

Universidade Federal de Campina Grande
Centro de Engenharia Elétrica e Informática
Coordenação de Pós-Graduação em Engenharia Elétrica

**Reconciliação de Chave Secreta do Tipo CVQKD
Utilizando o Protocolo CASCADE**

Micael Andrade Souza

Área de Concentração: Processamento da Informação
Linhas de Pesquisa: Eletrônica e Telecomunicações

Francisco Marcos de Assis
(orientador)

Campina Grande, Paraíba, Brasil
© Micael Andrade Souza, 2019

Reconciliação de Chave Secreta do Tipo CVQKD Utilizando o Protocolo CASCADE

Micael Andrade Souza

Dissertação apresentada à Coordenação de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande (Campus I) como parte dos requisitos necessários para obtenção do grau de Mestre em Engenharia Elétrica.

Orientador: Francisco Marcos de Assis

Campina Grande, Paraíba, Brasil

2019

S729r

Souza, Micael Andrade.

Reconciliação de chave do tipo CVQKD utilizando o protocolo CASCADE / Micael Andrade Souza. – Campina Grande, 2019.
75 f. : il. color.

Dissertação (Mestrado em Engenharia Elétrica) – Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática, 2019.

"Orientação: Prof. Dr. Francisco Marcos de Assis".
Referências.

1. Distribuição quântica de chave. 2. CVQKD. 3. Reconciliação da informação. 4. CASCADE. I. Assis, Francisco Marcos de. II. Título.

CDU 004:530.145(043)

**"RECONCILIAÇÃO DE CHAVE SECRETA DO
TIPO CVQKD UTILIZANDO O PROTOCOLO CASCADE
"**

MICAEL ANDRADE SOUZA

DISSERTAÇÃO APROVADA EM 13/03/2019



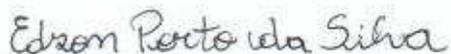
**FRANCISCO MARCOS DE ASSIS, Dr., UFCG
Orientador(a)**



**BENEMAR ALENCAR DE SOUZA, D.Sc., UFCG
Examinador(a)**



**BRUNO BARBOSA ALBERT, D.Sc., UFCG
Examinador(a)**



**EDSON PORTO DA SILVA, Dr., UFCG
Examinador(a)**

CAMPINA GRANDE - PB

Este trabalho é dedicado aos meus pais, Marinaldo e Adiles, e à minha esposa Chris.

Agradecimentos

Agradeço a Deus por sua bondade e misericórdia, as quais tem me acompanhado e possibilitado a caminhada.

Agradeço aos meus pais, os quais me apoiaram nos momentos mais difíceis quando estive longe de casa. À minha esposa que me apoiou de maneira inimaginável e sempre me incentivou e acreditou no meu potencial.

Ao meu orientador, professor Francisco Marcos, que me ensinou valiosos ensinamentos sobre ciência e pesquisa, sempre demonstrando extrema humildade e sabedoria.

A todos os professores do iQuanta que, de maneira direta ou indireta, contribuíram para o meu crescimento acadêmico.

A todos os amigos e colegas do iQuanta e IFPB que me incentivaram, compartilharam as dificuldades e preocupações, e que compartilham o desejo pela pesquisa e busca pelo conhecimento.

"A experiência mais bela e profunda que um homem pode ter é o sentido do mistério. Ele é o princípio fundamental da religião, bem como de todo esforço sério em termos de arte e ciência. Parece-me que aquele que nunca teve essa experiência, se não está morto, pelo menos está cego."

Albert Einstein, Meu credo, 1932

Resumo

A distribuição quântica de chave secreta está entre uma das principais aplicações práticas da teoria da informação quântica, fazendo uso das leis da mecânica quântica para garantir segurança incondicional na transmissão de informação por meio de estados quânticos e permitindo que duas partes possam compartilhar uma chave secreta de maneira segura sem a necessidade de compartilhamento prévio de informação. Neste trabalho é apresentada uma solução de reconciliação de chaves secretas geradas por esquemas de distribuição do tipo CVQKD utilizando o estabelecido protocolo de reconciliação CASCADE. Apesar de tradicionalmente ser aplicado na reconciliação de chaves geradas por esquemas DVQKD, os quais resultam em taxas de erro por *bit* menores que 0.15, o uso do protocolo CASCADE é viabilizado no contexto das variáveis contínuas por meio de modificações propostas no tamanho do bloco inicial e quantidade de passos de reconciliação executados. Este trabalho propõe modificações nos parâmetros fundamentais do protocolo de reconciliação de modo que sejam realizadas (1) a reconciliação completa de chaves que apresentam taxas de erro por *bit* menores que 0.25 e (2) uma solução de reconciliação parcial para chaves com taxas de erro por *bit* maiores que 0.25, na qual a quantidade de erros corrigidos durante o processo de reconciliação é controlada pela quantidade de informação vazada pelo protocolo.

Palavras-chaves: Distribuição Quântica de Chave. CVQKD. Reconciliação da Informação. CASCADE.

Abstract

The quantum secret key distribution is one of the main practical applications of quantum information theory, making use of quantum mechanics laws' to ensure unconditional security on information transmission through quantum states and allowing two parties to securely share a secret key with no need for previous shared information. In this work, a solution for secret key reconciliation is presented for keys generated by CVQKD distribution schemes using the established CASCADE reconciliation protocol. Although it is traditionally applied in the reconciliation of keys generated by DVQKD schemes, which results on bit error rates lower than 0.15, its use is made feasible in the context of continuous variables by means of proposed modifications in the initial block size and the number of reconciliation steps executed. This work proposes modifications on fundamental parameters of the reconciliation protocol such that (1) a complete secret key reconciliation be realized where the bit error rates are lower than 0.25 and (2) a partial reconciliation solution for secret keys with bit error rates greater than 0.25, which aims to control the amount of corrected errors during reconciliation by the amount of leaked information.

Key-words: Quantum Key Distribution. CVQKD. Information Reconciliation. CASCADE.

Lista de Figuras

Figura 2.1 – Canais de comunicação em sistemas QKD.	19
Figura 2.2 – Estimativas de probabilidade de transição e informação mútua de cada canal na expansão binária de uma variável aleatória gaussiana.	27
Figura 3.1 – Exemplo de correção de erro com BINARY	31
Figura 3.2 – Exemplo da busca recursiva de erros no protocolo CASCADE . (a) um erro é corrigido em K_4^4 , (b) K é formado, (c) B e (d) o conjunto K' é obtido.	33
Figura 3.3 – Fluxograma do procedimento de reconciliação realizado pelo protocolo CASCADE	33
Figura 4.1 – Eficiência de reconciliação f_{EC} dos protocolos simulados.	41
Figura 4.2 – Eficiência de reconciliação β	42
Figura 4.3 – Taxa de erro de quadro (FER)	43
Figura 4.4 – Erro residual médio (ϵ_R)	44
Figura 4.5 – Redução na taxa de erro por <i>bit</i> para $p = 0.25$ e diferentes valores de ϵ	46
Figura 4.6 – Evolução da capacidade do canal com o protocolo CASCADE	48
Figura C.1 – Modelo de um canal $BSC(p)$	74

Lista de Tabelas

Tabela 1 – Mapeamento de <i>bits</i> nas bases retilíneas e diagonais	20
Tabela 2 – Processo de transmissão e medição de estados do BB84.	20
Tabela 3 – CASCADE benchmark	36
Tabela 4 – Principais implementações de CASCADE e modificações	39
Tabela 5 – Comparação do vazamento de informação durante os primeiros dois passos de reconciliação utilizando a modificação do tamanho inicial para diferentes valores de ε	47
Tabela 6 – Ganho de capacidade para os dois primeiros passos de reconciliação apresentados na Tabela (5)	49
Tabela 7 – Comparação de informação vazada e ganho de correlação para dois passos de reconciliação parcial na chaves geradas por expansão binária.	50

Sumário

1	INTRODUÇÃO	14
1.1	Organização do Texto	17
1.2	Notação e Terminologia	17
2	DISTRIBUIÇÃO QUÂNTICA DE CHAVE SECRETA	18
2.1	Protocolos QKD e o BB84	18
2.2	Protocolos CVQKD	21
2.3	Reconciliação da Informação	23
2.3.1	Método de Quantização por Expansão Binária	24
2.3.2	Protocolo de Reconciliação	28
3	O PROTOCOLO CASCADE	30
3.1	Descrição de BINARY	31
3.2	Descrição de CASCADE	32
3.3	Tamanho de Bloco Inicial e Vazamento de Informação	34
4	PROTOCOLO PROPOSTO	38
4.1	Reconciliação de Chave Secreta para $p < 0.25$	38
4.1.1	Resultados	40
4.2	Ganho de correlação de Chave Secreta para $p > 0.25$	45
4.2.1	Resultados	48
5	CONCLUSÕES	51
	REFERÊNCIAS BIBLIOGRÁFICAS	53
A	POSTULADOS DA MECÂNICA QUÂNTICA	57
B	ELETROMAGNETISMO QUÂNTICO	60
B.1	Quantização de Campo Eletromagnético	60
B.1.1	Modos Normais	62
B.1.2	Modos Monocromáticos	63
B.2	Estados de Campo	64
B.2.1	Estados de Quadratura	65
B.2.2	Estados de Fock	66
B.2.3	Estados Coerentes	67

C	TÓPICOS EM TEORIA DA INFORMAÇÃO	71
C.1	Entropia, Entropia Relativa e Informação Mútua	71
C.2	Capacidade de Canal	73
C.3	Teoria da Informação Quântica	74

Capítulo 1

Introdução

A criptologia é a ciência que tem como foco o estudo das técnicas de comunicação segura. Dela, duas linhas se estendem, a criptografia (codificação de mensagem) e a criptoanálise (quebra de código ou de cifra), sendo o objetivo da criptografia proporcionar uma comunicação segura entre o transmissor e o receptor (tradicionalmente chamados de Alice e Bob, respectivamente) realizando a *cifragem* e *decifragem* de um texto plano (mensagem) através da utilização de uma chave secreta. Desta forma, uma transmissão segura de informação consiste no envio de informação por um canal de comunicação onde uma possível ação de uma espiã (Eva) não acarretará na obtenção da mesma informação compartilhada pelas partes autênticas (Alice e Bob) [1].

Historicamente, existem registros de esquemas criptográficos datados desde 500 A.C., baseados em mapeamentos do alfabeto, sendo formas fracas de criptografia que poderiam ser quebradas pelas simples análise de frequência dos símbolos. Os espartanos utilizavam o esquema de *transposição* que realizava um reordenamento nas letras de uma mensagem, enquanto os romanos utilizavam cifras de *substituição*, aplicando um mapeamento do tipo $A \rightarrow B, B \rightarrow C \dots$, a qual ficou conhecida como "Cifra de Cesar", por ter sido usada na comunicação entre os comandantes romanos em campo.

Os trabalhos realizados em criptografia se desenvolveram lentamente até o início do século XIX, quando os primeiros esquemas criptográficos complexos surgiram. Um dos mais notáveis é a *cifra de Vernam*, desenvolvida em 1926, tendo como princípio a utilização de uma chave aleatória secreta com tamanho igual à mensagem a ser cifrada para obtenção de uma mensagem secreta. O processo é realizado pela substituição das letras do alfabeto por números (m_i) (digamos, para um alfabeto de 27 letras, serão utilizados números de 1 a 27) e, para cada letra da mensagem será gerado um número aleatório dentro do conjunto $1, 2, \dots, k_i$ (chave aleatória secreta compartilhada por Alice e Bob), e realizada a operação de soma módulo 27 $c_i = m_i \otimes k_i$. As cifras de Vernam são também conhecidas

como *one-time pad*, uma vez que a chave secreta só pode ser utilizada uma vez, dado que a repetição da chave revela informação ao espião.

Um outro esquema criptográfico do século XIX é o algoritmo RSA [2], baseado na ideia de sistemas criptográficos assimétricos, propostos por Diffie e Hellman [3], utilizando uma chave pública. O sistema RSA é utilizado nos dias atuais, mesmo não tendo uma prova rigorosa de segurança, mas toma como vantagem a complexidade na fatoração de grandes números. As promessas do surgimento de computadores quânticos ameaça sua utilização.

A criptografia quântica tem como tarefa resolver o problema de distribuição de chaves secretas, resultando que não são "sistemas criptográficos quânticos", mas estados quânticos que servem como portadores de informação. Como mencionada, a cifra de Vernam é provadamente segura e sofre da necessidade de, a cada cifragem realizada, uma nova chave deve ser utilizada para a próxima mensagem (*one time pad*). Na distribuição quântica de chaves (*Quantum Key Distribution*, QKD), proposta por Bennet e Brassard com o protocolo BB84 [4] (implementado pela primeira vez oito anos depois, descrito em [5]), é proposta a distribuição de chaves de maneira segura, resguardada pela segurança incondicional garantida através do teorema da não clonagem e do princípio da incerteza [6, 7, 8], sendo uma das principais aplicações práticas de informação quântica. Enquanto nos sistemas clássicos de distribuição de chaves a chave de criptografia obtida tem a segurança baseada na limitação computacional de um possível espião (sistemas baseados em RSA), sistemas de criptografia que utilizam a transmissão de estados quânticos conseguem estabelecer chaves seguras mesmo quando submetidas a um espião com poder computacional ilimitado.

Uma vez que o objetivo da criptografia é a proposição de um método para cifragem e decifragem de uma mensagem, sendo a cifra de Vernam um método comprovadamente seguro (dado o uso de uma chave única a cada cifragem), o objetivo da distribuição quântica de chaves é exatamente viabilizar a operacionalidade da cifra de vernam, distribuindo e gerando chaves secretas, ao passo que a comunicação realizada por meios quânticos e clássicos é vista por uma espiã (Eva) a par de todos os passos do protocolo QKD utilizado. As implementações das soluções de QKD sofreram diversas modificações desde o protocolo BB84, mas seguem majoritariamente divididas entre as aplicações que fazem uso de modulações discretas, os protocolos QKD com variáveis discretas (*Discrete Variable Quantum Key Distribution*, DVQKD), e os protocolos que realizam modulações contínuas da informação em estados quânticos da luz (*Continuous Variable Quantum Key Distribution*, CVQKD).

Durante a transmissão da informação, os estados quânticos portadores da chave ale-

atória secreta estão sujeitos a diversos tipos de ruídos, sejam flutuações do canal quântico ou os ruídos gerados pelas tentativas de ataque realizados por Eva. Um dos trabalhos de uma distribuição de chaves secreta eficiente é realizar a reconciliação, ou correção de erros, das sequências binárias compartilhadas por Alice e Bob após a fase de transmissão quântica, realizado pelo protocolo de reconciliação da informação (IR, *Information Reconciliation*). No caso das distribuições que fazem uso de modulações contínuas de estados quânticos, os valores medidos e obtidos por Alice e Bob são contínuos. Logo, antes de realizar correção de erros, o protocolo IR deve obter sequências binárias a partir dos valores contínuos medidos para então realizar a correção de erros.

Neste ponto, as soluções de reconciliação de chaves distribuídas por protocolos CVQKD devem resolver dois problemas distintos e que podem ser tratados separadamente. O primeiro é a forma como são obtidas as sequências binárias. Esta é uma tarefa importante pois, quando realizada de maneira eficiente, viabiliza a obtenção de mais de um *bit* de informação por estado transmitido, dando uma grande vantagem em relação aos protocolos DVQKD com o aumento da taxa de chave secreta gerada. Tradicionalmente é utilizado o protocolo de correção de erros por fatiamento (SEC, *Slice Error Correction*) [9] que obtém sequências binárias através de um esquema de funções de fatiamento da reta real. Uma alternativa é a utilização de um esquema de quantização baseado na expansão binária de valores uniformemente distribuídos [10]. Neste esquema, é utilizada a propriedade da distribuição uniforme de uma função cumulativa de probabilidade para obter uma representação incompressível do valor real medido de estados coerentes transmitidos por protocolos CVQKD.

O segundo problema a ser solucionado por um protocolo IR é a correção efetiva das sequências binárias. O CASCADE foi o primeiro protocolo proposto para fins de reconciliação de chaves secretas [11], aplicado no contexto dos protocolos DVQKD, realizando a correção de erros entre duas sequências binárias correlacionadas e vazando uma quantidade de informação próxima ao limite teórico para taxas de erro menores que 0.15 por meio de troca de paridades entre Alice e Bob, sendo um protocolo altamente iterativo. O CASCADE não é um protocolo usualmente utilizado na correção de erros entre chaves geradas por protocolos CVQKD devido às altas taxas de erro por *bit* presentes entre as sequências obtidas, apesar de ser um protocolo de fácil implementação e baixo custo computacional na sua execução. Aplicações mais recentes de reconciliação da informação têm sido realizadas com a utilização de códigos LDPC (*Low Density Parity Check Codes*) e códigos polares [12, 13, 14, 15, 16], reconciliando chaves que apresentam taxas de erro por *bit* maiores que 0.15 e mantendo a segurança da chave reconciliada. A utilização de códigos LDPC, em contrapartida, demandam o uso de sequências muito grandes (na ordem de 10^6), o que acarreta no aumento do custo computacional geral do sistema.

Com base no que foi abordado, este trabalho propõe um protocolo IR para chaves distribuídas por protocolos CVQKD que façam uso da expansão binária como método de quantização dos estados quânticos transmitidos e realize a correção dos erros entre as sequências binárias obtidas por meio do protocolo CASCADE. Para contornar as limitações do protocolo CASCADE em cenários que apresentam altas taxas de erro por *bit*, serão propostas modificações nos seus parâmetros de operação de modo que seja viável sua utilização para taxas de erro por *bit* maiores que 0.1. As soluções com o protocolo CASCADE serão divididas entre as reconciliações completas para $p < 0.25$, na qual o CASCADE ainda se mostra eficiente e ainda competitivo frente às diferentes modificações encontradas na literatura, e uma solução de reconciliação em duas etapas, onde o CASCADE atua realizando um aumento na correlação entre as sequências binárias que apresentam $p > 0.25$ para possibilitar a reconciliação final das chaves por códigos LDPC com comprimento de bloco menor que 10^6 .

1.1 Organização do Texto

No Capítulo (2) é apresentada de forma mais detalhada o funcionamento de um protocolo QKD, como a descrição de protocolos de variáveis discretas e contínuas, e a descrição de um protocolo de reconciliação. No Capítulo (3) é apresentado o protocolo CASCADE, seu funcionamento e desempenho em diversos cenários. O Capítulo (4) contém as principais contribuições deste trabalho, onde são apresentadas as modificações realizadas no protocolo CASCADE para se tornar operacional em altas taxas de erro por *bit*, bem como os resultados obtidos. Por fim, no Capítulo (5) estão as conclusões gerais dessa dissertação, apontando os possíveis trabalhos futuros para otimização do protocolo CASCADE e a integração com outros métodos de reconciliação.

1.2 Notação e Terminologia

No decorrer do texto será utilizada a notação de Dirac, conforme apresentada no Apêndice (A), para o desenvolvimento teórico da transmissão de estados quânticos. Variáveis aleatórias são representadas por letras maiúsculas, suas realizações por letras minúsculas e o alfabeto de uma variável aleatória por letras caligráficas, sendo uma variável aleatória X com alfabeto \mathcal{X} e realização x . Sobrescritos indicam uma sequência de variáveis aleatórias, $p(\cdot)$ indica sua função densidade de probabilidade e $F(\cdot)$ sua função distribuição de probabilidade. O logaritmo usado é sempre em base 2, quando não indicado outro, afim de que a informação medida seja em *bits*.

Capítulo 2

Distribuição Quântica de Chave Secreta

Neste capítulo serão abordados os principais pontos da distribuição quântica de chave secreta necessários para o desenvolvimento do trabalho. Os protocolos com variáveis discretas e contínuas serão abordados bem como a formalização de um protocolo de reconciliação, apresentando métricas e indicadores de eficiência, e em seguida os métodos de quantização serão discutidos.

2.1 Protocolos QKD e o BB84

Um protocolo QKD tem como objetivo viabilizar a distribuição (ou geração) de chave secreta entre as partes autênticas da conversa (Alice e Bob), mesmo quando a conversa é submetida à ação de uma espiã (Eva) com poder computacional ilimitado. O protocolo opera em duas frentes, sendo uma fase quântica, compreendida pelo preparo, transmissão e medição de estados quânticos, e uma segunda fase que ocorre por um canal de comunicação clássico (admitido como um canal perfeito sem ruídos), por onde são realizadas as estimativas de ruído da comunicação quântica, correção de erros e o pós processamento da chave gerada, conforme Figura (2.1). Tendo em vista que durante o processo Eva tentará ganhar informação a respeito da chave que está sendo compartilhada, o protocolo deve minimizar a informação vazada tanto na fase quântica da transmissão de estados quanto na fase clássica, quando é realizado o processamento da chave [17].

O primeiro protocolo QKD proposto foi o BB84 [4], onde os autores Bennet e Brassard propuseram transmitir a chave secreta modulada na polarização de fótons. Embora a polarização de um fóton possa ser realizada continuamente no intervalo $[0, 2\pi)$, medições em bases não ortogonais à polarização original do fóton gera um comportamento probabilístico, de modo que para um fóton polarizado com ângulo α e direcionado à uma cavidade com ângulo β , sua transmissão ocorre com probabilidade $\cos^2(\alpha - \beta)$ e absorção

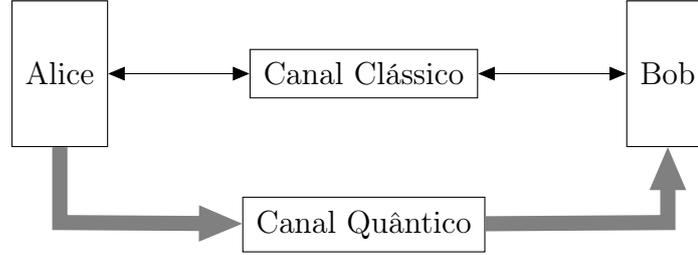


Figura 2.1 – Canais de comunicação em sistemas QKD.

com probabilidade $\sin^2(\alpha - \beta)$. Os fótons irão se comportar deterministicamente apenas quando os eixos de polarização e cavidade são paralelos ou perpendiculares, resultando na sua transmissão ou absorção, respectivamente [4]. Logo, um conjunto discreto de estados deve ser escolhido para transmissão de seqüências de *bits*, categorizando o BB84 como um protocolo de variáveis discretas, ou DVQKD.

O BB84 faz uso de bases conjugadas de espaços Hilbert bidimensionais para escolher quais estados (ou polarização do fóton) serão transmitidos. As polarizações retilíneas (horizontal/ 0° e vertical/ 90°) e diagonais (45° e 135°) podem ser mapeados nos vetores $r_1 = (1, 0)$, $r_2 = (0, 1)$, $d_1 = (0.707, 0.707)$ e $d_2 = (-0.707, 0.707)$, onde $R = \{r_1, r_2\}$ e $D = \{d_1, d_2\}$ formam bases para o espaço de Hilbert de duas dimensões. Note que as projeções de vetores de uma base em outra gera componentes de mesmo módulo, as tornando conjugadas e sendo uma escolha ótima para criptografia, uma vez que estados preparados em uma base se comportam de maneira completamente aleatória quando medidos na base conjugada. Os vetores r_1 e r_2 , d_1 e d_2 tem como representantes os *qubits* $|0\rangle$ e $|1\rangle$, $|+\rangle$ e $|-\rangle$, sendo os dois últimos definidos conforme a Equações (2.1) e (2.2).

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad (2.1)$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (2.2)$$

Para escolha de que estado será transmitido, o procedimento segue os seguintes passos. Alice gera duas seqüências de comprimento m , uma seqüência aleatória de *bits* e uma seqüência aleatória informando qual base será utilizada pra modular cada *bit*. O mapeamento de *bits* em estados, dada uma base específica, é realizado de acordo com a Tabela (1), a qual é compartilhada por Alice e Bob.

Alice inicia a transmissão, onde i -ésimo *bit* será enviado de acordo com a base indicada na i -ésima posição da seqüência de bases. Bob, por sua vez, irá escolher aleatoriamente uma seqüência de bases para realizar as medições, de modo que as medições serão corretas quando a base escolhida por Bob for a mesma base escolhida por Alice para

Tabela 1 – Mapeamento de *bits* nas bases retilíneas e diagonais

<i>bit</i>	Bases	
	Retilínea	Diagonal
0	$ 0\rangle$	$ +\rangle$
1	$ 1\rangle$	$ -\rangle$

preparação do fóton. Note que não faz sentido que Bob realize as medições em ambas as bases pois, após uma medição, toda informação a respeito da polarização original do fóton é perdida. Além da escolha errada de base de medição, eventos como ruído de detecção, distúrbios no canal quântico ou tentativas de ataques de Eva fazem com que as medições de Bob estejam em desacordo com os estados preparados por Alice, mesmo que as bases escolhidas sejam as mesmas. A quantidade de estados úteis após o processo de medição será $m \cdot g_q$, onde g_q representa o ganho do canal quântico [18]. O processo de preparo e medição dos estados quânticos, realizado por Alice e Bob, está descrito na Tabela (2), onde as três primeiras linhas representam as sequências aleatórias de bits, bases utilizadas para escolha dos estados e os respectivos estados preparados. As quartas e quinta linhas mostram as bases de medição escolhidas por Bob e os valores medidos.

Como as sequências de *bits* e bases de Alice e a sequência de bases de Bob são todos gerados aleatoriamente, após a transmissão e medição dos estados, a parte quântica do protocolo está finalizada e iniciada a fase de *sifting* (peneiramento), ocorrendo pelo canal clássico e público. Vale destacar que é admitido que o canal seja sem ruídos e que Eva não possa modificar as informações contidas nas mensagens trocadas por Alice e Bob. Caso fosse possível, Eva poderia realizar um ataque do tipo *homem-no-meio* onde, a partir da manipulação das mensagens pelo canal público, poderia compartilhar chaves com uma parte disfarçada da outra.

A fase de *sifting* inicia com Bob informando Alice em quais dos m estados transmitidos foram efetuadas as medições. Em seguida, Bob informa a sequência de bases utilizadas nas medições devidamente realizadas, com a qual Alice consegue identificar quais fótons foram medidos corretamente. O processo inverso é realizado por Alice, infor-

Tabela 2 – Processo de transmissão e medição de estados do BB84.

Sequência <i>bits</i> (Alice)	0	1	1	0	1	1	0	0	1	0	1
Sequência bases (Alice)	D	R	D	R	R	R	R	R	D	D	R
Estados transmitidos	$ +\rangle$	$ 1\rangle$	$ -\rangle$	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$	$ 0\rangle$	$ 0\rangle$	$ -\rangle$	$ +\rangle$	$ 1\rangle$
Sequência bases (Bob)	R	D	D	R	R	D	D	R	D	R	D
Bits recebidos por Bob	1		1		1	0	0	0		1	1

mando Bob as bases usadas para polarização dos fótons, permitindo que Bob saiba quais de suas medições estão corretas. Afim de se precaver contra ataques de Eva durante o processo, a sequência de *bits* resultante deve passar por um processo de autenticação [17].

Após Alice e Bob concordarem sobre as sequências de bases e concluírem os processos de *sifting* e autenticação, é iniciada a fase de reconciliação, dividida em duas etapas. A primeira etapa consiste na estimação da taxa de erro do canal. Devido a todo ruído ao qual os fótons polarizados são submetidos, as sequências binárias obtidas por Alice e Bob podem conter erros. Afim de estimar a correta taxa de erro presente em suas sequências, o BB84 realiza a comparação de um conjunto aleatório de tamanho r da sequência de *bits* obtida da fase de *sifting*, resultando em uma quantidade de erros e . Se o tamanho do conjunto usado para estimação for adequado, a taxa de erro estimada será

$$p = \frac{e}{r}, \quad (2.3)$$

e o canal quântico pode ser modelado como um canal binário simétrico (*Binary Symmetric Channel*, BSC), onde p é a probabilidade de transição do canal, ou seja, a probabilidade de que seja transmitido um *bit* 1 e seja recebido 0, e *vice-versa*.

Pra evitar que Eva ganhe informação pela comunicação dos r *bits*, eles devem ser removidos da chave. Após estimada, caso p se mostra demasiadamente grande, Alice e Bob podem concluir que durante a fase quântica Eva tenha obtido informação suficiente para comprometer a segurança da chave (Eva não pode espionar sem perturbar o sistema) ou o canal está ruidoso em excesso. Em ambos os casos, a chave compartilhada é descartada e o processo é reiniciado.

Para taxas de erro adequadas, é necessário que as sequências de *bits* passem por uma etapa de correção de erros. Para tal, é aplicado um protocolo de reconciliação R^p que, por meio da troca de mensagens de reconciliação C pelo canal público, irá corrigir os erros restantes entre as sequências de Alice e Bob sem revelar informação suficiente, de modo que Eva não possa reconstruir a chave tal qual as partes autênticas, gerando uma chave secreta K . Logo, é uma tarefa do protocolo R^p minimizar a quantidade de informação exposta por C . A quantidade de informação que Eva pode ganhar por meio da comunicação realizada pelo protocolo R^p será $I(K; E|C)$, sendo I a informação mútua de Shannon, conforme definido no Apêndice (C).

2.2 Protocolos CVQKD

O protocolo descrito na Seção (2.1) parte da distribuição de chave inserida em uma quantidade discreta de estados transmitidos, definido a classe dos protocolos DVQKD.

Apesar de ter sido o primeiro protocolo proposto e ainda ser amplamente utilizado, o uso de geradores de fóton único, detectores de fótons isolados e toda sensibilidade acarretada pelo sistema limita a implementação em larga escala com relação à distância atingível e à taxa de chave obtida¹.

O uso de modulações contínuas aparecem como uma alternativa aos sistemas DVQKD. Encorajada pela demonstração experimental de teletransporte quântico de estados coerentes [19], prova da versão contínua do teorema da não clonagem [20] e dos resultados experimentais apresentados em [21], relacionando a eficiência da clonagem e fidelidade quântica em sistemas de variáveis contínuas, os protocolos de variáveis contínuas (*Continuous Variable* QKD, CVQKD) fazem uso de modulação dos estados de quadratura de pulsos coerentes para transmissão de informação. Os estados coerentes são conhecidos por estarem na fronteira entre as esferas quânticas e clássicas são conhecidos por estarem na fronteira entre as esferas quânticas e clássicas, podendo ser utilizados para descrever um laser *ideal*. Estes estados são definidos como os autoestados do operador de aniquilação \hat{a} ,

$$\hat{a} |\alpha\rangle = \alpha |\alpha\rangle, \quad (2.4)$$

sendo $\alpha \in \mathbb{C}$. Para mais detalhes, o Apêndice (B) apresenta a fundamentação teórica necessária, sendo os estados coerentes abordados na Seção B.2.3.

O protocolo GG02 foi o primeiro a propor um esquema de distribuição quântica de chaves utilizando estados coerentes com modulação gaussiana ao invés de pulsos não clássicos de luz [22, 23]. Do ponto de vista prático, protocolos do tipo CVQKD seguram uma posição forte em relação aos protocolos de variáveis discretas devido à possibilidade de utilização de equipamentos de comunicação óptica comuns, como multiplexadores ópticos, moduladores I/Q , interferômetros de Mach-Zehnder, detecção coerente, entre outros [24, 25, 26].

De maneira geral, conforme descrito em [27, 28], um protocolo CVQKD do tipo GMCS (*Gaussian Modulated Coherent State*) utilizando estados coerentes funciona da seguinte maneira: (1) Alice gera realizações q_A e p_A de duas variáveis aleatórias gaussianas de média nula e variância $V_A N_0$ (sendo N_0 a variância do ruído) e (2) envia o estado coerente $|q_A + ip_A\rangle$. (3) Bob escolhe medir uma das duas quadraturas, onde a medição coerente pode ser realizada perfeitamente. (4) Bob informa qual base de medição foi utilizada (semelhante ao protocolo BB84, tendo em média metade da chave gerada descar-

¹ A emissão de um único fóton pode ser realizada pela atenuação de um *laser*, caracterizado pelo número médio de fótons (a taxa com a qual os fótons atravessam o atenuador). Usualmente, o número médio de fótons é 0,1 [17].

tada). (5) Ao fim do processo, Alice e Bob compartilham duas sequências de realizações de variáveis aleatórias correlacionadas, chamadas de *elementos de chave*. Terminado os passos descritos, Alice e Bob devem fazer uso de um protocolo de reconciliação que realize a extração de sequências binárias dos valores resultantes das medições coerentes dos estados transmitidos e a correção dos possíveis erros presentes entre as sequências. Na execução do protocolo de reconciliação, é possível que seja extraído mais de um *bit* por pulso, aumentando a taxa de chave gerada, mas exigindo esquemas de correção de erros robustos para que a extração seja realizada eficientemente [9, 14, 12].

2.3 Reconciliação da Informação

No contexto dos protocolos CVQKD, após a transmissão dos estados coerentes, ambas as partes estão de posse de variáveis aleatórias distintas, X para Alice e Y para Bob, cuja informação mútua $I(X; Y) > 0$. Para um protocolo que realiza a transmissão de r estados, X_1, X_2, \dots, X_r e Y_1, Y_2, \dots, Y_r são as sequências resultantes da fase de transmissão pelo canal quântico. A espiã Eva terá posse de uma sequência de variáveis aleatórias no mesmo formato, E_1, E_2, \dots, E_r . O objetivo de Alice e Bob é a obtenção de uma sequência binária não conhecida por Eva, denotada por $K(X)$ para um esquema de reconciliação direta. A reconciliação consiste numa troca de mensagens de reconciliação C pelo canal clássico público e autenticado, de modo que Bob possa recuperar $K(X_{1\dots r})$ a partir do conjunto de mensagens de reconciliação C e de $K(Y_{1\dots r})$ ² [9].

O tamanho da chave secreta final gerada é dependente de alguns fatores: a chave compartilhada após a correção de erros, a quantidade de informação revelada durante a reconciliação e a estimativa de informação obtida por Eva durante a fase quântica do protocolo representada pela informação de Holevo (vide Apêndice (C)), χ_{XE} para reconciliação direta e χ_{YE} para reconciliação reversa. Um protocolo de reconciliação perfeito irá conseguir extrair toda informação mútua entre as sequências compartilhadas, $I(X; Y)$, retirada a quantidade de informação obtida por Eva. Em contrapartida, esquemas de reconciliação dificilmente conseguirão extrair toda informação contida nas sequências correlacionadas, sendo um protocolo prático aquele que extrairá $\beta I(X; Y)$, sendo $\beta < 1$ a eficiência do protocolo [14]. As Equações (2.5) e (2.6) representam a quantidade de informação final para os casos de reconciliação direta e reversa, respectivamente.

² Na reconciliação reversa, o processo é realizado ao contrário, onde Alice que deve recuperar a sequência binária $K(X_{1\dots r})$ a partir do conjunto de mensagens de reconciliação C e de $K(Y_{1\dots r})$.

$$\Delta I_D = \beta I(X; Y) - \chi_{XE}, \quad (2.5)$$

$$\Delta I_R = \beta I(Y; X) - \chi_{YE}. \quad (2.6)$$

Para que os valores das Equações (2.5) e (2.6) possam ser diferentes, $\chi_{XE} \neq \chi_{YE}$, uma vez que $I(X; Y) = I(Y; X)$. Conforme [14], dois parâmetros do canal limitam a quantidade de informação que pode ser obtida por Eva durante a transmissão quântica: a transmissividade de linha T e o ruído excessivo ξ . Quando descartado o ruído excessivo, resta que a transmissividade da linha irá limitar χ_{YE} de modo que $\chi_{YE} < I(X; Y)$ para qualquer valor de T quando utilizado o esquema de reconciliação reversa. Para o caso de reconciliação direta, apenas no intervalo $T > 0.5$ é possível obter distribuição de estados quânticos de modo que $\chi_{XE} < I(X; Y)$, o que limita o protocolo a pequenas distâncias de distribuição de chave.

Outro ponto que merece discussão é a necessidade de extrair uma chave com valores discretos ao invés de utilizar chaves contínuas. Apesar de parecer natural que ao modular valores contínuos nas quadraturas de estados coerentes e obter elementos de chave que também possuem valores contínuos o sistema criptográfico seja completamente contínuo, é preferido que a chave contenha valores discretos por dois motivos.

Primeiro segue que, uma chave secreta contínua requer o uso de uma versão contínua do *one-time-pad*, a qual é possível que seja implementada [29], mas acarreta em limitações do protocolo quanto à susceptibilidade ao ruído. Logo, é mais conveniente que sejam obtidas sequências discretas para Alice e Bob do que lidar com erros limitados em números reais. Segundo, o uso de mensagens de reconciliação com valores contínuos influencia no processo de autenticação de mensagens, tornando chaves com valores discretos uma opção mais desejável.

2.3.1 Método de Quantização por Expansão Binária

Nas Seções (2.1) e (2.2) foram abordadas as metodologias para distribuição quântica de chave secreta, com a utilização de variáveis discretas ou contínuas, respectivamente. Além do aparato experimental para implementação dos protocolos, a obtenção de sequências binárias também acontece de maneira diferente em ambos os protocolos. Enquanto para os protocolos DVQKD as sequências binárias são diretamente moduladas na polarização de um fóton, por exemplo, e extraídas durante o processo de medição e divulgação de bases de medição (*sifting*), nos protocolos CVQKD são moduladas realizações de variáveis aleatórias contínuas nas quadraturas dos campos eletromagnéticos de estados coerentes. Logo, os valores obtidos após medição e divulgação das bases de

medição resultam também em variáveis aleatórias contínuas e, a menos que seja realizado um processo criptográfico baseado completamente em valores contínuos de chave, os protocolos CVQKD devem extrair sequências binárias das sequências de variáveis contínuas correlacionadas.

Uma das metodologias para realizar a quantização dos valores contínuos mais utilizado é o protocolo de correção de erros por fatiamento, SEC, consistindo de particionamentos do intervalo $(-\infty, \infty)$ em m partições por meio de funções de fatiamento S_m . Esse procedimento tende a aumentar a taxa de chave secreta à medida que o número de fatiamentos cresce, atingindo o ponto ótimo quando $m \rightarrow \infty$. Porém, alguns empecilhos computacionais são encontradas devido (1) à dificuldade de encontrar as funções S_m para uma quantidade grande de fatiamentos e (2) mesmo para $m > 2$, na maioria das implementações, a quantidade de *bits* extraídos é limitada à 2 durante o processo de reconciliação, devido à baixa quantidade de informação mútua entre os valores originais e fatiados. Como mostrado em [9], a divulgação completa de sequências com informação mútua menor que 0.02 *bit* é uma opção melhor do que a tentativa de reconciliação.

Uma solução mais simples foi proposta em [10], onde é realizada uma expansão binária de valores contínuos, atuando como método de quantização e assegurando os *bits* quantizados como independentes, baseados no seguinte Lema:

Lema 2.1 *Seja X uma variável aleatória com função de distribuição de probabilidade contínua $F(X)$. Seja $U = F(X)$. Então, U tem distribuição uniforme no intervalo $[0, 1]$.*

Prova *Uma vez que $F(x) \in [0, 1]$, a variável U está contida no mesmo intervalo. Logo, para $u \in [0, 1]$,*

$$F_U(u) = Pr[U \leq u] \tag{2.7}$$

$$= Pr[F(X) \leq u] \tag{2.8}$$

$$= Pr[X \leq F^{-1}(u)] \tag{2.9}$$

$$= F(F^{-1}(u)) \tag{2.10}$$

$$= u. \tag{2.11}$$

Um resultado direto do Lema (2.1) acima é que a função distribuição de probabilidade contínua de uma variável X mapeia os valores de chave bruta diretamente no intervalo $[0, 1]$ de maneira uniformemente distribuída. E ainda, com uma expansão binária dos valores uniformemente distribuídos, os *bits* serão independentes dois a dois e serão

distribuídos conforme uma variável de Bernoulli com parâmetro $\frac{1}{2}$, formando uma versão comprimida de X . A expansão do tipo

$$u = 0.F_1F_2F_3 \cdots F_l = \sum_{j=1}^l F_j 2^{-j} \quad (2.12)$$

de um $u \in [0, 1]$ tem o formato $0.F_1F_2 \cdots F_l$ [30], sendo cada símbolo $F_i \in GF(2)$, $1 \leq i \leq l$, com igual probabilidade de saída e sendo l a ordem da expansão. O processo para obtenção dos valores expandidos de uma distribuição de chaves com variáveis contínuas é:

1. Para os valores de chave bruta de Alice e Bob, calcular $F(X)$;
2. Expandir cada valor conforme Equação (2.12);
3. Tratar cada *bit* de dos r valores de chave bruta como um canal BSC independente.

Cada valor de chave bruta é uma realização de uma variável aleatória gaussiana e cada realização será expandida em l *bits*, conforme mostrado. Uma sequência de r realizações da variável aleatória gaussiana é representada como uma matriz $l \times r$, conforme a Equação (2.13), onde cada i -ésima coluna da matriz contém o i -ésimo *bit* da representação binária de todas as r realizações de X .

$$(x_1, x_2, \dots, x_r) = \begin{bmatrix} F_1^1 & F_1^1 & \cdots & F_r^1 \\ F_1^2 & F_2^2 & \cdots & F_r^2 \\ \vdots & \vdots & \ddots & \vdots \\ F_1^l & F_2^l & \cdots & F_r^l \end{bmatrix} \quad (2.13)$$

Exemplo 2.1 Para as cinco realizações $(0.65, -1.31, 0.14, -0.29, 1.51)$ de uma variável aleatória gaussiana X , seguindo o procedimento conforme descrito:

- Calcular $F(X)$: $(0.74, 0.1, 0.56, 0.39, 0.93)$,
- Expandir cada valor conforme Equação (2.12):

$$(0.65, -1.31, 0.14, -0.29, 1.51) = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix} \quad (2.14)$$

Cada *bit* na expansão pode ser visto como um canal BSC que responde de maneira diferente ao ruído aditivo à realização da variável aleatória Gaussiana, podendo ser modelado pela probabilidade de transição, conforme a Figura (2.2a). Para tal, um modelo de comunicação padrão com ruído aditivo $Y = X + Z$ foi usado. Seja $X \sim \mathcal{N}(0, 1)$ a entrada do canal, $Z \sim \mathcal{N}(0, \sigma_N^2)$ o ruído aditivo e $Y \sim \mathcal{N}(0, 1 + \sigma_N^2)$ a saída do canal. As estimativas da probabilidade de transição da Figura (2.2a) foram obtidas através de 1000 realizações de X , adicionado o ruído Z e observada a saída Y , conforme o modelo. Os valores de X e Y foram expandidos conforme a Equação (2.12) e observados as quantidades de *bits* diferentes em cada canal da expansão. As estimativas foram obtidas dos valores médios calculados de 1000 repetições do experimento. Em paralelo, as sequências binárias foram também utilizadas para estimar a informação mútua de cada canal, conforme a Figura (2.2b).

Pelos gráficos da Figura (2.2a), é possível identificar, a partir das probabilidades de erro estimadas, que os dois primeiros canais são os que se comportam de maneira menos susceptível ao ruído e os terceiros e quartos canais apresentaram probabilidades de erro de bit abaixo de 0.4 para níveis de SNR acima de 10dB e 17dB, respectivamente. A análise das informações mútuas estimadas é análoga à análise da probabilidade de erro, sendo os dois primeiros canais da expansão os que apresentam menor sensibilidade ao ruído. Com o método de expansão binária apresentado, é possível obter mais de um bit para formação da chave secreta por estado coerente transmitido, possibilitando um aumento na taxa de chave gerada, sendo o método para obtenção de sequências de *bits* utilizado neste trabalho.

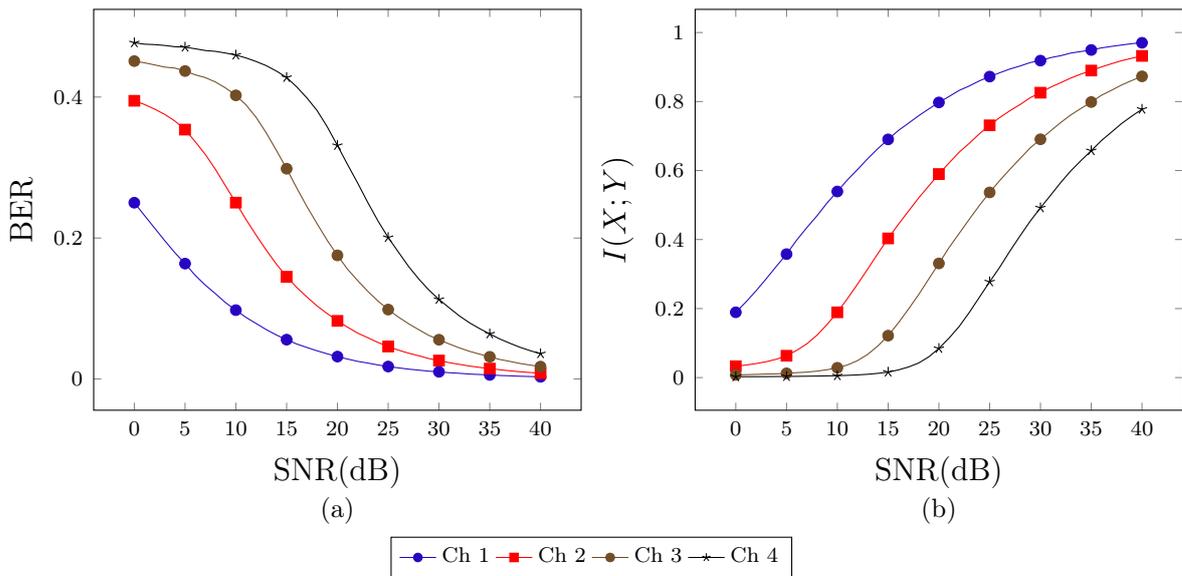


Figura 2.2 – Estimativas de probabilidade de transição e informação mútua de cada canal na expansão binária de uma variável aleatória gaussiana.

2.3.2 Protocolo de Reconciliação

Nesta Seção será abordada de maneira geral a tarefa de reconciliar, ou corrigir erros, entre duas sequências com valores binários, independente da forma de compartilhamento da chave. Na Seção (2.3.1) foi descrito o processo para obtenção de sequências binárias a partir de valores contínuos transmitidos por protocolos CVQKD, e na Seção (2.1) que os valores aleatórios de *bits* são diretamente escritos na variável discreta de protocolos DVQKD.

Sejam X e Y duas variáveis aleatórias discretas correlacionadas com alfabeto binário $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ e probabilidades conjuntas $p_{XY}(x, y) = \Pr(X = x, Y = y)$, a probabilidade condicionada $p(y|x)$ é a probabilidade condicional de modo que y possa ser visto como a saída de um canal discreto sem memória caracterizado pela probabilidade de transição $p(y|x)$ com entrada x . Podemos assumir sem perda de generalidade que um protocolo QKD realiza a transmissão de estados quânticos de modo que resulta em uma taxa de erro por *bit* estimada (p), possibilitando que as sequências obtidas por Alice e Bob sejam o resultado da transmissão de sequências binárias por um canal BSC(p).

Sejam $\mathbf{x} \in \mathcal{A}^n$ e $\mathbf{y} \in \mathcal{A}^n$ sequências de n realizações independentes e identicamente distribuídas (i.i.d) de X e Y , respectivamente, o problema de reconciliação se torna equivalente a um caso particular de codificação de fonte correlacionadas com informação lateral, também conhecido como o teorema de Slepian-Wolf [31]. Denotaremos como “quadro” o conjunto de n realizações das variáveis aleatórias sobre as quais será executado o protocolo de reconciliação. Dado que X representa uma fonte de informação e o decodificador tem acesso à informação lateral Y , a menor quantidade de informação necessária para que o decodificador recupere a informação da fonte de maneira confiável é $H(X|Y)$. Um protocolo prático, em contrapartida, usará uma quantidade de informação maior que $H(X|Y)$. Em [32] são indicadas algumas medidas de eficiência da execução do protocolo. Para um protocolo que transmite uma mensagem de tamanho m para corrigir os erros entre \mathbf{x} e \mathbf{y} , a medida de eficiência f_{EC} é definida por

$$f_{EC} = \frac{m}{nH(X|Y)}, \quad (2.15)$$

sendo $nH(X|Y)$ o menor comprimento de mensagem necessária para reconciliar as sequências, f_{EC} mede a fração de informação adicional que o protocolo precisou utilizar para reconciliar as mensagens, de modo que $f_{EC} \geq 1$, e $f_{EC} = 1$ indica uma reconciliação perfeita.

Como as sequências podem ser entendidas como o resultado da transmissão de sequências de *bits* por um canal BSC(p), onde sua capacidade é bem definida e indica o

limite da quantidade de informação transmitida por símbolo, uma medida de eficiência plausível é o quanto dessa capacidade o protocolo conseguiu atingir, indicada por β na Equação (2.16), onde r é a taxa efetiva do protocolo de reconciliação, $r = m/n$.

$$\beta = \frac{1 - r}{1 - H(p)}. \quad (2.16)$$

Como o parâmetro β indica a fração da capacidade do canal atingida, onde $\beta \leq 1$ e $\beta = 1$ o caso da reconciliação perfeita. Note que as medias f_{EC} e β são relacionadas pela Equação (2.17).

$$1 - f_{EC}H(p) = \beta(1 - H(p)). \quad (2.17)$$

Outras duas medidas de caracterização da eficiência do protocolo são: (1) a taxa de erro por quadro (*Frame error rate*, FEC), indicando a probabilidade de que, ao fim do processo de reconciliação, haja pelo menos um *bit* errado entre as sequências \mathbf{x} e \mathbf{y} ; (2) o erro residual (ϵ_r), sendo o número médio de *bits* diferentes entre as sequências ao fim da reconciliação.

Por fim, a taxa de chave secreta T_p gerada pelo protocolo pode ser calculada conforme a Equação (2.5) para reconciliação direta, por exemplo, quando levado em consideração um protocolo com eficiência β e a quantidade de informação χ_{XE} obtida por Eva durante a fase quântica. Porém, dada a taxa de erro por quadro do protocolo, o valor de taxa de chave secreta gerado pelo protocolo é dado pela Equação (2.18).

$$T_p = (1 - FER)(\beta I(X; Y) - \chi_{XE}) \quad (2.18)$$

Capítulo 3

O Protocolo CASCADE

Juntamente com a tarefa de transmitir informação através de estados quânticos, com o primeiro protocolo QKD (BB84), a correção dos erros presentes entre as sequências compartilhadas por um sistema QKD surgiu como uma necessidade para estabelecimento de chaves secretas devidamente compartilhadas. Em 1992, o trabalho “*Experimental Quantum Cryptography*” [5] apresenta o primeiro aparato experimental de QKD, inclusive propostas para o pós-processamento da chave secreta, como reconciliação da informação e amplificação de privacidade.

Inicialmente, foi proposto um método de reconciliação da informação (correção de erros) baseado na troca de paridade de blocos. As sequências correlacionadas compartilhadas seriam divididas em blocos de tamanho k , cada bloco teria sua paridade (soma módulo 2) computada e seus valores transmitidos por um canal público. Para cada bloco com paridade diferente, uma busca dicotômica é efetuada para correção de um erro. Ao final desse procedimento, é possível que ainda restem erros entre as sequências e o protocolo deva ser executado em passos. Nos passos seguintes, as sequências sofrem permutações e o processo de divisão em blocos, troca de paridades e buscas dicotômicas é repetido. Porém, para garantir privacidade, cada bloco onde um erro fora corrigido deve ter um bit descartado. Esse protocolo é conhecido como BBBSS [5].

O protocolo CASCADE [11] surgiu baseado no BBBSS, sendo realizadas algumas modificações. Primeiramente, foi identificado que os erros corrigidos revelam informação de erros não corrigidos em passos anteriores. O protocolo funciona também com divisão das sequências em blocos, transmitindo paridades por um canal público e aplicando uma busca dicotômica para correção de um erro entre as sequências. A grande diferença é que, ao contrário do BBBSS, CASCADE não descarta bits dos blocos corrigidos. Quando um erro é corrigido no segundo passo em diante, pelo menos um erro fica “descoberto” em blocos dos passos anteriores, e o protocolo segue corrigindo erros em “cascata”. CASCADE

se tornou um protocolo de reconciliação da informação bem estabelecido [32], sendo capaz de corrigir seqüências binárias enquanto vaza uma quantidade de informação próxima do limite teórico para um canal BSC (do inglês, *Binary Scimetric Channel*). No CASCADE, a correção de erros é realizada por uma função de correção de erros chamada BINARY, que realiza a busca dicotômica.

3.1 Descrição de BINARY

Para duas seqüências binárias A e B (de posse de Alice e Bob, respectivamente), um erro pode ser localizado e corrigido através de uma busca binária (ou dicotômica), realizando a comparação das paridades de partes das seqüências, caso haja uma quantidade ímpar de erros entre as seqüências. Logo, se A e B diferem em um número ímpar de posições (e para o caso de reconciliação direta, em que Bob corrige seus dados em relação à Alice), BINARY irá realizar o seguinte procedimento:

1. Alice envia para Bob a paridade da primeira metade de sua seqüência;
2. Bob compara a paridade recebida com a paridade da primeira metade de sua própria seqüência, determinando então se a quantidade ímpar de erros encontra-se na primeira ou segunda metade da seqüência;
3. Após localizada em qual metade os erros estão, os passos 1 e 2 são repetidos, dividindo e comparando paridades, até que a posição de um erro seja localizada.

Exemplo 3.1 A Figura (3.1) apresenta um exemplo de busca binária em uma seqüência de oito bits onde há um erro na sua quinta posição. O procedimento, como apresentado, irá calcular a paridade (\otimes) da primeira parte da seqüência, $\{b_0, b_1, b_2, b_3\}$, e não irá detectar incompatibilidade entre as paridades. Logo, a quantidade ímpar de erros deve estar na segunda metade da seqüência, e agora b_4 a b_7 estará sob análise: a paridade de $\{b_4, b_5\}$ é calculada e indica incompatibilidade das paridades. Finalmente, b_4 é transmitido e o erro é localizado na quinta posição.

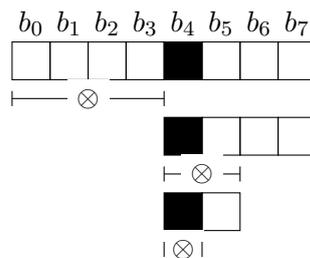


Figura 3.1 – Exemplo de correção de erro com BINARY.

3.2 Descrição de CASCADE

O funcionamento do protocolo é iterativo, sendo subdividido em passos. Antes de sua execução, Alice e Bob devem entrar em acordo quanto ao número de passos executados e o tamanho do bloco inicial (k_1). De forma geral, seja $A = A_1, A_2, \dots, A_n$ e $B = B_1, B_2, \dots, B_n$ ($A_i, B_i \in \{0, 1\}$) as sequências binárias de posse de Alice e Bob, respectivamente. No primeiro passo, ambas as partes irão dividir suas sequências em $\lceil \frac{n}{k_1} \rceil$ blocos de comprimento k_1 , em que o bloco na posição v no primeiro passo é definido por $K_v^1 = \{l | (v-1)k_1 < l \leq vk_1\}$, $v = 1, \dots, \lceil \frac{n}{k_1} \rceil$. Por exemplo, em uma sequência de comprimento 16 e $k_1 = 4$, $v = \{1, 2, 3, 4\}$ e os blocos K_v^1 irão indicar as posições $K_1^1 = \{1, 2, 3, 4\}$, $K_2^1 = \{5, 6, 7, 8\}$, e assim por diante. Após a divisão da sequência em blocos, será comparada a paridade de cada bloco e aplicada a função **BINARY** em cada bloco com paridades diferentes.

Ao final do primeiro passo, todos os blocos de comprimento k_1 tem um número par de erros, possivelmente zero. Então, para os passos $i > 1$, Alice e Bob escolhem um k_i e uma função aleatória $f_i : [1 \dots n] \rightarrow [1 \dots \lceil \frac{n}{k_1} \rceil]$ representando o padrão de permutação no passo i . Nessa etapa do protocolo, Alice e Bob repetem o processo de comparação de paridades de cada bloco K_j^i e aplica **BINARY** para corrigir um erro nos blocos de paridades diferentes.

Neste ponto, antes de prosseguir para o próximo passo ($i > 1$), quando um erro é localizado e corrigido na posição l em um bloco K_j^i , onde $i > 1$, indica que cada passo $u < i$ contém um bloco com paridade ímpar. Logo, é possível formar um conjunto \mathbf{K} composto por todos os blocos K_v^u , com $1 \leq u < i$, contendo o bit l , onde o protocolo deve escolher o menor bloco em \mathbf{K} para corrigir outro erro. Seja l' a posição do erro corrigido quando escolhido o menor bloco no conjunto \mathbf{K} . Outro conjunto, \mathbf{B} , é criado e composto por todos os blocos dos passos 1 a i que contém o bit corrigido na posição l' . Neste ponto, um conjunto \mathbf{K}' é formado pela operação $\mathbf{K} \cup \mathbf{B} \setminus \mathbf{K} \cap \mathbf{B}$ e conterá todos os blocos com paridade ímpar dos passos 1 a i . O protocolo prossegue escolhendo o menor bloco em \mathbf{K}' , corrigindo um erro e atualizando o conjunto \mathbf{K}' , até que $\mathbf{K}' = \emptyset$. O Exemplo (3.2) apresenta um processo de busca recursiva e a Figura (3.2) o procedimento geral da correção de erros realizada pelo protocolo **CASCADE**.

Exemplo 3.2 *Seja um caso de reconciliação de uma chave onde $\lceil \frac{n}{k_1} \rceil = 4$ e $k_i = k_1$, de modo que os blocos em cada passo possam ser representados matricialmente e um erro tenha sido corrigido no bloco K_4^4 , conforme representado na Figura (3.2a). Então, o processo para busca recursiva seguirá os seguintes procedimentos:*

1. O conjunto de blocos \mathbf{K} é formado: $\mathbf{K} = \{K_4^1, K_2^2, K_3^3\}$ (blocos circulados em verme-

lho, Figura (3.2b)),

2. Do conjunto K é escolhido K_4^1 para corrigir um erro (com certeza esse bloco conterá um número ímpar de erros),
3. Quando corrigido um erro em K_4^1 , o conjunto B é formado: $B = \{K_1^2, K_3^3, K_2^4\}$ (blocos circulados em azul, Figura (3.2c)),
4. É realizada a operação $K \cup B \setminus K \cap B$ para obter K' : $K' = \{K_1^2, K_2^2, K_2^4\}$ (blocos circulados em verde, Figura (3.2d)).

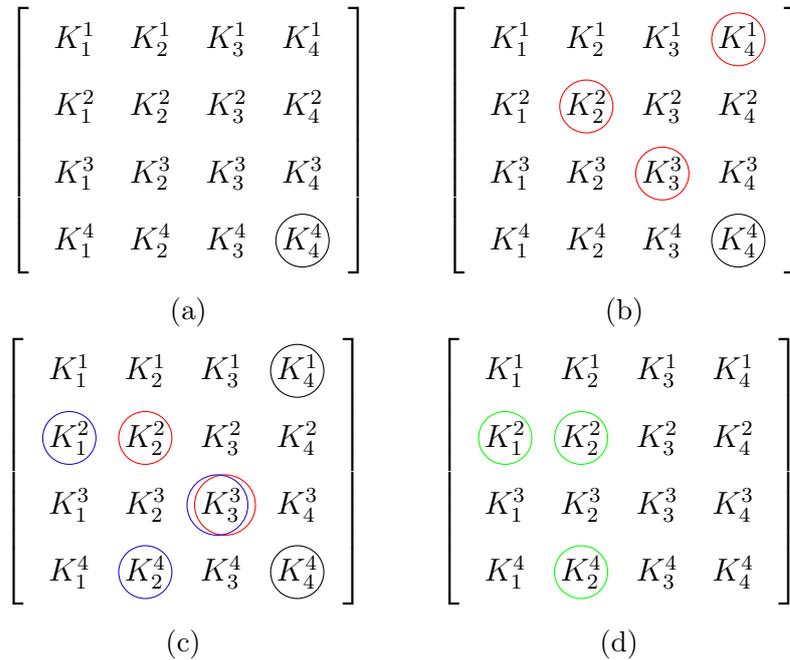


Figura 3.2 – Exemplo da busca recursiva de erros no protocolo CASCADE. (a) um erro é corrigido em K_4^1 , (b) K é formado, (c) B e (d) o conjunto K' é obtido.

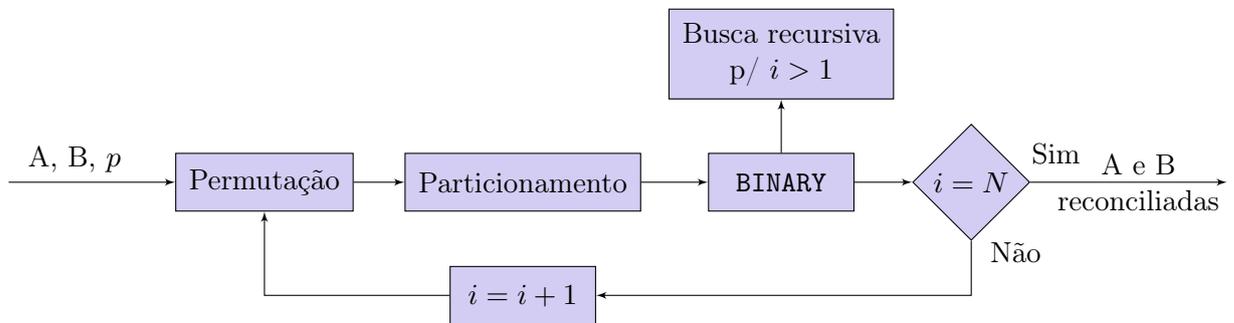


Figura 3.3 – Fluxograma do procedimento de reconciliação realizado pelo protocolo CASCADE.

3.3 Tamanho de Bloco Inicial e Vazamento de Informação

A escolha do tamanho do bloco inicial e a quantidade de informação vazada estão diretamente ligadas, inclusive influenciando no desempenho do protocolo, uma vez que qualquer protocolo de reconciliação da informação tem como objetivo corrigir os erros presentes na chave compartilhada vazando uma quantidade de informação o mais próxima possível do limite teórico. Quanto ao tamanho do bloco inicial, dois cenários são possíveis, em geral. O primeiro é na escolha de blocos curtos, que irá garantir maior número de erros corrigidos no passo inicial, mas também implica no vazamento maior de informação (proporcionalmente ao tamanho do bloco). Blocos mais longos tendem a vazarem menos informação em relação ao tamanho do bloco, mas também corrigem uma quantidade menor de erros à medida que o tamanho de k_1 aumenta.

Para explicar o procedimento de escolha de k_1 em [11], primeiro vamos definir uma variável aleatória binomial $X \sim \text{Bin}(k_1, p)$ onde k_1 representa seu comprimento (número de tentativas) e p a probabilidade de sucesso. A variável X irá então modelar a ocorrência de erros entre as sequências de Alice e Bob, sendo p a probabilidade de erro entre as sequências (ou, em um ponto de vista de sistemas de comunicação, a probabilidade de transição em um *BSC*), e um sucesso na posição l indica a ocorrência de um erro nessa dada posição.

Após o primeiro passo executado por CASCADE, a probabilidade de restarem $2j$ erros em um dado bloco de comprimento k_1 é (1) a probabilidade de que este bloco já tenha $2j$ erros iniciais (não será realizada nenhuma correção com BINARY) ou (2) a probabilidade do dado bloco ter $2j + 1$ erros iniciais (a correção realizada por BINARY irá corrigir um erro). Desta forma, a probabilidade $\delta(j)$ de um bloco de comprimento k_1 ter exatamente $2j$ erros ao final do primeiro passo pode ser expressa como

$$\delta_1(j) = P[X = 2j] + P[X = 2j + 1]. \quad (3.1)$$

Logo, o valor esperado de erros restantes em um bloco de comprimento k_1 depois do cumprimento do primeiro passo é

$$E_1 = \sum_{j=1}^{\lfloor \frac{k_1}{2} \rfloor} 2j\delta_1(j) = k_1 p - \frac{1 - (1 - 2p)^{k_1}}{2}. \quad (3.2)$$

Em [11] os autores limitaram a escolha do tamanho do bloco inicial como o maior

inteiro que satisfizesse duas condições, expressas nas Equações (3.3) e (3.4).

$$E_1 \leq 0.346 \quad (3.3)$$

$$\sum_{l=j+1}^{\lfloor \frac{k_1}{2} \rfloor} \delta_1(l) \leq \frac{1}{4} \delta_1(j) \rightarrow P[X > 2j] \leq \frac{1}{4} P[X = 2j] \quad (3.4)$$

A primeira condição impõe que uma quantidade pequena de erros reste ao final do primeiro passo de CASCADE. A segunda condição demanda que, para um dado j , a soma das probabilidades de restarem $2(j+1), \dots, \lfloor \frac{k_1}{2} \rfloor$ erros depois do primeiro passo seja menor que um quarto da probabilidade de restarem $2j$ erros. Como consequência das restrições definidas pelas Equações (3.3) e (3.4), o valor esperado de erros ao final de cada passo E_i cai exponencialmente com a execução do protocolo, conforme demonstrado em [11].

A quantidade de informação vazada durante o processo de reconciliação é um forte indicativo da eficiência da reconciliação realizada. Após a transmissão de estados quânticos, onde está a primeira tentativa de Eva conseguir informação a respeito da chave compartilhada, a espiã pode conseguir informação também observando o canal público por onde são transmitidas as mensagens de reconciliação.

Tendo o tamanho do bloco inicial sido escolhido de modo que atenda às restrições especificadas nas Equações (3.3) e (3.4) e estabelecendo que $k_i = 2 \cdot k_{i-1}$, a informação vazada (por bloco de tamanho k_1) depois de w passos, pode ser limitada superiormente pela Equação (3.5) [11].

$$I(w) \leq 2 + \frac{1 - (1 - 2p)^{k_1}}{2} [\log(k_1)] + \sum_{l=2}^w \sum_{j=1}^{\lfloor \frac{k_1}{2} \rfloor} \frac{2j \delta_1(j)}{2^{l-1}} [\log(k_1)] \quad (3.5)$$

Os primeiros dois termos do membro direito da inequação expressam o número máximo de bits expostos durante o primeiro passo de CASCADE. O ultimo termo representa a informação vazada para todos os passos $1 < i < w$, uma vez que a escolha de k_1 conforme descrito anteriormente assegura que o valor esperado de erros em um bloco decaia exponencialmente em cada passo do protocolo, e pode ser simplificado utilizando a Equação (3.2),

$$I(w) \leq 2 + \frac{1 - (1 - 2p)^{k_1}}{2} [\log(k_1)] + \sum_{l=2}^w \frac{E_1}{2^{l-1}} [\log(k_1)], \quad (3.6)$$

facilitando o processo de cálculo.

Tabela 3 – CASCADE benchmark

p	k_1	$I(4)$	$\hat{I}(4)$	$k_1 H(p)$	f_{EC}	β
0.01	73	6.81	6.67	5.89	1.166	0.985
0.05	14	4.64	4.60	4.01	1.134	0.954
0.10	7	3.99	3.81	3.28	1.116	0.897
0.15	5	4.12	3.80	3.05	1.308	0.518
0.20	4	3.51	3.36	2.89	1.164	0.573
0.25	3	3.42	3.22	2.43	1.325	-0.014
0.30	3	3.69	3.59	2.64	1.361	-0.023

A Tabela (3) mostra os valores de k_1 que satisfazem as restrições impostas¹, bem como a quantidade de informação vazada após o quarto passo de reconciliação ($I(4)$), de acordo com Equação (3.6), a quantidade de informação vazada estimada através de simulação de reconciliação (quantificação da quantidade de paridades expostas) utilizando quatro passos ($\hat{I}(4)$), de acordo com a implementação original, e o limitante inferior teórico da quantidade de informação vazada para reconciliar as chaves. O protocolo CASCADE foi implementado em linguagem *Python* e as simulações de reconciliação realizadas com $p < 0.15$ tem como finalidade validar a implementação realizada através da comparação das quantidades de informação vazada durante o processo de reconciliação simulado com os resultados apresentados originalmente em [11]. As quantidades de informação vazada estimadas durante as simulações apresentadas na Tabela (3) corroboram com os resultados originais, validando a implementação realizada e permitindo calcular os parâmetros de eficiência f_{EC} e β para a implementação original. Afim de observar o comportamento do protocolo para taxas de erro por *bit* maiores que 0.15, foram simuladas reconciliações com p igual a 0.20, 0.25 e 0.30.

É possível constatar que a quantidade de informação vazada durante a reconciliação se aproxima do limite teórico para taxas de erro menores que 0.10, com parâmetro $\beta > 0.89$, indicando bom aproveitamento da informação compartilhada originalmente entre as partes, e $f_{EC} < 1.15$, o que indica baixa quantidade de informação vazada excedente ao limite teórico. Para as taxas de erro entre 0.10 e 0.20 o aproveitamento do canal β cai consideravelmente para valores próximos de 0.50, apesar de que o protocolo, em alguns casos dentro dessa faixa o parâmetro f_{EC} se mantém abaixo do valor 1.20. Os piores cenários são para as taxas de erro maiores ou iguais a 0.25, quando o protocolo vaza mais bits de paridade do que o comprimento do quadro, resultando em $\beta < 0$.

A análise indica que na faixa $p < 0.10$ o protocolo CASCADE consegue realizar a

¹ o comprimento do bloco inicial ficou padronizado como $k_1 = \frac{0.73}{p}$, onde p é a taxa de erro por *bit*, obtendo um tamanho de bloco que satisfaz as Equações (3.3) e (3.4).

reconciliação das chaves de modo que os parâmetros de eficiência f_{EC} e β evidenciem reconciliações que preservam a segurança da chave, com $\beta \geq 0.89$. Na faixa $0.10 < p < 0.25$ é possível estabelecer uma chave secreta apesar da eficiência de reconciliação cair consideravelmente ($\beta < 0.60$) enquanto para $p \geq 0.25$ o protocolo tende a vazar uma quantidade de informação maior que o comprimento da chave compartilhada ($\beta < 0$), o que inviabiliza seu uso para reconciliação completa das chaves.

Capítulo 4

Protocolo Proposto

Neste Capítulo serão apresentadas as modificações propostas para utilização do protocolo **CASCADE** na reconciliação de chaves secretas geradas por protocolos CVQKD. Como abordado no Capítulo (3), o protocolo **CASCADE** é tradicionalmente utilizado na reconciliação de chave secreta com taxa de erro por *bit* $p < 0.15$, sendo o caso com $p < 0.10$ a faixa de operação onde o protocolo apresenta os melhores valores de eficiência e onde boa parte das modificações propostas presentes na literatura concentram seus esforços para otimizar o desempenho do protocolo [33, 34, 32]. Contudo, serão apresentadas modificações no tamanho do bloco inicial e na quantidade de passos de reconciliação que viabilizam a utilização eficiente do protocolo **CASCADE** em cenários com $p > 0.10$ para reconciliação completa das chaves e uma solução de utilização do **CASCADE** com fins de ganho de correlação entre chaves com taxas de erro muito elevadas ($p > 0.25$) sem comprometimento da segurança da chave compartilhada.

4.1 Reconciliação de Chave Secreta para $p < 0.25$

No Capítulo (3) foi discutido o funcionamento de busca e correção de erros do Tabela (3), inclusive a quantidade de informação vazada durante o processo de reconciliação. Afim de utilizar o protocolo **CASCADE** na reconciliação de chaves geradas por sistemas de variáveis contínuas, é necessário que o protocolo seja adaptado para situações onde a taxa de erro por *bit* se torna maior que 0.10. Essas adaptações, devem visar a modificação de parâmetros que otimize a eficiência do protocolo, ou seja, menor vazamento de informação e maior aproveitamento da informação compartilhada, principalmente. A taxa de erro por quadro e taxa de erro por *bit* ao final da reconciliação são indicativos da viabilidade do uso da chave após o processo de reconciliação.

Entre os parâmetros disponíveis para modificação, encontram-se: tamanho do bloco

inicial (k_1), evolução do tamanho do bloco (k_i), quantidade de passos de reconciliação executados e padrão de permutação (conjunto de funções f_i). A escolha de funções de permutação adequadas é compreendida como fator influenciador na taxa de *throughput* do sistema (sendo a quantidade de *bits* de chave secreta gerados por segundo), pois a correta escolha das funções f_i possibilitam a utilização de computação paralela no cálculo de paridades dos blocos, conforme investigado por Bellot em [33]. Os parâmetros diretamente ligados à eficiência do protocolo são o tamanho de bloco inicial e sua evolução no decorrer da execução do protocolo e a quantidade de passos de reconciliação executados, pois estão diretamente ligado ao limitante superior de informação vazada durante o processo de reconciliação, de acordo com a Equação (3.6).

O tamanho do bloco inicial é obtido como função da taxa de erro por *bit* estimada p resultante da fase de transmissão quântica. Neste trabalho, será realizada uma abordagem semelhante à realizada por Martinez-Mateo em [32], onde o bloco inicial é especificado conforme a Equação (4.1), sendo o termo $\frac{0.73}{p}$ o tamanho do bloco inicial conforme proposto originalmente em [11].

$$k_1 = 2^{\lceil \log(0.73/p) \rceil} \quad (4.1)$$

A motivação para esta modificação é baseada na contenção da quantidade média de informação vazada no primeiro passo para tamanhos de bloco dentro do intervalo compreendido entre duas potências de dois, $2^i < k_1 \leq 2^{i+1}$. Com relação à evolução do tamanho do bloco, a implementação original determina $k_i = 2 \cdot k_{i-1}$ para garantir que o valor esperado de erros ao final de cada passo caia exponencialmente, tendo a chave completamente reconciliada ao final do quarto passo, em média. Na Tabela (4) são apresentados parâmetros manipulados em diferentes modificações do CASCADE, bem como as informações sobre a modificação proposta, sendo n o comprimento da chave a ser reconciliada e N a quantidade de passos de reconciliação realizados.

Tabela 4 – Principais implementações de CASCADE e modificações

Protocolo	k_1	k_2	k_i	N
(Orig.) Brassard e Salvail [4]	$\lceil 0.73/p \rceil$	$2k_1$	$2k_{i-1}$	4
(SY) Sugimoto e Yamazaki [35]	$\lceil 0.92/p \rceil$	$3k_1$	-	2
(MM) Martinez-Mateo et. al. [32]	2^γ	$4k_1$	$n/2$	14
(Yan) Yan et. al. [36]	$\lceil 0.80/p \rceil$	$5k_1$	$n/2$	10
(Prop.) Modificação proposta	2^γ	$2k_1$	$2k_{i-1}$	4

^a $\gamma = \lceil \log(0.73/p) \rceil$.

4.1.1 Resultados

Para estimar os indicadores de eficiência apresentados na seção (2.3) (f_{EC} , β , ϵ_R e FER) para a modificação proposta, foram realizadas simulações de reconciliação para $0.01 \leq p < 0.25$, comprimento de chave $n = 1000$ e cada cenário foi repetido 10.000 vezes. Foram obtidos, ao fim de cada cenário, os valores médios da quantidade de *bits* vazados (para obtenção do indicadores de eficiência f_{EC} e β), o erro residual médio e a taxa de erro por quadro. Em conjunto, foram simuladas reconciliações utilizando o protocolo original [11] e as modificações propostas por Sugimoto [35], Yan et. al. [36] e Martinez-Mateo [32] para comparação de desempenho do protocolo proposto. Os resultados das simulações estão apresentados nas Figuras (4.2) a (4.4). Os resultados são apresentados comparando-se a modificação proposta com o protocolo original e as três modificações apresentadas na Tabela (4) dois a dois, sendo as comparações (Prop.) \times (Orig.), (Prop.) \times (SY), (Prop.) \times (MM) e (Prop.) \times (Yan).

Na Figura (4.1) são apresentados os resultados da eficiência de reconciliação f_{EC} , que mede a quantidade de informação excedente utilizada na reconciliação, com relação ao limite teórico $H(X|Y)$. Nas Figuras (4.1a) e (4.1d) são apresentadas as comparações (Prop.) \times (Orig.) e (Prop.) \times (Yan), onde é possível notar que, em ambos os casos, o protocolo proposto se mostra mais eficiente, uma vez que utiliza uma mensagem com menor quantidade de *bits* para reconciliar as sequências do que as duas outras soluções em toda a faixa da taxa de erro simulada, com exceção para alguns casos na comparação (Prop.) \times (Orig.) em que a eficiência dos dois protocolos é praticamente a mesma. Nas comparações (Prop.) \times (Orig.), vale salientar que os valores de p que apresentam os mesmos resultados de eficiência são devido a tamanhos de k_1 iguais, uma vez que a quantidade de passos e a evolução do tamanho de bloco é sempre a mesma em ambos os protocolos. Com relação ao cenário (Prop.) \times (SY) (Figura (4.1b)), é exibido uma aparente equivalência entre os protocolos, inclusive algumas faixas de QBER onde (SY) se mostra mais eficiente. Entretanto, como será visto na discussão do erro residual médio e taxa de erro por quadro, o protocolo (SY) tende a não conseguir corrigir todos os erros da sequência¹. Já a Figura (4.1b) trás os resultados para (Prop.) \times (MM), onde são identificados os desempenhos mais parecidos entre o protocolo proposto e uma modificação presente na literatura, uma vez que em praticamente toda a faixa da taxa de erro simulada o posto de protocolo mais eficiente alterna entre um dos dois. Este resultado aparece de forma interessante pois ambos os protocolos tem o mesmo tamanho de bloco inicial, mas diferindo no numeros de passos e na evolução do tamanho do bloco.

Nas Figuras (4.2a) a (4.2d) são apresentados os resultados para o parâmetro de

¹ O que explica os valores de $f_{EC} < 1$, os quais não são possíveis pois indicariam que todos os erros foram corrigidos usando uma mensagem de reconciliação menor que o limite teórico imposto.

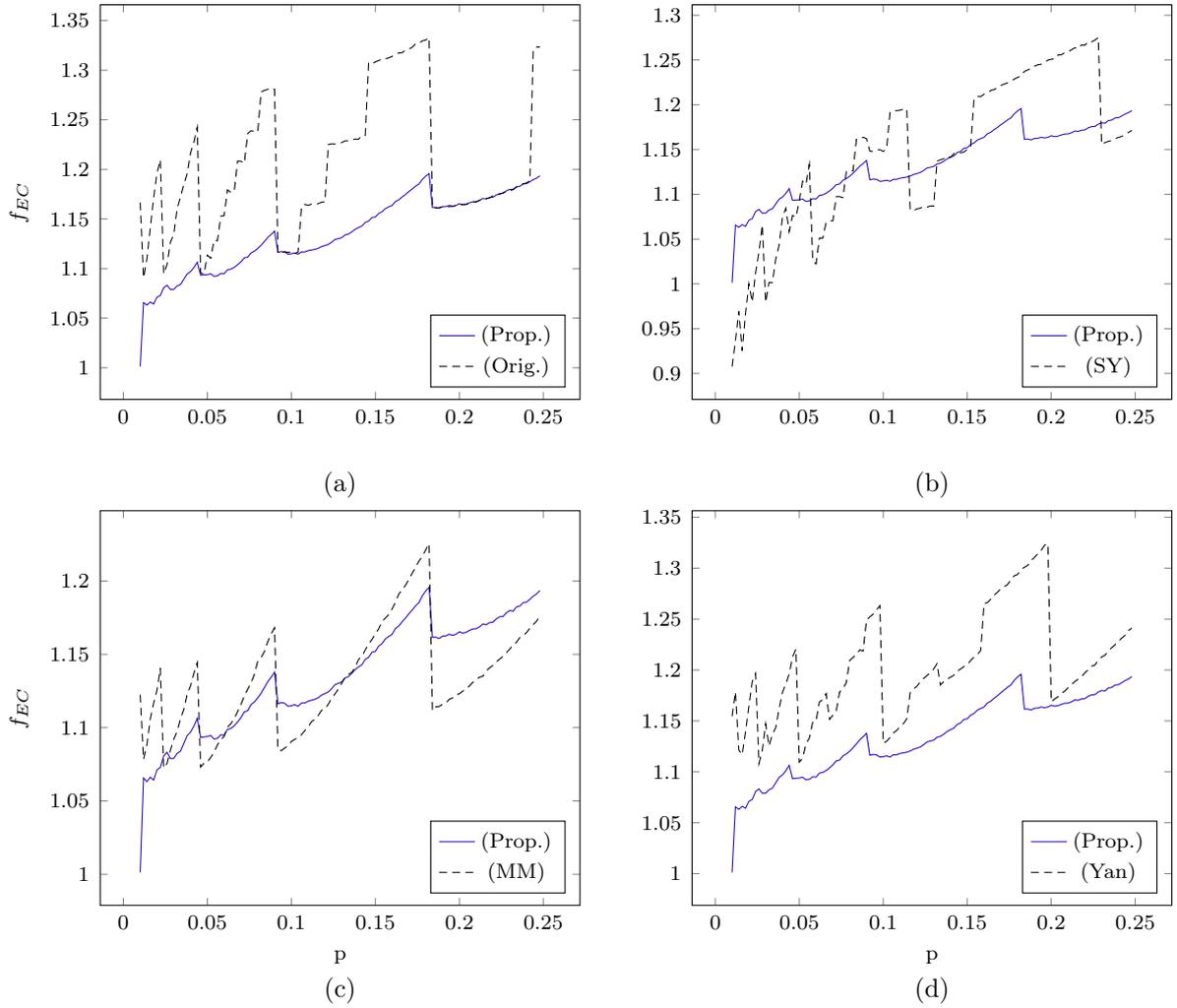
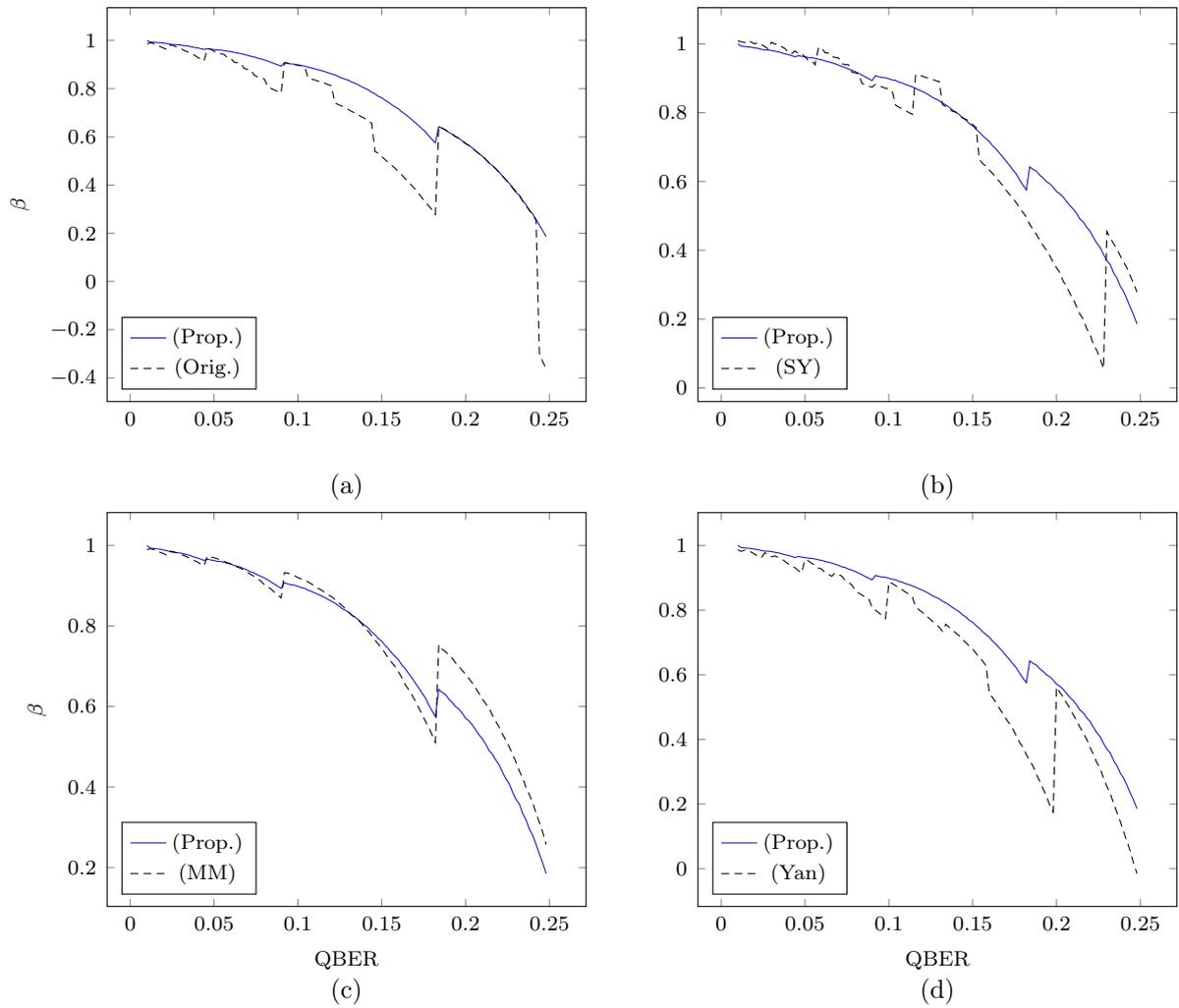
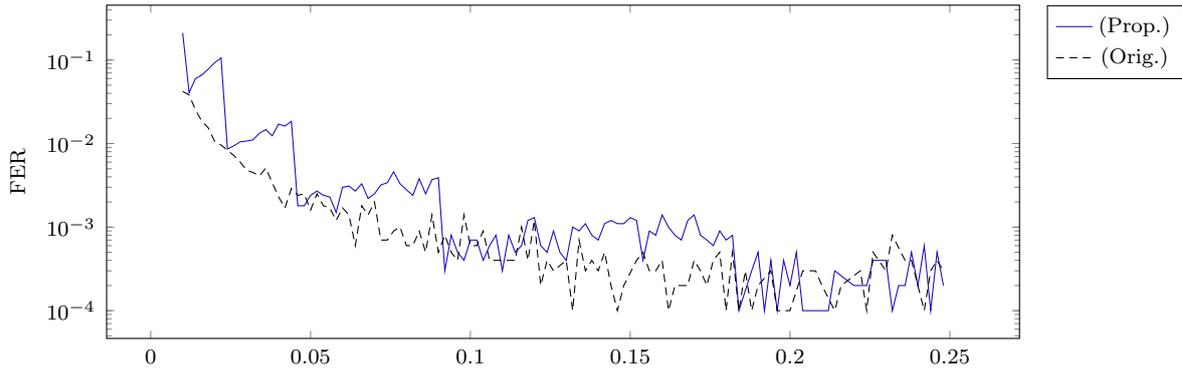


Figura 4.1 – Eficiência de reconciliação f_{EC} dos protocolos simulados.

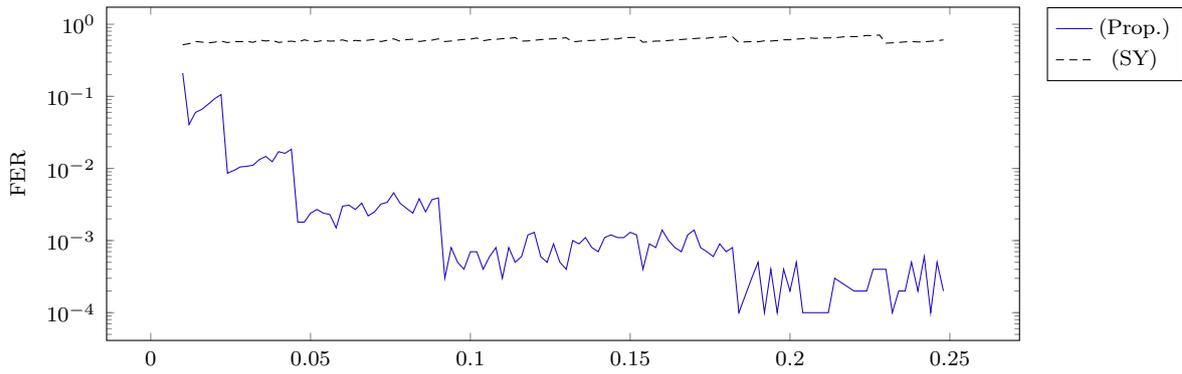
eficiência β , que indica a fração da informação mútua $I(X; Y)$ fo recuperada pelo protocolo de reconciliação quando as sequências são o resultado da transmissão por um canal BSC(p), seguindo a mesma estrutura de comparação dos resultados apresentados para f_{EC} . As conclusões tomadas a partir dos resultados apresentados na Figura (4.1) são também aplicadas para aos resultados obtidos para β , uma vez que os dois parâmetros são relacionados pela Equação (2.17). É observado nas Figuras (4.2a) e (4.2d) que nas comparações (Prop.) \times (Orig.) e (Prop.) \times (Yan) o protocolo proposto apresenta uma vantagem considerável, conseguindo valores mais elevados para β . No caso da Figura (4.2b) novamente o protocolo proposto por Sugimoto [35] aparenta competitividade em alguns valores de p mas, devido às taxas de erro residual médio e taxa de erro por quadro, os resultados se tornam invalidados. Mais uma vez, a modificação proposta por Martinez-Mateo [32] apresenta maior competitividade em relação ao protocolo proposto, sendo a diferença mais expressiva na faixa $0.184 < \text{QBER} < 0.25$.


 Figura 4.2 – Eficiência de reconciliação β

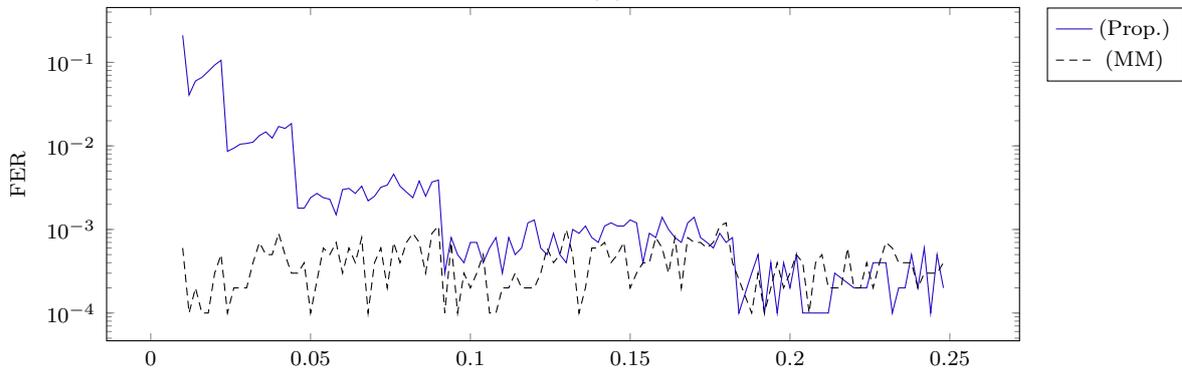
A análise para o erro residual e taxa de erro por quadro é semelhante, uma vez que para $\epsilon_R > 0$ necessariamente haverá uma taxa de erro por quadro expressiva. Com base nos resultados apresentados nas Figuras (4.3) e (4.4) é possível ver que os protocolos propostos por Sugimoto e Yan et. al. (Modif. 1 e Modif. 3, respectivamente) apresentam taxas de erro de quadro e erros residuais bem mais elevados que o protocolo proposto, sendo (SY) o protocolo que apresenta os piores valores de erro residual médio, $\epsilon_R > 1$ (Figura (4.4b)). Na comparação do protocolo proposto com o protocolo proposto e (MM), é possível ver que a implementação proposta não demonstra resultados superiores com relação ao erro residual ϵ_R e à taxa de erro por quadro. Porém, apesar do protocolo proposto não ser majoritariamente melhor, apresenta bons valores de ϵ_R e FER para $p > 0.10$ (faixa de atuação alvo do trabalho) se mantendo entre 10^{-3} e 10^{-4} . Inclusive, para (Prop.) \times (MM) e $0.10 < p < 0.184$, o protocolo proposto tem melhores resultados, com menores taxas de erro de quadro e menor erro residual.



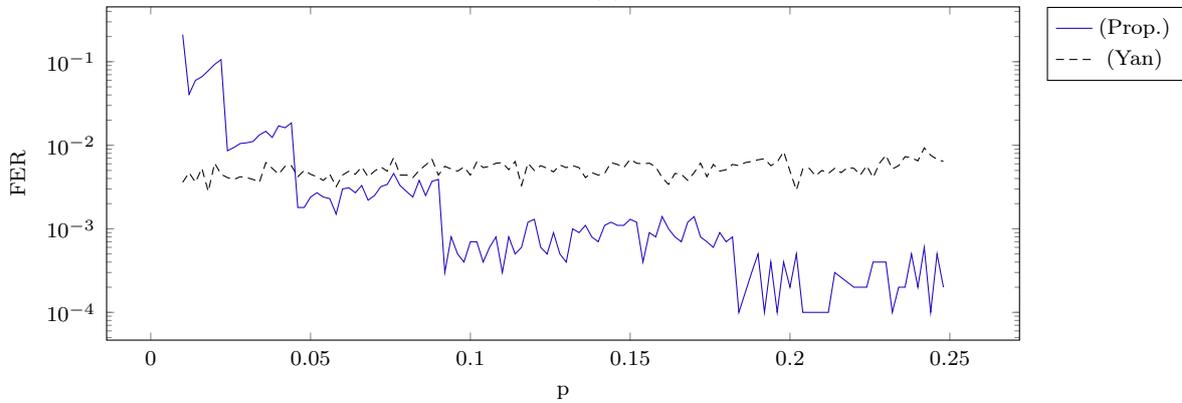
(a)



(b)

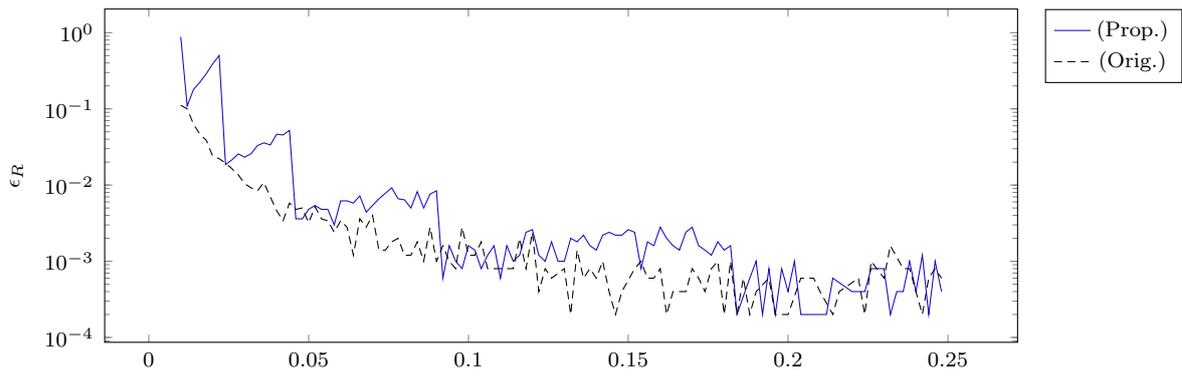


(c)

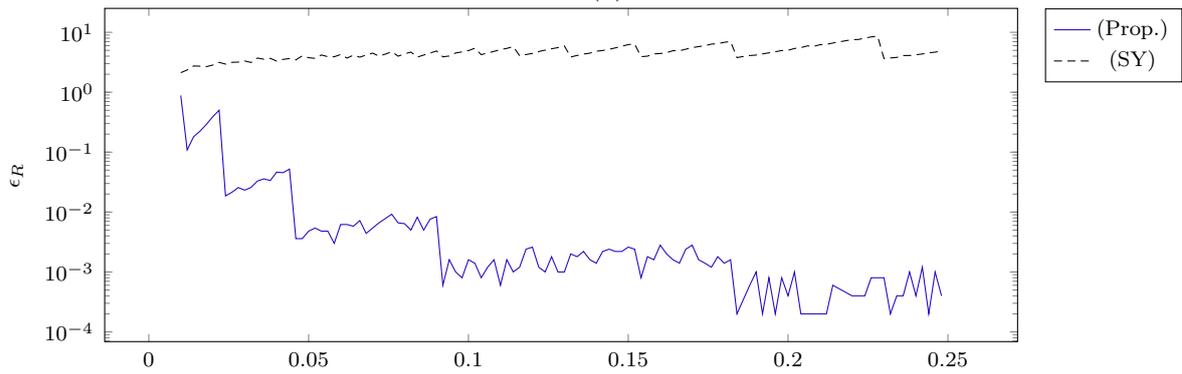


(d)

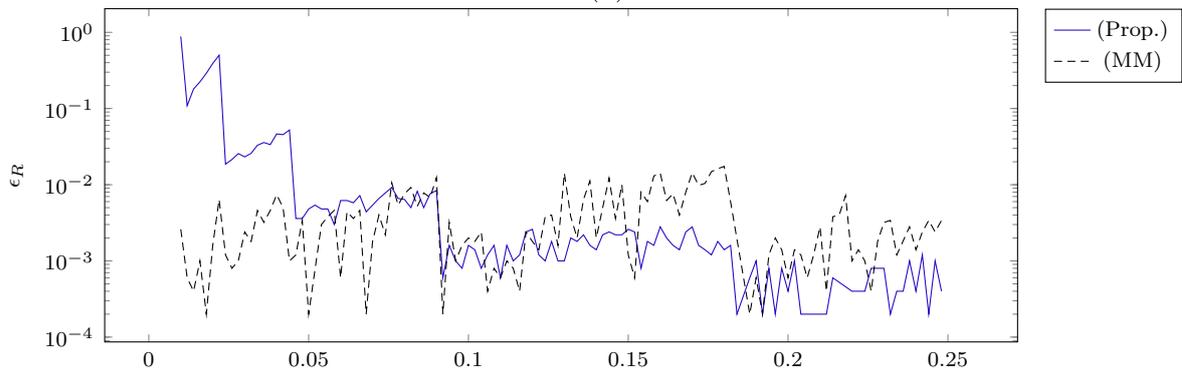
Figura 4.3 – Taxa de erro de quadro (FER)



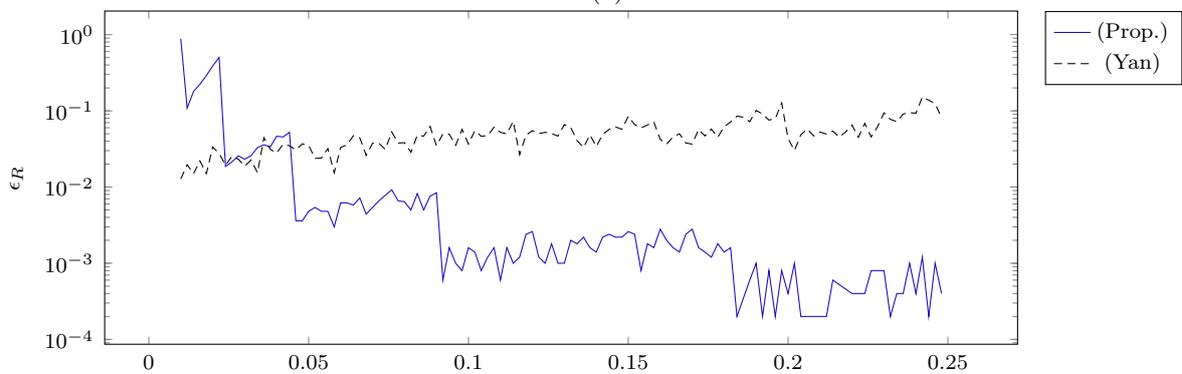
(a)



(b)



(c)



(d)

Figura 4.4 – Erro residual médio (ϵ_R)

4.2 Ganho de correlação de Chave Secreta para $p > 0.25$

No Capítulo (3) foi apresentado o desempenho do protocolo **CASCADE** e na Tabela (3) foi evidenciado que o protocolo tende a expor uma quantidade de informação que compromete a segurança da chave secreta para as taxas de erro acima de 0.25, uma vez que $\beta < 0$. Como nenhuma aplicação do protocolo **CASCADE** foi proposta para operar em tal faixa de taxa erro (inclusive, as modificações analisadas na Seção (4.1) apresentam $\beta < 0.60$ para taxas de erro de *bit* maiores que 0.20), é razoável concluir que o protocolo **CASCADE** não seja aplicável na reconciliação de chaves que apresentam tais taxas de erro por *bit*. Nesta seção é analisado o uso do protocolo **CASCADE** para gerar um ganho de correlação via reconciliação parcial das sequências. A principal solução para reconciliação de sequências com altas taxas de erro é o uso de códigos LDPC's, o qual é capaz de alcançar a capacidade do canal de comunicação para o tamanho de código adequado [37, 38, 39]. O impasse é que para canais de baixa capacidade, os LDPC's necessitam de palavras código com $n > 10^6$ [16, 14], resultando em alto custo computacional na decodificação. A reconciliação parcial consiste na correção de erros controlada pela quantidade de informação vazada durante o processo, sendo executada em uma quantidade menor de passos do que as implementações abordadas na Seção (4.1), visando diminuir as taxas de erro de *bit* presentes nas sequências para possibilitar o uso de códigos LDPC com comprimentos menores.

A ideia da reconciliação parcial é ajustar E_1 de acordo com um parâmetro arbitrário ε que irá indicar a fração de erros restantes após o primeiro passo do protocolo. Os passos subsequentes devem proceder sem modificações, dobrando o valor de k_1 a cada passo avançado e realizando buscas recursivas para cada erro corrigido nos passos $i > 1$.

A modificação proposta demanda que

$$E_1 \leq k_1 p \varepsilon, \quad (4.2)$$

e combinando as relações nas Equações (3.2) e (4.2), é obtido

$$k_1 p (1 - \varepsilon) - \frac{1 - (1 - 2p)^{k_1}}{2} \leq 0. \quad (4.3)$$

Logo, para uma taxa de erros fixa e um valor definido para ε , existe um conjunto finito de inteiros que satisfazem a Equação (4.3), sendo o maior valor utilizado para o tamanho do bloco inicial.

O processo de reconciliação com k_1 definido de acordo com as relações (4.2) e (4.3) devem corrigir uma quantidade de erros proporcionalmente ao valor do parâmetro ε defi-

nido, indicando uma correção de erros controlada no primeiro passo. O mesmo comportamento com relação à quantidade de erros corrigidos não pode ser assumido com relação aos demais passos do protocolo. Logo, tendo em vista o objetivo de modelar o comportamento do protocolo passo a passo, foram realizadas simulações de reconciliação de seqüências binárias aleatórias com uma taxa de erro por *bit* do 0.25 e $\varepsilon = \{0.80, 0.85, 0.90, 0.95\}$. O protocolo realizou quatro passos de reconciliação e os resultados são apresentados na Figura (4.5).

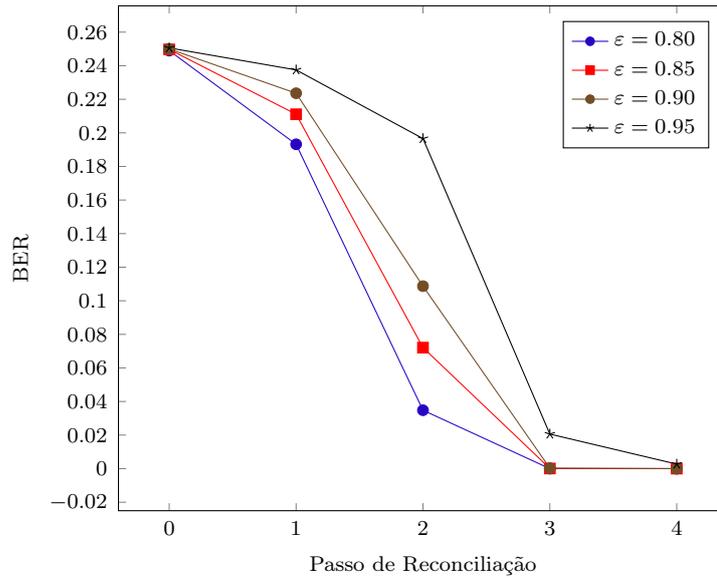


Figura 4.5 – Redução na taxa de erro por *bit* para $p = 0.25$ e diferentes valores de ε

A Figura (4.5) revela o comportamento do protocolo **CASCADE** com tamanho de bloco inicial conforme as Equações (4.2) e (4.3) e indica que durante o terceiro passo ocorre o maior vazamento de informação, devido à correção de erros ecentuada. As simulações confirmam que a utilização de k_1 de acordo como as restrições propostas irá reduzir a quantidade de erros restantes após o primeiro passo de acordo com o parâmetro ε . Outra importante característica observada dos resultados na Figura (4.5) é que, independente do valor do parâmetro ε^2 , poucos erros restam após o fim do terceiro passo de reconciliação, o que implica que nesse passo é onde se encontra a maior quantidade de informação vazada. Logo, a reconciliação com **CASCADE** visando ganho de correlação deve realizar, no máximo, dois passos de reconciliação.

Para estimar a quantidade de informação vazada durante a reconciliação, foram realizadas simulações para diferentes valores de p e ε e observadas as quantidades de

² Devido à busca recursiva realizada nos passos $i > 1$, o protocolo poderá realizar uma busca exaustiva por erros que podem ser corrigidos nos blocos dos passos anteriores para cada erro corrigido em um bloco do passo $i = 3$, resultando em uma grande quantidade de erros corrigidos ao final desse passo, conseqüentemente, uma grande quantidade de informação vazada.

Tabela 5 – Comparação do vazamento de informação durante os primeiros dois passos de reconciliação utilizando a modificação do tamanho inicial para diferentes valores de ε .

p	ε	k_1	$I(1)$	$\hat{I}(1)$	$I(2)$	$\hat{I}(2)$
0.25	0.80	9	3.996	2.986	7.498	9.801
	0.85	13	3.999	3.02	9.502	11.724
	0.90	19	4.499	3.467	15.125	15.868
	0.95	39	5,000	3.947	32.749	14.679
0.35	0.80	7	3.499	2.497	6.425	8.539
	0.85	9	3.990	2.984	2.298	11.674
	0.90	14	3.990	2.981	12.799	12.106
	0.95	28	4.499	3.486	27.749	13.233
0.45	0.80	5	3.499	2.499	6.120	8.215
	0.85	7	3.499	2.275	7.475	9.762
	0.90	11	3.999	2.994	12.899	13.691
	0.95	22	4.500	3.487	28.000	14.477

informação vazada em cada passo de reconciliação executado, conforme apresentado na Tabela (5). Foram analisados os resultados para os dois primeiros passos, sendo detalhados os valores do tamanho do bloco inicial (k_1) conforme Equação (4.3), quantidade de informação vazada estimada para cada passo ($\hat{I}(w)$) e o limitante superior de vazamento de informação ($I(w)$), conforme a Equação (3.6).

É possível observar no primeiro passo que a quantidade estimada de informação vazada permanece abaixo do limite teórico $I(1)$ para quaisquer combinações de p e ε . Para o segundo passo, o mesmo resultado não acontece em todos os cenários, onde a quantidade estimada de informação vazada fica acima do limite teórico $I(2)$ para algumas combinações de p e ε . Isso se deve ao fato de que, com as modificações do tamanho do bloco inicial propostas, as restrições presentes nas Equações (3.3) e (3.4) não são necessariamente satisfeitas, logo a estimativa da quantidade de informação vazada do segundo passo em diante presentes na Equação (3.2) não é sempre correta.

A correção de erros realizada pelo protocolo **CASCADE** pode ser interpretada como um melhoramento de canal a medida que os passos de reconciliação são executados, como exemplificado na Figura (4.6). Como no caso geral, Alice e Bob estão de posse de duas sequências binárias correlacionadas, A e B , onde uma delas deve ser modificada pelo processo de reconciliação afim de que os erros oriundos da transmissão de estados quânticos. Em ambos os casos das reconciliações direta ou reversa, uma das sequências deve permanecer não modificada, enquanto a outra irá sofrer modificações. Seja S a sequência

sofrendo alterações³, após o i -ésimo passo de reconciliação sendo representada como S^i . É evidente que a sequência S^i contém menos erros que a sequência S^{i-1} uma vez que as funções de permutação f_i aplicadas entre cada passo de reconciliação realizam a redistribuição dos bits errados ao longo das chaves, de modo que há uma baixa probabilidade de que nenhum erro existente seja corrigido. Logo, a taxa de erro por *bit* em cada passo é menor que no passo anterior.

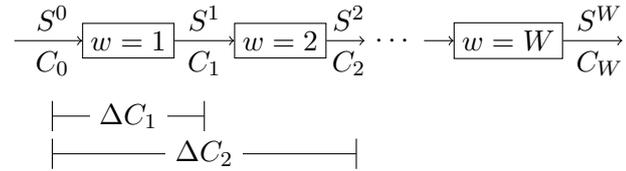


Figura 4.6 – Evolução da capacidade do canal com o protocolo CASCADE

Observando o processo de reconciliação conforme a Figura (4.6), a atuação do protocolo CASCADE resulta em um ganho de correlação entre as sequências. Em um ponto de vista da teoria da informação, se as sequências S^i podem ser interpretadas como o resultado de uma transmissão através de um canal BSC(p), cuja capacidade é conhecida (vide Apêndice (C.2)), qualquer código corretor de erro utilizado para reconciliação terá sua taxa limitada superiormente pela capacidade do canal de comunicação [30]. Logo, com o uso do protocolo CASCADE, a taxa de erro por *bit* entre as sequências devem decrescer conforme os passos são executados, implicando em um melhoramento na capacidade do canal de comunicação, no sentido de que a máxima taxa possível de um código é aumentada. Desta forma, a “capacidade do canal” obtida a partir das sequências após o i -ésimo passo é indicado por C_i , sendo C_0 a capacidade antes do processo de reconciliação, e a quantidade

$$\Delta C_i = C_i - C_0 \quad (4.4)$$

é definida como ganho de capacidade do canal após executado o i -ésimo passo de reconciliação. Os termos ganho de correlação e ganho de capacidade serão utilizados de forma intercambiável.

4.2.1 Resultados

Para simulação, será considerada a transmissão de estados coerentes por um protocolo CVQKD, permitindo modelar o canal como um canal aditivo de ruído gaussiano branco (*Additive White Gaussian Noise Channel*, AWGN). O experimentos realizados seguiram a metodologia da expansão binária de realizações de variáveis aleatórias, conforme

³ $S = B$ para o caso de reconciliação direta, $S = A$ para reconciliação reversa.

Tabela 6 – Ganho de capacidade para os dois primeiros passos de reconciliação apresentados na Tabela (5)

p	ε	C_1	C_2	ΔC_1	ΔC_2
0.25	0.80	0.292	0.782	0.111	0.601
	0.85	0.256	0.626	0.075	0.445
	0.90	0.233	0.504	0.052	0.323
	0.95	0.209	0.285	0.028	0.104
0.35	0.80	0.147	0.722	0.081	0.656
	0.85	0.128	0.567	0.062	0.501
	0.90	0.102	0.333	0.035	0.267
	0.95	0.082	0.155	0.016	0.089
0.45	0.80	0.066	0.706	0.059	0.699
	0.85	0.043	0.512	0.036	0.505
	0.90	0.027	0.272	0.019	0.265
	0.95	0.015	0.076	0.008	0.068

a Seção (2.3.1), tendo uma variável aleatória gaussiana X transmitida por um canal cuja saída é a variável aleatória Y . Ao obter a função $F(\cdot)$ para cada realização dos valores recebidos, as variáveis contínuas são expandidas de acordo com a Equação (2.12), garantindo que cada *bit* da expansão configure um BSC. Cada canal na expansão foi tratado individualmente, e simulações de reconciliação parcial com o protocolo **CASCADE** foram realizadas usando $0.75 \leq \varepsilon \leq 0.95$. Os experimentos operaram com SNR igual a 5dB e foi aplicada uma expansão binária de quatro *bits*, resultando em seqüências com taxas de erro de *bit* iguais a 0.1637, 0.3538, 0.4369, 0.4708 e as respectivas capacidades de canal (C_0) iguais a 0.357, 0.062, 0.011, 0.002, respectivamente. Os resultados obtidos para informação vazada e ganho de correlação são apresentados nas Tabela (7), respectivamente.

Com relação ao vazamento de informação, o primeiro *bit* da expansão binária (F^1 com $p = 0.1637$), apresenta a situação que é possível realizar a reconciliação completa, conforme abordado na Seção (4.1), apresentando os parâmetros de eficiência $f_{EC} = 1.169$ e $\beta = 0.694$ para o protocolo proposto na Seção anterior. No caso da aplicação de uma reconciliação parcial, o protocolo executou dois passos de reconciliação e a quantidade de informação vazada se manteve menor que o tamanho da chave. Dentre todos os valores de ε utilizados, o melhor resultado foi obtido para $\varepsilon = 0.75$ e dois passos de reconciliação, quando foram vazados 9 *bits* de informação por bloco de 12 *bits*, obtendo um ganho de capacidade $\Delta C_2 = 0.502$, o maior nessa categoria.

O segundo *bit*, F^2 , apresentou resultados bastante similares aos apresentados nas Tabelas (5) e (6) para $p = 0.35$. Os valores aplicáveis de ε para a reconciliação parcial com dois passos executada pelo protocolo **CASCADE** se encaixam no intervalo $[0.90, 0.95]$,

uma vez que para $\varepsilon < 0.90$ a reconciliação parcial resultou em $\hat{I}(2) > k_1$, tornando a chave inutilizável. Por outro lado, os resultados apresentados na Tabela (7) incluem $\varepsilon = 0.75$, fazendo $k_1 = 5$ e vazando 2.5 *bits* no primeiro passo e obtendo $\Delta C_1 = 0.120$. Este resultado é mais eficiente se comparado a usar $\varepsilon = 0.95$, quando $k_1 = 28$, $\hat{I}(2) = 13.658$ e $\Delta C_2 = 0.09$.

Para F^3 e F^4 , as taxas de erro de *bit* são extremamente altas (0.4369 e 0.4768, respectivamente), forçando ε assumir valores acima de 0.95 (possivelmente valores entre 0.90 e 0.95 poderiam resultar em vazamentos de informação admissíveis). Ambos os cenários se comportam de forma similar, o que implica que a reconciliação parcial se comporta de maneira também similar em cenários cujas taxas de erro de *bit* sejam maiores que 0.40. O melhor ganho de correlação foi obtido para a reconciliação parcial executando um passo de reconciliação e $\varepsilon = 0.75$, onde $\hat{I}(1) = 1.99$ e $\Delta C_1 = 0.093$ e $\Delta C_1 = 0.063$ para F^3 e F^4 , respectivamente.

Tabela 7 – Comparação de informação vazada e ganho de correlação para dois passos de reconciliação parcial na chaves geradas por expansão binária.

p	ε	k_1	$I(1)$	$\hat{I}(1)$	$I(2)$	$\hat{I}(2)$	C_1	C_2	ΔC_1	ΔC_2
0.1637	0.75	12	3.983	2.997	6.92	9.019	0.465	0.859	0.107	0.502
	0.80	15	3.995	2.994	7.908	10.18	0.441	0.793	0.085	0.436
	0.85	20	4.499	3.519	11.435	12.052	0.420	0.65	0.062	0.292
	0.90	30	4.500	3.532	15.527	13.228	0.399	0.563	0.042	0.206
	0.95	61	5.000	4.149	33.457	24.036	0.376	0.502	0.021	0.146
0.3538	0.75	5	3.497	2.498	5.402	7.102	0.182	0.865	0.120	0.803
	0.80	7	3.500	2.510	6.465	8.652	0.141	0.700	0.078	0.638
	0.85	9	4.000	3.009	9.368	11.730	0.122	0.557	0.059	0.494
	0.90	14	4.000	3.005	12.906	12.061	0.099	0.316	0.035	0.253
	0.95	28	4.500	3.512	28.016	13.658	0.079	0.153	0.017	0.090
0.4369	0.75	4	3.000	1.998	4.247	5.439	0.104	0.866	0.093	0.855
	0.80	5	3.500	2.497	6.027	8.067	0.078	0.726	0.067	0.714
	0.85	7	3.500	2.503	7.337	9.626	0.053	0.537	0.041	0.525
	0.90	11	4.000	3.002	12.612	13.299	0.034	0.299	0.023	0.288
	0.95	22	4.500	3.553	27.280	14.607	0.021	0.088	0.010	0.076
0.4768	0.75	4	3.000	1.997	4.407	5.758	0.064	0.817	0.063	0.816
	0.80	5	3.500	2.499	6.326	8.412	0.044	0.650	0.043	0.649
	0.85	6	3.500	2.499	7.041	9.463	0.033	0.588	0.032	0.586
	0.90	10	4.000	3.003	12.536	11.806	0.015	0.207	0.014	0.206
	0.95	20	4.500	3.499	27.090	13.493	0.007	0.055	0.005	0.053

Capítulo 5

Conclusões

O trabalho de projetar protocolos de reconciliação de chave secreta é uma das partes fundamentais da implementação de um protocolo de distribuição de chaves eficiente. O surgimento de protocolos CVQKD trouxe a vantagem operacional de utilização de equipamentos tradicionais de comunicações ópticas e a necessidade de soluções de reconciliações de chaves com taxas de erro por *bit* elevadas. Nesta dissertação foram propostas duas soluções para reconciliação de chaves geradas por protocolos CVQKD, sendo aplicadas em duas faixas de taxa de erro de *bit* diferentes.

A reconciliação completa, proposta para chaves com $p < 0.25$, contou com uma modificação no tamanho do bloco inicial (com relação à implementação original do **CASCADE**) de modo que a quantidade de informação vazada durante o processo de reconciliação fosse reduzida, mantendo o número de passos de reconciliação executados e a forma de evolução do tamanho do bloco k_i durante a reconciliação. Os resultados apresentados na Seção (4.1.1) mostraram que a modificação proposta no tamanho do bloco inicial resultou em uma melhor eficiência de reconciliação quando comparado ao protocolo original ($f_{ECorig} > f_{ECprop}$ e $\beta^{orig} < \beta^{prop}$, e se mantendo aceitável quando analisadas as taxas de erro por quadro e o erro residual médio. A comparação com o protocolo proposto em [32] é onde pode ser observado um comportamento mais parecido, principalmente pelo tamanho do bloco inicial ser o mesmo, diferindo na quantidade de passos de reconciliação realizados e na forma de evolução do tamanho do bloco k_i durante a reconciliação, mas ainda tendo desempenho superior para algumas faixas de taxa de erro. Na comparação com a modificação proposta em [36] o protocolo proposto apresentou melhor eficiência em toda os testes realizados.

A segunda modificação proposta foi a realização de uma reconciliação parcial de chaves que apresentam $p > 0.25$, para uma posterior reconciliação final utilizando LDPC's, por exemplo. Neste contexto, a utilização do protocolo **CASCADE** realizando a reconcilia-

ção completa vazava uma quantidade de informação que compromete a segurança da chave. A reconciliação parcial, além de utilizar tamanhos de bloco diferentes da implementação original, executa uma menor quantidade de passos de reconciliação, de modo que a quantidade de erros corrigidos seja controlada pela escolha do tamanho do bloco inicial, bem como a quantidade de informação vazada. Os resultados apresentados na Seção (4.2.1) mostram que o método proposto consegue realizar a correção de erros com controle da informação vazada, o que resulta em um ganho de capacidade entre as sequências. Como consequência, é possível diminuir o tamanho do comprimento do código LDPC que concluirá a reconciliação. Trabalhos futuros incluem a análise da redução do tamanho do comprimento do código LDPC utilizado na segunda fase da reconciliação parcial e estimando a redução do custo computacional para reconciliação das sequências.

Referências Bibliográficas

- 1 BENATTI, F. et al. (Ed.). *Quantum Information, Computation and Cryptography*. [S.l.]: Springer Berlin Heidelberg, 2010. Citado na página 14.
- 2 RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, ACM, New York, NY, USA, v. 21, n. 2, p. 120–126, fev. 1978. ISSN 0001-0782. Citado na página 15.
- 3 DIFFIE, W.; HELLMAN, M. New directions in cryptography. *IEEE Transactions on Information Theory*, Institute of Electrical and Electronics Engineers (IEEE), v. 22, n. 6, p. 644–654, nov 1976. Citado na página 15.
- 4 BENNETT, C. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, Elsevier BV, v. 560, p. 7–11, dec 2014. Citado nas páginas 15, 18, 19 e 39.
- 5 BENNETT, C. et al. Experimental quantum cryptography. *Journal of Cryptology*, Springer Nature, v. 5, n. 1, 1992. Citado nas páginas 15 e 30.
- 6 SHOR, P. W.; PRESKILL, J. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, American Physical Society (APS), v. 85, n. 2, p. 441–444, jul 2000. Citado na página 15.
- 7 LO, H.-K.; CHAU, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, American Association for the Advancement of Science (AAAS), v. 283, n. 5410, p. 2050–2056, mar 1999. Citado na página 15.
- 8 MAYERS, D. Unconditional security in quantum cryptography. *Journal of the ACM*, Association for Computing Machinery (ACM), v. 48, n. 3, p. 351–406, may 2001. Citado na página 15.
- 9 ASSCHE, G. V.; CARDINAL, J.; CERF, N. J. Reconciliation of a quantum-distributed gaussian key. *IEEE Transactions on Information Theory*, v. 50, n. 2, p. 394–400, fev. 2004. ISSN 0018-9448. Citado nas páginas 16, 23 e 25.
- 10 ARAÚJO, L. M. C.; ASSIS, F. M.; ALBERT, B. B. Novo protocolo de reconciliação de chaves secretas geradas quanticamente utilizando códigos LDPC no sentido Slepian-Wolf. In: *Simpósio Brasileiro de Telecomunicações e Processamento de Sinais*. [S.l.: s.n.], 2018. Citado nas páginas 16 e 25.

- 11 BRASSARD, G.; SALVAIL, L. Secret-key reconciliation by public discussion. In: *Advances in Cryptology – EUROCRYPT '93*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994. p. 410–423. ISSN 978-3-540-48285-7. Citado nas páginas 16, 30, 34, 35, 36, 39 e 40.
- 12 LODEWYCK, J. et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A*, American Physical Society, v. 76, n. 4, p. 042305, out. 2007. Citado nas páginas 16 e 23.
- 13 LEVERRIER, A. et al. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A*, American Physical Society, v. 77, n. 4, p. 042325, abr. 2008. Citado na página 16.
- 14 JOUGUET, P.; ELKOUSS, D.; KUNZ-JACQUES, S. High-bit-rate continuous-variable quantum key distribution. *Phys. Rev. A*, American Physical Society, v. 90, n. 4, p. 042329, out. 2014. Citado nas páginas 16, 23, 24 e 45.
- 15 JOUGUET, P.; KUNZ-JACQUES, S.; LEVERRIER, A. Long-distance continuous-variable quantum key distribution with a gaussian modulation. *Phys. Rev. A*, American Physical Society, v. 84, n. 6, p. 062317, dez. 2011. Citado na página 16.
- 16 BAI, Z.; YANG, S.; LI, Y. High-efficiency reconciliation for continuous variable quantum key distribution. *Japanese Journal of Applied Physics*, Japan Society of Applied Physics, v. 56, n. 4, p. 044401, mar 2017. Citado nas páginas 16 e 45.
- 17 KOLLMITZER, C.; PIVK, M. (Ed.). *Applied Quantum Cryptography*. Springer Berlin Heidelberg, 2010. ISBN 3642048293. Disponível em: <https://www.ebook.de/de/product/9271403/applied_quantum_cryptography.html>. Citado nas páginas 18, 21 e 22.
- 18 XU, H. et al. 1310-nm quantum key distribution system with up-conversion pump wavelength at 1550 nm. *Optics Express*, The Optical Society, v. 15, n. 12, p. 7247, 2007. Citado na página 20.
- 19 FURUSAWA, A. Unconditional quantum teleportation. *Science*, American Association for the Advancement of Science (AAAS), v. 282, n. 5389, p. 706–709, oct 1998. Citado na página 22.
- 20 CERF, N. J.; IPE, A.; ROTTENBERG, X. Cloning of continuous quantum variables. *Physical Review Letters*, American Physical Society (APS), v. 85, n. 8, p. 1754–1757, aug 2000. Citado na página 22.
- 21 GROSSHANS, F.; GRANGIER, P. Quantum cloning and teleportation criteria for continuous quantum variables. *Physical Review A*, American Physical Society (APS), v. 64, n. 1, jun 2001. Citado na página 22.
- 22 REID, M. D. Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations. *Physical Review A*, American Physical Society (APS), v. 62, n. 6, nov 2000. Citado na página 22.

- 23 RALPH, T. C. Continuous variable quantum cryptography. *Physical Review A*, American Physical Society (APS), v. 61, n. 1, dec 1999. Citado na página 22.
- 24 Laudenbach, F. et al. Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator. *ArXiv e-prints*, dez. 2017. Citado na página 22.
- 25 MARIE, A.; ALLÉAUME, R. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Physical Review A*, American Physical Society, v. 95, n. 1, p. 012316, jan. 2017. Citado na página 22.
- 26 SOH, D. B. et al. Self-referenced continuous-variable quantum key distribution protocol. *Physical Review X*, American Physical Society (APS), v. 5, n. 4, oct 2015. Citado na página 22.
- 27 GROSSHANS, F.; GRANGIER, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, American Physical Society, v. 88, p. 057902, Jan 2002. Citado na página 22.
- 28 GROSSHANS, F. et al. Quantum key distribution using gaussian-modulated coherent states. *Nature*, Macmillian Magazines Ltd., v. 421, p. 238, jan. 2003. Citado na página 22.
- 29 SHANNON, C. E. Analogue of the vernam system for continuous time SeriesBell laboratories memorandum, may 10, 1943. *SeriesBell Laboratories Memorandum*, IEEE, 1943. Citado na página 24.
- 30 COVER, J. A. T. T. M. *Elements of Information Theory*. [S.l.]: Wiley John + Sons, 2006. ISBN 0471241954. Citado nas páginas 26 e 48.
- 31 SLEPIAN, D.; WOLF, J. Noiseless coding of correlated information sources. *IEEE Transactions on Information Theory*, Institute of Electrical and Electronics Engineers (IEEE), v. 19, n. 4, p. 471–480, jul 1973. Citado na página 28.
- 32 MARTINEZ-MATEO, J. et al. Demystifying the information reconciliation protocol cascade. *Quantum Info. Comput.*, Rinton Press, Incorporated, Paramus, NJ, v. 15, n. 5-6, p. 453–477, abr. 2015. ISSN 1533-7146. Citado nas páginas 28, 31, 38, 39, 40, 41 e 51.
- 33 BELLOT, P.; DANG, M. D. Bb84 implementation and computer reality. In: *2009 IEEE-RIVF International Conference on Computing and Communication Technologies*. [S.l.: s.n.], 2008. p. 1–8. Citado nas páginas 38 e 39.
- 34 Brochmann Pedersen, T.; Toyran, M. High Performance Information Reconciliation for QKD with CASCADE. *ArXiv e-prints*, jul. 2013. Citado na página 38.
- 35 SUGIMOTO, T.; YAMAZAKI, K. A study on secret key reconciliation protocol "cascade". *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, E83-A, n. 10, p. 1987–1991, 2000. Citado nas páginas 39, 40 e 41.

- 36 YAN, H. et al. Information reconciliation protocol in quantum key distribution system. In: *2008 Fourth International Conference on Natural Computation*. [S.l.]: IEEE, 2008. Citado nas páginas 39, 40 e 51.
- 37 GALLAGER, R. Low-density parity-check codes. *IEEE Transactions on Information Theory*, Institute of Electrical and Electronics Engineers (IEEE), v. 8, n. 1, p. 21–28, jan 1962. Citado na página 45.
- 38 GALLAGER, R. G. *Low-Density Parity-Check Codes*. 1963. Citado na página 45.
- 39 RICHARDSON, T.; URBANKE, R. Efficient encoding of low-density parity-check codes. *IEEE Transactions on Information Theory*, Institute of Electrical and Electronics Engineers (IEEE), v. 47, n. 2, p. 638–656, 2001. Citado na página 45.
- 40 LEONHARDT, U. *Essential Quantum Optics: From Quantum Measurements to Black Holes*. [S.l.]: CAMBRIDGE UNIV PR, 2010. ISBN 0521869781. Citado nas páginas 60, 64 e 68.
- 41 NASCIMENTO, E. J. do. *Mapas de Shannon-Kotel'nikov na Distribuição Quântica de Chaves com Variáveis Contínuas*. Tese (Doutorado) — Universidade Federal de Campina Grande, 2017. Citado na página 67.
- 42 GERRY, C.; KNIGHT, P. *Introductory Quantum Optics*. [S.l.]: Cambridge University Press, 2004. ISBN 9780521820356. Citado nas páginas 68 e 69.
- 43 SHANNON, C. E. A mathematical theory of communication. *Bell System Technical Journal*, Institute of Electrical and Electronics Engineers (IEEE), v. 27, n. 3, p. 379–423, jul 1948. Citado na página 71.
- 44 NIELSEN, I. L. C. M. A. *Quantum Computation and Quantum Information*. [S.l.]: Cambridge University Pr., 2001. ISBN 1107002176. Citado na página 74.

Apêndice A

Postulados da mecânica quântica

Postulado A.1 (Espaço de estados) *Para qualquer sistema físico isolado existe um espaço vetorial com produto interno (um espaço de Hilbert) chamado de espaço de estados do sistema. O sistema é completamente descrito por um vetor de estados que é unitário no espaço de estados do sistema.*

Um sistema físico de grande interesse é o *qubit*, definido em um espaço de Hilbert bidimensional, sendo o sistema da mecânica quântica o mais simples possível. Utilizando a notação de Dirac e sendo $|0\rangle$ e $|1\rangle$ uma base ortonormal para o espaço de estados, um estado qualquer deste espaço pode ser escrito como

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (\text{A.1})$$

onde $\alpha, \beta \in \mathbb{C}$. Atendendo à unicidade do vetor de estados, $|\alpha|^2 + |\beta|^2 = 1$. O estado representado pela equação A.1 encontra-se em superposição (combinação linear de uma base ortonormal). Os estados $|0\rangle$ e $|1\rangle$ são ditos estados puros. O conjugado hermitiano (transposto conjugado) de $|\psi\rangle$ é representado por $\langle\psi|$. Logo, o produto interno entre vetores é representado por $\langle\psi_1|\psi_2\rangle$.

Uma representação conveniente de estados quânticos é a representação por operadores de densidade. Eles se mostram úteis quando os estados da composição do sistema não são completamente conhecidos (o que pode ser consequência das incertezas da preparação). O operador de densidade ρ é definido como uma combinação dos possíveis estados quânticos $|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_N\rangle$ associados às probabilidades p_1, p_2, \dots, p_N ($\sum_p p_i = 1$) do sistema estar no estado i , de modo que

$$\rho = \sum_{i=1}^N p_i |\psi_i\rangle \langle\psi_i|. \quad (\text{A.2})$$

Quando o estado do sistema é puro, $\rho = |\psi\rangle\langle\psi|$.

Postulado A.2 (Evolução do sistema quântico) *A evolução de um sistema quântico fechado é descrita por um operador unitário de transformação. Ou seja, um estado $|\psi\rangle$ no tempo t_1 evolui para o estado $|\psi'\rangle$ no tempo t_2 através do operador unitário U , de modo que*

$$|\psi'\rangle = U |\psi\rangle. \quad (\text{A.3})$$

Algumas matrizes apresentam utilização recorrente, uma vez que apresentam comportamentos de portas quânticas análogas ao modelo clássico. As matrizes de Pauli representam operações como a porta quântica *NOT* (matriz X) e a matriz Z a inversão de fase.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \quad (\text{A.4})$$

Postulado A.3 (Medição) *Medidas quânticas são descritas por uma coleção de operadores de medição M_m que agem no espaço de estados do sistema a ser medido, onde o índice m se refere à possível saída do experimento.*

Para um sistema quântico que se encontra no estado $|\psi\rangle$ imediatamente antes da medição, a probabilidade de que seja obtido o resultado m é dado pela expressão

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle \quad (\text{A.5})$$

e o sistema após a medida colapsa para o estado

$$|\psi\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}. \quad (\text{A.6})$$

Os operadores de medição precisam satisfazer a relação de completude,

$$\sum_m M_m^\dagger M_m = I. \quad (\text{A.7})$$

Na Equação A.7, é garantido que a soma das probabilidades dos resultados das medições realizadas seja igual a um.

Postulado A.4 (Sistemas compostos) *O espaço de estados de um sistema quântico composto é representado pelo produto tensorial do espaço de estados de cada componente físico do sistema. Em outras palavras, para n sistemas onde o i -ésimo sistema é preparado no estado $|\psi\rangle_i$, o sistema composto total é $|\psi_1\rangle \otimes |\psi_2\rangle \cdots |\psi_n\rangle$.*

Sistemas quânticos apresentam a possibilidade de criar correlações não locais a partir de interações entre os sistemas isolados, o que não é possível realizar em sistemas clássicos. Tal correlação é chamada de emaranhamento. Um estado $|\psi\rangle$ pertencente ao sistema composto $\mathcal{H}_A \otimes \mathcal{H}_B$ é dito emaranhado caso não possa ser escrito como o produto tensorial de estados pertencentes aos sistemas isolados \mathcal{H}_A e \mathcal{H}_B .

Apêndice B

Eletromagnetismo Quântico

B.1 Quantização de Campo Eletromagnético

A base da óptica quântica decai sobre a quantização dos campos eletromagnéticos, e esta parte da descrição clássica das equações de Maxwell. A associação entre campos clássicos e observáveis quânticos é o ponto de partida da descrição quântica de campos eletromagnéticos, juntamente com as relações de comutação entre observáveis. O desenvolvimento a seguir parte da abordagem adotada em [40].

Como visto no Apêndice (A), o estado de sistema quântico é representado por um vetor de estados $|\psi\rangle$ ou pela matriz de densidade ρ . Na representação de Heisenberg, os operadores quânticos evoluem com o tempo mas os estados não mudam. Na observação da luz como um campo os observáveis são funções do espaço e do tempo.

As equações de maxwell na forma macroscópica são na seguinte forma:

$$\nabla \cdot \mathbb{B} = 0, \tag{B.1}$$

$$\nabla \times \mathbb{E} = -\frac{\partial \mathbb{B}}{\partial t}, \tag{B.2}$$

$$\nabla \cdot \mathbb{D} = 0, \tag{B.3}$$

$$\nabla \times \mathbb{H} = \frac{\partial \mathbb{D}}{\partial t}. \tag{B.4}$$

Sendo \mathbb{B} a indução magnética. \mathbb{H} o campo magnético, \mathbb{D} o deslocamento elétrico e \mathbb{E} o campo elétrico, as Equações B.1 a B.4 satisfazem a condição de contorno de que os campos desvanecem no infinito. A quantização dos campos eletromagnéticos clássicos parte da ideia de que estes podem ser encarados como o valor esperado dos respectivos observáveis quânticos $\hat{\mathbb{E}}$, $\hat{\mathbb{D}}$, $\hat{\mathbb{B}}$ e $\hat{\mathbb{H}}$, sendo, por exemplo, \mathbb{E} igual a $\langle \psi | \hat{\mathbb{E}} | \psi \rangle$, o valor médio do operador $\hat{\mathbb{E}}$. Assumindo isto, segue-se que os campos quânticos obedecem as

equações de Maxwell da mesma forma. A fundação dessa afirmação está na linearidade das Equações B.1 a B.4. Assim, os campos clássicos podem ser substituídos pelos respectivos operadores quânticos e suas médias ainda irão satisfazer as equações de Maxwell.

Os campos \mathbb{B} , \mathbb{H} , \mathbb{D} e \mathbb{E} estão relacionados pelo conjunto de equações lineares conhecidas como *equações constitutivas*, representando a resposta do meio à aplicação dos campos eletromagnéticos. Devido sua linearidade, os campos quânticos obedecem às mesmas relações. Para um meio isotrópico, não dispersivos, com resposta linear e não absorvente, as equações constitutivas estão descritas em B.5:

$$\mathbb{D} = \varepsilon_o \varepsilon \mathbb{E}, \quad \hat{\mathbb{B}} = \mu_o \mu \mathbb{H}, \quad \varepsilon_o \mu_o = c^{-2}, \quad (\text{B.5})$$

onde ε_o e μ_o representam a permissividade e a permeabilidade do vácuo, respectivamente, sendo c a velocidade da luz no vácuo.

Assim como em eletrodinâmica, é conveniente representar os campos em termos de um vetor potencial onde, para eletromagnetismo quântico, tem-se o operador potencial $\hat{\mathbb{A}}$:

$$\hat{\mathbb{E}} = -\frac{\partial \hat{\mathbb{A}}}{\partial t}, \quad (\text{B.6})$$

$$\hat{\mathbb{B}} = \nabla \times \hat{\mathbb{A}}, \quad (\text{B.7})$$

$$\nabla \cdot \varepsilon \mathbb{A} = 0. \quad (\text{B.8})$$

As Equações B.6 e B.7 satisfazem automaticamente as duas primeiras equações de Maxwell, enquanto a terceira equação (Equação B.8, condição Calibre de Gauge) contribui na resolução da terceira equação de Maxwell, uma vez que $\nabla \cdot \hat{\mathbb{D}}$ vai a zero, como consequência das equações constitutivas, restando a ultima equação como não trivial. Aplicando as Equações B.6 e B.7 em B.4 e utilizando as relações constitutivas em B.5, é obtido o seguinte resultado:

$$\frac{1}{\mu \varepsilon} \nabla^2 \hat{\mathbb{A}} - \frac{1}{c^2} \frac{\partial^2 \hat{\mathbb{A}}}{\partial t^2} = 0. \quad (\text{B.9})$$

A Equação B.9 é dita *equação de onda eletromagnética*, representando o comportamento dos campos clássicos e quânticos.

A evolução temporal dos operadores de campo pode ser também descrita através das equações de movimento de Heisenberg, especificando as relações entre o Hamiltoniano

do sistema e as relações de comutação. Fazendo uso do Postulado A.2, o Hamiltoniano indica a evolução temporal de uma quantidade física \hat{F} , também descrevendo a energia total do sistema.

Assumindo que o Hamiltoniano da luz preserva a estrutura de energia de campos eletromagnéticos clássicos e fazendo uso das equações de Maxwell e as equações constitutivas, é possível obter

$$\hat{H} = \frac{1}{2} \int (\hat{\mathbb{E}} \cdot \hat{\mathbb{D}} + \hat{\mathbb{B}} \cdot \hat{\mathbb{H}}) dV = \int \left(\frac{\hat{\mathbb{D}}^2}{2\varepsilon_0\varepsilon} + \frac{\varepsilon_0 c^2}{2\mu} (\nabla \times \hat{\mathbb{A}})^2 \right) dV, \quad (\text{B.10})$$

integrando sobre todo o espaço.

B.1.1 Modos Normais

O conjunto de soluções para a Equação B.9 é composto por funções complexas, incluindo seus conjugados. Para o caso clássico, Se \mathbb{A}_k forma um conjunto de soluções, \mathbb{A}_k^* também será. As ondas planas do tipo $A \exp(i\mathbf{k} \cdot \mathbf{r} - i\omega t)$ formam um conjunto completo de soluções. Logo, as soluções da Equação B.9 podem ser expandidas na forma

$$\hat{\mathbb{A}}(\mathbf{r}, t) = \sum_k \left(\mathbb{A}_k(\mathbf{r}, t) \hat{a}_k + \mathbb{A}_k^*(\mathbf{r}, t) \hat{a}_k^\dagger \right). \quad (\text{B.11})$$

Na expansão em B.11, \mathbf{r} e t indicam a posição no espaço e o instante de tempo, respectivamente. Os termos \hat{a}_k e \hat{a}_k^\dagger são os operadores onde estão contidas as propriedades quânticas do campo expandido e são chamados de operadores de *criação* e *aniquilação* (\hat{a}_k^\dagger é o conjugado hermitiano de \hat{a}_k). As funções $\mathbb{A}_k(\mathbf{r}, t)$ são as funções de modo da expansão, cujo índice k indica o número de onda e a polarização dos campos.

Os modos $\mathbb{A}_k(\mathbf{r}, t)$ podem ser escolhidos livremente, desde que componham um conjunto completo de soluções para as formulações obtidas na seção anterior. Porém, afim de que as relações de comutação entre os operadores \hat{a}_k e \hat{a}_k^\dagger sejam mais simples, algumas restrições são comumente estabelecidas entre os modos escolhidos na forma do *produto escalar* definido na Equação B.12.

$$(\mathbb{A}_1, \mathbb{A}_2) \equiv \frac{1}{i\hbar} \int (\mathbb{A}_1^* \mathbb{D}_2 - \mathbb{A}_2 \mathbb{D}_1^*) dV, \quad \mathbb{D} = -\varepsilon_0 \varepsilon \frac{\partial \mathbb{A}}{\partial t} \quad (\text{B.12})$$

O produto escalar acima definido é uma medida do grau de disparidade entre modos e herda algumas propriedades de produtos internos, como a linearidade e a simetria do conjugado. Entretanto, o produto definido na Equação B.12 não é positivo definido: o

produto escalar da função de um modo com ela mesma pode ter resultado negativo ou nulo.

Os modos escolhidos podem ser ortogonalizados usando o processo de ortogonalização de Gram-Schmidt, de modo que durante a evolução do sistema esses modos continuarão ortogonais. Desta forma, os modos verifiquem a *condição de ortonormalidade*

$$(\mathbb{A}_k, \mathbb{A}_{k'}) = \delta_{kk'}, \quad (\mathbb{A}_k, \mathbb{A}_{k'}^*) = 0. \quad (\text{B.13})$$

Sendo então denominados *modos normais*. Um resultado direto das Equações B.13 é a obtenção dos operadores de modo como

$$\hat{a}_k = (\mathbb{A}_k, \hat{\mathbb{A}}), \quad \hat{a}_k^\dagger = -(\mathbb{A}_k^*, \hat{\mathbb{A}}). \quad (\text{B.14})$$

Utilizando a definição do produto escalar na Equação B.12 e as relações de comutação, são obtidas as relações de comutação de Bose

$$[\hat{a}_k, \hat{a}_{k'}^\dagger] = \delta_{kk'}, \quad [\hat{a}_k, \hat{a}_{k'}] = 0, \quad (\text{B.15})$$

das quais é obtido o Hamiltoniano (simplificado)

$$\hat{H} = \hbar\omega \left(\hat{a}\hat{a}^\dagger + \frac{1}{2} \right). \quad (\text{B.16})$$

Observando as Equações em B.15, é possível afirmar que operadores de modo de modos diferentes comutam, representando então sistemas físicos distintos. Logo, as relações de comutação de Bose são indicadoras de que os modos representam graus de liberdade do campo eletromagnético. Para cada modo está então associado um espaço de Hilbert, sendo o espaço de Hilbert total o produto tensorial dos espaços de Hilbert de todos os modos da expansão.

B.1.2 Modos Monocromáticos

A expansão apresentada na Equação B.11 admite modos de pacotes de ondas, admitindo o uso de uma faixa de frequência óptica. Um caso especial da expansão de modos é encontrado quando os modos são expandidos monocromaticamente, em uma única frequência,

$$\mathbb{A}_k(\mathbf{r}, t) = \mathbb{A}_k(\mathbf{r})e^{-i\omega_k t}. \quad (\text{B.17})$$

Para esses modos, o produto escalar definido (B.12) é simplificado para

$$(\mathbf{A}_1, \mathbf{A}_2) = \frac{2\epsilon_0\omega_k}{\hbar} \int \mathbf{A}_1^* \cdot \mathbf{A}_2 \varepsilon dV. \quad (\text{B.18})$$

Devido à estacionariedade dos modos monocromáticos, é esperado que a energia total do sistema seja a soma da energia dos modos individuais, obtido através do Hamiltoniano. Realizando as devidas manipulações, o Hamiltoniano do campo se resume a

$$\hat{H} = \frac{1}{2} \int \left(\hat{\mathbf{E}} \cdot \hat{\mathbf{D}} + \hat{\mathbf{A}} \cdot \frac{\partial \hat{\mathbf{D}}}{\partial t} \right) dV. \quad (\text{B.19})$$

Efetuando substituições nas Equações B.5 e B.6 em B.19 e fazendo uso das condições de normalização (Equação B.13) e das relações de comutação de Bose (Equação B.15), é possível obter a seguinte expressão para o Hamiltoniano:

$$\hat{H} = \sum_k \frac{\hbar\omega_k}{2} \left(\hat{a}_k \hat{a}_k^\dagger + \hat{a}_k^\dagger \hat{a}_k \right) = \sum_k \hbar\omega_k \left(\hat{a}_k \hat{a}_k^\dagger + \frac{1}{2} \right), \quad (\text{B.20})$$

mostrando que a energia total do campo é a soma da energia dos modos monocromáticos.

B.2 Estados de Campo

Na Seção anterior foi apresentado um método de quantização do campo eletromagnético, levando aos operadores \hat{a}_k e \hat{a}_k^\dagger que contêm as propriedades quânticas de cada modo do campo expandido. Porém, informações como médias e flutuações (desvio padrão) de quantidades observáveis são calculadas a partir dos estados quânticos do campo, uma vez que, para modos monocromáticos, o campo eletromagnético é proporcional à amplitude do modo [40].

No entanto, os operadores de modo \hat{a}_k e \hat{a}_k^\dagger obtidos anteriormente não podem ser utilizados para obtenção de média e desvio padrão, pois são não-Hermitianos (consequentemente não são observáveis), apesar de serem tradicionalmente utilizados na literatura. Porém, é possível obter operadores Hermitianos a partir das seguintes combinações:

$$\hat{q} = \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{a}), \quad \hat{p} = \frac{1}{i\sqrt{2}}(\hat{a}^\dagger - \hat{a}). \quad (\text{B.21})$$

Para modos monocromáticos, os operadores \hat{q} e \hat{p} correspondem às componentes em fase e fora de fase, respectivamente, da amplitude de um campo, sendo chamados de operadores de quadratura, sendo eles Hermitianos.

As relações de comutação podem ser entre \hat{q} e \hat{p} podem ser obtidas a partir da relação de comutação de Bose (Equação B.15)

$$[\hat{q}, \hat{p}] = \frac{i}{2}. \quad (\text{B.22})$$

Devido à similaridade com os operadores de posição e momento de um oscilador harmônico, os operadores de quadratura são considerados como operadores de momento e quadratura em que $\hbar = 1$.

B.2.1 Estados de Quadratura

A partir dos operadores de quadratura \hat{q} e \hat{p} , obtidos das combinações dos operadores de criação e aniquilação, seus auto estados $|q\rangle$ e $|p\rangle$ serão chamados de estados de quadratura, satisfazendo a as seguintes condições

$$\hat{q}|q\rangle = q|q\rangle, \quad \hat{p}|p\rangle = p|p\rangle, \quad (\text{B.23})$$

em que $q, p \in \mathbb{R}$ são os autovalores associados aos respectivos auto-estados $|q\rangle$ e $|p\rangle$. Devido à continuidade de x e p , os observáveis de quadratura são de espectro contínuo. Além disso, os autoestados dos operadores são ortogonais (Equação B.24) e completos (Equação B.25),

$$\langle q|q'\rangle = \delta(q - q'), \quad \langle p|p'\rangle = \delta(p - p'), \quad (\text{B.24})$$

$$\int_{-\infty}^{\infty} |q\rangle \langle q| dq = \int_{-\infty}^{\infty} |p\rangle \langle p| dp = 1. \quad (\text{B.25})$$

Os estados de quadratura estão também relacionados pela transformada de Fourier:

$$|p\rangle = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{ipq} |q\rangle dq \quad (\text{B.26})$$

$$|q\rangle = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-ipq} |p\rangle dp \quad (\text{B.27})$$

B.2.2 Estados de Fock

Para definição dos estados de Fock, será apresentado primeiro o operador de número. A partir dos operadores de criação e aniquilação, é definido um operador \hat{n} , de modo que

$$\hat{n} \equiv \hat{a}\hat{a}^\dagger. \quad (\text{B.28})$$

Os estados de Fock são os auto estados $|n\rangle$ do operador de número:

$$\hat{n}|n\rangle = n|n\rangle. \quad (\text{B.29})$$

Os estados de Fock, nomeados em homenagem ao físico russo Vladimir A. Fock, são largamente utilizados na teoria de campos quânticos e, como autoestados do operador \hat{n} , tem um número de fótons fixos. Algumas propriedades dos estados de Fock merecem ser destacados.

Os estados de Fock são autoestados do Hamiltoniano (B.16):

$$\hat{H}|n\rangle = \hbar\omega \left(\hat{a}^\dagger \hat{a} + \frac{1}{2} \right) |n\rangle = \hbar\omega \left(\hat{n} + \frac{1}{2} \right) |n\rangle = \hbar\omega \left(n + \frac{1}{2} \right) |n\rangle = E_n |n\rangle, \quad (\text{B.30})$$

onde E_n é a energia do modo, o que mostra que os estados de Fock formam uma base ortonormal e completa, conhecida como base de Fock. Outra propriedade é que, se $|n\rangle$ é um autoestado do operador \hat{n} , $\hat{a}|n\rangle$ também é um auto estado, com autovalor $n - 1$

$$\hat{n}\hat{a}|n\rangle = \hat{a}^\dagger \hat{a}^2 |n\rangle = (\hat{a}\hat{a}^\dagger \hat{a} - \hat{a}) |n\rangle = (n - 1)\hat{a}|n\rangle. \quad (\text{B.31})$$

O mesmo desenvolvimento pode ser realizado para o operador \hat{a}^\dagger , levando ao autoestado de \hat{n} com autovalor $n + 1$. Deste resultado, as seguintes relações podem ser derivadas:

$$\hat{a}|n\rangle = \sqrt{n}|n - 1\rangle, \quad (\text{B.32})$$

$$\hat{a}^\dagger |n\rangle = \sqrt{n + 1}|n + 1\rangle. \quad (\text{B.33})$$

Os resultados das Equações B.32 e B.33 indicam que a atuação do operador \hat{a} no estado $|n\rangle$ resulta na diminuição de uma unidade do número de fótons do modo, ao passo

que a atuação do operador \hat{a}^\dagger aumenta em uma unidade. A Equação B.34 apresenta a generalização dos efeitos vistos nas Equações B.32 e B.33.

$$|n\rangle = \frac{\hat{a}^{\dagger n}}{\sqrt{n!}} |0\rangle. \quad (\text{B.34})$$

O Estado $|0\rangle$ é chamado de estado de vácuo que, apesar de não possuir fótons, apresenta flutuações mensuráveis, conforme os seguintes operadores [41]:

$$\langle \hat{q} \rangle_0 = \langle 0 | \hat{q} | 0 \rangle = \sqrt{N_0} \langle 0 | (\hat{a}^\dagger + \hat{a} | 0 \rangle = 0, \quad (\text{B.35})$$

$$\langle \hat{p} \rangle_0 = \langle 0 | \hat{p} | 0 \rangle = -i\sqrt{N_0} \langle 0 | (\hat{a}^\dagger - \hat{a} | 0 \rangle = 0, \quad (\text{B.36})$$

$$\langle \hat{\mathbf{E}}_k \rangle = -\frac{E_0}{\sqrt{N_0}} \left[\langle \hat{q} \rangle_{|0\rangle} \text{sen}(\mathbf{k} \cdot \mathbf{r} - \omega_k t) + \langle \hat{p} \rangle_{|0\rangle} \text{cos}(\mathbf{k} \cdot \mathbf{r} - \omega_k t) \right], \quad (\text{B.37})$$

$$\langle \hat{q}^2 \rangle_0 = N_0 \langle 0 | (\hat{a}^\dagger + \hat{a})^2 | 0 \rangle = N_0 \langle 0 | (\hat{a}^\dagger \hat{a}^\dagger + 2\hat{a}^\dagger \hat{a} + \hat{a} \hat{a} + 1) | 0 \rangle = N_0, \quad (\text{B.38})$$

$$\langle \hat{p}^2 \rangle_0 = -N_0 \langle 0 | (\hat{a}^\dagger - \hat{a})^2 | 0 \rangle = -N_0 \langle 0 | (\hat{a}^\dagger \hat{a}^\dagger - 2\hat{a}^\dagger \hat{a} + \hat{a} \hat{a} - 1) | 0 \rangle = N_0, \quad (\text{B.39})$$

$$\langle \hat{\mathbf{E}}_k \rangle_0 = E_0^2 \langle 0 | (1 + 2\hat{a}^\dagger \hat{a} - \hat{a}^2 e^{2i(\mathbf{k} \cdot \mathbf{r} - \omega_k t)} - (\hat{a}^\dagger)^2 e^{-2i(\mathbf{k} \cdot \mathbf{r} - \omega_k t)}) | 0 \rangle = E_0^2, \quad (\text{B.40})$$

$$(\Delta \hat{q})_0 = \sqrt{\langle \hat{q}^2 \rangle_0 - \langle \hat{q} \rangle_0^2} = \sqrt{N_0}, \quad (\text{B.41})$$

$$(\Delta \hat{p})_0 = \sqrt{\langle \hat{p}^2 \rangle_0 - \langle \hat{p} \rangle_0^2} = \sqrt{N_0}, \quad (\text{B.42})$$

$$\langle \hat{\mathbf{E}}_k \rangle = \sqrt{\langle \hat{\mathbf{E}}_k^2 \rangle_0 - \langle \hat{\mathbf{E}}_k \rangle_0^2} = E_0. \quad (\text{B.43})$$

Outra propriedade importante dos estados de Fock é que formam um conjunto completo,

$$\sum_{n=0}^{\infty} |n\rangle \langle n| = 1, \quad (\text{B.44})$$

resultando que eles expandem (ou geram) todo o espaço de Hilbert do oscilado eletromagnético. Além disso, os estados são ortonormais:

$$\langle n | n' \rangle = \delta_{nn'}. \quad (\text{B.45})$$

B.2.3 Estados Coerentes

Estados coerentes, também conhecidos como estados de Glauber (em memória do físico estadunidense Roy J. Glauber que introduziu os estados coerentes na óptica quântica) são conhecidos por estarem na fronteira entre as esferas quânticas e clássicas, descritos

por serem os "mais clássicos" dos estados quânticos de um oscilador harmônico [42] ou o paralelo quântico mais próximo de uma onda eletromagnética clássica [40].

Desta maneira, os estados coerentes podem ser utilizados para descrever um laser *ideal*. Estes estados são definidos como os autoestados do operador de aniquilação \hat{a} ,

$$\hat{a} |\alpha\rangle = \alpha |\alpha\rangle. \quad (\text{B.46})$$

Os autoestados α da Equação B.46 assumem valores complexos, uma vez que o operador de aniquilação não é hermitiano, correspondendo às amplitudes complexas de ondas na óptica clássica, com magnitude $|\alpha|$ e fase $\arg\alpha$. No caso da luz emitida por um *laser*, sua fase sofre flutuações devido às emissões espontâneas oriundas do material do *laser*, o levando a emitir estados quânticos de luz que são um conjunto de estados coerentes com fases aleatórias. Entretanto, os experimentos utilizam um *laser* mestre como referência, levando os feixes emitidos trem fases que flutuam em uníssono. Desta forma, a fase flutuante não será percebida e leva à conclusão que um feixe coerente de luz pode ser tratado como um estado coerente (B.46).

Outra propriedade dos estados coerentes é a obtenção da Equação B.46 equivalente para o operador de criação

$$\langle\alpha| \hat{a}^\dagger = \alpha^* \langle\alpha|, \quad (\text{B.47})$$

nomeando os estados $|\alpha\rangle$ como *autoestados diretos* do operador de aniquilação e os estados $\langle\alpha|$ os autoestados esquerdos do operador de criação, com autovalor α^* . A energia de um estado coerente é dada pela Equação B.48.

$$\langle\hat{E}\rangle = \langle\alpha| \hat{a}^\dagger \hat{a} + \frac{1}{2} |\alpha\rangle = |\alpha|^2 + \frac{1}{2}, \quad (\text{B.48})$$

sendo $|\alpha|^2$ a intensidade da onda clássica e $\frac{1}{2}$ a energia do vácuo.

Como os estados de Fock formam uma conjunto completo (B.44), estados coerentes podem ser expandidos como a soma dos estados $|n\rangle$ [42]:

$$|\alpha\rangle = \sum_{n=0}^{\infty} C_n |n\rangle. \quad (\text{B.49})$$

Aplicando o operador de aniquilação em ambos os lados da expansão, utilizando

(B.46) e (B.32),

$$\hat{a}|\alpha\rangle = \sum_{n=1}^{\infty} C_n \sqrt{n} |n-1\rangle = \alpha \sum_{n=0}^{\infty} C_n |n\rangle. \quad (\text{B.50})$$

Equacionando os coeficientes dos estados $|n\rangle$ em ambos os lados, a Equação B.50 é resumida para

$$\begin{aligned} C_n \sqrt{n} = \alpha C_{n-1} \Rightarrow C_n &= \frac{\alpha}{\sqrt{n}} C_{n-1} = \frac{\alpha^2}{\sqrt{n(n-1)}} C_{n-2} = \dots \\ &= \frac{\alpha^n}{\sqrt{n!}} C_0. \end{aligned} \quad (\text{B.51})$$

o que leva, substituindo o resultado de (B.51) em B.49, ao seguinte resultado

$$|\alpha\rangle = C_0 \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (\text{B.52})$$

A partir da normalização, é possível determinar os coeficientes C_0 :

$$\begin{aligned} \langle \alpha | \alpha \rangle &= 1 = |C_0|^2 \sum_n \sum_n \frac{\alpha^n n \alpha^{n*}}{\sqrt{n! n!} \langle n | n' \rangle}, \\ &= |C_0|^2 \sum_{n=0}^{\infty} \frac{|\alpha|^{2n}}{n!} = |C_0|^2 e^{|\alpha|^2} \Rightarrow C_0 = e^{-\frac{1}{2}|\alpha|^2}, \end{aligned} \quad (\text{B.53})$$

implicando que $C_0 = \exp(-\frac{1}{2}|\alpha|^2)$, levando ao estado coerente normalizado e expandido pelos estados de Fock

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right) \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (\text{B.54})$$

O termo α em (B.46) tem sentido físico relacionado à amplitude do campo eletromagnético [42]. Sendo o valor esperado do operador número $\hat{n} = \hat{a}^\dagger \hat{a}$ dado por

$$\bar{n} = \langle \alpha | \hat{n} | \alpha \rangle = |\alpha|^2, \quad (\text{B.55})$$

onde $|\alpha|^2$ representa o número médio de fótons contidos no campo. As flutuações do número de fótons podem também ser calculadas:

$$\langle \alpha | \hat{n}^2 | \alpha \rangle = \langle \alpha | \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} | \alpha \rangle, \quad (\text{B.56})$$

$$= \langle \alpha | \hat{a}^\dagger \hat{a}^\dagger \hat{a} \hat{a} + \hat{a}^\dagger \hat{a} | \alpha \rangle, \quad (\text{B.57})$$

$$= |\alpha|^4 + |\alpha|^2 = \bar{\alpha}^2 + \bar{n}. \quad (\text{B.58})$$

Logo,

$$\Delta n = \sqrt{\langle \hat{n}^2 \rangle - \langle \hat{n} \rangle^2} = \bar{n}, \quad (\text{B.59})$$

caracterizando um processo de Poisson, levando a medição do número de fótons no campo ser regida pela probabilidade de detecção de n fótons, dada por

$$p_n = |\langle n | \alpha \rangle|^2 = \frac{|\alpha|^{2n}}{n!} e^{-|\alpha|^2} = e^{-\bar{n}} \frac{\bar{n}^n}{n!}, \quad (\text{B.60})$$

a qual pode também ser obtida através da representação de Fock B.54. Os estados coerentes não são exatamente ortogonais entre si, como consequência de serem autoestados de operadores não hermitianos (operadores de criação e aniquilação). É possível observar, a partir da representação de Fock, que os estados coerentes aproximam a ortogonalidade na medida que suas amplitudes se tornam suficientemente diferentes:

$$\langle \alpha' | \alpha \rangle = \exp\left(-\frac{|\alpha|^2}{2} - \frac{|\alpha'|^2}{2}\right) \sum_{n=0}^{\infty} \frac{(\alpha'^* \alpha)^n}{n!}, \quad (\text{B.61})$$

$$= \exp\left(-\frac{|\alpha|^2}{2} - \frac{|\alpha'|^2}{2} + \alpha'^* \alpha\right), \quad (\text{B.62})$$

o que leva a:

$$|\langle \alpha' | \alpha \rangle|^2 = \exp(-|\alpha - \alpha'|^2). \quad (\text{B.63})$$

Apêndice C

Tópicos em Teoria da Informação

Nesta Seção serão abordados os tópicos básicos da teoria da informação, sendo definidas as quantidades de entropia, entropia relativa e informação mútua, que serão vistas como medidas razoáveis de informação e, a partir destas definições, será apresentado a capacidade de um canal de comunicação. Os conceitos abordados nesta seção foram formalizados matematicamente por Claude E. Shannon em seu trabalho intitulado “*A Mathematical Theory of Communication*” [43].

C.1 Entropia, Entropia Relativa e Informação Mútua

Começaremos pela definição de *entropia*, que informa a respeito da incerteza de uma variável aleatória. Seja X uma variável aleatória discreta com alfabeto \mathcal{X} e função massa de probabilidade $p(x) = P[X = x], x \in \mathcal{X}$.

Definição C.1 (Entropia) *A entropia de uma variável aleatória discreta X é definida como*

$$H(X) = - \sum_{x \in \mathcal{X}} p(x) \log(p(x)). \quad (\text{C.1})$$

É admitido que $0 \log(0) = 0$, justificado pelo fato de que o limite $x \log(x) \rightarrow 0$ na medida que x se aproxima de zero, e sendo mantida a continuidade. $H(X)$ pode também ser escrita como $H(p)$, uma vez que a entropia de uma variável aleatória é uma função de sua distribuição de probabilidades. A entropia de uma fonte com alfabeto $\mathcal{X} = \{0, 1\}$ e distribuição de probabilidade $P[X = 1] = p$ e $P[X = 0] = 1 - p$ apresenta maior incerteza quando os símbolos da fonte são distribuídos uniformemente.

A entropia também pode ser entendida como o valor esperado da variável aleatória $g(X) = \log\left(\frac{1}{p(x)}\right)$, onde $X \sim p(x)$. Logo,

$$H(X) = E \log \left(\frac{1}{p(x)} \right) \quad (\text{C.2})$$

Para o caso de duas variáveis aleatórias conjuntamente distribuídas, sua entropia pode ser entendida como a entropia de um vetor aleatório.

Definição C.2 (Entropia conjunta) Para duas variáveis aleatórias (X, Y) com distribuição conjunta de probabilidades $p(x, y)$, a entropia conjunta é definida como

$$H(X, Y) = - \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log p(x, y) \quad (\text{C.3})$$

$$= -E \log p(X, Y) \quad (\text{C.4})$$

Também é definida a entropia de uma variável aleatória dada outra variável aleatória:

Definição C.3 (Entropia condicional) Para duas variáveis aleatórias (X, Y) com distribuição conjunta de probabilidades $p(x, y)$, a entropia condicional é definida como

$$H(Y|X) = \sum_{x \in \mathcal{X}} p(x) H(Y|X = x) \quad (\text{C.5})$$

$$= - \sum_{x \in \mathcal{X}} p(x) \sum_{y \in \mathcal{Y}} p(y|x) \log(p(y|x)) \quad (\text{C.6})$$

$$= - \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log(p(y|x)) \quad (\text{C.7})$$

$$= -E \log p(Y|X) \quad (\text{C.8})$$

A entropia é uma medida de incerteza de uma variável aleatória baseada na sua distribuição de probabilidades, medindo a quantidade de informação necessária para representá-la. A entropia relativa é uma medida de distância entre duas distribuições de probabilidades.

Definição C.4 (Entropia Relativa) A entropia relativa, ou distância de Kullback-Leibler entre duas funções massa de probabilidade $p_X(x)q_X(x)$ é definida como

$$D(p||q) = \sum_{x \in \mathcal{X}} p_X(x) \log \left(\frac{p(x)}{q(x)} \right) \quad (\text{C.9})$$

A entropia relativa pode ser encarada como uma medida de ineficiência entre duas distribuições de probabilidades p e q . A informação mútua é uma medida de informação sobre o quanto uma variável aleatória diz sobre a outra.

Definição C.5 (Informação Mútua) *Sejam duas variáveis aleatórias X e Y com distribuição conjunta de probabilidade $p(x, y)$ e distribuições marginais $p(x)$ e $p(y)$. A informação mútua é definida como a entropia relativa entre a distribuição conjunta e o produto as distribuições marginais:*

$$I(X; Y) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log \left(\frac{p(x, y)}{p(x)p(y)} \right) \quad (\text{C.10})$$

A Informação mútua informa qual a redução de incerteza sobre a variável X quando Y é conhecido, e vice-versa. Na Figura ?? é apresentada a relação geral entre as entropias e a informação mútua.

C.2 Capacidade de Canal

Um canal discreto é definido como um sistema constituído de um alfabeto de entrada \mathcal{X} e um alfabeto de saída \mathcal{Y} e uma matriz de probabilidade de transição $p(y|x)$ que representa a probabilidade de observar um símbolos de saída y quando foi enviado x . O canal é dito sem memória quando a saída o canal é independente das entradas anteriores.

Definição C.6 (Capacidade de Canal) *A capacidade de um canal discreto e sem memória é definida como*

$$C = \max_{p(x)} I(X; Y), \quad (\text{C.11})$$

onde a maximização é realizada sobre todas as distribuições do alfabeto de entrada.

Para o caso de um canal binário simétrico (*Binary Symmetric Channel*, BSC), sendo o modelo de canal com erros mais simples, onde um erro ocorre quando 0 é recebido como 1 e vice versa, com probabilidade p , conforme exemplificado na fig. (C.1).

É possível limitar a informação mútua por

$$I(X;Y) = H(Y) - H(Y|X) \quad (\text{C.12})$$

$$= H(Y) - \sum p(x)H(Y|X = x) \quad (\text{C.13})$$

$$= H(Y) - \sum p(x)H(p) \quad (\text{C.14})$$

$$= H(Y) - H(p) \quad (\text{C.15})$$

$$\leq 1 - H(p) \quad (\text{C.16})$$

Como Y é uma variável aleatória binária, a igualdade na Equação (C.16) é atingida quando os símbolos na entrada do canal tem distribuição uniforme. Logo, a capacidade de informação de um canal BSC com parâmetro (p) é dado pela Equação (C.17).

$$C = 1 - H(p) \quad (\text{C.17})$$

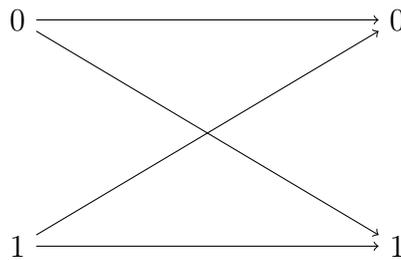


Figura C.1 – Modelo de um canal BSC(p).

C.3 Teoria da Informação Quântica

A entropia de Shannon se estabeleceu como uma medida de incerteza associada a distribuições de probabilidade clássicas. No paradigma quântico, estados quânticos são descritos de maneira similar, com operadores de densidade substituindo as distribuições de probabilidade. Nesta seção, serão abordadas as generalizações das definições da entropia de Shannon para estados quânticos, seguindo a abordagem em [44].

A entropia de Von Neumann é definida como a entropia de um estado quântico ρ pela expressão na Equação (C.18).

$$S(\rho) = -\text{tr}(\rho \log \rho). \quad (\text{C.18})$$

A expressão para a entropia de Von Neumann utiliza o logaritmo com base dois. Se λ_x são os autovalores de ρ , então a Equação (C.18) pode ser reescrita como

$$S(\rho) = - \sum_x \lambda_x \log \lambda_x. \quad (\text{C.19})$$

De maneira similar à entropia de Shannon, é definido que $0 \log 0 = 0$. Outra medida de informação importante é a definição de entropia relativa entre estados quânticos. Sejam ρ e σ dois operadores de densidade, a entropia relativa entre ρ e σ é definida como

$$S(\rho||\sigma) = \text{tr}(\rho \log \rho) - \text{tr}(\rho \log \sigma). \quad (\text{C.20})$$

Por fim, para o escopo deste trabalho, é necessário indicar um limitante para a informação acessível de um estado quântico. Este limite é conhecido como o limitante de Holevo (ou informação de Holevo), definido no seguinte teorema:

Teorema C.1 (limitante de Holevo) *Suponha que Alice prepara um estado ρ_X , onde $X = 0, 1, \dots, n$ com probabilidades p_0, \dots, p_n , e Bob realize medições descritas por elementos de medição POVM $\{E_y\} = \{E_0, \dots, E_m\}$ no estado ρ_X , resultando na saída Y . O limitante de Holevo estabelece que para qualquer medição realizada conforme descrito, a informação mútua entre X e Y será:*

$$I(X; Y) < S(\rho) - \sum_x p_x S(\rho) \quad (\text{C.21})$$

O limitante de Holevo é então um limitante superior sobre a informação acessível de um estado quântico. A quantidade descrita no lado direito da Equação (C.21) é nomeada como a quantidade de Holevo χ .