\nwarrow	\uparrow	\blacklozenge	\nwarrow	\nearrow	\uparrow	\blacklozenge	\nwarrow
Polarização coincidente de Bob com Alice	\blacklozenge	?	?	\uparrow	?	\nwarrow	?	?	\blacklozenge	\nwarrow
Bits de Bob	0	-	-	1	-	1	-	-	0	1

Fonte: Elaborada pela autora.

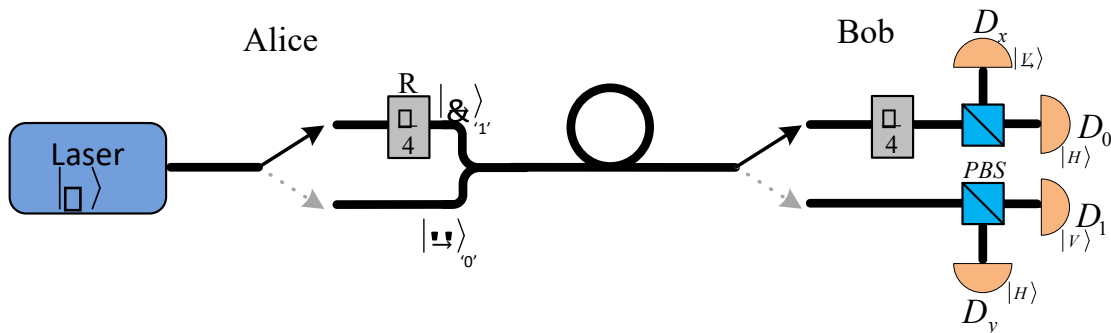
2.1.2 Protocolo B92

O protocolo B92 foi criado em 1992 por Charles Henry Bennett e difere do BB84 no que tange à quantidade de estados quânticos utilizada na implementação do protocolo. Enquanto o protocolo BB84 usa duas bases ortogonais, ou seja, quatro estados quânticos, o B92 utiliza apenas dois estados quânticos não ortogonais (\rightarrow, \nearrow ou \uparrow, \nwarrow ou \rightarrow, \nwarrow ou \uparrow, \nearrow). Por

exemplo, o bit ‘0’ pode ser um fóton polarizado horizontalmente e o bit ‘1’ um fóton com polarização diagonal à direita (Bennett, 1992).

A Figura 3 apresenta o esquema óptico que implementa este protocolo e a sua execução acontece da seguinte forma: Alice envia para Bob uma sequência de fótons, cada um polarizado aleatoriamente em um dos dois estados quânticos (aqui serão utilizados os estados $|\rightarrow\rangle$ e $|\nearrow\rangle$). Para cada fóton, Bob escolhe aleatoriamente se rotaciona ou não de $\pi/4$ a polarização do fóton que chega ao seu aparato óptico.

Figura 3 – Esquema óptico para o protocolo B92



Fonte: Elaborada pela autora.

Caso Alice tenha enviado o estado $|\rightarrow\rangle$ (bit ‘0’) e Bob escolha rotacionar o estado, então poderá haver detecção em D_0 ou em D_x com 50% de probabilidade cada, pois após a rotação o estado será $|\nearrow\rangle = 1/\sqrt{2}|\rightarrow\rangle + 1/\sqrt{2}|\uparrow\rangle$. Entretanto, se Bob decidir não rotacionar o estado, então poderá haver detecção apenas em D_y .

Similarmente, se Alice enviar o estado $|\nearrow\rangle$ (‘1’) e Bob escolher rotacioná-lo poderá haver 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 $|\nearrow\rangle = 1/\sqrt{2}|\rightarrow\rangle + 1/\sqrt{2}|\uparrow\rangle$ (Bennett, 1992).

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 Bob a respeito da rotação, mas apenas o estado $|\rightarrow\rangle$ pode produzir uma contagem em D_0 assim como apenas o estado $|\nearrow\rangle$ pode produzir uma contagem em D_1 . Dessa forma, Bob consegue concluir com certeza qual fora o bit enviado por Alice. Percebe-se que, ao contrário do BB84, não é necessário passar pela fase de discussão pública de divulgação das bases, mas Bob precisa avisar para Alice quando ele obteve uma detecção válida.

No Quadro 2 abaixo pode-se verificar o procedimento do protocolo B92.

Quadro 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: Elaborada pela autora.

2.2 Distribuição Caótica de Chaves CKD)

Comunicações seguras baseadas em caos usam uma portadora da informação cuja amplitude varia caoticamente e mascara o sinal de informação. Os métodos de criptografia baseado no caos podem ser usados para criptografar dados com altas taxas de bits, mas frequentemente com um baixo nível de confidencialidade, pois podem apresentar dependência condicional devido à interação dos mapas caóticos, quando estes são inadequados (Ma *et al.*, 2005; Namekata *et al.*, 2007).

Há dois métodos amplamente conhecidos para realizar comunicações através do caos. O primeiro método deriva do método OGY Ott-Grebogoy-Yorke) (Ott; Grebogi; Yorke, 1990), o qual utiliza o caos controlado, ou seja, a dinâmica do sistema caótico é projetada de forma que ele esteja em um dos seus atratores periódicos instáveis através do uso de pequenas perturbações, consequentemente possibilitando a codificação da mensagem.

O segundo método, que possibilita mais velocidade na codificação da mensagem, é baseado numa abordagem diferente desenvolvida por Pecora e Carrol (1990), a qual é uma técnica para sincronizar sistemas caóticos. A mensagem é misturada com uma portadora caótica usada como uma portadora banda larga para mascarar a mensagem. Para implementar um sistema de comunicação seguro usando as propriedades de pseudoaleatoriedade e de alta

dependência dos valores iniciais dos parâmetros dos sistemas caóticos, estes devem estar sincronizados. O sincronismo dos sistemas caóticos é necessário para que o receptor possa recuperar a informação.

Dois sistemas caóticos distantes, um em Bob e outro em Alice, sincronizados podem gerar a mesma sequência de bits para ser utilizada como chave criptográfica. Para estarem sincronizados, Alice e Bob precisam trocar informações dados de sincronização através do canal óptico. Para um espião, Eva, que queira espionar, basta capturar os dados de sincronização para tentar sincronizar seu próprio sistema caótico. Essa vulnerabilidade reduz a confiabilidade da chave (Oliveira, 2018).

Mais recentemente, outro método de comunicação por caos foi reportado (Kocarev; Parlitz, 1995; Goedgebuer, 1998). Este método utiliza sistemas óptico não lineares com laço de atraso e pode apresentar alta dimensionalidade com número de expoentes de Lyapunov positivos que pode ser até 100 vezes maior do que os sistemas baseados em circuitos elétricos na faixa de frequência audível (Beth; Lazic; Mathias, 1994; Perez; Cerdeira, 1995).

2.3 Distribuição Quantum-Caótica de Chaves QCKD)

Como visto anteriormente, a QKD e a CKD são duas formas de segurança de dados em redes ópticas baseadas em sistemas físicos (Bennetti; Brassard, 2014; Ekert, 1991; Namekata et al., 2007; Van Wiggeren, 1998; Lo; Zhao, 2012; Argyris, 2005). Como explicado anteriormente neste capítulo, a distribuição quântica de chaves promete segurança incondicional, contanto que sejam usados pulsos de luz muito fracos fótons únicos ou estados coerentes fortemente atenuados). Alcançar altas taxas de transmissão e transmissão de dados m -ários ($m > 2$) neste cenário é complicado.

Por outro lado, a distribuição caótica de chaves tanto permite altas taxas de transmissão como a transmissão de dados m -ários pode ser facilmente alcançada desde que as variáveis caóticas sejam variáveis contínuas. Contudo, a distribuição caótica não garante a perfeita inviolabilidade da informação.

Na verdade, na criptografia simétrica existe uma forte distinção entre a distribuição quântica e a caótica no que diz respeito à análise de segurança da chave produzida. A distribuição quântica de chaves implementada com dispositivos ideais permite encriptação com perfeita segurança devido à independência e à equiprobabilidade dos eventos que geram a chave. Do outro lado, a distribuição caótica de chaves pode apresentar dependência condicional

devida às iterações dos mapas caóticos gerando insegurança quando os seus respectivos mapas não são adequados (Akhavan; Samsudin; Akhshani, 2015; Li, 2016).

O uso conjunto da QKD com a CKD pode ser muito vantajoso. Nas primeiras propostas de uso conjunto, os sistemas quânticos e caóticos trabalhavam separadamente, sendo que o último servia apenas como um gerador de números pseudoaleatórios para o primeiro (Kartalopoulos, 2008; Stojanovic; Ramos; Matavulj, 2016). Em 2018, uma nova proposta para usar conjuntamente as duas tecnologias foi apresentada (Oliveira; Ramos, 2018). Nesta proposta, chamada de Criptografia QuantumCaótica, a informação usada para manter os sistemas caóticos sincronizados era carregada por estados quânticos. Como consequência, as partes quântica e caótica estavam integradas de tal forma que era impossível separá-las. Em outras palavras, não era possível fazer nenhum cálculo ou simulação dos sistemas caóticos sincronizados sem levar em consideração as probabilidades quânticas.

Além disso, os bits da chave são obtidos a partir da discretização da variável caótica de saída e conseqüentemente os bits da chave não viajam ao longo do canal. Um espião teria que atacar o sinal de sincronismo e tentar reconstruir o mapa caótico. O problema é que perturbando os sinais de sincronismo carregados por estados quânticos) a taxa de erro aumenta e isso revela o ataque. Portanto, nesta proposta de distribuição quantum-caótica de chaves, a segurança do protocolo é baseada nas regras da física quântica e do caos.

Foi comentado anteriormente que um mapa caótico pode introduzir alguma correlação na chave gerada na distribuição caótica de chave e por este motivo é importante checar se a inserção do caos na distribuição quântica de chaves pode levar à existência de correlação entre os símbolos da chave. Esta correlação não pode ser negligenciada, caso ela exista, pois ela pode reduzir o segredo da chave.

A fim de analisar a segurança da QCKD, em Kokarev (2001) foi feita uma verificação das semelhanças entre cifras e mapas caóticos: rodadas de encriptação e mapas caóticos interativos. Uma vez que a análise criptográfica permite o modelo de cifras de Markov estabelecendo probabilidades de transição em cada rodada, em Wu, Shastri e Prucnal (2013) foram estabelecidas probabilidades de transição condicionadas a eventos prévios devidos às interações do mapa caótico usado no protocolo de distribuição quantum-caótica de chaves. Considerando este modelo, a simulação feita em Wu, Shastri e Prucnal (2013) verificou que a correlação entre os símbolos da chave é quase zero, mostrando que a distribuição quantum-caótica de chaves proposta em Oliveira e Ramos (2018) tem segredo quase idêntico ao observado numa distribuição quântica de chaves ideal.

Apesar de suas propriedades de segurança adequadas, o esquema óptico para QCKD proposta em Oliveira e Ramos (2018) apresenta algumas dificuldades de implementação, principalmente porque utiliza polarização da luz para transportar informações e sistemas caóticos implementados com osciladores optoeletrônicos.

No capítulo 3 desta tese é apresentado um esquema de QCKD mais simples que pode ser facilmente implementado com a tecnologia atual. A informação é codificada na fase e os sistemas caóticos são equações discretas sendo executadas em computadores. A equação não linear discreta escolhida foi o mapa logístico. A configuração óptica proposta para implementação utiliza o interferômetro de Sagnac, no entanto, também é possível implementar o protocolo de QCKD usando o interferômetro de Mach – Zehnder ou de Michelson.

3 DISTRIBUIÇÃO QUANTUM-CAÓTICA DE CHAVES EM REDES ÓPTICAS: DO SEGREDO À IMPLEMENTAÇÃO COM MAPA LOGÍSTICO

Este capítulo amplia a teoria da QCKD em duas vertentes. A primeira propõe o uso dos ensaios dependentes de Bernoulli para modelar a geração de chaves na QCKD. A segunda vertente mostra um novo esquema óptico para QCKD no qual os esquemas ópticos caóticos a serem sincronizados são equações discretas não lineares e a propriedade usada para transportar a informação é a fase da luz.

3.1 QCKD usando o modelo de geração de chave de Markov-Bernoulli

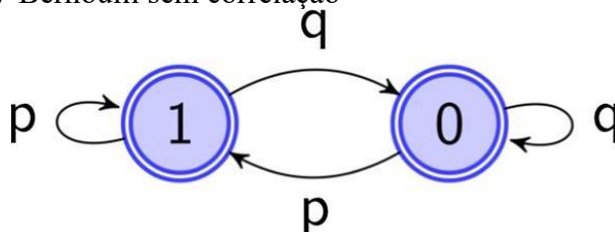
Chama-se símbolo o sinal codificado que representa um dígito binário, rotulado por '0' ou '1', enquanto o bit é uma unidade de informação incerteza). Assim, a sequência binária gerada por Alice e Bob, usada como chave em um esquema criptográfico simétrico, é composta por símbolos, enquanto a quantidade de bits representa a incerteza de que um espião possui sobre um determinado número de símbolos. Esses dois conceitos podem ser tratados como sinônimos quando a coleção de variáveis aleatórias é independente e identicamente distribuída (i.i.d.) (Nascimento *et al.* 2018).

Um protocolo de distribuição quântica de chaves é independente e identicamente distribuído quando cada interação bem-sucedida entre Alice e Bob é resultado de escolhas e medições independentes. Sob essas condições, pode-se considerar a geração de cada símbolo '0' ou '1' como um teste de Bernoulli. Por exemplo, uma sequência de chave de n símbolos 0110 ... 00 pode ser o resultado de n ensaios de Bernoulli em que se tem n variáveis aleatórias K_1, K_2, \dots, K_n cujos possíveis valores '0' e '1' são resultados de um processo aleatório, como uma medição quântica em H^2): $K_1 = 0, K_2 = 0, K_3 = 0, K_4 = 0, \dots, K_n = 0$. A matriz de probabilidade de transição de Markov para uma sequência de Bernoulli é:

$$T = \begin{bmatrix} \Pr(K_n = 1|K_{n-1} = 1) & \Pr(K_n = 0|K_{n-1} = 1) \\ \Pr(K_n = 1|K_{n-1} = 0) & \Pr(K_n = 0|K_{n-1} = 0) \end{bmatrix} = \begin{bmatrix} p & q \\ p & q \end{bmatrix}, \quad (4)$$

e a representação de T em diagrama de estados é dado na Figura 4 abaixo:

Figura 4 – Diagrama de estado representando as probabilidades de transição nos ensaios de Markov-Bernoulli sem correlação



Fonte: Nascimento *et al.* (2018).

Neste modelo, a QKD como proposta em Bennett e Brassard (1984) e Ekert (1991) é exatamente um ensaio de Bernoulli. Neste caso, tem-se $\Pr(0|0) = \Pr(0|1) = q$ e $\Pr(1|0) = \Pr(1|1) = p$, sendo $p + q = 1$, e cada símbolo é gerado independentemente. Para ter entropia máxima, tem-se $p = q = 1/2$. A probabilidade de uma sequência de n ensaios independentes de Bernoulli ter m símbolos '1' pode ser facilmente calculada, resultando em uma distribuição binomial. Agora, a pergunta é: qual é a distribuição de probabilidade dos m símbolos '1' em uma chave de n símbolos obtidos em um protocolo de QCKD? Para responder a essa pergunta, é preciso obter uma matriz de transição com propriedades que descrevam as condições da QCKD. Essas condições são:

1. O circuito de Alice e de Bob é estático por exemplo, a eficiência quântica dos detectores não muda com o tempo);
2. A única variável dinâmica é o sinal caótico do mapa $x_n = f(x_{n-1})$;
3. O mapa caótico não é acessível a um espião porque é apenas localmente observável no circuito de Alice e Bob;
4. A frequência dos símbolos '0' e '1' é aproximadamente a mesma.

Para satisfazer as condições 1 a 3, pode ser usada uma cadeia homogênea de Markov em que a probabilidade condicional não depende do tempo, ou seja, $\Pr(K_n = a|K_{n-1} = b) = \Pr(K_n = a|K_{n-2} = b) = \dots = \Pr(K_2 = a|K_1 = b)$ para todos $a, b \in \{0,1\}$. Pode-se notar que Alice e Bob podem determinar essas probabilidades de transição e, portanto, podem estimar/prever os símbolos principais. No entanto, prever símbolos é interessante apenas para Eva (a espiã), mas ela não pode identificar as probabilidades de transições preferíveis porque x_n não está acessível para ela. Portanto, a cadeia homogênea de Markov é um bom modelo analítico para identificar a correlação entre os eventos que geram os símbolos da chave. Por fim, a condição 4 requer uma distribuição estacionária que ocorre

quando $\text{Pr}(0)$ e $\text{Pr}(1)$ tendem aos valores constantes p e q respectivamente, após muitas transições na cadeia de Markov. Para um bom protocolo, usa-se $p = q = 1/2$.

Um modelo simples e homogêneo de cadeia de Markov-Bernoulli com correlação pode ser encontrado em Edwards (1960), no qual cada símbolo da chave é casualmente correlacionado ao resultado do símbolo anterior por um coeficiente de correlação r . Para esse tipo de cadeia de Markov, a matriz de transição é escrita como:

$$T = \begin{bmatrix} p + rq & q - rq \\ p - rp & q + rp \end{bmatrix} = \begin{bmatrix} p & q \\ p & q \end{bmatrix} + r \begin{bmatrix} q & -q \\ -p & p \end{bmatrix} = B + rC, \quad (3.2)$$

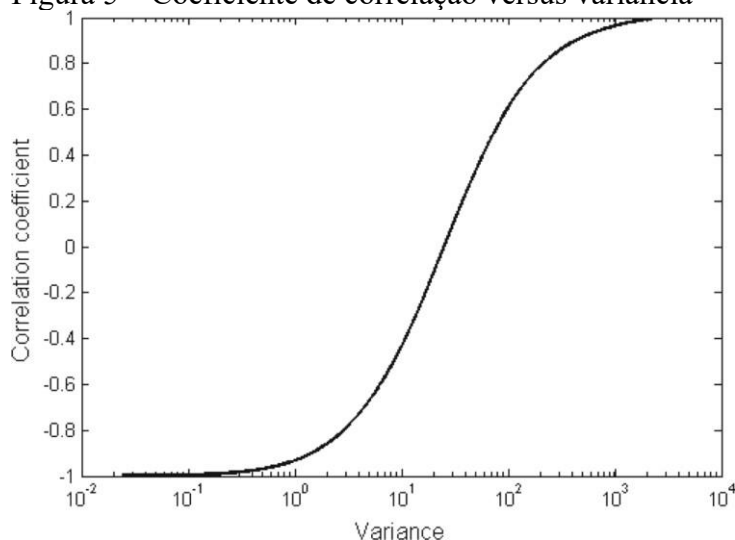
onde rC representa a correlação entre os ensaios de Bernoulli. Pode-se verificar que $T^n = B + r^n C$, uma vez que as matrizes B e C possuem as seguintes propriedades: (1) $B^n = B$ e $C^n = C$; (2) $BC = CB = 0$. Também é possível verificar que $\text{Det}(T^n) = r^n$.

Como o protocolo de QCKD possui uma distribuição estacionária (quando os sistemas caóticos são sincronizados), o valor médio em uma única tentativa é $E[K_i] = 1 \times p + 0 \times q = p$. Além disso, a variação da distribuição (variância $-\sigma^2$) do número de símbolos '1' em uma sequência com N símbolos é dada por Edwards (1960):

$$\sigma^2 = Npq + 2pq \frac{r}{(1-r)^2} [N(1-r) - 1 + r^N]. \quad (3.3)$$

Se $\sigma^2 > Npq$, há uma correlação positiva. Isso significa que há uma tendência para o símbolo permanecer o mesmo em cada transição. Por outro lado, se $\sigma^2 < Npq$, existe uma correlação negativa. Nessa situação, a alteração do símbolo é uma tendência em cada transição. Ambos os fenômenos alteram o sigilo da chave. Na Figura 4 pode-se ver o coeficiente de correlação r (*'Correlation coefficient'* na figura) versus a variância (σ^2) obtida em (3.3) (*'Variance'*, na figura). Ainda na Figura 4, pode-se notar que uma pequena variação no coeficiente de correlação resulta em uma grande variação da variância. Daí resulta três tipos de distribuição: distribuição binomial quando a correlação não existe, ou seja, coeficiente de correlação igual a zero; distribuições de cauda gorda quando o coeficiente de correlação é positivo; e distribuições de cauda fina quando o coeficiente de correlação é negativo.

Figura 5 – Coeficiente de correlação versus variância



Fonte: Nascimento *et al.* (2018).

Em uma distribuição binomial, os eventos extremos são muito improváveis como uma sequência de N símbolos '0', enquanto os eventos centrais são prováveis e bem distribuídos em um grande número de possibilidades. Por outro lado, quando há correlação positiva, as caudas gordas indicam que eventos extremos serão mais comuns. Quanto maior o coeficiente de correlação, mais comuns eles se tornam.

Na criptografia simétrica, eventos extremos representam chaves frágeis. Por exemplo, grandes correlações positivas podem gerar uma chave nula que resultará em um texto cifrado igual ao texto sem formatação ($\text{xor}(M,0) = M$).

3.2 Taxa de entropia

Em um protocolo de QKD, cada símbolo da chave é gerado independentemente do símbolo anterior com probabilidade uniforme, então a entropia é $H(K^n) = H(K_1, K_2, \dots, K_n) = nH(K)$. Assim, a taxa de entropia (Kartalopoulos, 2008), que caracteriza o crescimento linear da entropia, é $H(K) = H(K^n)/n$. Isso significa que a entropia da chave cresce linearmente em $H(K)$ bits/símbolo. Pode-se notar que a taxa de entropia tem a mesma magnitude da entropia de um único ensaio dependente de Bernoulli.

Na QCKD, deseja-se saber se cada símbolo da chave pode ser gerado independentemente do símbolo anterior. Assumiu-se que esse tipo de distribuição de chaves pode ser modelado por uma cadeia homogênea de Markov com distribuição estacionária, onde o coeficiente de correlação está presente na matriz de transição. Assim, o crescimento da

entropia linear é obtido equiparando a taxa de entropia da QCKD à entropia de um ensaio dependente de Bernoulli $H(K) = H(K_n|K_{n-1})$, onde $H(K)$ é dado por:

$$H(K) = -p[(p + rq) \log(p + rq) + (q - rq) \log(q - rq)] - q[(p - rq) \log(p - rp) + (q + rp) \log(q + rp)]. \quad (3.4)$$

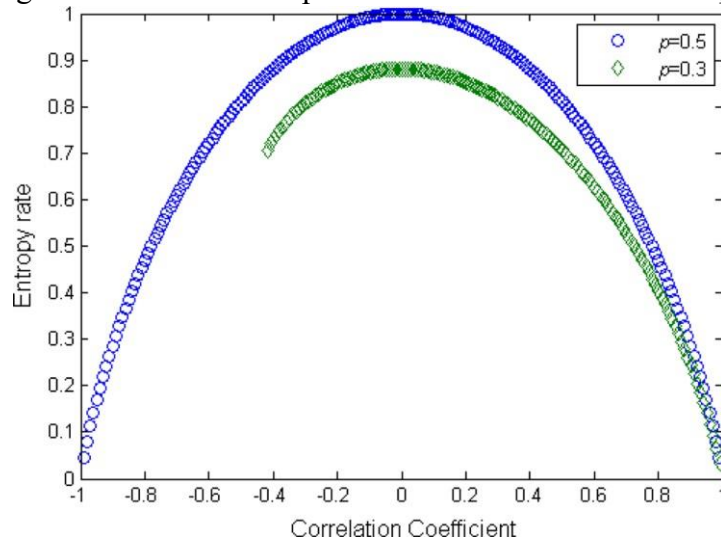
A Figura 6 mostra a curva da taxa de entropia ‘Entropy rate’ na figura) como uma função do coeficiente de correlação r ‘Correlation coefficient’ na figura) para um ensaio dependente de Bernoulli. Quando $p = 1/2$, a curva tem a máxima taxa de entropia em $r = 0$. Neste caso, a taxa de entropia é 1 bit/símbolo como observado na QKD. Em outros casos $p \neq 1/2$, as condições a seguir devem ser observadas: Se $p < q$, então $r > p/q$ ou se $q < p$ então $r > -q/p$. A Figura 6 também mostra a curva da taxa de entropia quando $p = 0.3$.

A dinâmica da QCKD proposta em (41) é basicamente descrita pelo mapa estocástico não linear dado por

$$V_{in}^A(t + \tau) = K_A |\alpha_A|^2 \left[1 - x_A \cos^2 \left(\frac{\pi V_{in}^A(t)}{2 V_\pi} + \varphi \right) \right], \quad (3.5)$$

$$V_{in}^B(t + \tau) = K_B |\alpha_B|^2 \left[1 - x_B \cos^2 \left(\frac{\pi V_{in}^B(t)}{2 V_\pi} + \varphi \right) \right]. \quad (3.6)$$

Figura 6 – Taxa de entropia versus coeficiente de correlação



Fonte: Nascimento et al. (2018).

Nas Equações (3.5) e (3.6), x_A (x_B) é uma variável binária aleatória que assume o valor 0 com a probabilidade q_A (q_B) dada por

$$q_A = \min \left\{ p_A t_c |\alpha_B|^2 \sin^2 \left(\frac{\pi [V_{in}^A(t) - V_{in}^B(t)]}{2 V_\pi} \right), 1 \right\}, \quad (3.7)$$

$$q_B = \min \left\{ p_B t_c |\alpha_A|^2 \sin^2 \left(\frac{\pi [V_{in}^A(t) - V_{in}^B(t)]}{2 V_\pi} \right), 1 \right\}. \quad (3.8)$$

Em (3.5)-(3.8), $|\alpha_A|^2$ ($|\alpha_B|^2$) é a potência óptica de entrada em Alice (Bob), $\varphi = \pi/4$, V_π é a tensão aplicada ao modulador óptico que desloca a fase de $\pi/2$ e K modela o ganho do amplificador elétrico, as perdas ópticas, e a eficiência do detector. Ainda, p_A (p_B) é a probabilidade do detector de fóton 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 (menor que 1) do pulso que sai de Alice (Bob), ou seja, após a atenuação, e t_c é o coeficiente de transmissão do canal.

Em Oliveira e Ramos (2018), a QCKD tem as seguintes propriedades:

- O esquema de Alice e Bob são estáticos os parâmetros α , φ e K são constantes);
- A única variável dinâmica é o sinal da tensão de modulação V_{int});
- A espiã não tem acesso ao V_{int}), e conseqüentemente, ela não pode identificar as probabilidades de transição.

Portanto, a QCKD obedece às condições exigidas pelo modelo de Markov anteriormente discutido. A fim de verificar como o mapa caótico interfere com o sigilo em uma QCKD, como proposto em Oliveira e Ramos (2018), foi calculado o coeficiente de correlação em três situações:

- (1) Coef. de correlação (r) usando as eqs. (3.5) e (3.6) com $x_A = x_B = 1$.
- (2) r na QCKD com espiã.
- (3) r na QCKD sem espiã.

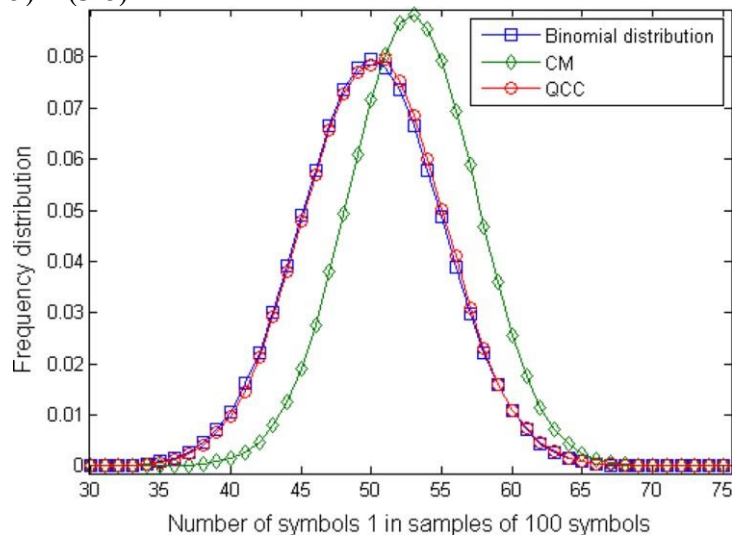
Para a simulação, os mesmos valores dos parâmetros descritos em Oliveira e Ramos (2018) foram usados: $|\alpha|^2 = 2500$ (Alice e Bob), $\varphi = \pi/4$, $V_\pi = 1V$, $K_A = K_B = 0,0133$, $V_{in}^A(t=0) = 0,1$ e $V_{in}^B(t=0) = 0,2$. Nas simulações realizadas, foram criadas 100 chaves com 10^6 símbolos e a frequência relativa dos símbolos 1 em palavras de 100 símbolos foi calculada. A distribuição de frequência deve ser similar a uma distribuição binomial, portanto,

também foram simulados 10^8 ensaios de Bernoulli para comparar, onde $p = 0.5$ resulta em $\sigma^2 = 25,2454$ para $N = 100$.

Na Figura 7 nota-se que o mapa caótico curva CM, 1ª situação, quando $x_A = x_B = 1$) gera uma distribuição deslocada à direita ($\mu/N = 0,5291$). Adicionalmente, nota-se que o mapa caótico sozinho curva CM apresenta uma variância bem acima da observada na simulação dos ensaios de Bernoulli ($\sigma_{CM}^2 = 28,1955$) e assim o limite para o coeficiente de correlação pode ser estabelecido, $r_{CM} < 0,0622$.

Por outro lado, quando o mesmo mapa está trabalhando no regime quantum-caótico (x_A e x_B são variáveis aleatórias, QCKD com e sem espiã, 2ª e 3ª situação), a distribuição de frequência (curva QCC) está bem próxima de uma distribuição binomial. Neste caso, $\mu_{AB}/N = 0,5015$ e $\sigma_{AB}^2 = 25,4123$ e conseqüentemente a variância é um pouco maior do que seria esperado para uma distribuição binomial real.

Figura 7 – Distribuição de frequências de símbolos ‘1’ em palavras de 100 símbolos. A curva CM representa a distribuição de frequência do mapa caótico sozinho ($x_A = x_B = 1$) em (3.5) e (3.6) e a curva QCC representa a distribuição de frequência da criptografia quantum-caótica (3.5) – (3.8).

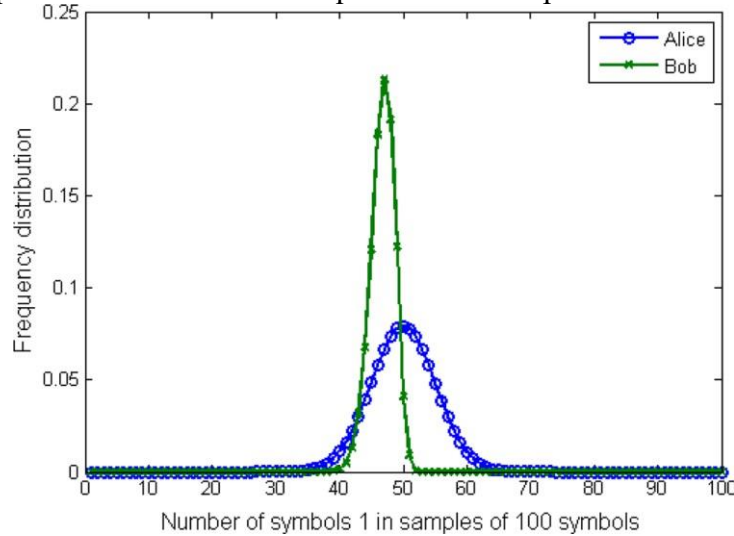


Fonte: Nascimento et al. (2018).

Isso é evidência da correlação positiva dos símbolos da chave de Alice e Bob, $r_{AB} < 0,008$. Nesta curva, nota-se uma leve assimetria que não é percebida na distribuição binomial. Por exemplo, a frequência de 51 símbolos ‘1’ 0,07947 é maior do que a frequência de 50 símbolos ‘1’ 0,07831 e, portanto, a inserção de dispositivos quânticos reduz significativamente a correlação símbolo a símbolo no mapa caótico e aumenta significativamente a taxa de entropia para 0,999 bits/símbolo muito perto do valor ideal de 1 bit/símbolo.

Na Figura 8, observa-se a distribuição de frequências quando o canal de Bob está sob o ataque por máquina de clonagem. A distribuição de frequência de Alice é simétrica e perto de uma distribuição binomial, $\mu_A/N = 0,5001$ e $\sigma_A^2 = 25,2597$, mas a distribuição de frequência de Bob é significativamente modificada, $\mu_B/N = 0,4674$ e $\sigma_B^2 = 21,8771$, indicando uma forte correlação negativa dos símbolos de Bob, $r > -0,068$, sendo portanto a sua distribuição de frequência mais fina e assimétrica.

Figura 8 – Distribuição de frequências de símbolos ‘1’ em palavras de 100 símbolos quando há um espião no canal.



Fonte: Nascimento et al. (2018).

3.3 QCKD usando mapas logísticos

O uso de mapas logísticos sincronizados para comunicações seguras foi proposto em (45). O conjunto de equações que descrevem a sincronização são

$$x_{n+1} = \lambda x_n(1 - x_n) \quad (3.9)$$

$$y_{n+1} = \lambda y_n(1 - y_n) + c[k - \lambda(1 - y_n - x_n)](y_n - x_n). \quad (3.10)$$

Como pode ser notado nas eqs. (3.9) e (3.10), a fim de obter a sincronização o sistema mestre X envia a informação x_n , um valor contínuo na faixa de $(0,1)$, para o sistema escravo Y . Para passar da segurança caótica para a segurança quantum-caótica, a informação enviada do emissor para o receptor que mantém seus sistemas não lineares sincronizados tem que ser discretizada.

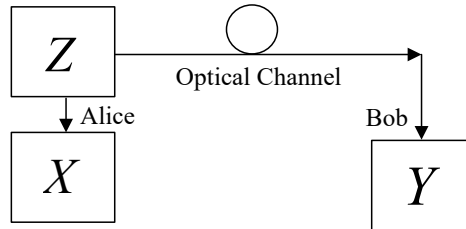
Nesta tese, adotamos uma estratégia diferente para sincronização dos mapas logísticos. Pode-se ver na Figura 9 abaixo que Alice tem o sistema mestre Z , um gerador quântico de números aleatórios (QRNG), e o sistema escravo X , enquanto Bob tem o sistema escravo Y . As equações que descrevem a dinâmica de sincronização são:

$$z_n = QRNG, \quad (3.11)$$

$$x_{n+1} = \lambda x_n(1 - x_n) + c[k - \lambda(1 - x_n - dz_n)](x_n - dz_n), \quad (3.12)$$

$$y_{n+1} = \lambda y_n(1 - y_n) + c[k - \lambda(1 - y_n - dz_n)](y_n - dz_n). \quad (3.13)$$

Figura 9 – Esquema em blocos para a sincronização de dois mapas logísticos escravos/secundários.

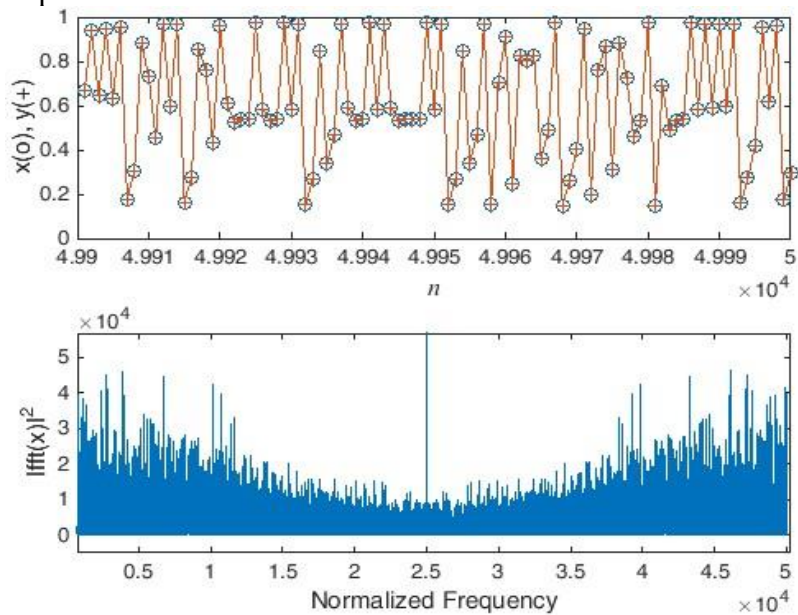


Fonte: Nascimento *et al.* (2018).

O objetivo é manter os sistemas X e Y sincronizados. Isso é alcançado porque ambos os sistemas são alimentados pela mesma fonte, o sistema Z , um gerador quântico de números aleatórios que produz os valores ‘0’ e ‘1’ com a mesma probabilidade. Conseqüentemente, a informação de sincronização vinda do sistema mestre Z é discreta. A variável d nas Equações (3.12) e (3.13) reduz ou amplia o papel de z_n .

A Figura 10 a seguir mostra um exemplo de sincronização entre X e Y , assim como a transformada de Fourier de x_n . Os valores dos parâmetros usados são $\lambda = 3.9$, $k = 0.2$, $c = 0.5$, $d = 0.5$, enquanto os valores iniciais das variáveis dinâmicas são $x(1) = 0.8$, $y(1) = 0.16$, $z(1) = 0$.

Figura 10 – Sincronização dos sistemas caóticos $X(o)$ e $(Y+)$. Apenas os últimos 100 valores de uma simulação com 50.000 execuções são mostrados. A parte de baixo é a transformada de Fourier da saída x_n completa.

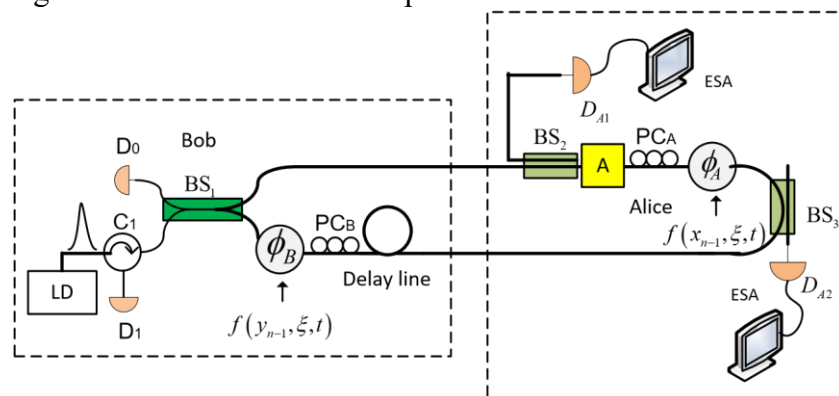


Fonte: Nascimento *et al.* (2018).

Vemos na Figura 10 que X e Y estão perfeitamente sincronizados, pois todos os ‘+’ estão centralizadas nos ‘o’. A transformada de Fourier apresentando um caráter contínuo nos confirma o caráter aleatório de x_n .

A fim de implementar um sistema quantum-caótico de distribuição de chaves usando sincronização de mapas logísticos, o esquema óptico para QCKD usando interferômetro de Sagnac (46, 47) mostrado na Figura 11 pode ser usado.

Figura 11 – Esquema óptico para QCKD usando interferômetro de Sagnac. ESA – analisador de espectro elétrico.



Fonte: Nascimento *et al.* (2018).

O esquema óptico na Figura 11 trabalha da seguinte forma: Inicialmente Bob envia um pulso óptico forte para Alice. Esse pulso é dividido em dois pelo divisor de feixe balanceado BS_1 . Uma parte vai para Alice seguindo no sentido horário (P_{Clk}) enquanto a outra parte vai para Alice seguindo no sentido anti-horário (P_{CClk}).

O pulso P_{Clk} chega primeiro em Alice, uma vez que o pulso P_{CClk} tem que passar através da linha de atraso em Bob. Uma vez em Alice, o pulso P_{Clk} é fortemente atenuado pelo atenuador óptico A , a sua polarização é corrigida pelo PC_A e ele passa pelo modulador de fase ϕ_A sem ser modulado. Finalmente, ele retorna para Bob. Uma vez em Bob, P_{Clk} passa pela linha de atraso, tem sua polarização corrigida pelo PC_B , é modulado pelo $\phi_B = f(y_{n-1}, \xi, t)\pi$ e, por fim, chega no BS_1 .

Por outro lado, o pulso P_{CClk} passa pelo ϕ_B sem ser modulado, segue pelo PC_B e pela linha de atraso e continua em direção a Alice. Uma vez em Alice, o pulso P_{CClk} tem sua fase modulada por ϕ_A , de acordo com os valores de z_n e x_{n-1} , respectivamente: $\phi_A = [z_n + f(x_{n-1}, \xi, t)]\pi$. Ele tem sua polarização corrigida por PC_A , é atenuado por A e finalmente viaja direto para o BS_1 em Bob. Ambos os pulsos, P_{CClk} e P_{Clk} , chegam no BS_1 ao mesmo tempo, com a mesma polarização e dessa forma a interferência acontece.

A função f é o mapa logístico $f_{m+1} = \xi f_m (1 - f_m)$. O valor de entrada f_0 é x_{n-1} para Alice e y_{n-1} para Bob e o valor de saída é f_t . Os parâmetros ξ e t são conhecidos apenas por Alice e Bob. Desde que os dois pulsos tomem o mesmo caminho, as flutuações da fase são automaticamente compensadas. O valor da atenuação A é tal que o pulso P_{CClk} deixando Alice tenha o número médio de fótons perto de 0,1 depois de passar por A . Dependendo da diferença de fases aplicada por Alice em P_{CClk} e por Bob em P_{Clk} , o fóton será guiado pelo detector de fóton único SPD) D_0 ou D_1 . As probabilidades de detecção em D_0 e D_1 são dadas por

$$p_0 = [1 - \exp(-|\alpha|^2 \eta)(1 - p_d)] \cos^2 \left[\frac{\pi(z_k \oplus a + f(x_{n-1}, \xi, t) - f(y_{n-1}, \xi, t))}{2} \right], \quad (3.14)$$

$$p_1 = (1 - \exp(-|\alpha|^2 \eta)(1 - p_d)) \sin^2 \left[\frac{\pi(z_k \oplus a + f(x_{n-1}, \xi, t) - f(y_{n-1}, \xi, t))}{2} \right]. \quad (3.15)$$

Nas eqs (3.14) e (3.15), $|\alpha|^2$ é o número médio de fótons do pulso chegando em Bob, η é a eficiência quântica dos detectores e p_d é a probabilidade de contagem de escuro dos detectores de fóton único. Por fim, a é a paridade do i -ésimo dígito de $f(x_{n-1}, \xi, t)$ (i é conhecido somente por Alice e Bob).

Para Bob, detecção em D_0 implica $z_n \oplus a = 0$ enquanto detecção em D_1 implica $z_n \oplus a = 1$. Assim, depois de calcular a paridade do i -ésimo dígito de $f(y_{n-1}, \xi, t)$, Bob finalmente obtém o valor de z_n . Como pode ser visto nas Equações (3.14) e (3.15), a probabilidade de detecção (p_0 e p_1) depende do sincronismo (z_n) e o sincronismo depende da probabilidade de detecção.

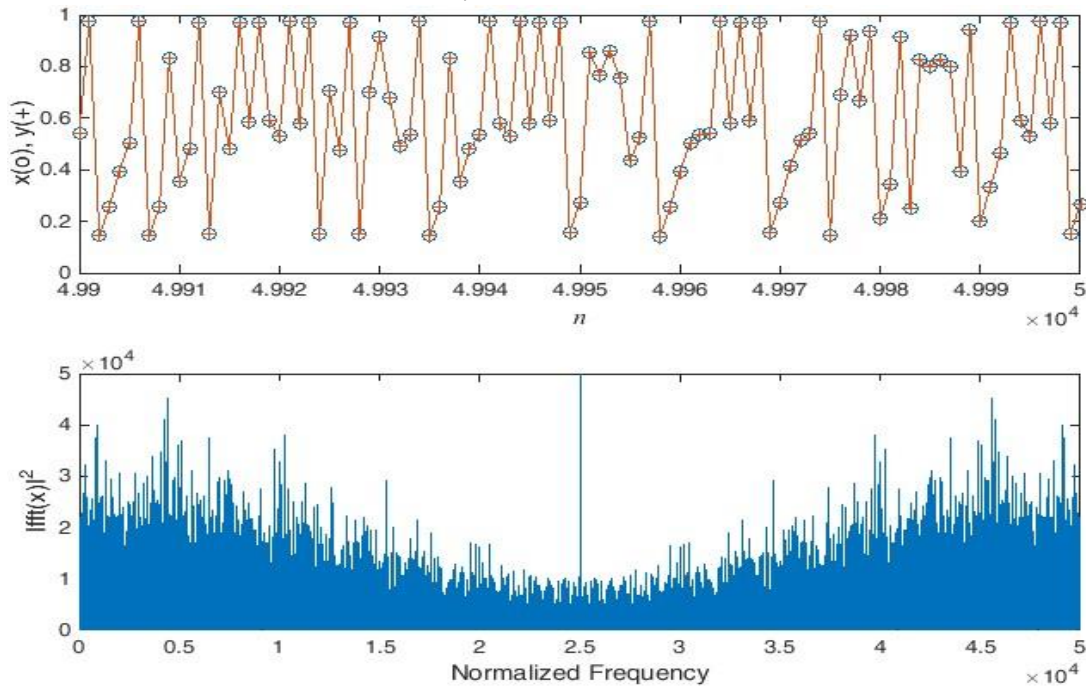
A falta de sinais de sincronização causará a desincronização dos mapas logísticos, resultando numa alta taxa de erro. A fim de evitar esse problema, Alice e Bob devem atualizar os valores de x_n e y_n apenas quando Bob tiver detecção. Isto implica dizer que quando Bob não tiver nenhuma detecção, ele informa a Alice e ela atualizará z_k e calculará um novo valor de f usando $t + \delta$ δ é um número inteiro conhecido apenas por Alice e Bob, ao invés de t . Consequentemente, cada pulso enviado por Alice terá um valor de fase diferente mesmo quando x_n não está atualizado. Bob fará a mesma coisa até que ele tenha detecção. Depois da detecção, Alice e Bob podem imediatamente reiniciar t para o valor inicial ou apenas continuar atualizando-o quando necessário até que um máximo valor previamente escolhido seja alcançado, e só então reiniciar t para o valor inicial.

A taxa de erro cresce se o sinal de sincronismo não for corretamente recebido por Bob quando ele obtém $1 - z_n$ ao invés de z_n . Consequentemente, num ataque, o espião não pode enviar para Bob um sinal com o valor incorreto da fase. Além disso, BS₂, BS₃,

A , os detectores de fóton único, D_{A1} e D_{A2} , e o analisador de espectro formam um “cão de guarda” (Cavalcanti; Mendonça; Ramos, 2011; Pinheiro; Ramos, 2015) que impedem Eva de implementar um ataque do tipo cavalo de Tróia enviando pulsos fortes para Alice com o objetivo de determinar os valores de fase usados. A Figura 12 abaixo mostra a simulação do protocolo QCKD que acabamos de descrever e cujo esquema óptico foi mostrado na Figura 11.

Em Oliveira e Ramos (2018), os estados quânticos viajando pelo canal são estados de polarização contínua, pois neste caso a polarização é função de uma variável contínua. Similarmente, na configuração mostrada na Figura 12 estados coerentes com fase contínua (sua fase pode assumir qualquer valor entre 0 e 2π) são usados para carregar a informação de sincronismo.

Figura 12 – Sincronização dos sistemas caóticos (X_0 e Y_+). Apenas os últimos 100 valores de uma simulação com 50.000 execuções são mostrados. A parte de baixo é a transformada de Fourier da saída x_n .



Fonte: Nascimento *et al.* (2018).

Sem saber qual base de medição usar, um ataque do tipo intercepta-reenvia é complicado para Eva. Ela pode tentar usar uma máquina Gaussiana de clonagem quântica.

Neste caso, a fidelidade ($1 \rightarrow 2$) é de $2/3$ para qualquer número médio de fótons do estado coerente copiado. Eva mantém um estado com ela e envia o outro para Bob. Nessas circunstâncias, as probabilidades de detecção em Bob são

$$p_0 \sim F \cos^2[\pi(z_k \oplus a + f(x_{n-1}, \xi, t) - f(y_{n-1}, \xi, t))/2] + (1 - F) \sin^2[\pi(z_k \oplus a + f(x_{n-1}, \xi, t) - f(y_{n-1}, \xi, t))/2], \quad (3.16)$$

$$p_1 \sim F \sin^2[\pi(z_k \oplus a + f(x_{n-1}, \xi, t) - f(y_{n-1}, \xi, t))/2] + (1 - F) \cos^2[\pi(z_k \oplus a + f(x_{n-1}, \xi, t) - f(y_{n-1}, \xi, t))/2]. \quad (3.17)$$

Simulando novamente o protocolo QCKD sob o ataque com máquina de clonagem quântica produz uma taxa de erro de $\sim 0,4$, denunciando o ataque.

4 PULSOS MULTIFÓTONS E ATAQUE POR TOMOGRAFIA QUÂNTICA EM DISTRIBUIÇÃO QUANTUM-CAÓTICA DE CHAVES COM MAPA LOGÍSTICO

A referência Oliveira e Ramos (2018) introduziu a QCKD em redes ópticas, como demonstrou o Capítulo 2 desta tese, além disso, várias diferenças entre QKD e QCKD foram apontadas. Este capítulo mostra que para um espião que se utiliza de um ataque de tomografia quântica com detecção homodina, o número médio de fótons usado por Alice no protocolo de QCKD pode ser muito maior que 0,1 sem comprometer a segurança da chave.

4.1 QCKD usando pulsos multifóton e mapa logístico

Para a QKD usando estados discretos, quanto maior o número de bases usadas, mais seguro é o protocolo. Entretanto, como Alice e Bob mantêm apenas as informações obtidas nos intervalos de tempo em que escolheram as mesmas bases, a taxa de transmissão de bits da chave diminui quando o número de bases aumenta (Bourennane; Karlsson; Björk, 2001).

O problema de aumentar a segurança através do aumento do número de estados quânticos usados sem que isso diminua a taxa de transmissão pode ser superado através do uso da QCKD (Qi *et al.*, 2016). Neste caso, embora as informações enviadas sejam discretas bits ('0' e '1'), o conjunto de estados quânticos que trafegam pelo canal é contínuo, o que aumenta a segurança. Além disso, a QCKD não necessita do procedimento de reconciliação de bases, consequentemente a taxa de transmissão da chave não diminui.

Se o número de diferentes estados quânticos usados para carregar a informação aumenta, uma pergunta surge imediatamente: A quantidade de fótons por estado quântico pode ser incrementada sem enfraquecer ou destruir a segurança do protocolo? Se um protocolo de QKD usa pulsos multifótons, a espiã pode usar duas estratégias de ataque: 1 - Se ela tiver uma memória quântica, ela pode pegar alguns fótons dos pulsos multifótons enviados por Alice e armazená-los na sua memória quântica. Depois do estágio de reconciliação de bases, Eva pode medir os fótons armazenados na base correta e obter a informação correta. 2 - Se Eva não tiver uma memória quântica, ela pode tentar pegar o máximo número de fótons do pulso multifótons sem perturbar as estatísticas de detecção de Bob e realizar medições neles. A partir dos dados medidos, Eva infere o estado quântico enviado por Alice.

Para a QCKD, ter uma memória quântica não é útil, uma vez que não há o estágio de reconciliação de bases. Consequentemente, resta para Eva a estratégia de pegar fótons e realizar medições neles a fim de conseguir inferir o estado enviado por Alice. Dessa forma, a

questão importante é: Quantos fótons Eva pode pegar e ainda assim não conseguir obter informações úteis sobre a chave? A fim de responder esta pergunta, mais adiante neste capítulo serão apresentadas as simulações numéricas de um protocolo de

QCKD usando mapa logístico e sua implementação com interferômetro de MachZehnder, assumindo que Eva usa um ataque por tomografia homodina. Diferentemente do que foi feito em Oliveira e Ramos (2018), visando simplificar o esquema óptico utilizado, aqui os sistemas não lineares usados são equações diferenciais não lineares sendo executadas em computadores. A QCKD usando mapas logísticos sincronizados foi discutida em (2). Sua dinâmica não linear é governada pelo conjunto de equações abaixo:

$$z_{k+1} = \delta z_k(1 - z_k), \quad (4.1)$$

$$x_{n+1} = \lambda x_n(1 - x_n) + c[k - \lambda(1 - x_n - d\bar{z}_{k+1})](x_n - d\bar{z}_{k+1}), \quad (4.2)$$

$$y_{n+1} = \lambda y_n(1 - y_n) + c[k - \lambda(1 - y_n - d\bar{z}_{k+1})](y_n - d\bar{z}_{k+1}), \quad (4.3)$$

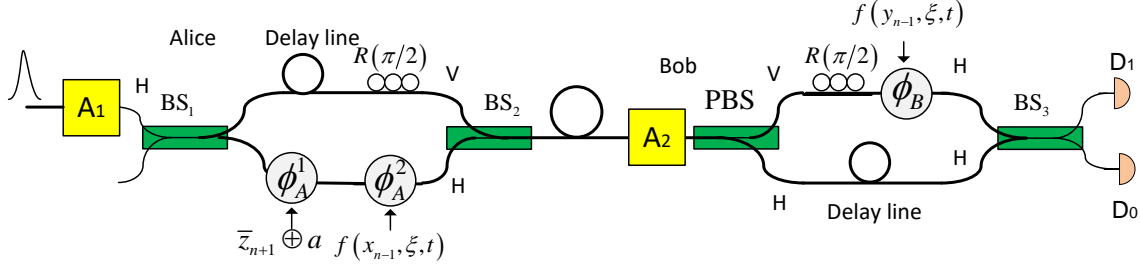
$$\begin{cases} \bar{z}_{k+1} = 0, \text{ se } z_{k+1} < 0.5 \\ \bar{z}_{k+1} = 1, \text{ se } z_{k+1} \geq 0.5 \end{cases} \quad (4.4)$$

Diferentemente do que fora discutido no Capítulo 3, aqui a variável z é a discretização do mapa logístico. Como se pode notar nas eqs. (4.1) - (4.4), novamente o sistema Z alimenta os sistemas X e Y com uma variável discreta, z_n , que assume apenas dois valores (0 e 1), e a variável d nas eqs. (4.2) e 4.3) controla a força de z_n .

Uma vez que os sistemas caóticos X e Y estejam sincronizados, uma chave comum pode ser estabelecida a partir da discretização das variáveis de saída x_n para Alice e y_n para Bob. Por exemplo, um valor de referência V_{ref} é escolhido. Se $x_n \geq V_{ref}$ ($y_n \geq V_{ref}$) um bit '1' é registrado por Alice (Bob), caso contrário um bit '0' é registrado. Se $x_n = y_n$, os bits da chave de Alice e Bob serão os mesmos. Note que, como x_n e y_n assumem valores contínuos entre 0 e 1, uma codificação m -ária também é possível implicando em uma taxa de transmissão mais alta, entretanto este não é objeto da discussão nesta tese.

A fim de implementar um sistema de QCKD usando mapa logístico e pulsos multifótons, um esquema óptico usando o interferômetro de Mach-Zehnder MZI é mostrado na Figura 13.

Figura 13 – Esquema óptico para QCKD usando pulsos multifótons com interferômetro Mach-Zehnder. A_1 e A_2 são atenuadores ópticos, D_0 e D_1 são detectores de fótons únicos, PBS é um divisor de feixe por polarização e H e V representam os modos horizontal e vertical.



Fonte: Elaborada pela autora.

O funcionamento do MZI visto na Figura 12 foi amplamente discutido na literatura (Gisin, 2002) e por isso ele não é objeto de explicação nesta tese. Os pontos principais do esquema da Figura 13 são:

1. O pulso de Alice no braço inferior tem sua fase modulada por ϕ_A^1 e ϕ_A^2 , de acordo com os valores $\bar{z}_{k+1} \oplus a$ e $f(x_{n-1}, \xi, t)$: $\phi_A^1 = \pi(\bar{z}_{k+1} \oplus a)$ e $\phi_A^2 = \pi f(x_{n-1}, \xi, t)$. Aqui a função f é o mapa logístico dado na eq. (4.2) para Alice e na eq. (4.3) para Bob. O valor de entrada f_0 é x_{n-1} e o valor de saída é f_t a equação logística sofre t iterações. Os parâmetros ξ e t são conhecidos somente por Alice e Bob (fazem parte do segredo que autentica o canal). Por fim, a é a paridade do i -ésimo dígito de f_t .
2. No lado de Bob, o pulso no braço superior sofre um deslocamento de fase dado $\phi_B = \pi f(y_{n-1}, \xi, t)$. Para Bob, o valor de entrada f_0 é y_{n-1} e o valor de saída é f_t .
3. Por causa do código de polarização, ambos os pulsos chegam ao BS_3 ao mesmo tempo, com a mesma polarização e a interferência acontecerá. Dependendo da diferença de fase aplicada por Alice e por Bob, o pulso de luz será guiado para o detector de fóton único (SPD) D_0 ou D_1 . As probabilidades de detecção em D_0 e D_1 são dadas por:

$$p_0 = (1 - \exp(-|\alpha_B|^2 \eta))(1 - p_d) \cos^2[\pi(\bar{z}_{k+1} \oplus a + f(x_{n-1}, \xi, t) - f(y_{n-1}, \xi, t))/2], \quad (4.5)$$

$$p_1 = (1 - \exp(-|\alpha_B|^2 \eta))(1 - p_d) \sin^2[\pi(\bar{z}_{k+1} \oplus a + f(x_{n-1}, \xi, t) - f(y_{n-1}, \xi, t))/2], \quad (4.6)$$

Nas eqs. (4.5) e (4.6), $|\alpha_B|^2$ é o número médio de fótons depois do atenuador A_2 , η é a eficiência quântica do detector e p_d é a probabilidade de contagem de escuro de D_0 e D_1 (consideradas iguais). Para Bob, detecção em D_0 implica $\bar{z}_{k+1} \oplus a = 0$ enquanto detecção em D_1 implica $\bar{z}_{k+1} \oplus a = 1$.

Como pode ser visto nas eqs. (4.5) e (4.6), a probabilidade de detecção depende do sincronismo e o sincronismo depende das probabilidades de detecção. A falta de sinais de sincronismo causará a falta de sincronismo dos mapas logísticos, resultando em alta taxa de erro. A fim de evitar tal problema, Alice e Bob devem atualizar os valores de x_n e y_n apenas quando Bob tiver detecção. Isto implica que, quando Bob não tiver detecção ele informará a Alice que atualizará z_{k+1} e calculará um novo valor para f usando $t + 1$, ao invés de t . consequentemente, cada pulso enviado por Alice terá um valor diferente de fase mesmo quando x_n não for atualizado. Bob fará o mesmo até obter detecção.

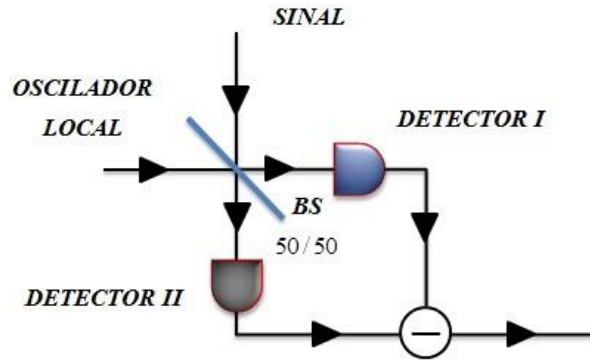
Se Alice envia um estado coerente para Bob com número médio de fóton $|\alpha|^2$, qual é o máximo valor seguro de $|\alpha|^2$ se $[\bar{z}_{n+1} \oplus a + f(x_{n-1}, \xi, t)]\pi$ é uma fase que varia de forma continua no intervalo $[0, 2\pi]$?

Como Eva não sabe a base de medição a ser utilizada, assume-se que ela pode realizar uma tomografia homodina do estado que sai de Alice (Nishioka *et al.*, 2002). Se a fidelidade da matriz densidade reconstruída, F , for menor do que 1, haverá um erro na fase estimada. Simulações numéricas mostram que um erro de 0,05 rad no valor da fase do estado coerente enviado por Alice causa um erro de cerca de 13% nos bits da chave, indicando a presença da espiã.

A fidelidade entre dois estados coerentes com o mesmo número médio de fótons (considera-se que Eva sabe o número médio de fótons usado por Alice), $\langle n \rangle$, é dada por $F = \exp\{-2\langle n \rangle[1 - \cos(\Delta)]\}$, onde Δ é a diferença entre os ângulos dos dois estados coerentes considerados. Usando $\Delta = 0,05 \text{ rad}$, a fidelidade é $F \approx 0,95$ quando $\langle n \rangle = 20$. Portanto, daqui em diante consideramos $F = 0,95$ como o valor máximo para a fidelidade permitida para Eva. Dessa forma, 20 é a resposta à pergunta inicial sobre o número médio de fótons por pulso que Alice pode enviar para Bob sem que Eva consiga obter informações úteis sobre a chave.

Surge então uma nova questão: Quantos estados coerentes com número médio de fótons $|\beta|^2$ são necessários a fim de obter uma boa estimativa da fase? Assume-se que Eva usa o esquema homodino mostrado na Figura 14.

Figura 14— Esquema homodino usando divisor de feixe balanceado e contadores de fótons D_1 e D_2 .



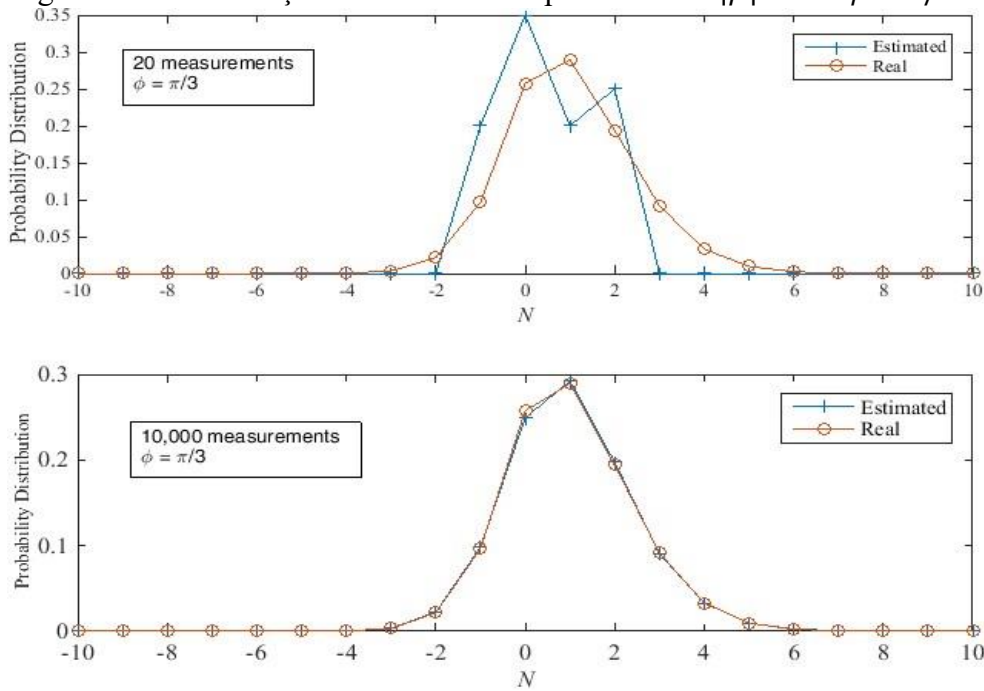
Fonte: Elaborada pela autora.

Na Figura 14, D_1 e D_2 são contadores de fótons. Eva divide o estado coerente enviado por Alice em r cópias com número médio de fótons $|\beta|^2$, $r = |\alpha|^2/|\beta|^2$, conseqüentemente, o estado sinal é $|\beta|e^{i\phi}$ onde ϕ é a fase total escolhida por Alice. O oscilador local usado por Eva é o estado coerente $|\beta|$ (com fase igual a 0 rad). A distribuição de probabilidade da diferença do número de fótons medidos por D_1 (n_1) e D_2 (n_2), $N = n_1 - n_2$, é dado pela distribuição de Skellam:

$$P_N = e^{-2|\beta|^2} |\tan(\phi)|^N I_N(2|\beta|^2 |\sin(2\phi)|). \quad (4.7)$$

Na eq. (4.7), I_N é a função de Bessel modificada de primeira ordem. Assim, se Eva medir a variável N um número r de vezes, ela pode ter uma estimativa para P_N e, usando esta estimativa e a eq. (4.7), ela obtém uma estimativa de ϕ . Como se pode notar, Eva não pode usar $|\beta|^2$ muito perto de zero uma vez que neste caso o ângulo ϕ perde a sua importância (para $\beta = 0$, $P_0 = 1$ para qualquer valor de ϕ). Uma boa estimativa de P_N vai requerer um grande valor de r . Sendo muito conservador, assume-se que Eva usa $|\beta|^2 = 1$ e que Alice usa $|\alpha|^2 = 20$, logo Eva poderia ter apenas $r = 20$ cópias para fazer sua estimativa de P_N . Usando uma simulação numérica, pode-se ver na Figura 4.3 abaixo as distribuições real eq. (4.7) - traço vermelho) e estimada (traço azul) de N para $r = 20$ (superior) e $r = 10.000$ (inferior) em que $|\beta| = 1$ e $\phi = \pi/3$.

Figura 15 – Distribuições real e estimada para N tendo $|\beta| = 1$ e $\phi = \pi/3$.



Fonte: Elaborada pela autora.

Como podemos ver na Figura 16, 20 medições não proverão dados suficientes para uma boa estimativa de P_N . A estimativa da fase obtida por $\min_{\phi} \sum_n [P_N(\phi) - \hat{P}_N]^2$, onde \hat{P}_N é a estimativa de P_N mostrada na Figura 16, são $\phi = 0,845801322478620 \text{ rad}$ para 20 medições e $\phi = 1,04059954682362 \text{ rad}$ para 10.000 medições ($\phi = \frac{\pi}{3} = 1,04719755119660 \text{ rad}$). Usando $|\beta|^2 = 2$ e $r = 10$, obtém-se $\phi = 0,593159 \text{ rad}$, enquanto usando $|\beta|^2 = 0,5$ e $r = 40$, obtém-se $\phi = 0,246024 \text{ rad}$.

Por outro lado, a fim de garantir que Bob terá detecção de fótons únicos, deve-se ter

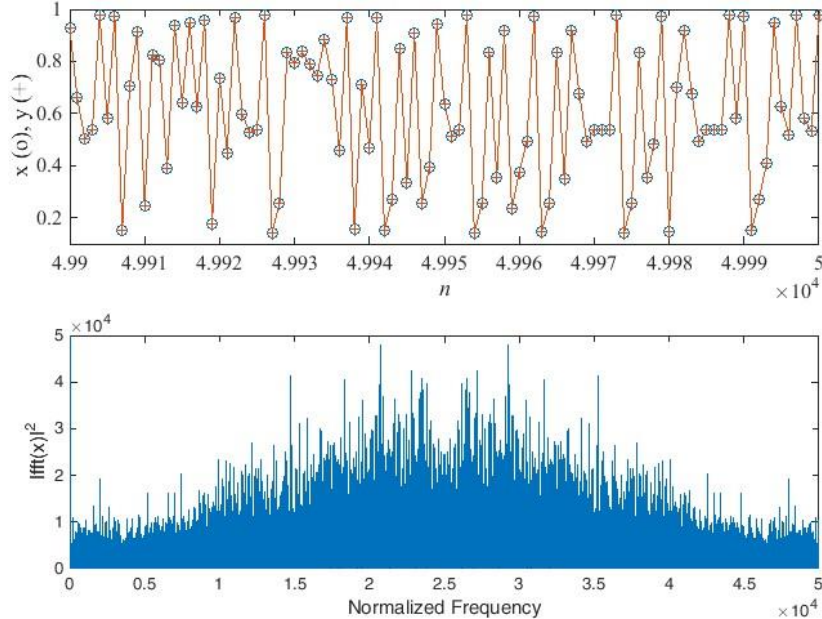
$$|\alpha_B|^2 = |\alpha|^2 10^{\frac{-(\sigma L + A_2)}{10}} = 0,1. \quad (4.8)$$

onde $\sigma = 0,27 \text{ dB/km}$ é o coeficiente de perda da fibra e L é o comprimento da fibra entre Alice e Bob. O comprimento máximo da fibra que obedece à eq. (4.8) é obtido quando $A_2 = 0$. Neste caso, tem-se $L_{max} = 85 \text{ km}$.

A Figura 16 mostra uma simulação de sincronização entre os sistemas não lineares de Alice e Bob para os seguintes parâmetros: $p_d = 0,15$, $L = 85 \text{ km}$, $|\alpha|^2 = 20$, $\sigma = 0,27 \text{ dB/km}$, $\delta = 4$, $\lambda = 3,9$, $k = 0,2$, $c = 0,5$, $d = 0,5$, enquanto os valores iniciais das variáveis dinâmicas são $x(1) = 0,7$, $y(1) = 0,7$, $z(1) = 0,2$. Para o mapa logístico f foi usado $\xi = 3,97$ e $t = 1000$. A parte de baixo da Figura 16 é a transformada de Fourier de x_n . Seu

comportamento contínuo reforça o caráter aleatório de x_n e vemos a perfeita sincronização dos sistemas de Alice $X(o)$ e de Bob $Y(+)$.

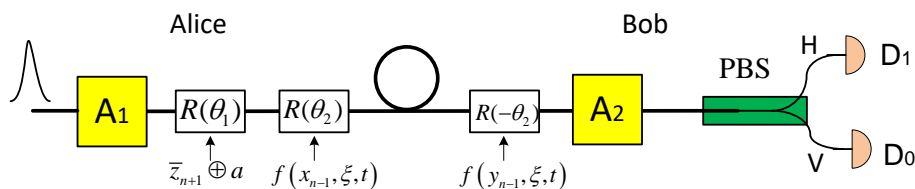
Figura 16 – Sincronização do sistema caótico (Xo) e $Y+$). Apenas os últimos 100 valores de uma simulação com 50.000 execuções são mostrados. Na parte inferior observa-se a transformada de Fourier da saída x_n .



Fonte: Elaborada pela autora.

É possível implementar o protocolo de QCKD aqui descrito usando um esquema óptico baseado na polarização da luz. Ele pode ser visto na Figura 17.

Figura 17 – Esquema óptico para QCKD usando polarização da luz. A_1 e A_2 são atenuadores ópticos, D_0 e D_1 são detectores de fótons únicos, R é um rotacionador de polarização, PBS é um divisor de feixe por polarização e H e V representam os modos horizontal e vertical.



Fonte: Elaborada pela autora.

Alice e Bob tem o mesmo sistema não linear descrito anteriormente. Inicialmente, o pulso de luz com polarização horizontal produzido por Alice é atenuado por A_1 a fim de ter $\langle n \rangle = 20$. Antes de deixar Alice, cada pulso óptico sofre rotações em $R(\theta_1)$ e $R(\theta_2)$ dado por $[\bar{z}_{n+1} \oplus a + f(x_{n-1}, \xi, t)]\pi/2$. Este pulso é enviado para Bob através de um canal óptico. Em

Bob, o pulso sofre outra rotação na sua polarização dada por $-f(y_{n-1}, \xi, t)\pi/2$. Após o rotacionador de polarização de Bob, o pulso óptico é atenuado por A_2 e passa por um divisor de feixe por polarização. Se $\bar{z}_{n+1} \oplus a = 1$, espera-se uma detecção na saída horizontal, caso contrário uma detecção na saída vertical é esperada. Novamente o atenuador A_2 é usado a fim de garantir que Bob terá detecção de fóton único. As probabilidades de detecção em D_0 e D_1 também são dadas por p_0 e p_1 , dados nas eqs. (4.5) e (4.6).

No esquema visto na Figura 17, como apenas polarização linear está sendo considerada, Eva pode tentar um ataque por máquina de clonagem quântica. Se ela tentar clonar o pulso de luz que está deixando Alice ($1 \rightarrow 2$), ela produz clones com fidelidade igual a $4/9$ (ela tem que clonar os modos horizontal e vertical e a fidelidade de estados coerentes depende do número médio de fótons). Este valor de fidelidade é muito menor do que o valor $F = 0.95$ considerado anteriormente, conseqüentemente, o ataque de Eva dessincronizará os sistemas caóticos causando alta taxa de erro.

Por outro lado, se Alice e Bob usarem sistemas caóticos de dimensões mais altas (como o sistema caótico de Lorenz), polarização elíptica pode ser utilizada e neste caso, ao invés de usar a máquina de clonagem quântica, Eva pode usar o ataque homodino.

A vida de Eva pode ser facilitada ainda mais se for considerado que ela sabe o número médio de fótons dos modos horizontal e vertical. A fim de determinar a polarização usada por Alice (e usar isto para tentar sincronizar seu próprio sistema caótico com os de Alice e Bob) ela ainda tem que estimar as fases dos modos horizontal e vertical e, como visto antes, usando $\langle n \rangle = 20$ ela não terá fótons suficientes para fazer uma boa estimativa.

5 USO DA FUNÇÃO DE LAMBERT-TSALLIS NA ANÁLISE DO IMPACTO DO ESPALHAMENTO RAMAN ESPONTÂNEO NA DISTRIBUIÇÃO QUÂNTICA DE CHAVES EM REDES ÓPTICAS PASSIVAS

A coexistência de dados quânticos e dados clássicos (sinal luminoso com alto número de fótons) é um requisito essencial para a integração de QKD em uma infraestrutura de telecomunicações já existente. Enquanto enlaces de fibra escura dedicadas permitem a transmissão de estados quânticos em longas distâncias, a presença de sinais clássicos em uma fibra (fibra viva) dificulta a recuperação de informações quânticas devido ao excesso de ruído gerado pelo espalhamento Raman espontâneo. Como uma contribuição à análise de sistemas de QKD integrados em redes ópticas clássicas, esse capítulo apresenta uma fórmula inédita para encontrar analiticamente o comprimento do canal quando a probabilidade de uma contagem no lado do receptor, sem que nenhum fóton incidente tenha vindo do transmissor, é conhecida a priori.

5.1 Coexistência da rede quântica com a rede de acesso clássica numa mesma rede óptica passiva

A QKD está estabelecida como uma tecnologia viável sobre fibras ópticas dedicadas (fibra escura), alcançando taxas de chave segura de mais de 1 Mbps em distâncias superiores a 250 km. Sendo as fibras escuras um recurso escasso e caro, há uma necessidade premente de permitir a coexistência de QKD e de sinais de dados na mesma fibra. O principal desafio para a coexistência de sinais clássicos e quânticos na mesma fibra é o grande contraste nas suas intensidades. Tipicamente, o sinal quântico contém menos que 0,5 fótons por pulso, aproximadamente, quando protocolos de estado isca com pulsos de laser fracos são implementados. Por outro lado, o sinal clássico de dados pode conter pelo menos 1 milhão de fótons por pulso, ou mais, para links com taxa de transmissão na faixa de giga bits por segundo (Patel, 2012).

Embora o sinal clássico possa ser facilmente filtrado usando multiplexação de comprimento de onda, fótons secundários, resultantes do efeito Raman e de outros efeitos não lineares, são impossíveis de rejeitar completamente por causa de sua sobreposição espectral com o sinal quântico. Colocar o sinal quântico espectralmente longe do canal de dados clássicos pode reduzir a sobreposição espectral, entretanto, em tais sistemas o canal quântico está frequentemente na banda de 1.310 nm, onde as perdas de transmissão são muito maiores, o que restringe ainda mais o comprimento do canal de QKD e a taxa de chave segura.

Os fótons resultantes do efeito Raman atingem o detector em momentos aleatórios em relação aos sinais quânticos pulsados regularmente e em Patel (2012) foi mostrado que essa aleatoriedade pode ser explorada para melhorar a relação sinal quântico para ruído Raman usando fotodiodos de avalanche de InGaAs de subnanossegundos para alcançar um aumento de dez vezes na relação sinal quântico/ruído Raman por meio de filtragem temporal, demonstrando assim QKD de alta taxa de bits em uma única fibra multiplexada com sinais de dados clássicos bidirecionais sem erros de 1 Gbps.

Pensando em configurações de rede de multiusuário, tem-se a Rede de Acesso Clássica (RAC) que é um tipo importante de rede de telecomunicações que conecta os usuários finais à infraestrutura de rede. Uma das formas mais típicas de RAC é a rede óptica passiva (do inglês, PON – *Passive Optical Network*), onde o sinal *downstream* do terminal de linha óptica (do inglês, OLT – *Optical Line Terminal*) na central é transmitido para todos os usuários por um divisor de potência, e o sinal *upstream* de apenas uma unidade de rede óptica (do inglês, ONU – *Optical Network Unit*) no nó do usuário é transmitida para OLT em cada *slot* de tempo.

Estrutura semelhante também pode ser usada para construir uma Rede Quântica de Acesso (RQA), que pode ser implementada em duas configurações: *downstream* receptor de fótons únicos nos nós do usuário; e *upstream* (transmissor de fótons únicos/luz coerente com baixo número médio de fótons nos nós do usuário). A RQA com conexões ponto-a-multiponto é uma abordagem prática para prover chaves seguras para múltiplos usuários e estender a escala da QKD, enquanto isso a inserção de sinais quânticos em fibras vivas (com a presença de sinal de dados clássicos) é um método viável para reduzir o custo do canal quântico e aumentar a escalabilidade da rede de QKD. Portanto, implementar uma RQA em uma PON fornece chaves seguras para a "última milha" e reduz bastante o custo dos recursos de fibra óptica.

O principal desafio na coexistência de RQA e PON é o ruído gerado pelo espalhamento Raman espontâneo (do inglês, SRS – *Spontaneous Raman Scattering*) dos sinais de dados (Wang, 2021). Os efeitos do ruído SRS são diferentes para as configurações *upstream* e *downstream*. Devido ao SRS de retorno, a configuração *upstream* sofre de maior ruído. Além disso, a implementação da RQA *upstream* é mais complicada, pois um receptor de QKD é alocado para todos os transmissores de QKD pela tecnologia de multiplexação por divisão de tempo.

Um método de realizar *upstream* é que diferentes transmissores de QKD emitam alternadamente pulsos para compartilhar a largura de banda do detector. No entanto, à medida que o número de usuários aumenta, a dificuldade na atribuição precisa de intervalos de tempo aumentará e a taxa de chave segura de cada usuário diminuirá significativamente. O outro

método é que apenas um transmissor QKD ocupa o detector em cada vez. No entanto, após alternar entre diferentes transmissores de QKD, o link do sistema QKD precisa ser restabelecido, o que aumenta o tempo total da sessão. A vantagem da RQA upstream é a economia, pois o receptor QKD com detectores de fótons únicos é relativamente caro, principalmente se detectores baseados em supercondutores forem utilizados. Comparado com a configuração upstream, a configuração downstream tem ainda menos ruído SRS, e a geração de chave segura de cada usuário não é influenciada por outros usuários, pois cada usuário detém detectores de fótons independentemente de outros usuários (Wang, 2021).

Assim, realizar links ponto-a-multiponto multiplexados depende criticamente de novas abordagens para superar a influência do ruído Raman e das perdas em divisores, aumentada em redes passivas que empregam divisores de potência para atender cada usuário. Numa rede de 128 usuários, os divisores adicionam, pelo menos, 21 dB de perda óptica extra ao canal quântico.

A integração da QKD em redes ópticas passivas gigabit (do inglês, GPON – *Gigabit Passive Optical Network*) é uma ideia atraente, pois nas redes GPON a espionagem é sempre possível na direção de *downstream*, uma vez que a transmissão de dados é feita para todos os usuários e, a princípio, qualquer usuário pode interceptar todo o tráfego downstream. A QKD permite fechar esta brecha de segurança, fornecendo as chaves de criptografia.

Em Fröhlich *et al.* (2021), foi demonstrado um método para integrar multiusuários de QKD numa rede GPON que suporta redes de larga escala. Foi mostrado que o ruído Raman normalmente restringe fortemente a capacidade alcançável da rede. Essa limitação foi superada com uma arquitetura com dupla fibra de alimentação, onde as chaves seguras podem ser transmitidas juntamente com sinais de dados GPON de potência total sem a necessidade de pós-processamento ou alinhamento de tempo, tornando-o compatível com esta tecnologia de rede de acesso óptico largamente utilizada. Esse método permite a operação de QKD com até 128 usuários em uma rede real, mantendo a vantagem de ter enlaces de fibra única na parte principal e multiusuário da rede.

5.2 Análise do impacto do espalhamento Raman espontâneo na QKD em redes ópticas passivas usando a função W_q de Lambert-Tsallis

Devido à enorme diferença da potência óptica usada pelos protocolos de comunicação quântica e clássica, a coexistência dos sinais quântico e clássico na mesma fibra óptica pode ser prejudicial para o protocolo quântico. Se houver amplificadores ópticos na rede

óptica, a QKD não pode ser realizada na janela de 1550 nm devido ao forte ruído decorrente da amplificação das emissões espontâneas nesta parte do espectro. Neste caso, a QKD pode ser realizada na janela de 1310 nm. No entanto, devido à alta perda da fibra neste comprimento de onda, a distância entre transmissor e receptor é muito limitada.

A fim de alcançar longas distâncias, a QKD deve ser executada no comprimento de 1550 nm e os dados clássicos em 1310 nm ou 1480 nm, por exemplo. Os dados clássicos e quânticos podem ambos ser colocados na janela de 1550 nm se uma fibra multinúcleos for usada, porém estas fibras ainda são caras e existe o acoplamento entre diferentes núcleos que deve ser considerado. Em todos os casos sem amplificadores ópticos, o problema mais importante é a contagem falsa gerada pelo espalhamento Raman espontâneo (Patel, 2012; Fröhlich, 2016; Cai; Sun, 2020).

O espalhamento Raman espontâneo aumenta a taxa de erro de bit quântica (QBER – *Quantum Bit Error Rate*) diminuindo a taxa de transmissão de bits seguros da chave. Assim, um projeto cuidadoso de redes ópticas que suportam serviços quânticos e clássicos deve considerar a geração de espalhamento Raman espontâneo.

Por outro lado, a função W_q de Lambert-Tsallis tem encontrado aplicações em várias áreas da engenharia e da física, provendo soluções analíticas a problemas cujas soluções são comumente encontradas usando simulações numéricas. A função W_q de Lambert-Tsallis é uma generalização da função W de Lambert que pode ser definida como a solução da equação:

$$W_q(z) e_q^{W_q(z)} = z. \quad (5.1)$$

Na equação eq. (5.1) $e_q(z)$ é a função q -exponencial de Tsallis que é dada por

$$e_q^z = \begin{cases} [1+(1-q)z]^{1/(1-q)} & q \neq 1 \text{ \& } 1+(1-q)z \geq 0 \\ 0 & q \neq 1 \text{ \& } 1+(1-q)z < 0 \end{cases}. \quad (5.2)$$

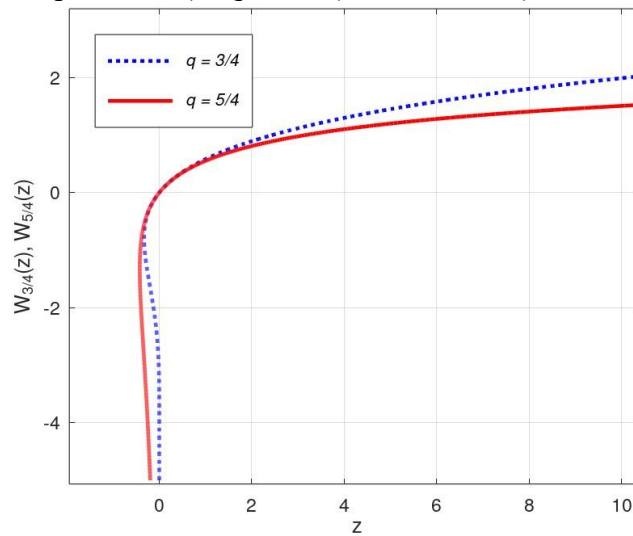
Pode-se notar que $\lim_{q \rightarrow 1} e_q^z = e^z$ e $\lim_{q \rightarrow 1} W_q(z) = W(z)$. Dois exemplos simples de $W_q(z)$ são obtidos quando $q = 2$ e $q = 3/2$:

$$W_2(z) = z/(z+1), \quad z > -1, \quad (5.3)$$

$$W_{3/2}^{\pm}(z) = \left[2(z+1) \pm 2\sqrt{2z+1} \right] / z, \quad z > -1/2, \quad (5.4)$$

Em geral, não é fácil encontrar uma expressão analítica para W_q , por isso um método numérico pode ser usado. A Figura 18 mostra as curvas de $W_q(z)$ versus z para $q = 3/4$ e $q = 5/4$.

Figura 18 – $W_q(z)$ versus z para $q = 3/4$ (linha pontilhada) e $q = 5/4$ (linha contínua).



Fonte: Elaborada pela autora.

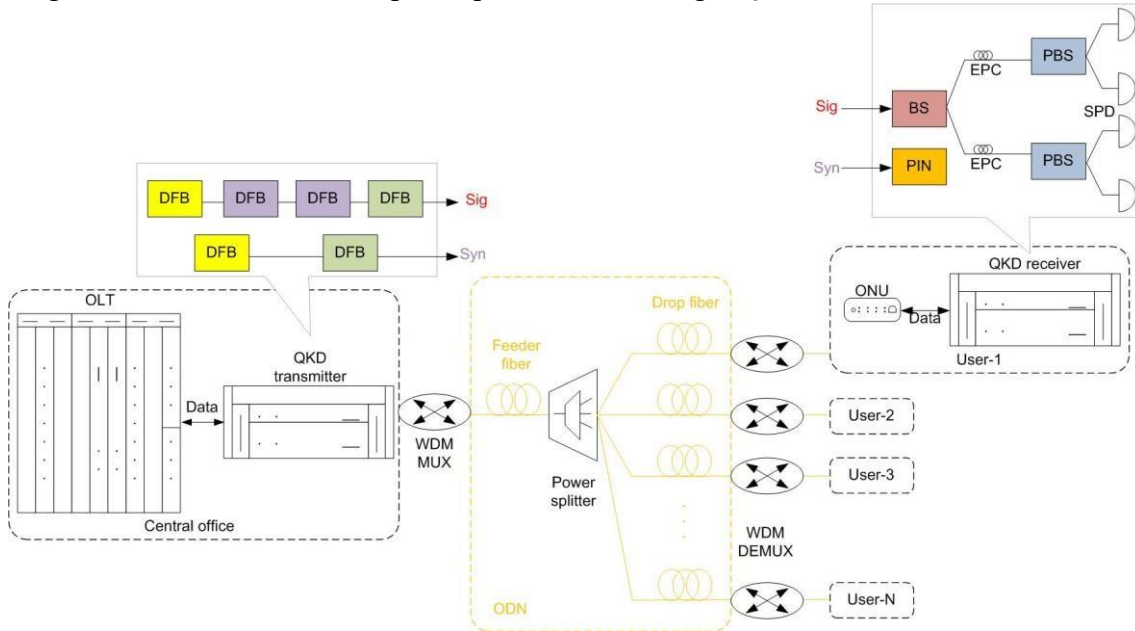
Considerando redes ópticas passivas (PON) como discutido em (Wang *et al.*, 2021, Fröhlich *et al.*, 2016), para a comunicação clássica, o sinal de descida (downstream) vindo do terminal de linha óptica (OLT) do ponto central é transmitido para todos os usuários por um divisor de potência e o sinal de subida (upstream) de cada uma das unidades de rede óptica (ONU) localizado no nó do usuário é transmitido para a OLT em cada time slot. Para uma rede quântica de acesso (RQA) usando estrutura PON, pode haver duas configurações:

- 1) downstream, onde o receptor de QKD está localizado nos nós dos usuários
- 2) upstream, onde o transmissor de QKD está localizado nos nós dos usuários

Uma vez que a configuração downstream tem menos ruído de espalhamento Raman espontâneo do que a configuração upstream e a taxa de geração de chave segura não depende do número de usuários, este capítulo trata apenas da configuração downstream, considerando uma configuração 1 x N, ou seja, uma OLT com um transmissor de QKD e N ONU's cada uma com um receptor QKD. Entre a OLT e a ONU existe a fibra de alimentação com comprimento

L_F , um divisor de potência passivo $1 \times N$ single feeder e as fibras de descida com comprimento $L_D \ll L_F$. O esquema é mostrado na Figura 19.

Figura 19 – QKD em redes ópticas passivas na configuração de downstream.



Fonte: Elaborada pela autora.

No esquema da Figura 18 apresentamos uma configuração downstream onde temos o ‘Central office’ onde estão a OLT com o transmissor QKD, a ODN onde fica o divisor de potência passivo ‘Power splitter’ e as fibras de alimentação ‘Feeder fiber’ e de descida ‘Drop fiber’ e N ‘Users’ onde está a ONU e o receptor QKD).

Assim como em Wang (2021), considera-se que os fótons gerados pelo ruído do espalhamento Raman espontâneo são principalmente gerados pelo sinal da OLT. Além disso, os dados clássicos são transmitidos em 1310 nm e 1480 nm, enquanto os dados quânticos são transmitidos em 1550 nm. O sinal da OLT gera fótons de ruído de espalhamento Raman espontâneo tanto na fibra de alimentação S_F quanto na fibra de descida S_D . Os valores de S_F e S_D são dados por

$$S_F = \left\{ P\beta / \left[N(\alpha_q - \alpha_c) \right] \right\} \left(e^{-\alpha_c L_F} - e^{-\alpha_q L_F} \right) e^{-\alpha_q L_D} \quad (5.5)$$

$$S_D = \left\{ P\beta / \left[N(\alpha_q - \alpha_c) \right] \right\} \left(e^{-\alpha_c L_D} - e^{-\alpha_q L_D} \right) e^{-\alpha_c L_F}, \quad (5.6)$$

onde P é a potência de lançamento do sinal da OLT, N é a taxa de divisão do divisor de potência, β é o coeficiente de espalhamento Raman espontâneo, α_c α_q é a perda da fibra no comprimento

de onda dos dados clássicos quânticos. Foi considerado o protocolo de QKD BB84 com dois estados-isca. A taxa de transmissão de bit seguros da chave do protocolo de QKD é limitada por

$$R = q \left\{ Q_1 [1 - H_2(e_1)] - f_{ec} Q_\mu H_2(e_\mu) \right\}, \quad (5.7)$$

na qual $q = 1/2$ para o protocolo BB84, f_{ec} é a eficiência de correção de erro, $H_2(x) = (-x \log_2 x) - (1-x) \log_2(1-x)$, Q_μ e e_μ são o ganho geral e o QBER dos sinais estado do fóton único. Assumindo o sinal de QKD com número médio de fótons μ e dois estados isca com número médio de fótons ($v < u$) e 0, a equação (5.7) é calculada usando (Ramos; Souza, 2000; Bourennane; Karlsson; Björk, 2001):

$$Q_{\mu(v)} = 1 - (1 - Y_0) \exp\left(-\mu(v) \eta_B e^{-\alpha_q L - 10 \log_{10}(N)}\right) \quad (5.8)$$

$$e_{\mu(v)} = e_d + [(1/2 - e_d) Y_0] / Q_{\mu(v)} \quad (5.9)$$

$$Q_1 = \frac{\mu^2 e^{-\mu}}{\mu v - v^2} \left(Q_v e^v - Q_\mu e^\mu \frac{v^2}{\mu^2} - \frac{\mu^2 - v^2}{\mu^2} Y_0 \right) \quad (5.10)$$

$$e_1 = (e_v Q_v e^v - 0.5 Y_0) / (Y_1 v) \quad (5.11)$$

$$Y_1 = \frac{\mu}{\mu v - v^2} \left(Q_v e^v - Q_\mu e^\mu \frac{v^2}{\mu^2} - \frac{\mu^2 - v^2}{\mu^2} Y_0 \right) \quad (5.12)$$

$$Y_0 = 2 p_{dark} + p_R(L). \quad (5.13)$$

Em (5.8) e (5.9) o comprimento do canal é igual a L e η_B é a eficiência quântica dos detectores de fóton único, e_d representa o erro de desalinhamento, a visibilidade não unitária do interferômetro e a modulação imperfeita, p_{dark} é a taxa de contagem de escuro dos detectores de fóton único e $p_R L$ é o ruído de fóton causado pelo espalhamento Raman espontâneo na fibra óptica dado por

$$p_R(L) = \left\{ [S_F(L) + S_D(L)] \Delta f \Delta t \eta_B \right\} / (hf). \quad (5.14)$$

Em (5.14) h é a constante de Planck, f é a frequência do canal quântico, Δf é a largura de banda de recepção do canal quântico e Δt é a largura da janela de gatilho efetiva do detector. Começando com um valor para p_R , usa-se (5.14) a fim de obter o valor de $S_F + S_D$. O

valor de $S_F + S_D$, por sua vez é usado em (5.5)+(5.6). Por fim, o comprimento do canal, $L = L_D + L_F$, é obtido usando a função W_q de Lambert-Tsallis para inverter (5.5)+(5.6). O resultado é ($\alpha_q < \alpha_c$):

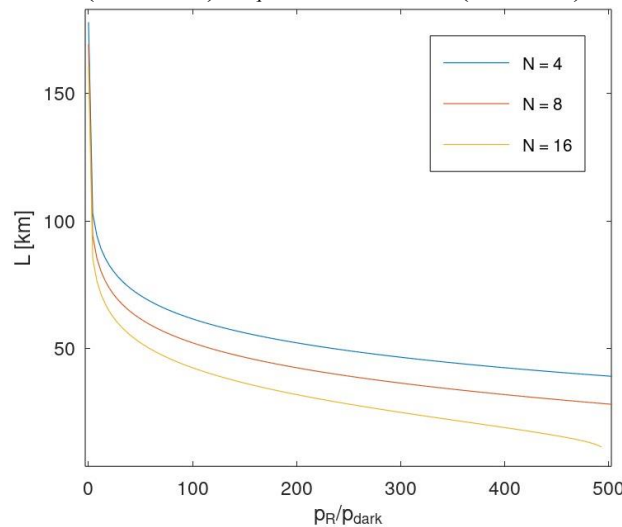
$$L = \frac{1}{\alpha_q - \alpha_c} \ln \left(\frac{\alpha_q}{\alpha_q - \alpha_c} W_{1 - \frac{\alpha_q}{\alpha_c - \alpha_q}} \left[\frac{\alpha_q - \alpha_c}{\alpha_q} (-z)^{\frac{\alpha_c - \alpha_q}{\alpha_q}} \right] \right) \quad (5.15)$$

$$z = \frac{N(S_F + S_D)(\alpha_q - \alpha_c)}{P\beta} = \frac{N h f p_R (\alpha_q - \alpha_c)}{\Delta f \Delta t \eta_B P \beta}. \quad (5.16)$$

Nas simulações realizadas foram usados $\alpha_c = 0,48$ dB/km (1310 nm) e $\alpha_c = 0,38$ dB/km (1480 nm), $\alpha_q = 0,35$ dB/km (1550 nm), $\eta_B = 0,15$, $P = 0,5$ mW, $N = \{4,8,16\}$ h_f é a energia do fóton em 1550 nm, $p_{dark} = 2 * 10^{-7}$, $\Delta t = 1$ ns, $\Delta f = 100$ GHz, $f_{ec} = 1,2$, $\mu = 0,4$, $\nu = 0,1$, $e_d = 0,02$ e $\beta = 7 * 10^{-9}$ nm⁻¹. A perda de inserção dos divisores de potência são 6,2 dB, 9,2 dB, 12,7 dB para 1×4 , 1×8 , 1×16 , respectivamente. O “*afterpulsing*” não foi considerado.

Como pode ser observado em (5.5) e (5.6), para uma potência de entrada fixa, quanto maior o comprimento da fibra menor o valor de $S_D + S_F$, portanto o valor p_R decresce à medida que o comprimento da fibra aumenta (como podemos ver na Figura 5.3 e 5.6. Além disso, quanto menor o valor de N , menor o argumento da função logarítmica em (5.15) e, portanto, maior o valor de L . Esse comportamento pode ser visto nas Figura 5.3 (1310 nm) e 5.6 (1480 nm) que mostram as curvas L versus p_R para $p_R \in [p_{dark}, 500p_{dark}]$.

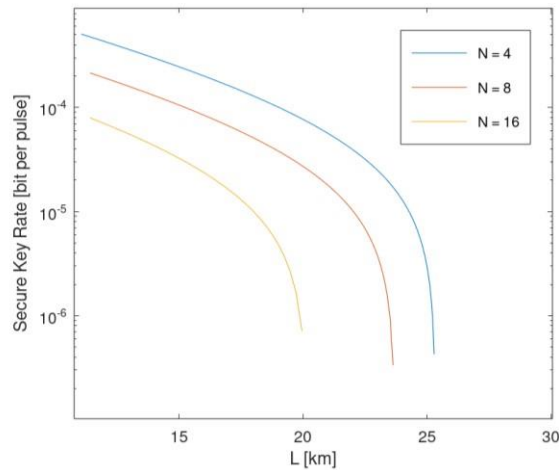
Figura 20 – p_R versus L . $\alpha_c = 0.48$ dB/km (1310 nm), $\alpha_q = 0.35$ dB/km (1550nm)



Fonte: Elaborada pela autora.

Nas Figuras 21 (1310 nm) e 23 (1480 nm) podem-se ver as curvas para a taxa de segurança da chave versus o comprimento do canal obtido de (5.15) e (5.16). É possível perceber que a taxa de chave segura é maior quando há menos usuários na rede para um mesmo comprimento de fibra.

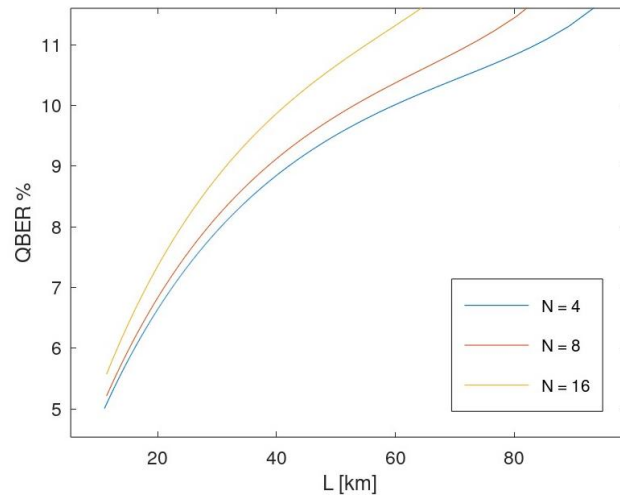
Figura 21 – R versus L . $\alpha_c = 0.48$ dB/km (1310 nm), $\alpha_q = 0.35$ dB/km (1550nm)



Fonte: Elaborada pela autora.

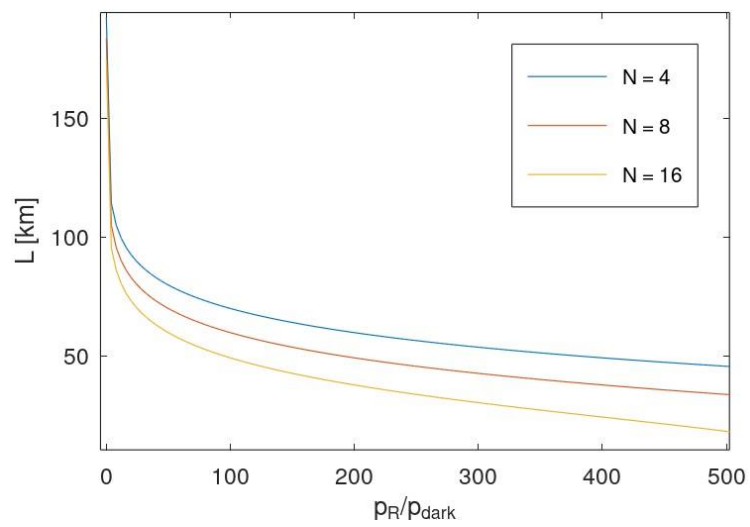
Para um valor dado de p_R , o comprimento da fibra diminui e a perda de inserção do divisor de potência cresce quando N aumenta, portanto, a taxa R é maior para os valores de N que minimizam $[\alpha_q L(N) + 10 \log_{10}(N)]$. A fim de ter alta taxa de transmissão de bits seguros da chave, enlaces curtos são necessários, entretanto, neste caso o espalhamento Raman espontâneo cresce, fazendo crescer o QBER e diminuindo a taxa de chave segura. O resultado desta disputa pode ser visto nas Figuras 21 (1310 nm) e 23 (1480 nm), onde o QBER aumenta quando N aumenta.

Figura 22 – $QBER$ versus L . $\alpha_c = 0.48$ dB/km (1310 nm), $\alpha_q = 0.35$ dB/km (1550nm)



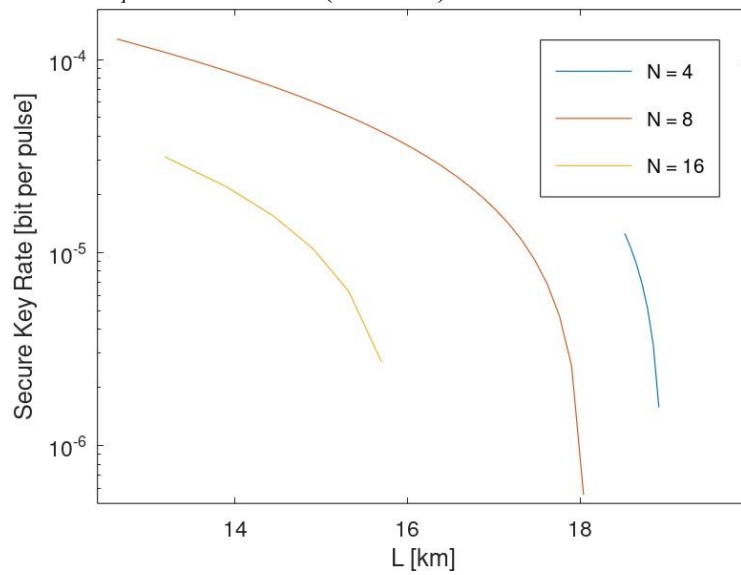
Fonte: Elaborada pela autora.

Figura 23 – L versus p_R . $\alpha_c = 0.38$ dB/km (1480 nm), $\alpha_q = 0.35$ dB/km (1550nm)



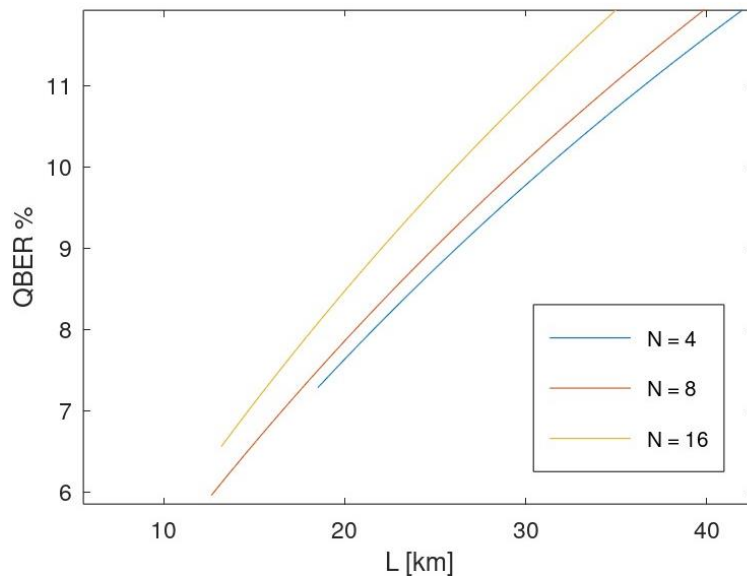
Fonte: Elaborada pela autora.

Figura 24 – R versus L . $\alpha_c = 0.38$ dB/km (1480 nm),
 $\alpha_q = 0.35$ dB/km (1550nm)



Fonte: Elaborada pela autora.

Figura 25 – QBER versus L . $\alpha_c = 0.38$ dB/km
(1480 nm), $\alpha_q = 0.35$ dB/km (1550nm).



Fonte: Elaborada pela autora.

6 CONCLUSÕES E PERSPECTIVAS DE TRABALHOS FUTUROS

6.1 Conclusões

Para o propósito de obter maiores taxas de transmissão de chaves mantendo a segurança do sistema, a QCKD apresenta-se como uma solução, pois ela oferece a vantagem de poder aumentar o número de médio de fótons por pulso mantendo a segurança da chave. Em particular, a correlação entre símbolos, comum na criptografia caótica clássica, é significativamente reduzida quando as probabilidades da mecânica quântica são incluídas. Isto acontece porque os sistemas não lineares determinísticos usados na criptografia caótica são transformados em sistemas não lineares estocásticos na QCKD. Isto permite concluir que os protocolos de QCKD estão longe de apresentar os problemas observados em várias propostas de criptografia caótica e pode estar perto da máxima segurança oferecida pelos esquemas de criptografia quântica ideal.

No que diz respeito à nova configuração óptica proposta no Capítulo 3 para realizar QCKD, tem-se:

- 1) Os sistemas não lineares usados são mapas logísticos programados em computadores. Isto simplifica o esquema óptico requerido para QCKD, entretanto, várias outras equações discretas não lineares com propriedades de criptografia melhores podem ser usadas ao invés do mapa logístico equações discretas não lineares com um número maior de parâmetros fornecem mais segurança, uma vez que a espiã terá que adivinhar mais valores de parâmetros.
- 2) O conjunto de estados coerentes viajando no canal é contínuo, uma vez que x_n é uma variável contínua no intervalo $(0, 1)$.
- 3) A informação da chave não é carregada pelos estados quânticos. Estes são responsáveis pela sincronização dos mapas logísticos de Alice e Bob. Os bits da chave dependem da dinâmica caótica das variáveis x_n e y_n e são obtidos através da discretização de $(x_n \text{ Alice})$ e $(y_n \text{ Bob})$.
- 4) Não há estágio de reconciliação de base.
- 5) A segurança é garantida pelas propriedades quânticas e caóticas. A espiã pode atacar o sinal de sincronização, entretanto uma vez que estados coerentes atenuados são usados e a fase é uma variável contínua, ela não pode usar esta informação para tentar reconstruir o comportamento caótico das equações discretas de Alice e Bob.

Em outras palavras, o teorema da não clonagem e o parâmetro de erro de incompatibilidade Eva não conhece os valores dos parâmetros usados por Alice e Bob) impedem Eva de ter um mapa logístico sincronizado com os mapas de Alice e de Bob. Sendo incapaz de ser sincronizado com Alice e Bob, Eva não pode obter os bits corretos da chave final.

O Capítulo 4 mostrou que, desde que a QCKD use estados coerentes com fase contínua e que não exista estágio de reconciliação de bases, Alice pode usar estados coerentes com o número médio de fótons igual a 20 muito maior do que 0,1 – o valor tradicionalmente usado nos esquemas de (QKD). Isto é possível porque um erro de 0,05 rad na estimação da fase do estado coerente enviado por Alice indica a presença da espiã no canal, considerando $F \approx 0,95$ o máximo valor para a fidelidade permitida para Eva.

Com um número médio de 20 fótons/pulso ainda não é possível para Eva conseguir uma boa estimativa do estado enviado por Alice, pois ela não sabe qual base de medição usar e por isso realiza um ataque por tomografia homodina.

A QCKD requer que Alice e Bob compartilhem antecipadamente os mesmos dados dos seus sistemas não lineares parâmetros e valores iniciais. Entretanto, neste caso, poder-se-ia imaginar que desde que Alice e Bob compartilhassem os mesmos parâmetros e valores iniciais, seus sistemas não lineares estariam sempre sincronizados e por isso não seria necessário a comunicação quântica entre eles. Isto é verdade, mas sem a comunicação quântica a dinâmica dos sistemas seria determinística, e isso enfraqueceria o esquema criptográfico usado.

A detecção de fóton único em Bob introduz um ruído aleatório nos sistemas não lineares fazendo suas dinâmicas não linear e estocástica mas ainda sincronizadas. Além do mais, também é possível trocar o sistema não linear Z por um gerador de bits aleatórios verdadeiro e aumentar ainda mais a imprevisibilidade dos sistemas não lineares usados por Alice e Bob.

É preciso ratificar ainda que se Eva medir o valor correto para $\phi = \phi_A^1 + \phi_A^2$, ela poderia usar um ataque de força bruta, escolher valores para ξ e t a fim de determinar os valores para x_{n-1} , o que implicaria no conhecimento dos bits da chave. Consequentemente, pulsos “clássicos” devem ser evitados por Alice.

No Capítulo 5 a função W_q de Lambert-Tsallis foi utilizada para se obter de forma analítica o comprimento do canal óptico a partir da predefinição de um valor para o ruído nos detectores do receptor causado pelo espalhamento Raman espontâneo na fibra óptica. Portanto, um engenheiro que esteja projetando uma rede quântica pode usar a fórmula apresentada neste capítulo para determinar o alcance da rede de acesso quântica quando a probabilidade de uma

contagem no lado do receptor sem que nenhum fóton incidente tenha vindo do transmissor for conhecida a priori.

6.2 Perspectivas de trabalhos futuros

De modo a dar continuidade aos estudos apresentados nesta tese sobre QCKD, um dos trabalhos que podem ser feitos é implementar o esquema óptico de QCKD proposto no Capítulo 3. Uma outra possibilidade é usar equações discretas não lineares com maior número de parâmetros para realizar a QCKD proposta no Capítulo 3 e analisar o coeficiente de correlação para verificar o sigilo da chave em uma QCKD.

Além dessas, ainda é possível implementar o esquema óptico de QCKD usando pulsos multifótons proposto no Capítulo 4 (Figura 12) e implementar o esquema óptico de QCKD usando polarização da luz proposto no Capítulo 4 (Figura 16).

REFERÊNCIAS

- BENNETT, C. H.; BRASSARD, G. Quantum Cryptography: Public key distribution and coin tossing. **Theoretical Computer Science**, [S.l.], v. 560, pp. 7-11, 2014. Disponível em: <https://arxiv.org/abs/2003.06557>. Acesso em: 13 out. 2020.
- BENNETT, C. H. Quantum cryptography using any two nonorthogonal states. **Physical Review Letters**, [S.l.], v. 68, n. 21, p. 3121 – 2124, 1992. Disponível em: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.68.3121>. Acesso em: 19 jun. 2021.
- BETH, T.; LAZIC, D. E.; MATHIAS, A. Cryptanalysis of cryptosystems based on remote chaos replication. *In: Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1994. pp. 318–331.
- BRASSARD, G. **Brief History of Quantum Cryptography**: a personal perspective. Montreal: Universidade de Montreal, 2005. Disponível em: <https://arxiv.org/pdf/quant-ph/0604072.pdf>. Acesso em: 05 jan. 2020.
- CAI, C.; SUN, Y. Intercore spontaneous Raman scattering impact on quantum key distribution in multicore fiber. **New Journal of Physics**, [S.l.], v. 22, n. 08, p. 1-13, 2020. Disponível em: <https://doi.org/10.1088/1367-2630/aba023>. Acesso em: 12 maio 2021.
- EDWARDS, A.W.F. The meaning of binomial distribution. **Nature**, [S.l.], v. 186, p. 1074, 1960. Disponível em: <https://www.scirp.org/reference/referencespapers?referenceid=1043673>. Acesso em: 12 out. 2021.
- EKERT, A. K. Quantum cryptography based on Bell’s theorem. **Physical Review Letters**, [S.l.], v. 67, n. 6, ago. 1991. Disponível em: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.67.661>. Acesso em: 18 jun. 2021.
- FRÖHLICH, B. *et al.* Quantum secured gigabit optical access networks, **Scientific Reports**, [S.l.], v. 5, n. 18, 2016. Disponível em: <https://doi.org/10.1038/srep18121>. Acesso em: 13 jun. 2021.
- GOEDGEBUER, J. P.; LARGER, L.; PORTE, H. Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode, **Physical Review Letters**, [S.l.], v. 80, n. 10, jun. 1998. Disponível em: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.80.2249>. Acesso em: 25 jul. 2021.
- KARTALOPOULOS, S. V. Chaotic quantum cryptography. *In: Fourth International Conference on Information Assurance and Security*, 2008.
- KOCAREV, L.; PARLITZ, U. General approach for chaotic synchronization with applications to communications, **Physical Review Letters**, [S.l.], v. 74, n. 25, pp. 5028– 5031, jun. 1995. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/10058665/>. Acesso em: 7 jul. 2021.
- LI, C. Cracking a hierarchical chaotic image encryption algorithm based on permutation. **Signal Process.**, [S.l.], v. 118, p. 203–210, 2016. Disponível em: <https://arxiv.org/abs/1505.00335>. Acesso em: 12 abr. 2021.

LO, H. K.; ZHAO, Y. Quantum Cryptography. **Encyclopedia of Complexity and Systems Science**, Springer New York, v. 8, p. 7265-7289, 2009. Disponível em: https://link.springer.com/referenceworkentry/10.1007/978-0-387-30440-3_432. Acesso em: 19 out. 2021.

LO, H.-K.; ZHAO, Y. Quantum cryptography. **Comput. Complex.**, [S.l.], v. 64, p. 2453, 2012. Disponível em: <https://arxiv.org/abs/0803.2507>. Acesso em: 11 set. 2021.

MA, X.; QI, B.; ZHAO, Y.; LO, H. Practical decoy state for quantum key distribution, **Physical Review A**, [S.l.], v. 72, jul. 2005. DOI:10.1103/PhysRevA.72.012326. Disponível em: <https://journals.aps.org/pr/abstract/10.1103/PhysRevA.72.012326>. Acesso em: 10 jun. 2021.

MENDONÇA, F. A. **Análise Teórica e Resultados Experimentais de Sistemas de Distribuição Quântica de Chaves Usando Fótons Isolados e Estados Coerentes Mesoscópicos**. 2006. 96 f. Dissertação (Mestrado em Engenharia de Teleinformática) – Departamento de Engenharia de Teleinformática, Universidade Federal do Ceará, Ceará, 2006.

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. **Appl. Phys. Lett.**, [S.l.], v. 91, 2007. Disponível em: <https://ui.adsabs.harvard.edu/abs/2007ApPhL..91a1112N/abstract>. Acesso em: 18 maio 2021.

NASCIMENTO, J. C.; DAMASCENO, R. L. C.; DE OLIVEIRA, G. L.; RAMOS, R. V. Quantum-chaotic key distribution in optical networks: from secrecy to implementation with logistic map. **Quantum Information Processing**, [S.l.], v. 17, n. 329, 2018. Disponível em: <https://doi.org/10.1007/s11128-018-2097-1>. Acesso em: 18 jun. 2021.

NISHIOKA, T.; ISHIZUKA, H.; HASEGAWA, T.; ABE, J. Circular type quantum key distribution. **J. IEEE Photonics Technol. Lett.**, [S.l.], v. 144, p. 576–578, 2002. Disponível em: <https://arxiv.org/abs/quant-ph/0106083>. Acesso em 17 dez. 2020.

OLIVEIRA, G. L. **Distribuição Quantum-Caótica de Chaves Usando Osciladores Optoeletrônicos**. 2018. 116 f. Tese (Doutorado em Engenharia de Teleinformática). – Departamento de Engenharia de Teleinformática, Universidade Federal do Ceará, Ceará, 2018.

OLIVEIRA, G. L.; RAMOS, R. V. Quantum-chaotic cryptography. **Quantum Inf. Process.**, [S.l.], v. 17, n. 40, 2018. Disponível em: <https://doi.org/10.1007/s11128-017-1765-x>. Acesso em: 11 maio 2020.

OTT, E.; GREBOGI, C.; YORKE, J. A. Controlling chaos, **Physical Review Letters**, [S.l.], v. 64, n. 11, pp. 1196–1199, mar. 1990. Disponível em: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.64.1196>. Acesso em: 18 jun. 2021.

PATEL, K. A. C. *et al.* Coexistence of high-bit-rate quantum key distribution and data on optical fiber. **Physical Review X**, [S.l.], v. 2, 2012. DOI: 10.1103/PhysRevX.2.041010. Disponível em: <https://journals.aps.org/prx/abstract/10.1103/PhysRevX.2.041010>. Acesso em: 18 fev. 2021.

PECORA, L. M.; CARROLL, T. L. Synchronization in chaotic systems, **Physical Review Letters**, [S.l.], v. 64, n. 8, pp. 821–824, nov. 1990. Disponível em: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.64.821>. Acesso em: 19 jun. 2020.

PEREZ, G.; CERDEIRA, H. Extracting messages masked by chaos, **Physical Review Letters**, [S.l.], v. 74, n. 11, pp. 1970–1973, 1995. Disponível em: <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.74.1970>. Acesso em: 10 out. 2020.

QI, B.; HUANG, L.-L.; LO, H.-K.; QIAN, L. Polarization insensitive phase modulator for quantum cryptosystems. **Opt. Express.**, [S.l.], v. 14, n. 10, p. 4264–4269, 2006. Disponível em: https://www.researchgate.net/publication/26282718_Polarization_insensitive_phase_modulator_for_quantum_cryptosystems. Acesso em: 19 maio 2020.

VAN WIGGEREN, G.; ROY, R. Communicating with chaotic lasers, **Science**, [S.l.], v. 279, n. 3, pp. 1198–1200, fev. 1998. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/10058665/>. Acesso em: 17 jun. 2021.

WANG, B. *et al.* **Practical quantum access network over a 10 Gbit/s ethernet passive optical network**. 2021. Disponível em: [arXiv:2110.14126v1](https://arxiv.org/abs/2110.14126v1). Acesso em: 13 mar. 2021.

WU, B.; SHASTRI, B. J.; PRUCNAL, P. R. Chapter 11 – Secure Communication in Fiber-Optic Networks. *In*: KAUFMANN, M. **Emerging Trends in ICT Security**, [S.l.]: Babak Akhgar and Hamid R. Arabnia, 2013. p. 173 – 183.

APÊNDICE A – CAOS

A Teoria do Caos é um campo da ciência que surgiu apenas nos 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” (Marietto; Sanches; Meireles, 2011; Martins, 2016).

A1. Introdução

Para Katz (2010), 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 (Marietto; Sanches; Meireles, 2011).

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 (Marietto; Sanches; Meireles, 2011).

A não linearidade está relacionada à estrutura matemática utilizada para representar o comportamento do sistema real (Marietto; Sanches; Meireles, 2011). 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 prever o comportamento de um sistema real. Em um sistema pouco complexo pode-se prever 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 sensível às condições iniciais. O comportamento caótico não está relacionado com as influências de fatores externos, mas tem origem interna ao próprio sistema (Marietto; Sanches; Meireles, 2011).

A2. Caos em Sistemas Determinísticos Não Lineares

O estudo do caos em sistemas determinísticos não lineares tornou-se relevante nas recentes décadas (Martins, 2016). Sistemas simples e modelados por equações determinísticas podem ter comportamento imprevisível em determinadas 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 (Nussenzveig, 1991), 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" (Savi, 2006). 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* (Stewart, 1991). Lorenz trabalhava com modelos para a previsão do tempo e, como conta (Gleick, 1987), 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 nas Equações (EQ A.1 – A.3) as equações diferenciais que Lorenz utilizou para descrever seu problema:

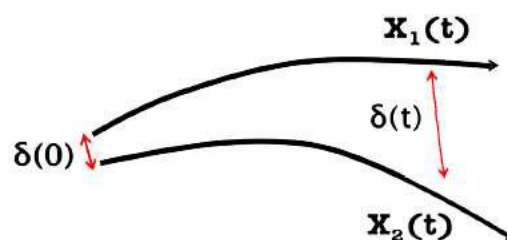
$$\dot{x} = \sigma(y - x). \quad \text{EQ A.1}$$

$$\dot{y} = rx - y - xz. \quad \text{EO A.2}$$

$$\dot{z} = xy - bz. \quad \text{EO A.3}$$

Um sistema caótico tem como característica ser altamente sensível às condições iniciais. Essa sensibilidade pode ser medida através do expoente de Lyapunov. Se duas trajetórias do mapa de Lorenz são próximas, devido às condições iniciais muito próximas, elas se afastarão 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 Figura A1.

Figura A.1 – Evolução de duas condições iniciais próximas



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 (Santos, 2007):

$$|\delta(t)| \approx |\delta(0)|e^{\lambda t}. \quad \text{EQ A.4}$$

Se o expoente de Lyapunov $\lambda < 0$, a distância entre os pontos x_1 e x_2 diminui exponencialmente, mas 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 comportamento caótico (Onias, 2012; Strogatz, 2014).

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 de três dimensões. O teorema de Poincaré Bendixson limita as possibilidades da dinâmica e impossibilita a existência do caos em duas dimensões (Onias, 2012). 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 (Strogatz, 2014).

A3. 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 (Santos, 2007).

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 Santos (2007), 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:

$$x_{n+1} = ax_n. \quad \text{EQ A.5}$$

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

$$x_n = a^n x_0. \quad \text{EQ A.6}$$

Analisando a Equação (EQ A.6) 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 (Martins, 2016):

$$x_{n+1} = ax_n(1 - x_n). \quad \text{EQ A.7}$$

Na Equação (EQ A.7), 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 $-\infty$, 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 $-\infty$, e nos dois casos acontecerá a extinção (Santos, 2007).

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:

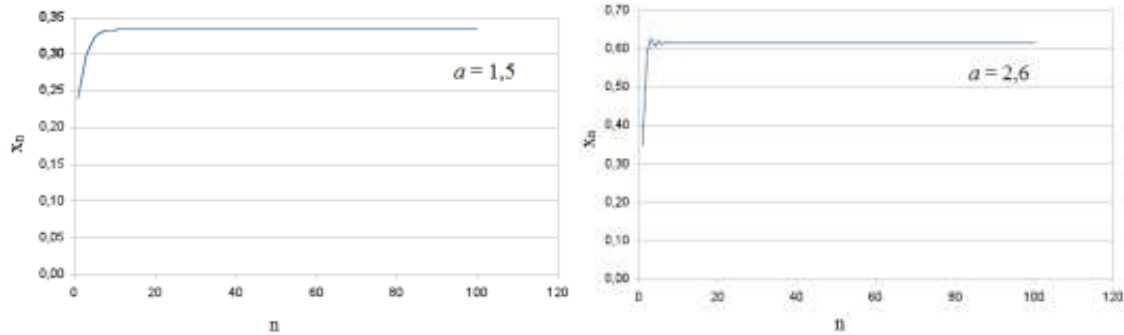
$$x^* = M(x^*) = ax^*(1 - x^*), \quad \text{EQ A.8}$$

e como resultado os pontos fixos são as raízes da Equação (EQ A.8): $x_1^* = 0$ 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 transcítica (A2, A8). O aumento de a faz as órbitas convergirem para o ponto atrator $1 - \frac{1}{a}$. 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:

$$\lambda_1 \equiv \frac{dM(x^*)}{dx} = 2 - a. \quad \text{EQ A.9}$$

As Figuras A.2 e A.3 mostram as duas séries temporais e o diagrama *stair-step* para os valores de $a = 1,5$ e $a = 2,6$. Pode-se verificar nas figuras que a partir de uma condição inicial, depois de algumas iterações, o sistema converge suavemente para um ponto fixo.

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

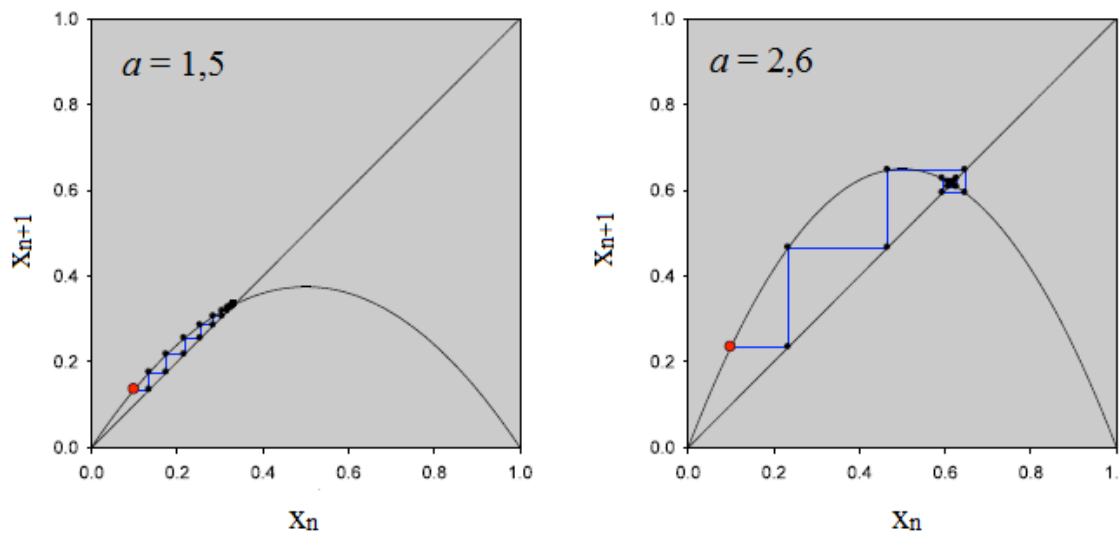


(a)

(b)

Fonte: Araújo (2009).

Figura A.3 – Diagramas *stair-step* do mapa logístico. (a) $a = 1,5$ e (b) $a = 2,6$.



(a)

(b)

Fonte: Araújo (2009).

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 (Martins, 2016). No caso do ciclo atrator de período dois, os pontos fixos de período dois são dados por:

$$x_2^* = M^2(x_2^*). \quad \text{EQ A.10}$$

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

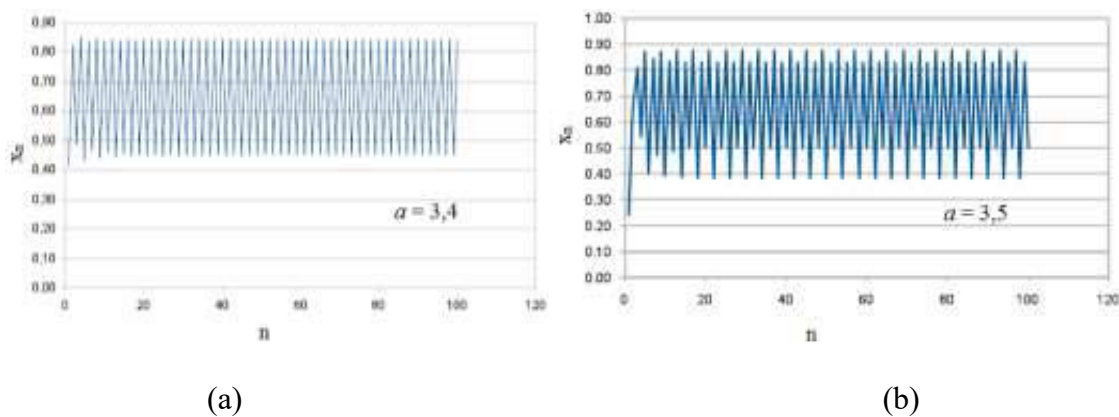
$$\lambda_1 = \lambda_1^2. \quad \text{EQ A.11}$$

Assim, quando $\lambda_1 < -1$, x^* se torna instável. Com $\lambda_2 > 1$, M^2 forma um laço e com isso aparecem 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 acontecer 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 (Onias, 2012; Santos, 2007).

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

A Figura A.4 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.

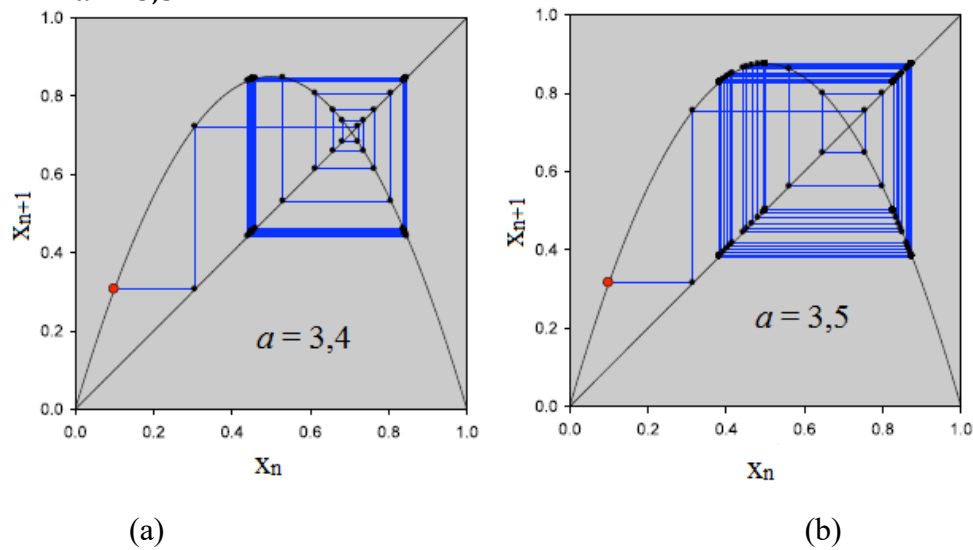
Figura A.4 – Séries temporais de período 2 e 4 do mapa logístico. (a) $a = 3,4$ e (b) $a = 3,5$.



Fonte: Araújo (2009).

A Figura A.5 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.

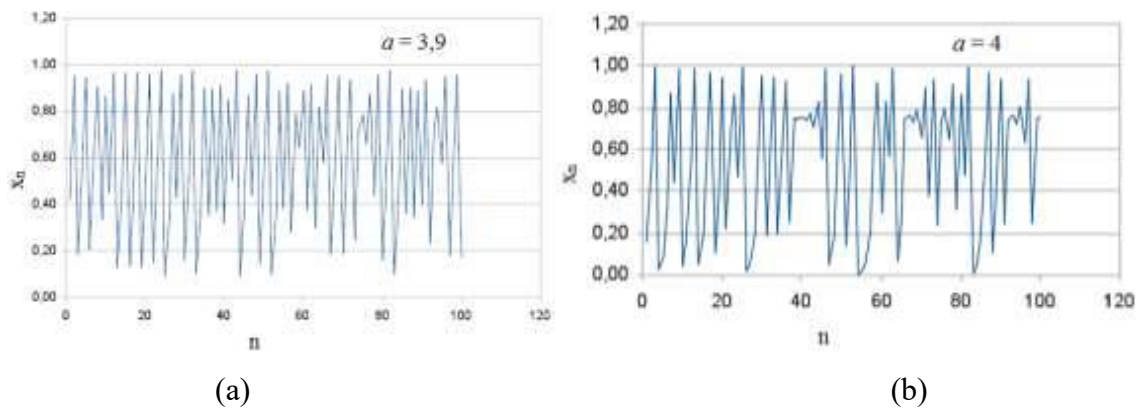
Figura A.5 – Diagramas *stair-step* do mapa logístico. (a) $a = 3,4$ e (b) $a = 3,5$.



Fonte: Araújo (2009).

Na Figura A.6 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.

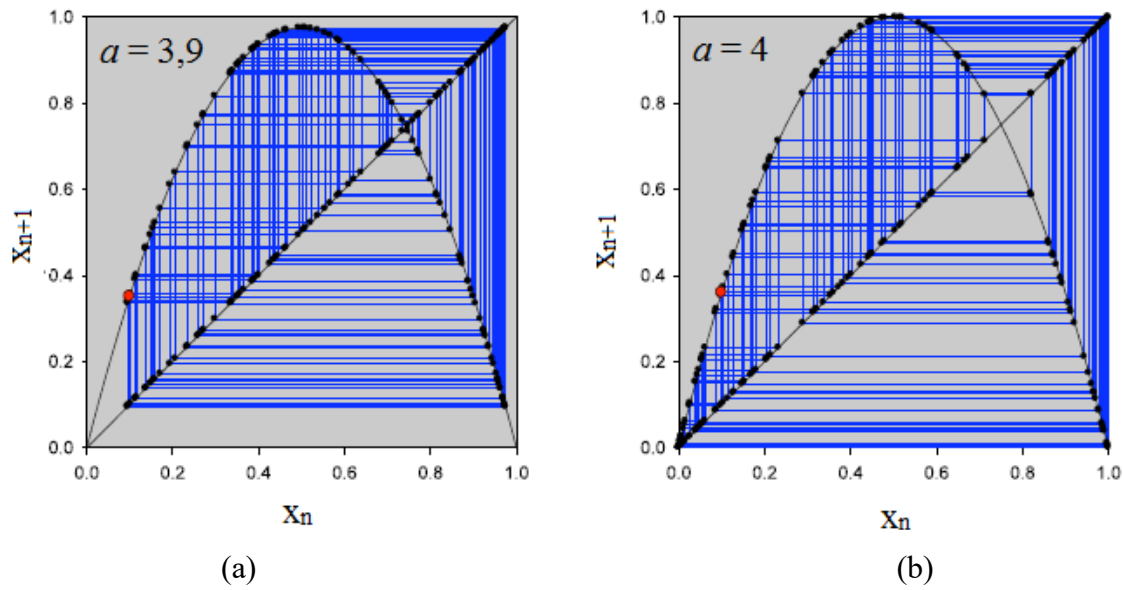
Figura A.6 – Séries temporais do aparecimento do caos. (a) $a = 3,9$ e (b) $a = 4$.



Fonte: Araújo (2009).

Os diagramas *stair-step* do mapa logístico para os valores de $a = 3,9$ e (b) $a = 4$ são mostrados na Figura A.7. No caos, como se verifica na Figura A.6, a parábola toda é percorrida pelos ciclos, porém com uma probabilidade não uniforme de taxa de visitação (Santos, 2007).

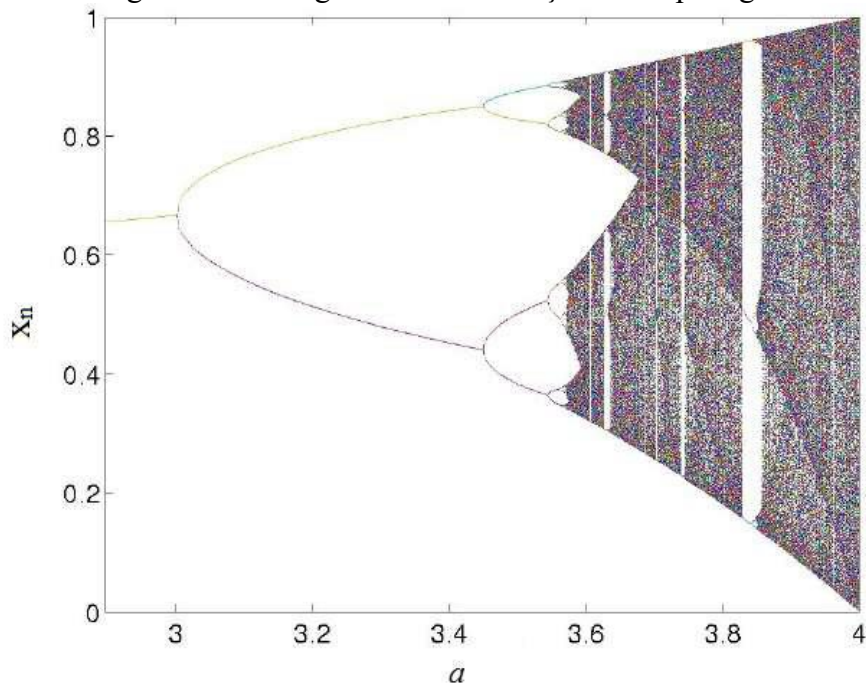
Figura A.7 – Diagramas *stair-step* do caos. (a) $a = 3,9$ e (b) $a = 4$.



Fonte: Araújo (2009).

O diagrama de bifurcação para o mapa logístico é uma ferramenta muito utilizada para representar o caos. A Figura A.8 mostra o diagrama de bifurcação para o mapa logístico, onde é possível visualizar as janelas de bifurcações para o caos.

Figura A.8 – Diagramas de bifurcação do mapa logístico.



Fonte: Araújo (2009).

O diagrama de bifurcação mostra a alternância entre regiões de ordem e caos, onde janelas periódicas são intercaladas entre nuvens caóticas (Martins, 2016). 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.

A4. Referências

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

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

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 jul. 2017.

MARIETTO, M. L.; SANCHES, C.; MEIRELES, M. Teoria do caos: Uma contribuição para formação de estratégias, **Revista Ibero-Americana de Estratégias - RIAE**, [S.l.], v. 10, n. 3, p. 66-93, set./dez. 2011. Disponível em: <https://www.redalyc.org/pdf/3312/331227120005.pdf>. Acesso em: jul. 2020.

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

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

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

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

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

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

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

APÊNDICE B – FUNÇÃO W_q DE LAMBERT-TSALLIS

B1. Introdução

A função W_q de Lambert-Tsallis é uma generalização da função W de Lambert que pode ser definida como a solução da equação (Silva, 2022)

$$W_q(z)e_q^{W_q(z)} = z.$$

EQ B.1

A função q -exponencial de Tsallis, por sua vez, é definida como

$$e_q^x = \begin{cases} e^x & \text{se } q=1 \\ [1 + (1-q)x]^{\frac{1}{1-q}} & \text{se } q \neq 1 \text{ \& } 1+(1-q)x > 0 \\ 0^{\frac{1}{1-q}} & \text{se } q \neq 1 \text{ \& } 1+(1-q)x \leq 0 \end{cases} \quad \text{EQ B.2}$$

As propriedades das funções q -exponencial e q -logaritmo são

$$e_q^a e_q^b = e_q^{a+q^b} \quad \text{EQ B.3}$$

$$e_q^{a+b} = e_q^a \times_q e_q^b \quad \text{EQ B.4}$$

$$e_q^a / e_q^b = e_q^{a-q^b} \quad \text{EQ B.5}$$

$$e_q^{a-b} = e_q^a \div_q e_q^b \quad \text{EQ B.6}$$

A função inversa da função q -exponencial é o logaritmo natural de Tsallis, definida como

$$\ln_q(z) = \begin{cases} \ln(z) & \text{se } x > 0 \text{ e } q = 1 \\ \frac{x^{1-q}-1}{1-q} & \text{se } x > 0 \text{ e } q \neq 1 \\ \text{n\~{a}o definido} & \text{se } x \leq 0 \end{cases} \quad \text{EQ B.7}$$

Dessa forma,

$$e_q^{\ln_q(z)} = z \text{ para } z > 0 \quad \text{EQ B.8}$$

$$\ln_q(e_q^z) = z \text{ para } 0 < e_q^z < \infty \quad \text{EQ B.9}$$

As seguintes relações podem ser obtidas a partir das equações acima [B1]

$$ye_q^y = z \therefore y = W_q(z) \quad \text{EQ B.10}$$

$$e_0^z = 1 + z \text{ para } q = 0 \quad \text{EO B.11}$$

$$(e_q^z)^a = \left\{ [1 + (1-q)z]^{\frac{1}{(1-q)}} \right\}^a = [1 + (1-q)z]^{\frac{a}{(1-q)}} = \left[1 + \frac{(1-q)}{a}az \right]^{\frac{a}{(1-q)}} \rightarrow$$

$$(e_q^z)^a = e_{\left(\frac{1-q}{a}\right)}^{az} \quad \text{EQ B.12}$$

B2. Exemplos

a. Encontre x : $x(1+x)^3 = 5$

$$x(1+x)^3 = 5$$

$$x(e_0^x)^3 = 5$$

$$x \left(e_{\frac{1-0}{3}}^{3x} \right)^3 = 5$$

$$xe_{\frac{2}{3}}^{3x} = 5$$

multiplicando ambos os lados da equação por 3

$$3xe_{\frac{2}{3}}^{3x} = 15$$

usando a relação $ye_q^y = z$ é $y = W_q(z)$ com $y = 3x, q = \frac{2}{3}, z = 15$

$$3x = W_{\frac{2}{3}}(15)$$

$$x = \frac{W_{\frac{2}{3}}(15)}{3}$$

b. Encontre x : $\frac{ax}{\sqrt{b-x^2}} = c$

$$\frac{ax}{\sqrt{b-x^2}} = c$$

$$\frac{x}{\sqrt{b-x^2}} = \frac{c}{a}$$

$$\frac{x}{\sqrt{b}\sqrt{1-\frac{x^2}{b}}} = \frac{c}{a}$$

$$\frac{x}{\sqrt{1-\frac{x^2}{b}}} = \sqrt{b}\frac{c}{a}$$

$$x\left(1-\frac{x^2}{b}\right)^{-\frac{1}{2}} = \sqrt{b}\frac{c}{a}$$

$$x\left(e_0^{-\frac{x^2}{b}}\right)^{\frac{1}{2}} = \sqrt{b}\frac{c}{a}$$

usando a relação $(e_q^z)^a = e_{\left(1-\frac{1-q}{a}\right)}^{az}$ com $q = 0, z = -\frac{x^2}{b}, a = \frac{1}{2}$

$$x\left(e_{1-\frac{1-0}{\frac{1}{2}}}\left(e^{-\frac{x^2}{2b}}\right)\right) = \sqrt{b}\frac{c}{a}$$

multiplicando ambos os lados da equação por $-\frac{x}{2b}$

$$-\frac{x^2}{2b}\left(e_{1-\frac{1-0}{\frac{1}{2}}}\left(e^{-\frac{x^2}{2b}}\right)\right) = \sqrt{b} - \frac{xc}{2ba}$$

usando a relação $ye_q^y = z = W_q(z)$ com $y = -\frac{x^2}{2b}, q = -1, z = \sqrt{b} - \frac{xc}{2ab}$

$$\sqrt{b} - \frac{xc}{2ab} = W_{-1}\left(\sqrt{b} - \frac{xc}{2ba}\right)$$

$$x = \frac{(-W_{-1}\left(\sqrt{b} - \frac{xc}{2ba}\right) + \sqrt{b})2ab}{c}$$

c. Escreva $I(V)$ – corrente que circula em um tipo de diodo: $I = k(V - RI)^{\frac{3}{2}}$

$$I = k(V - RI)^{\frac{3}{2}}$$

$$I = k \left[V \left(1 - \frac{RI}{V} \right) \right]^{\frac{3}{2}}$$

$$I = kV^{\frac{3}{2}} \left[\left(1 - \frac{RI}{V} \right) \right]^{\frac{3}{2}}$$

usando a relação $e_0^z = 1 + z$ com $z = -\frac{RI}{V}$

$$I = kV^{\frac{3}{2}} \left[\left(e_0^{-\frac{RI}{V}} \right) \right]^{\frac{3}{2}}$$

usando a relação $(e_q^z)^a = e^{\frac{az}{1-\frac{1-q}{a}}}$ com $q = 0, z = -\frac{RI}{V}, a = \frac{3}{2}$

$$I = kV^{\frac{3}{2}} \left[\left(e_{\frac{1-\frac{1-0}{\frac{3}{2}}}}^{-\frac{3RI}{2V}} \right) \right]^{\frac{3}{2}}$$

$$I = kV^{\frac{3}{2}} \left(e_{\frac{1}{3}}^{-\frac{3RI}{2V}} \right)$$

$$I \left(e_{\frac{1}{3}}^{-\frac{3RI}{2V}} \right)^{-1} = kV^{\frac{3}{2}}$$

usando a relação $(e_q^z)^a = e^{\frac{az}{1-\frac{1-q}{a}}}$ com $q = \frac{1}{3}, z = -\frac{3RI}{2V}, a = -1$

$$I e_{\frac{5}{3}}^{\frac{3RI}{2V}} = kV^{\frac{3}{2}}$$

multiplicando ambos os lados da equação por $\frac{3R}{2V}$

$$\frac{3RI}{2V} e_{\frac{5}{3}}^{\frac{3RI}{2V}} = \frac{3R}{2V} kV^{\frac{3}{2}}$$

usando a relação $ye_q^y = z = W_q(z)$ com $y = \frac{3RI}{2V}, q = \frac{5}{3}, z = \frac{3RkV^{\frac{3}{2}}}{2V}$

$$\frac{3RI}{2V} = W_{\frac{5}{3}} \left(\frac{3RkV^{\frac{3}{2}}}{2V} \right)$$

$$I = \frac{2V}{3R} W_{\frac{5}{3}} \left(\frac{3RkV^2}{2V} \right)$$

B3. Cálculo do comprimento da fibra óptica

Encontrar o comprimento L da fibra óptica: $e^{-\alpha_c L} - e^{-\alpha_q L} = z$. Onde:
 α_c perda da fibra no comprimento de 1.310nm por onde o sinal clássico é enviado;
 α_q perda da fibra no comprimento de 1.550nm por onde o sinal quântico é enviado;
 $\alpha_c > \alpha_q$.

$$e^{-\alpha_c L} - e^{-\alpha_q L} = z$$

multiplicando ambos os lados por (-1)

$$-e^{-\alpha_c L} + e^{-\alpha_q L} = -z$$

evidenciando $e^{-\alpha_q L}$

$$e^{-\alpha_q L} \left(1 - \frac{e^{-\alpha_c L}}{e^{-\alpha_q L}} \right) = -z$$

$$e^{-\alpha_q L} (1 - e^{-(\alpha_c - \alpha_q)L}) = -z$$

usando a relação $e_0^z = 1 + z$ com $z = -e^{-(\alpha_c - \alpha_q)L}$

$$e^{-\alpha_q L} \left(e_0^{-e^{-(\alpha_c - \alpha_q)L}} \right) = -z$$

elevando ambos os lados por $\left(\frac{\alpha_c - \alpha_q}{\alpha_q} \right)$

$$\left[e^{-\alpha_q L} \left(e_0^{-e^{-(\alpha_c - \alpha_q)L}} \right) \right]^{\left(\frac{\alpha_c - \alpha_q}{\alpha_q} \right)} = [-z]^{\left(\frac{\alpha_c - \alpha_q}{\alpha_q} \right)}$$

$$e^{-(\alpha_c - \alpha_q)L} \left[\left(e_0^{-e^{-(\alpha_c - \alpha_q)L}} \right) \right]^{\left(\frac{\alpha_c - \alpha_q}{\alpha_q} \right)} = [-z]^{\left(\frac{\alpha_c - \alpha_q}{\alpha_q} \right)}$$

usando a relação $(e_0^z)^a = e^{\frac{az}{1-\frac{1}{a}}}$ com $q = 0, z = -e^{-(\alpha_c - \alpha_q)L}, a = \left(\frac{\alpha_c - \alpha_q}{\alpha_q} \right)$

$$e^{-(\alpha_c - \alpha_q)L} \left[e^{\left[-\left(\frac{\alpha_c - \alpha_q}{\alpha_q} \right) \left(e^{-(\alpha_c - \alpha_q)L} \right) \right]} \right]^{\left(\frac{\alpha_c - \alpha_q}{\alpha_q} \right)} = [-z]^{\left(\frac{\alpha_c - \alpha_q}{\alpha_q} \right)}$$

multiplicando ambos os lados por $-\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)$

$$\left[-\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)\right] \left[e^{-(\alpha_c - \alpha_q)L}\right] \left[e^{\left[\frac{\alpha_c - \alpha_q}{\alpha_q}\right] e^{-\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)(\alpha_c - \alpha_q)L}}\right] = \left[-\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)\right] \left\{[-z]^{\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)}\right\}$$

usando a relação $ye_q^y = z = W_q(z)$ com $y = \left[-\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)\right] \left[e^{-(\alpha_c - \alpha_q)L}\right]$,

$$q = \left(\frac{\alpha_c - 2\alpha_q}{\alpha_c - \alpha_q}\right), z = \left[-\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)\right] \left\{[-z]^{\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)}\right\}$$

$$-\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right) e^{-(\alpha_c - \alpha_q)L} = W_{\left(\frac{\alpha_c - 2\alpha_q}{\alpha_c - \alpha_q}\right)} \left\{ \left[-\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)\right] \left[(-z)^{\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)}\right] \right\}$$

$$e^{-(\alpha_c - \alpha_q)L} = -\left(\frac{\alpha_q}{\alpha_c - \alpha_q}\right) W_{\left(\frac{\alpha_c - 2\alpha_q}{\alpha_c - \alpha_q}\right)} \left\{ \left[-\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)\right] \left[(-z)^{\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)}\right] \right\}$$

tomando o logaritmo natural em ambos os lados

$$\ln(e^{-(\alpha_c - \alpha_q)L}) = \ln \left(-\left(\frac{\alpha_q}{\alpha_c - \alpha_q}\right) W_{\left(\frac{\alpha_c - 2\alpha_q}{\alpha_c - \alpha_q}\right)} \left\{ \left[-\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)\right] \left[(-z)^{\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)}\right] \right\} \right)$$

$$-(\alpha_c - \alpha_q)L = \ln \left(-\left(\frac{\alpha_q}{\alpha_c - \alpha_q}\right) W_{\left(\frac{\alpha_c - 2\alpha_q}{\alpha_c - \alpha_q}\right)} \left\{ \left[-\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)\right] \left[(-z)^{\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)}\right] \right\} \right)$$

$$L = -\frac{\ln \left(-\left(\frac{\alpha_q}{\alpha_c - \alpha_q}\right) W_{\left(\frac{\alpha_c - 2\alpha_q}{\alpha_c - \alpha_q}\right)} \left\{ \left[-\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)\right] \left[(-z)^{\left(\frac{\alpha_c - \alpha_q}{\alpha_q}\right)}\right] \right\} \right)}{\alpha_c - \alpha_q}$$

B4. Referências

SILVA, G. B., **A Função W_q de Lambert-Tsallis e suas Aplicações**. Tese (Doutorado em Engenharia de Teleinformática) – Departamento de Engenharia de Teleinformática, Universidade Federal do Ceará. Ceará, 2022.


APÊNDICE C – ARTIGOS DECORRENTES DA TESE

- C1. NASCIMENTO, J. C.; DAMASCENO, R. L. C.; OLIVEIRA, G. L.; RAMOS, R. V. Quantum-chaotic key distribution in optical networks: from secrecy to implementation with logistic map. **Quantum Information Processing**, [S.l.], v. 17, n. 329, 2018. Disponível em: <https://doi.org/10.1007/s11128-018-2097-1>. Acesso em: 12 jun. 2020.

Quantum Information Processing (2018) 17:329
<https://doi.org/10.1007/s11128-018-2097-1>



Quantum-chaotic key distribution in optical networks: from secrecy to implementation with logistic map

J. C. do Nascimento^{1,2} · R. L. C. Damasceno^{1,3} · G. L. de Oliveira⁴ ·
R. V. Ramos¹ 

Received: 12 July 2018 / Accepted: 13 October 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract

In a recent paper, the quantum-chaotic key distribution (QCKD) in optical networks was introduced. In the present work, we extend the QCKD theory in two ways: Firstly, we propose to use the dependent Bernoulli trials to model the key generation in QCKD. Using this model, we show that the key generated by QCKD is far from presenting the observed correlations in chaos-based cryptography, and it is very close to the maximum secrecy offered by ideal quantum cryptography. Secondly, we show a new optical scheme for QCKD in which the optical chaotic scheme using optoelectronic oscillators is substituted by nonlinear discrete equations running in computers and the information carrier used is the phase instead of the light polarization. These changes make much easier its implementation with today technology while keeping the same security level guaranteed by chaotic and quantum rules.


Keywords Quantum key distribution · Chaos · Security

C2. DAMASCENO, R. L. C.; RIOS, F. F. S.; RAMOS, R. V. Multiphoton pulses and homodyne tomography attack in quantum-chaotic key distribution, **Optical and Quantum Electronics**, [S.l.], v. 52, n. 50, 2020. Disponível em: <https://doi.org/10.1007/s11082-019-2166-4>. Acesso em: 18 maio 2021.

Optical and Quantum Electronics 2020)52:50
<https://doi.org/10.1007/s11082-019-2166-4>



Multiphoton pulses and homodyne tomography attack in quantum-chaotic key distribution

R. L. C. Damasceno¹ · F. F. S. Rios¹ · R. V. Ramos¹ 

Received: 21 February 2019 / Accepted: 18 December 2019
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract

The quantum-chaotic key distribution (QCKD) in optical networks was introduced in a recent paper. In that work, several differences between QKD and QCKD were pointed out. In this direction, the present work shows that, for a eavesdropper that uses a quantum homodyne attack, the mean photon number used by Alice in the QCKD protocol can be much larger than 0.1 without compromising its security.

Keywords Quantum key distribution · Homodyne tomography · Security analysis

1 Introduction

For quantum key distribution using discrete states, the larger the number of bases used the more secure is the protocol. However, since Alice and Bob keep only the information obtained in those time slots in which they chose the same bases, the key transmission rate decreases when the number of bases increases (Bourennane et al. 2001). The problem of

- a. DAMASCENO, R. L. C.; RAMOS, R. V. **Analysis of spontaneous Raman scattering impact on quantum key distribution in passive optical networks using the Lambert-Tsallis W_q function.** ResearchGate. 2022. Disponível em: <https://www.researchgate.net/publication/359560472>. Acesso em: 11 abr. 2022.

[ResearchGate](#)


See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/359560472>

Analysis of Spontaneous Raman Scattering Impact on Quantum Key Distribution in Passive Optical Networks Using the Lambert-Tsallis W_q Function

Preprint · March 2022

CITATIONS	READS
0	86


2 authors, including:




Rubens Ramos
Universidade Federal do Ceará
162 PUBLICATIONS 602 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



Quantum physics and number theory [View project](#)



Quantum physics and number theory [View project](#)