

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

Novo Método de Quantização para Protocolos de Reconciliação
de Chaves Secretas Geradas Quanticamente Utilizando Códigos
LDPC no Sentido Slepian-Wolf

Laryssa Mirelly Carvalho de Araújo

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

Campina Grande – Paraíba – Brasil
© Laryssa Mirelly Carvalho de Araújo, 2018

Laryssa Mirelly Carvalho de Araújo

Novo Método de Quantização para Protocolos de Reconciliação
de Chaves Secretas Geradas Quanticamente Utilizando Códigos
LDPC no Sentido Slepian-Wolf

Dissertação apresentada à Coordenação de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande para obtenção do grau de Mestre em Engenharia Elétrica.

Orientador: Francisco Marcos de Assis

Campina Grande – Paraíba – Brasil

2018

A663n

Araújo, Laryssa Mirelly Carvalho de.

Novo método de quantização para protocolos de reconciliação de chaves secretas geradas quanticamente utilizando códigos LDPC no sentido Slepian-Wolf / Laryssa Mirelly Carvalho de Araújo. - Campina Grande-PB, 2018.

58 f. : il. color.

Dissertação (Mestrado em Engenharia Elétrica) - Universidade Federal de Campina Grande, Centro de Engenharia Elétrica e Informática, 2018.

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

Referências.

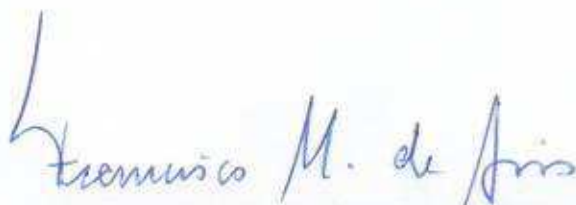
1. Funções *Slice* - Reconciliação de Variáveis Aleatórias. 2. Criptografia. 3. Códigos LDPC. 4. Teorema de Slepian-Wolf. I. Assis, Francisco Marcos de. II. Título.

CDU 621.3:004.056.55(043)

"NOVO MÉTODO DE QUANTIZAÇÃO PARA PROTOCOLOS DE RECONCILIAÇÃO DE CHAVES SECRETAS GERADAS QUANTICAMENTE UTILIZANDO CÓDIGOS LDPC NO SENTIDO SLEPIAN-WOLF"

LARYSSA MIRELLY CARVALHO DE ARAÚJO

DISSERTAÇÃO APROVADA EM 25/09/2018



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



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



WASHINGTON LUIZ ARAÚJO NEVES, Ph.D., UFCG
Examinador(a)

CAMPINA GRANDE - PB

Agradecimentos

Primeiramente, agradeço aos meus pais, Enildo e Ligiane, pelo amor e dedicação e por sempre terem me incentivado aos estudos.

A meu namorado Alequine, por todo amor, companheirismo e apoio à realização dos meus projetos pessoais e acadêmicos.

A todos que fazem parte da Pós-Graduação em Engenharia Elétrica da Universidade Federal de Campina Grande, em especial ao professor Francisco Marcos de Assis, por todo o auxílio fornecido durante a orientação desta pesquisa, pelo incentivo a busca de conhecimento e pela confiança em mim depositada e ao professor Bruno Barbosa Albert, pelo suporte no desenvolvimento deste trabalho de dissertação.

A minha irmã, Bruna, pelas palavras de incentivo e momentos de descontração a cada dia, e minha companhia de estudos, Lolita, por ajudar a tornar o trabalho menos árduo.

Aos amigos por compreenderem os momentos de ausência dedicados à pesquisa e pelo companheirismo.

A todos que contribuíram para o sucesso deste trabalho, muito obrigada.

Resumo

Este trabalho apresenta uma solução alternativa ao uso das funções *Slice* para reconciliação de variáveis aleatórias contínuas em um contexto de geração de chaves secretas para fins de criptografia. O protocolo de reconciliação proposto baseia-se na função distribuição de probabilidade das variáveis aleatórias e se mostra um método competitivo por sua capacidade de produzir maior quantidade de *bits* por cada realização de variável contínua que o esquema atualmente em uso, para baixos valores de SNR, com uma vantagem de menor iteratividade. O processo de correção de erros é feito com base no uso de códigos LDPC a partir de uma compressão da sequência de *bits* a ser utilizada como chave, fundamentado no teorema de Slepian-Wolf, minimizando a informação vazada pelo canal clássico – assumido perfeito – para um possível espião que observa o canal.

Palavras-chave: Funções *Slice*; SEC; Criptografia; Reconciliação de chaves secretas; Códigos LDPC; Teorema de Slepian-Wolf.

Abstract

This work presents an alternative solution to the use of the Slice functions to reconcile continuous random variables in a secret key generation context for encryption purposes. The proposed reconciliation protocol is based on the probability distribution function of the random variables and shows a competitive method for its ability to generate a greater amount of bits per each continuous variable than the scheme currently in use, for low SNR values, with a lower iterativity. The process of error correction is performed based on the use of LDPC codes from a compression of the sequence of bits to be used as key, based on the Slepian-Wolf theorem, minimizing the information leaked through the classic channel – assumed perfect – for a possible spy who observes the channel.

Keywords: Slice functions; SEC; Cryptography; Reconciliation of secret keys; LDPC Codes; Slepian-Wolf Theorem.

Lista de Figuras

1	Protocolo SEC.	21
2	Exemplo para o protocolo SEC.	23
3	Processo $T(X)$ do protocolo SEC, para $t = 8$	25
4	Grafo bipartido para código LDPC de comprimento de palavra-código $N = 6$ e distribuições $\lambda(x) = \frac{4}{7}x + \frac{3}{7}x^2$ e $\rho(x) = \frac{3}{7}x^2 + \frac{4}{7}x^3$	28
5	Decodificação conjunta de fontes de informação correlacionadas.	29
6	Taxas para codificação Slepian-Wolf.	30
7	Sequências conjuntamente típicas	31
8	Esquema de reconciliação reversa considerado para fins de reconciliação das realizações de variáveis gaussianas correlacionadas X e X'	39
9	Probabilidade de erro estimada de cada canal.	43
10	Contribuição de cada canal para a informação mútua total $I(X, \hat{Y})$	44
11	Informação mútua entre os <i>bits</i> não-reconciliados F_i e F'_i	45
12	Reconciliação para os dois primeiros níveis de quantização segundo protocolo proposto.	46
13	Esquema de reconciliação direta através de um canal clássico pelo qual Alice envia R bits para ajudar Bob a corrigir sua sequência $x'_1x'_2x'_3$ para $x_1x_2x_3$	58
14	Esquema de reconciliação reversa através de um canal clássico pelo qual Bob envia R bits para ajudar Alice a corrigir sua sequência $x_1x_2x_3$ para $x'_1x'_2x'_3$	58
15	Valores de I_{AB} , I_{AE} e I_{BE} em função da transmissividade de linha G para $V \approx 40$, onde V representa a variância das quadraturas de Alice. Retirado de (GROSSHANS et al., 2003).	59

Lista de Tabelas

1	Mapeamento da base	16
2	Mapeamento do valor	16
3	Tabela de probablidades para o canal BSC	32
4	Distribuição conjunta para o primeiro <i>bit</i> da discretização de x e x' para o Exemplo 2.	33
5	Contribuição de cada canal para informação mútua total para $1 \text{ dB} \leq SNR \leq 5 \text{ dB}$	44
6	Parâmetros obtidos para o canal 1.	45
7	Parâmetros obtidos para o canal 2.	46
8	Comparação entre taxas utilizadas para reconciliação no esquema proposto e aquelas apresentadas na literatura.	47

Sumário

1	INTRODUÇÃO	12
2	FUNDAMENTAÇÃO TEÓRICA	15
2.1	Notação e Terminologia	15
2.2	Distribuição Quântica de Chaves Secretas	15
2.2.1	Distribuição Quântica de Chaves com Variáveis Contínuas	18
2.2.2	Fase de reconciliação	19
2.3	Correção de Erros por Fatiamento	21
2.4	Códigos Corretores de Erros	26
2.4.1	Códigos LDPC	27
2.5	Codificação de Fontes de Informação Correlacionadas	29
3	REVISÃO BIBLIOGRÁFICA	34
3.1	Parâmetros para protocolo SEC	36
4	CONTRIBUIÇÃO DO TRABALHO	37
4.1	Método de Quantização Baseado na Função Distribuição de Probabilidade	37
4.2	Reconciliação utilizando códigos LDPC no sentido Slepian-Wolf	38
4.2.1	Codificação	40
4.2.2	Decodificação	40
5	MATERIAIS E MÉTODOS	41
6	RESULTADOS E DISCUSSÃO	43
6.1	Estimação dos Canais	43
6.2	Codificação e Decodificação	45
7	CONSIDERAÇÕES FINAIS	48
	REFERÊNCIAS	50
	APÊNDICE A NOÇÕES GERAIS DA MECÂNICA QUÂNTICA	53
A.0.1	Postulados básicos da mecânica quântica	53
A.0.2	Estados não-ortogonais e distinguibilidade	55
	APÊNDICE B RECONCILIAÇÃO DIRETA E REVERSA	56
B.1	Reconciliação Direta	56
B.2	Reconciliação Reversa	57

APÊNDICE C LEMA IMPORTANTE DA CODIFICAÇÃO ARITMÉTICA

Capítulo 1

Introdução

A criptografia trata do problema de realizar comunicação ou computação envolvendo duas ou mais partes que podem ou não confiar umas nas outras, através de técnicas de codificação de mensagens voltadas à proteção da informação que estas contêm (NIELSEN; CHUANG, 2010). Para que duas partes legítimas, Alice e Bob, se comuniquem sob sigilo é necessário que estas façam uso de um algoritmo para cifrar e decifrar suas mensagens e de uma chave secreta (NASCIMENTO, 2017). É feita a suposição de que o sigilo é provido unicamente pelo desconhecimento que uma intrusa, que observa o canal de comunicação (Eva), tenha acerca da chave secreta utilizada, ou seja, o algoritmo é de conhecimento público.

O criptossistema em questão pode ser de chave pública ou privada. No primeiro caso, as partes legítimas não precisam compartilhar uma chave secreta antecipadamente, pois uma chave pública é divulgada e utilizada para cifrar a mensagem a ser enviada. A segurança desse sistema baseia-se no fato de que a transformação da criptografia é escolhida de modo não-trivial para que seja extremamente improvável que alguém disponha de poder computacional suficiente para invertê-la com conhecimento apenas da chave pública (NIELSEN; CHUANG, 2010). Uma chave secreta aliada à chave divulgada publicamente permite a decifragem da mensagem. Criptossistemas de chave privada, por sua vez, requerem o compartilhamento prévio de uma chave secreta pelas partes legítimas conhecida apenas por eles (NIELSEN; CHUANG, 2010).

Uma vez que a segurança dos criptossistemas de chave pública se baseia na inexistência de algoritmos clássicos eficientes para determinados problemas como fatoração ou computação de logaritmo discreto, o advento da computação quântica pode comprometer a segurança de tais sistemas. Neste cenário, a criptografia quântica surge como um método promissor de distribuição de chaves privadas (que quando de comprimento idêntico ao da mensagem a ser trocada e utilizada uma única vez, garante segurança incondicional ao criptossistema de chave privada conforme demonstrado por Claude Shannon (NASCIMENTO, 2017)) por se basear nos princípios da Mecânica Quântica e não em hipóteses computacionais. A ideia básica, portanto, reside em explorar o princípio básico da Mecânica Quântica de que a observação em geral per-

turba o sistema sendo observado; logo, a existência de uma espiã que observa o canal quântico enquanto Alice e Bob tentam transmitir uma chave é perceptível como uma perturbação no canal de comunicação e os *bits* da chave estabelecidos enquanto da presença da espiã podem ser descartados (NIELSEN; CHUANG, 2010).

O estudo da distribuição quântica de chaves (QKD – *Quantum Key Distribution*), que oferece segurança incondicional fundamentado nos princípios básicos da mecânica quântica (BAI et al., 2017) (ASSCHE; CARDINAL; CERF, 2004), com variáveis discretas (DV-QKD – *Discrete Variable Quantum Key Distribution*) – que se baseia na codificação de informação em variáveis discretas de sistemas quânticos através da transmissão de fótons isolados com informação codificada nas polarizações ou fases destes – apesar de anteceder aquele com variáveis contínuas (CV-QKD – *Continuous Variable Quantum Key Distribution*) – baseado na transmissão de distribuições aleatórias de estados coerentes (consistindo de pulsos de laser contendo algumas centenas de fótons) – apresenta alguns problemas que podem ser minimizados com o uso de variáveis contínuas: no esquema de DV-QKD há dificuldade na geração e transmissão eficiente de fótons isolados, visto requerir uma aparelhagem óptica especializada como geradores de fótons únicos e APDs (*Avalanche Photodiodes*) de grande eficiência (NASCIMENTO, 2017), ao passo que naquele utilizando a CV-QKD a fonte de luz é simples e estável, levando a uma eficiência de detecção de até 90% com taxa de repetição elevada, o que mostra que a CV-QKD permite alcançar taxas de chave secreta mais elevadas (LI et al., 2016), com menos pulsos de luz e aparelhagem padrão de telecomunicações (GROSSHANS et al., 2003).

A utilização de CV-QKD, entretanto, torna mais onerosa a tarefa de reconciliar eficientemente os erros encontrados após a transmissão quântica em regime de baixa SNR (LI et al., 2016). Neste sentido, em 2004, Assche e outros (ASSCHE; CARDINAL; CERF, 2004) propuseram o algoritmo de Correção de Erros por Fatiamento (SEC – *Sliced Error Correction*) – no qual uma variável contínua é quantizada em uma sequência binária e um protocolo de correção binário (BCP – *Binary Correction Protocol*) é aplicado a cada *bit* da sequência para obtenção de uma chave secreta comum às partes legítimas do protocolo considerado – utilizado por Nguyen e outros (NGUYEN; ASSCHE; CERF, 2004) combinando códigos turbo e o algoritmo iterativo Cascade empregados de acordo com a taxa de erro para as sequências binárias obtendo eficiência de reconciliação ainda insatisfatória, isto é, menor que 0,9 (LI et al., 2016) (BAI et al., 2017). Bloch e outros (BLOCH et al., 2006) utilizaram técnicas de modulação de códigos tais como codificação multinível (MLC – *multilevel coding*) e decodificação multi-estágio (MSD – *multistage decoding*) adaptadas e aplicadas com códigos LDPC obtendo uma eficiência de reconciliação $\beta = 0,887$ para uma SNR de aproximadamente 4,8 dB, para apenas dois níveis de quantização. Jouguet e outros (JOUGUET et al., 2012) realizaram algumas melhorias na reconciliação CV-QKD baseada em estados coerente, possibilitando comunicação por mais de 80km. Li e outros (LI et al., 2016) fizeram simulações utilizando o protocolo SEC codificando dois de quatro níveis de quantização, obtendo eficiência de reconciliação de 91,8%. Em 2017, Bai e outros (BAI et al., 2017) implementaram a reconciliação SEC com uma quantização de

cinco *bits* dos quais apenas dois são codificados, e códigos LDPC com comprimento de bloco $n = 10^6$, conseguindo eficiências superiores a 95%.

O objetivo geral desse trabalho é de propor um novo método de reconciliação de variáveis contínuas no contexto de distribuição quântica de chaves competitivo com o método mais utilizado para tal fim, através do uso um esquema de quantização nunca antes utilizado, baseado em um importante lema da teoria da informação apresentado no Apêndice C e códigos LDPC no sentido Slepian-Wolf, isto é, levando em conta a correlação entre as sequências de Alice e Bob após a comunicação quântica, para realizar uma compressão da informação transmitida pelo canal clássico e público como meio de minimizar a informação disponível para Eva. Pode-se verificar como objetivos específicos a avaliação de medidas de informação clássicas, tais como entropia e informação mútua, para fins de comparação da eficiência entre protocolos; e, ainda, o estudo de codificação LDPC para fins de correção de erros.

A estrutura desse trabalho está organizada da seguinte forma: no Capítulo 2 são apresentados conceitos fundamentais necessários para compreensão do trabalho, explanando inicialmente o protocolo de distribuição quântica de chaves com enfoque na etapa de reconciliação das sequências binárias; o método mais amplamente utilizado para reconciliação de variáveis contínuas, o SEC, é abordado com o intuito de comparação posterior com o método proposto no presente trabalho. Em seguida, o capítulo traz um resumo acerca de códigos LDPC utilizados para correção de erros e o teorema de Slepian-Wolf, que fornece uma maneira de alcançar máxima compressão das mensagens trocadas por um canal clássico entre Alice e Bob, reduzindo a informação vazada para uma possível espiã. O Capítulo 3 apresenta a revisão bibliográfica realizada sobre o SEC para situar este trabalho em relação ao que é visto na literatura e o Capítulo 4 exhibe a contribuição do estudo, pontuando as diferenças do método proposto de quantização de realizações de variáveis aleatórias contínuas para o SEC. No Capítulo 5 são expostos os procedimentos utilizados para obtenção dos resultados exibidos no Capítulo 6, junto a discussão dos dados apresentados. Por fim, o Capítulo 7 traz as considerações finais e sintetiza a contribuição do trabalho.

Capítulo 2

Fundamentação Teórica

Este capítulo apresenta os conceitos fundamentais necessários para compreensão deste trabalho, assim como notações e terminologias. É apresentado um resumo acerca do protocolo de distribuição quântica de chaves para variáveis contínuas a ser considerado ao longo da pesquisa, trazendo um maior enfoque no processo de quantização para reconciliação da informação.

2.1 Notação e Terminologia

É usada a notação de Dirac, conforme apresentada no Apêndice A, para estados quânticos. Variáveis aleatórias, a título de padronização das discussões, são denotadas por letras maiúsculas e seus alfabetos por letras caligráficas, ou seja, uma variável aleatória X tem alfabeto \mathcal{X} , sua função de densidade de probabilidade é representada por $p(\cdot)$ e sua função distribuição por $F(\cdot)$. Sobrescritos de uma variável aleatória indicam o comprimento de sequências daquela variável. O logaritmo é sempre calculado referente à base 2, salvo quando indicado, de modo que a informação medida será sempre em *bits*.

2.2 Distribuição Quântica de Chaves Secretas

A distribuição quântica de chaves é uma maneira de compartilhar, entre duas partes legítimas, uma chave secreta através de propriedades não-clássicas de estados quânticos com a ajuda de um canal auxiliar de comunicação clássico público e autenticado, que pode ser utilizada para troca de informações sigilosas (JOUQUET; KUNZ-JACQUES; LEVERRIER, 2011). A segurança da QKD se baseia fundamentalmente no fato de que medições de variáveis incompatíveis inevitavelmente afetam o estado do sistema quântico, de modo que, com a informação codificada em variáveis incompatíveis a espionagem se torna mensurável (ASSCHE; CARDINAL; CERF, 2004), conforme pode ser verificado de acordo com a prova da inexistência de medições quânticas capazes de distinguir estados não-ortogonais no apêndice A.0.2: ao realizar uma medição com a base incorreta, Eva tem apenas 50% de chances de acerto (CHRISTIAN; PIVK,

Tabela 1 – Mapeamento da base

Base	Bit de representação
Rectilinear	0
Diagonal	1

Tabela 2 – Mapeamento do valor

Rectilinear	Diagonal	Valor do bit
Horizontal (0°)	+45°	0
Vertical (90°)	-45°	1

2010), (ASSCHE; CARDINAL; CERF, 2004).

A QKD minimiza a quantidade de informação vazada para uma espiã que observa o canal sem nenhuma suposição computacional, em contraste com a criptografia clássica (ASSCHE; CARDINAL; CERF, 2004) e fornece a Bob uma vantagem sobre Eva: a capacidade de conversar com Alice em um canal clássico autenticado para combinar uma chave comum e descartar o conhecimento de Eva sobre a mesma (ASSCHE; CARDINAL; CERF, 2004).

O protocolo de distribuição quântica de chave mais conhecido é o BB84 (BENNETT; BRASSARD., 1984), proposto por Charles Bennett e Gilles Brassard, para o qual, no primeiro estágio, há a transmissão de fótons¹ de Alice para Bob – compartilham o mesmo esquema de mapeamento como pode ser visto nas tabelas 1 e 2 –, na qual Alice escolhe aleatoriamente duas sequências independentes com comprimento m :

- A primeira sequência representa a base para a transmissão quântica;
- A segunda sequência representa o valor do bit específico.

Nessa fase, Alice toma o primeiro *bit* da primeira e o primeiro *bit* da segunda sequência, indicando a base utilizada e o valor a ser tomado, respectivamente, e aplica este procedimento para todos os m -bits das duas sequências que são enviados para Bob pelo canal quântico. Bob também escolhe uma sequência aleatória de comprimento m para suas escolhas de base para medição².

Segundo (CHRISTIAN; PIVK, 2010), as medições de Bob não são perfeitamente casadas com as de Alice devido a desalinhamentos ópticos, perturbações no canal quântico, ruído no detector de Bob ou presença de uma espiã, ainda que os dois escolham a mesma base, desta forma, ao fim da comunicação quântica, Alice possui duas sequências de tamanho m contendo sua escolha de base e valor e Bob, uma sequência de tamanho m referente a escolha de base e

¹ Fótons podem ser utilizados para representar *qubits* por dificilmente interagirem entre si e serem capazes de percorrer longas distâncias com baixa perda nas fibras ópticas.

² É necessário que Bob escolha uma das bases para realizar as medições por não existir a possibilidade de se medir com os dois filtros uma vez que após a medição a polarização original é perdida (CHRISTIAN; PIVK, 2010)

os resultados de suas medições de comprimento $g_q \cdot m$, onde g_q representa as várias perdas no canal quântico.

A comunicação então passa para o canal público no qual a primeira fase é de peneiramento (*sifting phase*): Alice e Bob negociam quais *bits* serão usados e quais serão descartados. Para tal, Alice precisa saber quais fótons Bob mediu, assim, ele envia uma mensagem no canal público para informá-la quais fótons foram medidos, através de uma sequência tão longa quanto aquela escolhida a princípio para a base (CHRISTIAN; PIVK, 2010). Com essa mensagem, Alice tem conhecimento acerca de quais posições Bob mediu mas não o tem sobre a base utilizada, assim Bob envia uma segunda mensagem, na qual ele informa quais as bases usou para medição, de modo que essa mensagem tem comprimento igual ao da chave bruta.

Quando Alice está em posse de ambas as mensagens, ela pode reduzir sua sequência de *bits* anulando as posições para as quais Bob não realizou medições e aquelas nas quais utilizou bases diferentes na transmissão. Para garantir que Bob compartilhe da mesma sequência binária que ela, Alice o envia uma mensagem contendo suas escolhas de base para aquelas posições onde Bob recebeu um fóton para que ele realize o mesmo procedimento feito anteriormente por ela e anule as posições para as quais as bases diferem. Para evitar um ataque do tipo “homem no meio” por Eva no qual o intruso intercepta a mensagem e a reenvia, a troca de mensagem nesse estágio deve ser autenticada (CHRISTIAN; PIVK, 2010).

Após decididos os *bits* a serem usados e garantido que Eva não modificou as mensagens pelo uso de um esquema de autenticação, Alice e Bob passam para a fase de reconciliação (ou fase de correção de erros). Como o canal quântico não é livre de ruído, Alice e Bob não compartilham a mesma sequência, logo, essa fase visa estimar e corrigir todos os erros na sequência de Bob através de um canal clássico público autenticado, devido novamente à possibilidade de Eva modificar as mensagens trocadas.

Nessa etapa, a taxa de erro p é estimada tomando-se um pequeno subconjunto aleatório de *bits* com comprimento r que será a sequência comparada publicamente por Alice e Bob levando a um certo número de erros, e . Se o comprimento da sequência de teste for escolhido adequado ao comprimento da chave peneirada n , então a probabilidade de erro estimada é calculada por

$$p = \frac{e}{r} \quad (2.1)$$

Os *bits* divulgados pelo canal clássico são descartados e, caso a probabilidade de erros p se torne muito elevada Alice e Bob recomeçam todo o protocolo em outro canal quântico porque uma espionagem pode ter acontecido durante a transmissão ou o canal é excepcionalmente ruidoso e incoerente com a aplicação.

O canal quântico é modelado como um canal simétrico binário (BSC – *Binary Symetric Channel*), para o qual p é a probabilidade de ruído a ser adicionado ao símbolo transmitido e $1 - p$ a probabilidade do símbolo ser corretamente recebido.

Com o intuito de corrigir a sequência de Bob sem divulgar informação suficiente que forneça a Eva meios de reconstruir a mesma sequência, um protocolo de reconciliação R^n é definido e executado resultando em uma sequência S conhecida unicamente pelas duas partes legítimas através da troca de informação C no canal público. Como C é trocada pelo canal público, Eva pode ganhar alguma informação sobre S , $I_E(S|C)$, motivo pelo qual apesar de Alice e Bob compartilham uma sequência binária idêntica com elevada probabilidade após a fase de reconciliação, essa não pode ser utilizada como uma chave.

Portanto, Alice e Bob devem mapear suas sequências através de uma função em um subconjunto menor, de modo a diminuir a informação de Eva sobre a chave a quase zero. Esse estágio é chamado amplificação de privacidade após o qual Alice e Bob compartilham uma chave secreta conhecida apenas por eles dois.

2.2.1 Distribuição Quântica de Chaves com Variáveis Contínuas

O BB84 é um protocolo que considera fótons isolados, ou seja, pode ser utilizado para distribuição de chaves quânticas com variáveis discretas. Entretanto, existem algumas desvantagens em se trabalhar com informação codificada na polarização ou fase de fótons isolados³ (NASCI-MENTO, 2017), por exemplo, do ponto de vista experimental, é requerida aparelhagem óptica especializada como geradores de fótons únicos e APDs (*Avalanche Photodiodes*) de grande eficiência (que são os limitadores da velocidade de geração de *bits* da chave).

Protocolos CV-QKD (*Continuous Variable Quantum Key Distribution*) padrões empregam modulações contínuas ou discretas das quadraturas dos campos eletromagnéticos e suas configurações dependem de uma detecção coerente (homódina ou heteródina) entre o sinal quântico e um sinal de referência clássico (oscilador local); sua implementação requer apenas componentes padrões de telecomunicações de modo que sistemas CV-QKD podem ser implementados nas redes atuais de telecomunicações utilizando redes de fibras ópticas bem estabelecidas e dispositivos práticos (JOUGUET; KUNZ-JACQUES; LEVERRIER, 2011), (JOUGUET; ELKOUSS; KUNZ-JACQUES, 2014). Além disso, são esperadas taxas de chave secreta mais elevadas quando comparado com protocolos DV-QKD (*Discrete Variable Quantum Key Distribution*) devido à possibilidade de codificar mais de um bit por pulso (JOUGUET; ELKOUSS; KUNZ-JACQUES, 2014), (ASSCHE; CARDINAL; CERF, 2004). Por outro lado, protocolos CV-QKD exigem algoritmos clássicos de correção de erros bem elaborados para extrair eficientemente *bits* secretos das variáveis contínuas correlacionadas (LODEWYCK et al., 2007).

A primeira etapa para implementação de um protocolo CV-QKD consiste na fase de comunicação quântica, na qual há a geração e transmissão de distribuições aleatórias de estados coerentes: Alice gera dois números aleatórios x_A e p_A com distribuição gaussiana e variância σ_x^2 e envia o estado coerente $|x_a + ip_A\rangle$ para Bob que, por sua vez, escolhe aleatoriamente me-

³ Para que a informação possa ser codificada na polarização, devido à a instabilidade de polarização induzida pela fibra óptica, esta necessita ter propriedades de manutenção da polarização.

dir uma das duas quadraturas X ou P ; através do canal clássico, fazendo uso de um esquema de autenticação para garantir que Eva não modificou as mensagens, ele informa a Alice sobre o observável que utilizou nas medições para que os erros provenientes de escolhas de bases diferentes sejam descartados, assim como no protocolo DV-QKD. Após a fase quântica, as partes legítimas compartilham duas sequências de realizações de variáveis aleatórias gaussianas correlacionadas (GROSSHANS; GRANGIER, 2002a), (ASSCHE; CARDINAL, 2003).

2.2.2 Fase de reconciliação

Devido ao canal quântico utilizado para QKD ser ruidoso, os valores possuídos por Alice e Bob após a fase quântica do processo divergem. Além disso, as leis da mecânica quântica afirmam que espionagem leva a discrepâncias adicionais, tornando a espia detectável. Uma compensação pode ser realizada em termos de correção dos erros entre as duas sequências através de um protocolo de reconciliação realizado através de um canal público autenticado.

As duas partes legítimas, Alice e Bob, têm acesso a variáveis aleatórias distintas: X para Alice e X' para Bob – que são os elementos brutos da chave e correspondem a variáveis aleatórias Gaussianas correlacionadas (GROSSHANS; GRANGIER, 2002a) – com informação mútua maior que zero, ou seja, $I_{AB} = I(X, X') > 0$. Quando o mesmo protocolo QKD é executado repetidas vezes, as instâncias de X são denotadas $X_1 \cdots X_r$ para os intervalos de tempo $1 \cdots r$, e são supostas independentes para diferentes intervalos de tempo. As variáveis aleatórias E , às quais uma espia tem acesso, também podem ser consideradas independentes para diferentes intervalos de tempo, ou seja, ataques individuais são assumidos (ASSCHE; CARDINAL; CERF, 2004). Pode-se assumir, ainda, sem perda de generalidade, que as saídas X de Alice determinam a chave bruta $K(X)$ – escolhida discreta ainda que X seja contínua⁴.

O processo de reconciliação consiste, portanto, na troca de mensagens de reconciliação pelo canal público autenticado (assumido perfeito, isto é, sem ruído) coletivamente denotadas C , de modo que Bob pode recuperar $K(X_{1..l})$ de C e $X'_{1..l}$.

Comprimindo $K(X_{1..l})$, Alice e Bob podem obter cerca de $IH(K(X))$ bits aleatórios em comum. Com a amplificação de privacidade a diminuição no comprimento da chave é aproximadamente igual a $I(K(X); E) + |C|$, onde $|C|$ é o número de bits trocados e $I(K(X); E)$ é determinado pela perturbação medida durante o procedimento QKD. Assim, maximizar a taxa

⁴ Apesar de se trabalhar com estados quânticos contínuos como portadoras de informação, tanto a chave secreta quanto as mensagens de reconciliação podem ser feitas discretas por essa abordagem apresentar uma série de vantagens: 1) é mais conveniente lidar com a igualdade dos valores de Alice e Bob em um caso discreto do que com limites de erros para números reais; 2) a não ser que o canal clássico público autenticado tenha capacidade infinita, as mensagens de reconciliação podem ser discretas ou valores contínuos com distorção. O último caso adiciona incertezas no protocolo, o que não é de interesse. Portanto, mensagens de reconciliação discretas são preferíveis; 3) uma mensagem de reconciliação ruidosa contínua se beneficiaria menos da característica de autenticação do canal clássico; um protocolo de autenticação terá dificuldade em reconhecer o ruído de um adversário ativo em oposição a um ruído intrinsecamente presente nas mensagens; 4) a escolha de uma chave final discreta induz efeitos discretos no protocolo, tornando natural a escolha de uma conversão contínuo-paradisco durante a reconciliação. (ASSCHE; CARDINAL; CERF, 2004)

da chave secreta

$$IH(K(X)) - [I(K(X); E) + |C|] \quad (2.2)$$

ou

$$H(K(X)) - I(K(X); E) - l^{-1}|C| \quad (2.3)$$

envolve levar em conta todas as estratégias de espionagem durante a otimização.

Assim, o tamanho final da chave secreta gerada pelo procedimento de QKD depende:

1. dos dados brutos em comum após a correção de erros, $K(X)$;
2. da quantidade de informação que foi revelada durante a fase de correção de erros, $|C|$;
3. de uma estimativa superior da quantidade de informação obtida por Eva através de sua interação com o canal quântico, $I(K(X); E)$.

No entanto, pode-se notar pela desigualdade do processamento de dados que $I(K(X); E) \leq I(X; E)$, onde $I(X; E)$ é independente do processo de reconciliação. Logo, busca-se maximizar

$$I_{Rec} = H(K(X)) - l^{-1}|C| \quad (2.4)$$

Um esquema de correção de erros perfeito recupera a informação mútua entre Alice e Bob, ou seja, a quantidade de dados auxiliares revelados para realizar a correção de erros subtraída da quantidade de informação comum após a correção de erros é igual a I_{AB} . Entretanto, esquemas práticos extraem apenas uma quantidade de informação βI_{AB} , com $0 < \beta < 1$ (JOUQUET; EL-KOUSS; KUNZ-JACQUES, 2014) de modo que a quantidade final de chave secreta produzida por um protocolo QKD com reconciliação direta⁵ e reversa⁶, respectivamente, pode ser dada por

$$\Delta I = \beta I_{AB} - \chi_{AE} \quad (2.5)$$

$$\Delta I = \beta I_{AB} - \chi_{BE} \quad (2.6)$$

onde β é o fator de eficiência da reconciliação, que caracteriza quão próximo do limite de Shannon o algoritmo de reconciliação opera (LODEWYCK et al., 2007), I_{AB} é a informação mútua clássica entre Alice e Bob e χ_{AE} e χ_{BE} , representam a informação de Holevo⁷ de Alice para Eva e Bob para Eva, respectivamente.

⁵ Bob reconstrói o que foi enviado por Alice a partir de dados adicionais revelados por ela, de modo que a informação clássica flui na mesma direção que a informação quântica (GROSSHANS; GRANGIER, 2002b).

⁶ Alice adapta sua sequência binária para o que foi recebido por Bob, a partir de dados adicionais revelados por ele.

⁷ Relacionada à quantidade de informação clássica que pode ser armazenada e recuperada de um sistema quântico (CALTECH, 2015), também chamada de informação vazada para reconciliação direta e reversa (BAI et al., 2017).

2.3 Correção de Erros por Fatiamento

A correção de erros por fatiamento foi proposta em (ASSCHE; CARDINAL; CERF, 2004) como um esquema genérico de reconciliação para fontes não-binárias usando códigos de correção de erros binários.

Uma aplicação importante da correção de erro por fatiamento é corrigir variáveis aleatórias Gaussianas correlacionadas, $X \sim N(0, \Sigma)$ e $X' = X + \epsilon$ com $\epsilon \sim N(0, \sigma)$, com X e X' definidas nos conjuntos \mathcal{X} e \mathcal{X}' . Para manter a generalidade, Alice e Bob podem processar valores de chaves multidimensionais, agrupados em vetores d-dimensionais, de modo que $X, X' \in \mathbb{R}^d$, ou seja, assumem valores no espaço da chave bruta, \mathbb{R}^d , para variáveis Gaussianas.

Para compreensão do protocolo, faz-se importante definir as funções de fatiamento.

Definição: Se $S(x)$ é uma função de fatiamento do espaço da chave bruta de Alice, \mathcal{X} , para $\text{GF}(2)^8$, ou seja, $\{0, 1\}$, um vetor de funções de fatiamento $S_{1\dots m}(x) = (S_1(x), \dots, S_m(x))$ é assim definido quando mapeia os elementos de chave bruta de Alice em dígitos binários, ou seja, $K(x) = S_{1\dots m}(x)$, de modo que o alfabeto discreto tem tamanho máximo 2^m , como pode ser visto na figura 1.

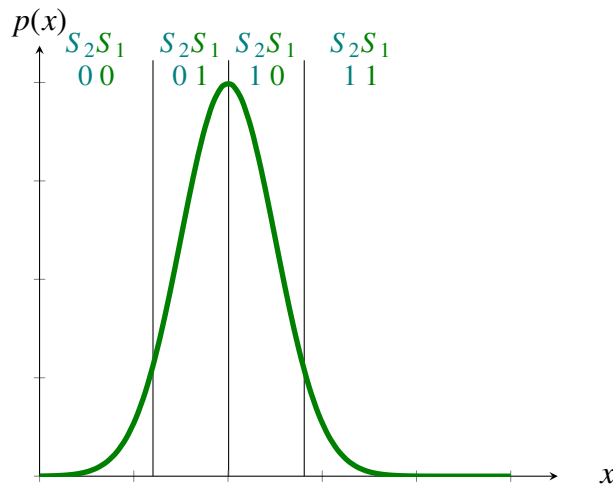


Figura 1 – Protocolo SEC.

Cada um dos estimadores

$$\tilde{S}_1(x'), \tilde{S}_2(x', S_1(x)), \dots, \tilde{S}_m(x', S_1(x), \dots, S_{m-1}(x)) \quad (2.7)$$

define um mapeamento do espaço da chave bruta de Bob e das funções de fatiamento de Alice de índices menores em $\text{GF}(2)$. Tais estimadores são usados por Bob para “adivinhar” $S_i(X)$ com conhecimento de X' e dos *bits* previamente corrigidos. A construção das funções de fatiamento $S_i(X)$ e dos seus estimadores depende da natureza e distribuição dos elementos da chave bruta.

⁸ $\text{GF}(2)$, em álgebra abstrata, é o corpo finito com dois elementos, 0 e 1.

Uma descrição do protocolo genérico assume que as partes definem e concordam nas funções S_i e \tilde{S}_i , e escolhem um comprimento de bloco l , independente da dimensão de X e X' , de modo que Alice processa l elementos da chave x_j , $j = 1, \dots, l$ assim como Bob para x'_j , $j = 1, \dots, l$. Assume-se, ainda, que os l valores x_j (ou x'_j) são saídas independentes de x (ou x') para diferentes índices j .

De $i = 1$ a m , sucessivamente, Alice e Bob realizam os seguintes passos:

- Alice prepara a sequência de *bits* $(S_i(x_1), \dots, S_i(x_l))$;
- Bob prepara uma sequência de *bits* $(\tilde{S}_i(x'_1, S_1(x), \dots, S_{1\dots i-1}(x_1)), \dots, \tilde{S}_i(x'_1, S_1(x), \dots, S_{1\dots i-1}(x_l)))$, onde a fatia $S_{1\dots i-1}(x_1)$ é conhecida por Bob, com elevada probabilidade, dos $i - 1$ passos anteriores;
- Alice e Bob fazem uso de um BCP escolhido de modo que Bob adquira conhecimento dos bits de Alice $(S_i(x_1), \dots, S_i(x_l))$.

Exemplo 1: Considerando que as variáveis aleatórias de Alice e Bob sejam desenhadas seguindo as distribuições mostradas na figura 2, se Alice envia uma realização de X , $x = 0, 2$ e Bob mede $x' = -0, 1$ devido ao ruído no canal quântico, a quantização do valor de Alice é feita diretamente, de modo que, $S_3(x_1)S_2(x_1)S_1(x_1) = 100$, enquanto que a sequência binária de Bob é gerada em uma série de passos que leva em conta as realizações de X' conjuntamente com as funções $S(x)$ de índices menores, conhecidas com elevada probabilidade por Bob: seja porque Alice as divulgou para ajudá-lo na estimação, no caso das fatias mais ruidosas, ou porque a probabilidade de erro para as últimas fatias é relativamente baixa. Nesse caso, Bob estima $\tilde{S}_1(x'_1 = -0, 1) = 1$; considerando que Alice divulga essa fatia por ser a mais ruidosa, Bob então passa a conhecer $S_1(x_1) = 0$ e corrige a sua estimação $\tilde{S}_1(x'_1) = S_1(x_1) = 0$. Em seguida ele repete o procedimento para $\tilde{S}_2(x'_1 = -0, 1; S_1(x_1) = 0)$, se essa estimação levasse em conta apenas o fato de que x'_1 é conhecido, $\tilde{S}_2(x'_1) = 1$, devido ao intervalo no qual o valor da realização de x' se encontra; entretanto, sendo conhecido por Bob o valor de $S_1(x_1)$, a possibilidade de intervalos nos quais x_1 pode se encontrar fica restrito a apenas quatro, para os quais x'_1 se aproxima mais daquele que leva $\tilde{S}_2(x'_1 = -0, 1; S_1(x_1) = 0) = 0$. Repetindo o mesmo procedimento para a terceira função de fatiamento, Bob chega a conclusão que $\tilde{S}_3(x'_1 = -0, 1; S_1(x_1) = 0; S_2(x_1) = 0) = 1$ e, portanto, $\tilde{S}_3(x'_1; S_1(x_1); S_2(x_1))\tilde{S}_2(x'_1; S_1(x_1))\tilde{S}_1(x'_1) = 100$.

O objetivo do SEC é obter *bits* comuns a Alice e Bob (isto é, $l \times m$ bits $K(x) = S_{1\dots m}(x_j)$, $j = 1, \dots, l$) divulgando o mínimo de informação possível. A quantidade de informação vazada no canal público durante o protocolo depende do BCP primitivo utilizado (ASSCHE; CARDINAL; CERF, 2004).

Se o SEC não é aplicado, em teoria, quando $l \rightarrow \infty$, a informação vazada em função da

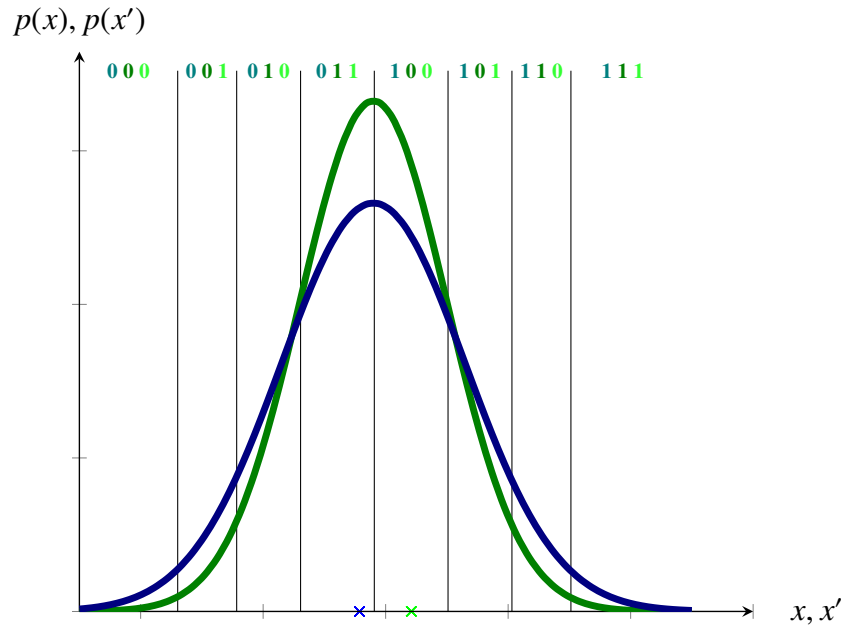


Figura 2 – Exemplo para o protocolo SEC.

incerteza sobre a sequência binária de Alice dado que Bob conhece X' é de:

$$I^{-1}|C| = I_0 \triangleq H(S_{1\dots m(X)}|X') \quad (2.8)$$

Quando se usam as funções de fatiamento, no entanto, o BCP não utiliza o X' diretamente, em vez disso, processa os *bits* calculados por Alice $S_i(X)$ de um lado e aqueles calculados por Bob, $\tilde{S}_i(X', S_{1\dots i-1}(X))$, do outro lado – onde os l *bits* produzidos pelas funções são independentes para diferentes intervalos de tempo. Assumindo um BCP perfeito, tem-se

$$I^{-1}|C| = I_s \triangleq \sum_{i=1}^m H(S_i(X)|\tilde{S}_i(X', S_{1\dots i-1}(X))) \geq I_0 \quad (2.9)$$

Cuja desigualdade vem do fato de que

$$H(S_{1\dots m(X)}|X') = \sum_{i=1}^m H(S_i(X)|X', S_{1\dots i-1}(X)) \quad (2.10)$$

e que, pela desigualdade do processamento de dados, o termo do somatório não pode diminuir se substituído por $H(S_i(X)|\tilde{S}_i(X', S_{1\dots i-1}(X)))$.

Para o BCP trabalhando em um canal binário simétrico (BSC-BCP) em escala sub-ótima para sequências não-balanceadas das quais não se reduz todas as redundâncias, Assche e outros (ASSCHE; CARDINAL; CERF, 2004) afirmam que o número de *bits* revelados se torna:

$$I^{-1}|C| = I_e \triangleq \sum_{i=1}^m h(e_i) \geq I_s \quad (2.11)$$

com $h(e) = -e \log e - (1 - e) \log(1 - e)$ e $e_i = Pr[S_i(X) \neq \tilde{S}_i(X', S_{1 \dots i-1}(X))]$; onde a desigualdade vem da desigualdade de Fano aplicada a um alfabeto binário. Na prática, é esperado que um BSC-BCP divulgue um número de *bits* aproximadamente proporcional a $h(e)$, ou seja, $(1 + \epsilon)h(e)$ para alguma constante ϵ de modo que $l^{-1}|C| \geq I_e$.

É possível minimizar localmente o número de *bits* vazados $l^{-1}|C|$ sem afetar o número de *bits* produzidos $H(K(X))$ através da minimização de I_e atuando em cada estimador individualmente⁹.

Assumindo variáveis contínuas X e X' com função densidade de probabilidade $P_{XX'}(x, x')$, a probabilidade de erro na fatia i é a probabilidade do estimador de Bob levar a um resultado diferente da função de fatiamento de Alice

$$e_i = Pr[S_i(X) \neq \tilde{S}_i(X', S_{1 \dots i-1}(X))] \quad (2.12)$$

$$e_i = \int dx' \sum_{\gamma \in GF(2)^{i-1}} Pr[S_i(X) \neq \tilde{S}_i(x', \gamma) | S_{1 \dots i-1}(X) = \gamma, X' = x'] \quad (2.13)$$

onde cada termo no lado direito da equação (2.13) integra $p_{XX'}(x, x')$ sobre áreas não sobrepostas do plano (x, x') e γ representa os valores correspondentes às funções de fatiamento de índices menores de Alice, conhecidas por Bob com elevada probabilidade.

Para minimizar e_i , \tilde{S}_i deve satisfazer

$$\tilde{S}_i(x', \beta) = \arg \min_{\tilde{s}} Pr[S_i(X) \neq \tilde{s} \wedge S_{1 \dots i-1}(X) = \beta \wedge X' = x'] \quad (2.14)$$

$$= \arg \max_{\tilde{s}} Pr[S_i(X) = \tilde{s} | S_{1 \dots i-1}(X) = \beta, X' = x'] \quad (2.15)$$

com uma regra apropriada de desempate.

Segundo (ASSCHE; CARDINAL; CERF, 2004), a probabilidade de erro é mínima quando as variáveis x' e $\beta_{1 \dots i-1}$ determinam $S_i(x)$ sem ambiguidade.

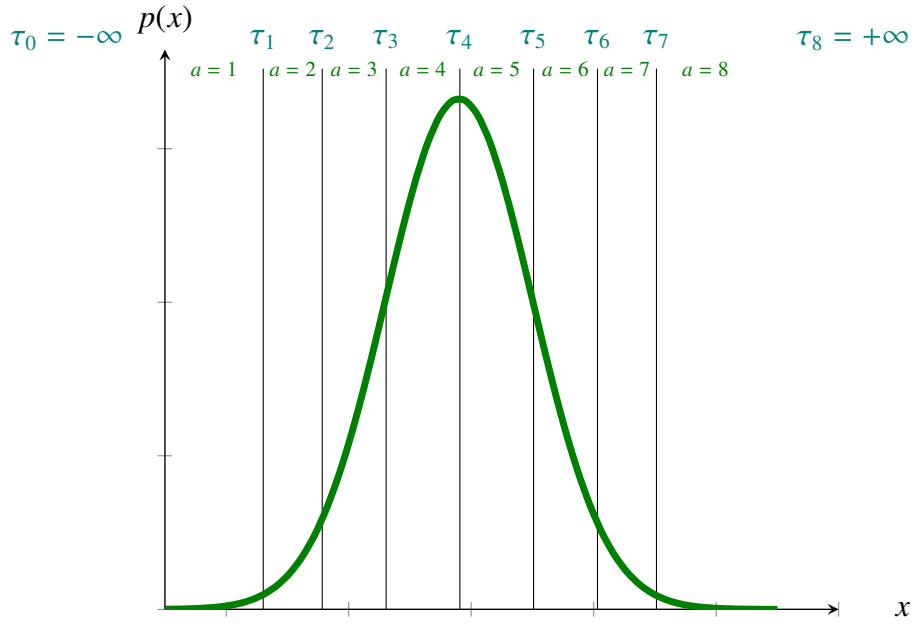
Uma forma de otimizar as funções S_i é, primeiramente, dividir o conjunto de números reais em um número escolhido de intervalos – chamando esse processo por $T(X)$ – para que Alice mapeie seu valor X em um valor binário $K = T(X)$; ou seja, para o número escolhido de intervalos busca-se maximizar $I(T(X); X')$ para que em seguida seja possível a associação de m valores binários a esses intervalos de modo que as fatias possam ser corrigidas com tão pouca informação vazada quanto possível.

Conforme apresentado em (ASSCHE; CARDINAL, 2003), um limite superior para a quantidade de informação compartilhada entre Alice e Bob, em *bits*, é de

$$I(K; X') = H(K) - H(K|X') \quad (2.16)$$

O processo $T(X)$ de dividir os números reais em t intervalos é definido por $t - 1$ variáveis $\tau_1, \dots, \tau_{t-1}$ e o intervalo a , com $1 \leq a \leq t$, pelo conjunto $x : \tau_{a-1} \leq x < \tau_a$ com $\tau_0 = -\infty$ e $\tau_t = +\infty$, como pode ser observado na Figura 3 para $t = 8$.

⁹ Minimização de cada e_i , para o qual $h(e_i)$ é uma função crescente para o intervalo $0 \leq e_i \leq 1/2$


 Figura 3 – Processo $T(X)$ do protocolo SEC, para $t = 8$.

De acordo com a prova exibida em (ASSCHE; CARDINAL, 2003), o processo $T(X)$ é, portanto, solução de

$$\arg \max_T I(K; X') = \arg \min_T E_X [D(P_{X'|X} \| P_{X'|K})] \quad (2.17)$$

onde a função $D(p||q)$ é a divergência de Kullback-Leibler (KL) ou entropia relativa de p em relação a q .

Assim, em concordância com (ASSCHE; CARDINAL, 2003) e (XUDONG; GUANGQI-ANG; GUIHUA, 2009), a realização de x do valor contínuo X do lado de Alice deve ser mapeado por $T(X)$ no valor K da chave tal que

$$T(x) = \arg \min_k D(P_{X'|X=x} \| P_{X'|K=k}) \quad (2.18)$$

ou seja, para o k cuja distribuição $P_{X'|K=k}$ seja o vizinho mais próximo de $P_{X'|X=x}$ em termos da distância de KL. Portanto, o mapeamento $T(X)$ é definido através das distribuições $P_{X'|K=k}$ que, por sua vez, dependem de $T(X)$, sendo necessário um algoritmo no qual o mapeamento e as probabilidades condicionais sejam atualizadas alternadamente (ASSCHE; CARDINAL, 2003).

Definindo $\{f_k\}_{k=1}^t$ como o dicionário de distribuições de probabilidade de X' e as células de quantização $Q_k = \{x | T(x) = k\}$ – subconjuntos dos reais cujos elementos são mapeados no mesmo índice k –, o quantizador é completamente definido pela partição $\{Q_k\}_k$. O seguinte algoritmo é então aplicado:

1. Escolher aleatoriamente t intervalos Q_k ;

2. Calcular a densidade de probabilidade condicional média de cada intervalo

$$\forall k : f_k = E[p(x'|X)|X \in Q_k] \quad (2.19)$$

3. Atualizar as células de quantização com os valores de x que levam a uma menor distância no sentido KL entre $p(x'|X = x)$ e f_k

$$\forall k : Q_k \leftarrow \{x | \forall j \neq k D(p(x'|X = x) || f_j) > D(p(x'|X = x) || f_k)\} \quad (2.20)$$

4. Continuar os passos acima até a convergência.

Uma vez otimizada a informação mútua entre $T(X)$ e X' em função do número de intervalos escolhido, o próximo passo é construir m funções $S(x)$ que retornem valores binários para cada intervalo: Assche e outros (ASSCHE; CARDINAL; CERF, 2004) propõem que o *bit* menos significativo seja associado à primeira função de fatiamento e o mais significativo à última, $S_m(x)$, de modo que as primeiras fatias contendo os valores mais ruidosos são normalmente aquelas divulgadas sem utilização de códigos corretores de erros ajudando Bob a estreitar seu palpite tão rápido quanto possível, pela redução na taxa de erro das últimas fatias, que compõem a informação secreta compartilhada (ASSCHE; CARDINAL; CERF, 2004).

2.4 Códigos Corretores de Erros

Através da codificação é possível transmitir informação de maneira eficiente e confiável, isto é, recriar a informação transmitida com tão pouca distorção quanto desejado para o receptor faz-se uma tarefa exequível (RICHARDSON; URBANKE, 2008). Para reduzir a complexidade de descrição de códigos corretores de erros, em termos da memória exigida para definir o código, que se torna excessiva quando o comprimento, n , fica suficientemente elevado – condição necessária para que o código seja adequado para transmissão confiável com taxas próximas a capacidade de Shannon com probabilidade de erro baixa (RICHARDSON; URBANKE, 2008) – pode-se restringir a atenção a códigos lineares, definidos sobre o corpo \mathbb{F} como

$$\alpha x + \alpha' x' \in C, \forall x, x' \in C \text{ e } \alpha, \alpha' \in \mathbb{F} \quad (2.21)$$

A dimensão d de um código C é definida como o inteiro, $0 \leq d \leq n$, que determina o número de palavras-código que C contém, isto é, $|\mathbb{F}|^d$. A matriz geradora de C , $G \in \mathbb{F}^{d \times n}$, é aquela que descreve o código, tal que:

$$C(G) = \{x \in \mathbb{F}^n : x = uG, u \in \mathbb{F}^d\} \quad (2.22)$$

Para cada código linear C é associado um código dual C^\perp , cuja base é chamada matriz teste de paridade, H , do código original C , descrito por

$$C^\perp = \{v \in \mathbb{F}^n : xv^T = 0, \forall x \in C\} = \{v \in \mathbb{F}^n : Gv^T = 0^T\} \quad (2.23)$$

Ou seja, as linhas de H formam a base de um espaço ortogonal ao espaço gerado pelo código C .

A taxa de um código, R , é definida como a razão entre os *bits* de informação, k , e o número total de *bits* transmitidos no canal, n , de modo que quanto menor a taxa de um código, mais redundâncias este possui. Logo, corrigir erros para baixos valores de SNR requer projetar códigos com baixas taxas para que a maior quantidade de redundâncias auxilie a corrigir maior quantidade de *bits* (JOUGUET; KUNZ-JACQUES; LEVERRIER, 2011). Assim, os códigos em questão devem ser projetados para canais e SNRs específicos.

A taxa da codificação é limitada superiormente pela capacidade do canal associado, entretanto, este limite só pode ser alcançado no limite de códigos assintoticamente grandes, de modo que códigos reais, de tamanho finito, introduzem outra fonte de ineficiência (JOUGUET; ELKOUSS; KUNZ-JACQUES, 2014). Bai e outros (BAI et al., 2017) mostram que a eficiência da reconciliação por fatiamento, onde cada uma das m fatias é codificada independentemente como a síndrome de um código corretor de erros com taxa R_i ($1 \leq i \leq m$) é dada por

$$\beta_{rec} = \beta_{slice} \cdot \beta_{code} \quad (2.24)$$

$$\beta_{slice} = \frac{I(X; Q(X'))}{I(X; X')} \quad (2.25)$$

$$\beta_{code} = \frac{H(Q(X')) - m + \sum_{i=1}^m R_i}{I(X; Q(X'))} \quad (2.26)$$

Onde $Q(X')$ representa a versão quantizada de X' . Deste modo,

$$\beta_{rec} = \frac{H(Q(X')) - m + \sum_{i=1}^m R_i}{I(X; X')} \quad (2.27)$$

Portanto, evidencia-se que β depende das taxas dos códigos disponíveis (e do quão próximos estes encontram-se das capacidades dos canais), razão pela qual os códigos LDPC (Low Density Parity Check) se apresentam como uma boa alternativa ao problema exposto, por operarem próximo à capacidade dos canais binários simétricos (BSCs – *Binary Symmetric Channels*) (JOUGUET; ELKOUSS; KUNZ-JACQUES, 2014) e por apresentarem desempenhos que podem se encontrar bem próximos ao limite de Shannon (ZHIXIN et al., 2010).

2.4.1 Códigos LDPC

Os códigos LDPC (ou códigos de Gallager) são códigos lineares de correção de erros, logo, podem ser expressos como o espaço nulo de uma matriz teste de paridade H , isto é, x é uma palavra-código se e somente se

$$Hx^T = 0^T \quad (2.28)$$

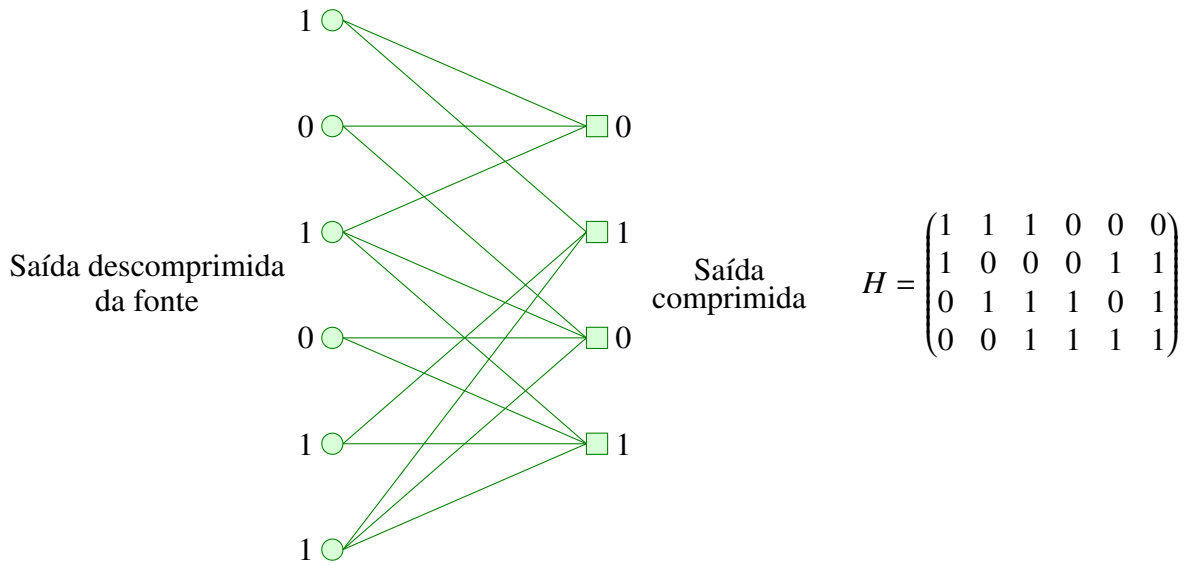


Figura 4 – Grafo bipartido para código LDPC de comprimento de palavra-código $N = 6$ e distribuições $\lambda(x) = \frac{4}{7}x + \frac{3}{7}x^2$ e $\rho(x) = \frac{3}{7}x^2 + \frac{4}{7}x^3$.

A matriz de teste de paridade – que é escolhida aleatoriamente – deve ser esparsa, caracterizando o termo “baixa densidade”, o que permite uma baixa complexidade para realizar o processo de decodificação. A esparsidade de H permite decodificação eficiente (sub-ótima) e a aleatoriedade garante um bom código com elevada probabilidade (RICHARDSON; URBANKE, 2001).

Associado a $H_{m \times n}$ existem diversos grafos de Tanner, isto é, grafos bipartidos com n nós de variável, correspondendo às componentes da palavra-código, e m nós de paridade, correspondendo ao conjunto de restrições¹⁰ de teste de paridade (linhas de H). O nó de paridade j é conectado ao nó de variável i se $H_{ji} = 1$ (RICHARDSON; URBANKE, 2008), conforme ilustrado na figura 4.

Um conjunto de grafos bipartidos pode ser definido em termos de um par de distribuições de graus $\gamma(x) = \sum_i \gamma_i x^{i-1}$, que são polinômios com coeficientes não-negativos satisfazendo $\gamma(1) = 1$ onde γ_i representa a fração dos arcos em um grafo que incidem em um nó de grau i (RICHARDSON; URBANKE, 2001). Assim, todos os grafos em um conjunto $\mathcal{C}^n(\lambda, \rho)$ têm nós à esquerda (de variáveis) associados a λ e nós à direita (de paridades) associados a ρ :

$$\lambda(x) = \sum_{i \geq 1} \lambda_i x^{i-1} \tag{2.29}$$

$$\rho(x) = \sum_{i \geq 1} \rho_i x^{i-1} \tag{2.30}$$

(RICHARDSON; URBANKE, 2008) garantem que o uso de códigos irregulares – códigos para os quais os graus dos nós são escolhidos seguindo alguma distribuição de probabilidade

¹⁰ Conjunto de equações de teste de paridade que definem o código.

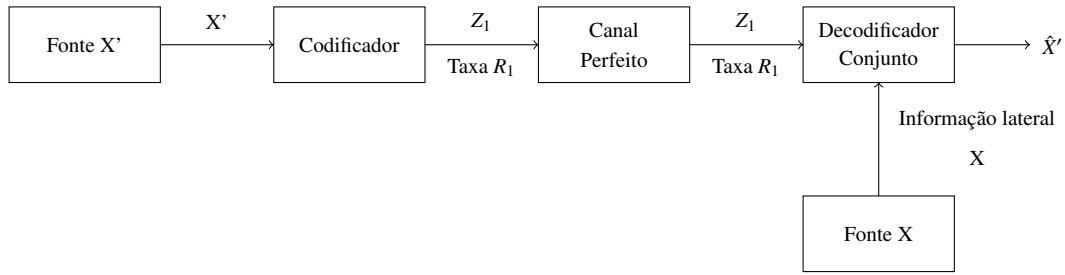


Figura 5 – Decodificação conjunta de fontes de informação correlacionadas.

– dentre outras melhorias estruturais, pode melhorar o comportamento de códigos LDPC; e, ainda, podem ser construídos de modo a garantir complexidade de codificação linear com o comprimento de bloco N (RICHARDSON; URBANKE, 2001).

A decodificação geralmente é feita através de decodificadores por passagem de mensagens: partindo do conhecimento de que existem mensagens recebidas associadas aos nós de variáveis resultantes da passagem dos correspondentes *bits* da palavra-código pelo canal, em cada etapa do algoritmo de decodificação, uma mensagem é enviada de cada nó de variável para cada nó de paridade vizinho, indicando alguma estimativa do valor do *bit* associado. Com base nessa informação, cada nó de paridade envia de volta mensagens para os nós de variáveis, com a ressalva de enviar apenas informação extrínseca, isto é, a mensagem enviada ao longo de um arco não pode depender da mensagem que é recebida pelo mesmo arco (RICHARDSON; URBANKE, 2001).

2.5 Codificação de Fontes de Informação Correlacionadas

Devido à correlação existente entre as variáveis aleatórias gaussianas das quais Alice e Bob estão em posse ao fim da transmissão quântica, de modo que a informação mútua entre as sequências das realizações de tais variáveis é maior que zero, $I_{AB} = I(X; X') > 0$ (GROSSHANS; GRANGIER, 2002a), garante-se que Bob já possui alguma informação sobre a chave $K(X)$ a ser compartilhada, que pode ser utilizada como informação lateral para auxiliá-lo na obtenção desta, no caso de um protocolo de reconciliação direta, possibilitando a divulgação de menos *bits* pelo canal clássico público (versão comprimida de X). Desta forma, o modelo adotado neste trabalho para a reconciliação das chaves secretas considera as partes legítimas como fontes correlacionadas¹¹ que geram realizações de variáveis aleatórias gaussianas independentes para diferentes intervalos de tempo, conforme abordado por (LIVERIS; XIONG; GEORGHIADIS, 2002) e mostrado na Figura 5.

Cover e Thomas (COVER; THOMAS, 2006) mostraram que para codificar unicamente uma fonte X uma taxa $R > H(X)$ é suficiente para que esta possa ser recuperada perfeitamente e, para duas fontes $(X, X') \sim p(x, x')$, uma taxa $R > H(X, X')$ é suficiente para codificá-las conjunta-

¹¹ Sequência de variáveis aleatórias i.i.d. distribuídas conjuntamente $\sim p(x, x'), (X_1, X'_1), (X_2, X'_2), \dots, (X_n, X'_n)$, assumindo uma sequência X disponível em uma localização A e uma sequência X' disponível em B.

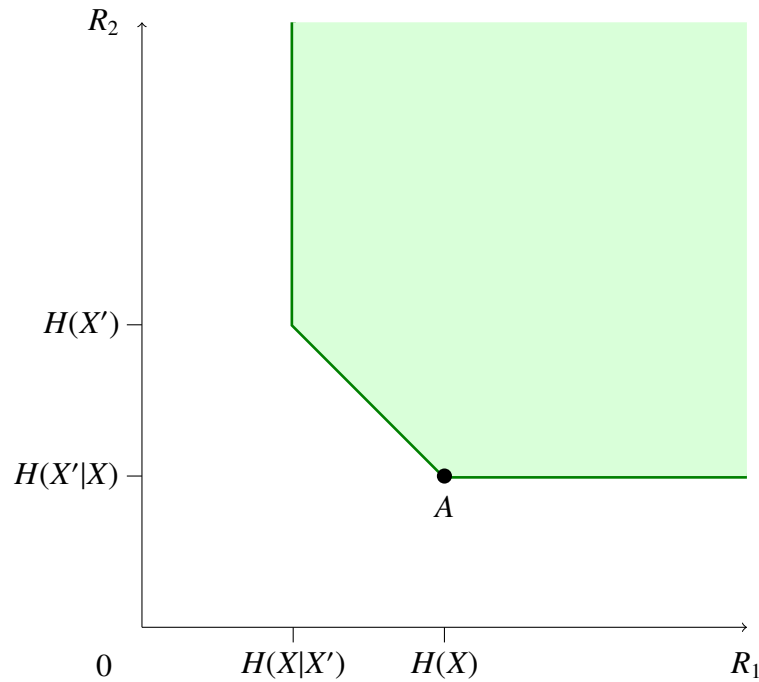


Figura 6 – Taxas para codificação Slepian-Wolf.

mente. O caso de interesse, entretanto, requer descrição das fontes X e X' separadamente para que o usuário possa reconstruir tanto X quanto X' , caso para o qual a codificação separada de X e X' com taxa $R = R_X + R_{X'} > H(X) + H(X')$ mostra-se suficiente para reconstruir as duas sequências separadamente (COVER; THOMAS, 2006). (SLEPIAN; WOLF, 1973), todavia, mostraram que a região de taxas alcançáveis para esse problema, para recuperação perfeita das duas sequências em um receptor comum, é aquela identificada por

$$R_1 \geq H(X|X') \quad (2.31)$$

$$R_2 \geq H(X'|X) \quad (2.32)$$

$$R_1 + R_2 \geq H(X, X') \quad (2.33)$$

onde $H(X|X')$ é a entropia condicional da fonte X dado a fonte X' , $H(X'|X)$ é a entropia condicional da fonte X' dado a fonte X e $H(X, X')$ é a entropia conjunta. A região descrita pelo teorema de Slepian-Wolf é ilustrada na Figura 6.

Considerando um esquema de reconciliação reversa e codificando independentemente a sequência binária de Bob com um codificador de fonte que conhece a correlação média entre as fontes X e X' e assumindo que a sequência discretizada de Alice é comprimida para sua entropia de fonte $H(X)$, sendo conhecida pelo decodificador como informação lateral, o objetivo é comprimir a sequência X^m com uma taxa $R_{X'}$ o mais próxima possível da entropia condicio-

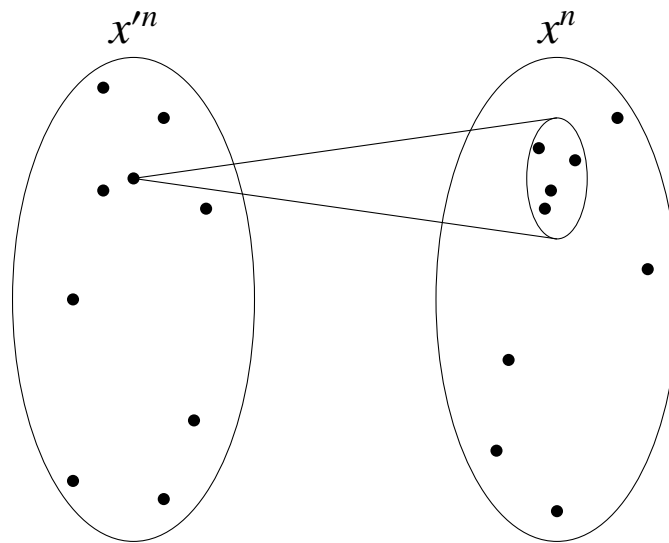


Figura 7 – Sequências conjuntamente típicas

nal $R_{X'} \geq H(X'|X)$ alcançando o ponto A na Figura 6. Uma forma de interpretar tal codificação baseada no teorema de Slepian-Wolf é verificar que, para este ponto,

1. Utilizando $nH(X')$ bits pode-se codificar X^m eficientemente de modo que o decodificador possa reconstruir X^m com probabilidade de erro arbitrariamente baixa.
2. Associado com cada X^m existem sequências de X^n que são conjuntamente típicas com o X^m dado (ver Figura 7);
3. Se o decodificador de X^n conhece X^m com elevada probabilidade:
 - O codificador pode enviar o índice de X^n dentro de um subconjunto de X^n que é conjuntamente típico com o X^m fornecido;
 - O decodificador pode construir esse subconjunto e assim reconstruir X^n .

Assim, a sequência X' da fonte de tamanho k é codificada e transmite-se em um canal perfeito apenas a sequência de paridade Z . De acordo com o teorema de Slepian-Wolf, o problema consiste em codificar a fonte X' com uma taxa $R_{X'}$ tão próxima de $H(X'|X)$ quanto possível. O objetivo do decodificador conjunto é recuperar X' a partir de uma fonte X correlacionada usada como informação lateral e da estimativa de correlação entre ambas as fontes obtida a partir do conhecimento da SNR do canal em uso.

Teorema: Como a sequência X está disponível sem erros no decodificador ($R_X = 1$), o limite teórico para compressão de X' é $R_{X'} \geq H(X'|X) = \mathcal{H}(p)$ ¹², em que $p = P(x'_j \neq x_j)$, $\forall j = 1, \dots, k$.

¹² $\mathcal{H}(p)$ é a entropia binária

Prova Para o canal binário simétrico, representado pela Tabela 3, tem-se

Tabela 3 – Tabela de probabilidades para o canal BSC

$X' \setminus X$	0	1	$P(X)$
0	$\frac{1-p}{2}$	$\frac{p}{2}$	$\frac{1}{2}$
1	$\frac{p}{2}$	$\frac{1-p}{2}$	$\frac{1}{2}$
$P(X')$	$\frac{1}{2}$	$\frac{1}{2}$	1

$$\begin{aligned}
 H(X, X') &= -2\frac{p}{2} \log \frac{p}{2} - 2\frac{1-p}{2} \log \frac{1-p}{2} \\
 &= -p \log p + p \log 2 - (1-p) \log(1-p) + (1-p) \log 2 \\
 &= \mathcal{H}(p) + p + 1 - p \\
 &= \mathcal{H}(p) + 1
 \end{aligned} \tag{2.34}$$

Como a taxa para codificar a fonte X' deve ser $R_{X'} \geq H(X'|X)$, tem-se

$$\begin{aligned}
 R_{X'} &\geq H(X, X') - H(X) \\
 &= \mathcal{H}(p) + 1 - 1 \\
 &= \mathcal{H}(p)
 \end{aligned} \tag{2.35}$$

□

O codificador tem conhecimento da SNR do canal, logo, da correlação média, de modo a escolher uma taxa próxima de $\mathcal{H}(p)$ mantendo k constante e escolhendo n de forma apropriada (nenhuma informação acerca da taxa é passada ao decodificador, este conhece a correlação média de forma implícita a partir do tamanho de bloco n).

EXEMPLO 2: Após a discretização das realizações das variáveis aleatórias gaussianas correlacionadas de Alice e Bob e assumindo que o primeiro *bit* da sequência binária gerada por uma realização de X' é zero com probabilidade 0,5 e que o primeiro *bit* da sequência binária gerada por uma realização de X é igual ao de Bob com probabilidade 0,89. A distribuição conjunta para o primeiro *bit* é dada pela Tabela 4.

Assumindo um esquema de compressão de fontes trabalhando no ponto A da Figura 6, para o qual Alice e Bob desejam compartilhar apenas o primeiro *bit* da discretização de 100 realizações das variáveis aleatórias correlacionadas X e X' , Bob irá utilizar $100 \cdot H(X') = 100 \cdot \mathcal{H}(0,5) = 100$ *bits* da sua sequência como informação lateral no decodificador; de maneira análoga, Alice codifica sua sequência fazendo uso de $100 \cdot H(X|X') = 100 \cdot H(0,89) = 50$ *bits* que são divulgados pelo canal clássico para que Bob consiga corrigir os erros da sua sequência. Através do teorema

de Slepian-Wolf, caso Alice e Bob divulgem conjuntamente $H(X') + H(X|X') = 100 + 50 \text{ bits}$ no total, Eva é capaz de recuperar ambas as sequências.

$p(x, x')$	x=0	x=1
x'=0	0,445	0,055
x'=1	0,055	0,445

Tabela 4 – Distribuição conjunta para o primeiro *bit* da discretização de x e x' para o Exemplo 2.

Capítulo 3

Revisão Bibliográfica

Um dos desafios de protocolos CV-QKD é o projeto de algoritmos clássicos de correção de erros bem elaborados que permitam extrair eficientemente *bits* secretos a partir de variáveis contínuas correlacionadas (LODEWYCK et al., 2007), principalmente em regime de baixa SNR, para o qual é muito difícil para o CV-QKD conseguir uma reconciliação de erros eficiente (LI et al., 2016), limitando, muitas vezes, a operação a distâncias que podem ser insuficientes para aplicações criptográficas de rede (JOUGUET et al., 2012) (LODEWYCK et al., 2007).

Com o objetivo de distribuir uma chave secreta através de um protocolo CV-QKD com uma modulação Gaussiana, em regime de SNR baixa para alcançar maiores distâncias, diferentes abordagens foram exploradas para aumentar a eficiência de reconciliação, uma vez que a distância máxima de transmissão alcançável depende de β (BAI et al., 2017) (JOUGUET; KUNZ-JACQUES; LEVERRIER, 2011):

- Em 2004, Assche e outros (ASSCHE; CARDINAL; CERF, 2004) propuseram o algoritmo de Correção de Erros por Fatiamento (SEC – *Sliced Error Correction*) – no qual uma variável contínua é quantizada em uma sequência binária e um protocolo de correção binário (BCP – *Binary Correction Protocol*) é aplicado a cada *bit* da sequência para obtenção de uma chave secreta comum às partes legítimas do protocolo considerado, conforme apresentado na seção (2.3).
- Em 2006, Bloch e outros (BLOCH et al., 2006) utilizaram técnicas de modulação de códigos MLC/MSD¹ adaptadas e aplicadas com códigos LDPC para codificação de canal e correção de erros com SEC, utilizando uma quantização de quatro *bits*, dos quais apenas dois foram codificados, e códigos LDPC de comprimento $n = 200.000$, obtendo uma eficiência de reconciliação $\beta = 0,887$ para uma SNR de aproximadamente 4,8 dB. As

¹ Para reconciliação MLC/MSD, m códigos individuais são aplicados às m sequências binárias S_m , de modo que quando códigos que se aproximam da capacidade do canal são usados, MLC/MSD é ótimo (BAI et al., 2017). A codificação MLC protege os *bits* de informação com diferentes pesos através de diferentes taxas para níveis distintos (ZHIXIN et al., 2010).

taxas requeridas para cada um dos níveis foram de $R_1^{opt} = 0,002$, $R_2^{opt} = 0,016$, $R_3^{opt} = 0,259$ e $R_4^{opt} = 0,921$, ao passo que as taxas práticas foram $R_3 = 0,25$ e $R_4 = 0,86$.

- Em 2007, Lodewyck e outros (LODEWYCK et al., 2007) realizaram uma implementação prática da reconciliação *slice* com uma quantização de quatro *bits*, utilizando códigos LDPC de comprimento $n = 200.000$ e um código algébrico (código BCH – *Bose–Ray–Chaudhuri and Hocquenghem*)² aplicado a toda a sequência de dados para obtenção de *bits* de paridade extras, obtendo uma eficiência de reconciliação $\beta = 0,898$ para uma SNR de aproximadamente 5 dB, para a qual foi possível transmitir a chave secreta binária por 25 km de fibra óptica, com uma taxa de 2 kb/s.
- Em 2009, Fossier e outros (FOSSIER et al., 2009) realizaram uma implementação prática da reconciliação *slice* com uma quantização de quatro *bits*, utilizando códigos LDPC de maior comprimento, obtendo uma eficiência de reconciliação $\beta = 0,9$ para uma SNR de aproximadamente 5 dB, para a qual foi possível transmitir a chave secreta binária por, no máximo, 27 km de fibra óptica, com uma taxa média aproximada de 8 kb/s.
- Em 2010, Zhixin e outros (ZHIXIN et al., 2010) alcançaram uma eficiência de reconciliação $\beta = 0,89$ a partir do uso das técnicas MLC/MSD, com uma quantização de quatro *bits*, associado a códigos LDPC irregulares de desempenho elevado (cuja capacidade elevada de correção de erros é extremamente adequada para sistemas CV-QKD com nível elevado de ruído) de comprimento $n = 200.000$ com informação lateral³ para SNRs baixas da ordem de 3.2 dB, alcançando uma taxa média aproximada de 2,2 kb/s por 20 km de fibra óptica monomodo. Os valores de informação mútua apresentados são de $I_{L1} = 0,004$ bits/símbolo, $I_{L2} = 0,0165$ bits/símbolo, $I_{L3} = 0,1201$ bits/símbolo e $I_{L4} = 0,6706$ bits/símbolo, sendo conveniente a codificação de, no máximo, dois canais. As taxas dos códigos utilizadas foram de $R_{L3} = 0,11$ e $R_{L4} = 0,73$.
- Em 2012, Jouguet e outros (JOUQUET et al., 2012) realizaram algumas melhorias na reconciliação CV-QKD baseada em estados coerente, possibilitando comunicação por mais de 80km, através do uso de protocolos de reconciliação multidimensionais que transformam o canal gaussiano em um canal de modulação binária virtual, permitindo o uso de códigos corretores de erros projetados para o canal de ruído branco gaussiano aditivo com entrada binária (BIAWGNC – *Binary Input Additive White Gaussian Noise Channel*), cujas eficiências típicas para SNRs baixas (abaixo de 1,1 dB) são de 0,95. A decodificação foi feita utilizando GPU e códigos LDPC de comprimento $n = 10^8$ operando próximo à quantidade máxima de erros que são capazes de corrigir, para maximizar a eficiência do protocolo.

² Existe uma probabilidade de que os códigos LDPC deixem um certo número de erros na sequência final, que, na maioria das vezes, podem ser determinados por um código BCH; no entanto, se muitos erros permanecerem, o código BCH é incapaz de corrigi-los (FOSSIER et al., 2009)

³ Por este processo, a informação vazada é diminuída para a síndrome transmitida pelo canal clássico de modo que a quantidade final de *bits* da chave é protegida ao máximo (ZHIXIN et al., 2010).

- Em 2016, Li e outros (LI et al., 2016) fizeram simulações utilizando o protocolo SEC com 4 níveis de quantização, dos quais dois foram completamente expostos através do canal clássico para assistir a decodificação dos demais níveis. A correção dos erros foi feita através de códigos LDPC de comprimento $n = 10.000$, cujas taxas utilizadas foram $R_3^{opt} = 0,3$, $R_4^{opt} = 0,9$, para o terceiro e quarto nível. A eficiência de reconciliação alcançada nesse esquema foi de 91,8%. (LI et al., 2016) mostraram ainda que para um esquema de decodificação suave são necessárias 35 iterações para reconciliar a chave utilizando os dois últimos níveis.
- Em 2017, Bai e outros (BAI et al., 2017) implementaram a reconciliação SEC com uma quantização de cinco *bits* dos quais apenas dois são codificados, utilizando códigos LDPC irregulares com comprimento de bloco $n = 10^6$, obtendo eficiências de reconciliação acima de 95% para SNRs acima de 0dB, chegando a $\beta = 0,9526$ para uma SNR de aproximadamente 3 dB. A decodificação foi realizada através do algoritmo LLR-BP com informação lateral. As taxas ótimas apresentadas para $SNR = 3$ dB, que constituem um limite para as taxas práticas utilizadas no protocolo, são: $R_1^{opt} = 0,00059$, $R_2^{opt} = 0,00101$, $R_3^{opt} = 0,01239$, $R_4^{opt} = 0,46650$ e $R_5^{opt} = 0,98234$; verificando-se, portanto, a razão da utilização de apenas dois *bits* dos cinco níveis de quantização devido às baixíssimas taxas que seriam necessárias para codificar os três primeiros níveis. As taxas práticas utilizadas foram de $R_4 = 0,4480$ e $R_5 = 0,9725$ com um número máximo de iterações para decodificação de 180 e 60 para os níveis 4 e 5, respectivamente.

3.1 Parâmetros para protocolo SEC

Para o protocolo SEC utiliza-se entre 4 a 5 funções de fatiamento, ou seja, é feito um fatiamento do espaço de chave bruta de Alice em 16 ou 32 intervalos (BLOCH et al., 2006), (JOUQUET; ELKOUSS; KUNZ-JACQUES, 2014). Como cada função de fatiamento fornece um único *bit*, o processo de quantização pode resultar em 4 ou 5 *bits*, respectivamente. No entanto, as taxas requeridas para codificação dos 2 ou 3 últimos níveis geralmente são muito baixas para valores de SNR abaixo de 5dB (faixa de interesse para garantir comunicação por longas distâncias), menores que um limiar definido em 0,02 abaixo do qual considera-se mais vantajoso revelar completamente os *bits* do que projetar bons códigos LDPC com tais taxas (BLOCH et al., 2006). Logo, no protocolo SEC apenas os dois primeiros níveis são codificados e os demais *bits* são revelados para auxiliar Bob a desvendar os *bits* codificados (JOUQUET; ELKOUSS; KUNZ-JACQUES, 2014).

Capítulo 4

Contribuição do Trabalho

Este capítulo apresenta a contribuição deste trabalho, assim como o modelo assumido para fins de simulação e pontua as diferenças entre o método proposto para quantização e o SEC.

4.1 Método de Quantização Baseado na Função Distribuição de Probabilidade

Com foco na reconciliação de sequências de realizações de variáveis aleatórias gaussianas correlacionadas, foi proposto um novo esquema de quantização que leva em consideração a função distribuição de probabilidade das variáveis gaussianas medidas por Bob e enviadas por Alice¹, de modo a contornar as dificuldades do protocolo atualmente empregado. O uso da modulação Gaussiana coerente dos estados enviados pelo canal quântico permitiu a modelagem deste como um canal com ruído aditivo gaussiano (ZHIXIN et al., 2010), para o qual a sequência de variáveis contínuas X' que Bob recebe através do canal pode ser tratada como a superposição da sequência de variáveis de Alice $X \sim N(0, \Sigma)$ e do ruído Gaussiano $\epsilon \sim N(0, \sigma)$.

Da Teoria da Informação, extrai-se o lema apresentado em (COVER; THOMAS, 2006), sobre o qual se baseia a ideia para nova solução de discretização das chaves brutas:

Lema: Seja X uma variável aleatória com função de distribuição contínua $F(x)$, defina $U = F(X)$. Então, U é uniforme em $[0, 1]$.

Como resultado direto do lema enunciado, a função distribuição contínua da variável aleatória X leva os valores do espaço da chave bruta de Alice, \mathcal{X} , no intervalo $[0, 1]$ com distribuição uniforme, isto é, os *bits* resultantes da expansão binária de $F(X)$ são Bernoulli com parâmetro $\frac{1}{2}$, de modo que formam uma representação comprimida da sequência X (ver Apêndice C).

¹ O esquema de reconciliação reversa foi adotado para não levar em conta o limite de perda do canal de 3 dB (GROSSHANS et al., 2003) (BAI et al., 2017)

A expansão binária

$$x = 0.x_1x_2 \cdots x_{l_i} = \sum_{j=1}^{l_i} x_j 2^{-j} \quad (4.1)$$

de números no intervalo $[0, 1]$ apresenta o formato $0.F_1F_2 \cdots F_l$, onde cada realização $F_i \in GF(2)$, $1 \leq i \leq l$, com probabilidades iguais para as saídas 0 e 1, e l correspondendo ao número de *bits* escolhido para representar a variável contínua.

Propõe-se, portanto, a quantização das sequências de realizações de variáveis aleatórias gaussianas correlacionadas compartilhadas por Alice e Bob por meio de quatro passos:

1. Calcular o valor da função distribuição de probabilidade para cada realização de X e de X' , correspondendo a um valor no intervalo entre 0 e 1;
2. Realizar a expansão binária deste valor, obtendo valores no formato $0.F_1F_2 \cdots F_l$;
3. Utilizar a sequência binária após o ponto como a representação binária de cada x_i ou x'_i ;
4. Definir os canais BSC como as realizações de cada variável aleatória de Bernoulli F_1, F_2, \dots, F_l , isto é, dado o vetor de r realizações da variável aleatória gaussiana de Alice e a matriz $l \times r$ que representa a quantização desses valores em l *bits*, os canais são representados pelas linhas da matriz mostrada na formulação (4.2).²

$$(x_1 \quad x_2 \quad \cdots \quad x_r) = \begin{pmatrix} F_1^1 & F_2^1 & \cdots & F_r^1 \\ F_1^2 & F_2^2 & \cdots & F_r^2 \\ \vdots & \vdots & \ddots & \vdots \\ F_1^l & F_2^l & \cdots & F_r^l \end{pmatrix} \quad (4.2)$$

4.2 Reconciliação utilizando códigos LDPC no sentido Slepian-Wolf

Após quantização dos valores das realizações de variáveis aleatórias gaussianas correlacionadas de Alice e Bob obtidas através da comunicação pelo canal quântico, estes possuem sequências binárias discretas i.i.d. representadas por F_i^c e $F_i'^c$, respectivamente, para cada canal c em que $1 \leq c \leq l$ e cada realização de X e X' , $1 \leq i \leq r$, em que os pares de componentes (x_i, x'_i) têm função de massa de probabilidade conjunta $p(x, x')$. As duas sequências possuídas pelas partes legítimas, para cada canal, portanto, devem ser decodificadas conjuntamente em um receptor comum, conforme mostrado na Figura 8.

² Os canais foram assim definidos de modo a garantir a independência entre suas realizações, de modo que o i -ésimo canal represente a sequência dos i -ésimos *bits* da expansão binária da sequência enviada por Alice.

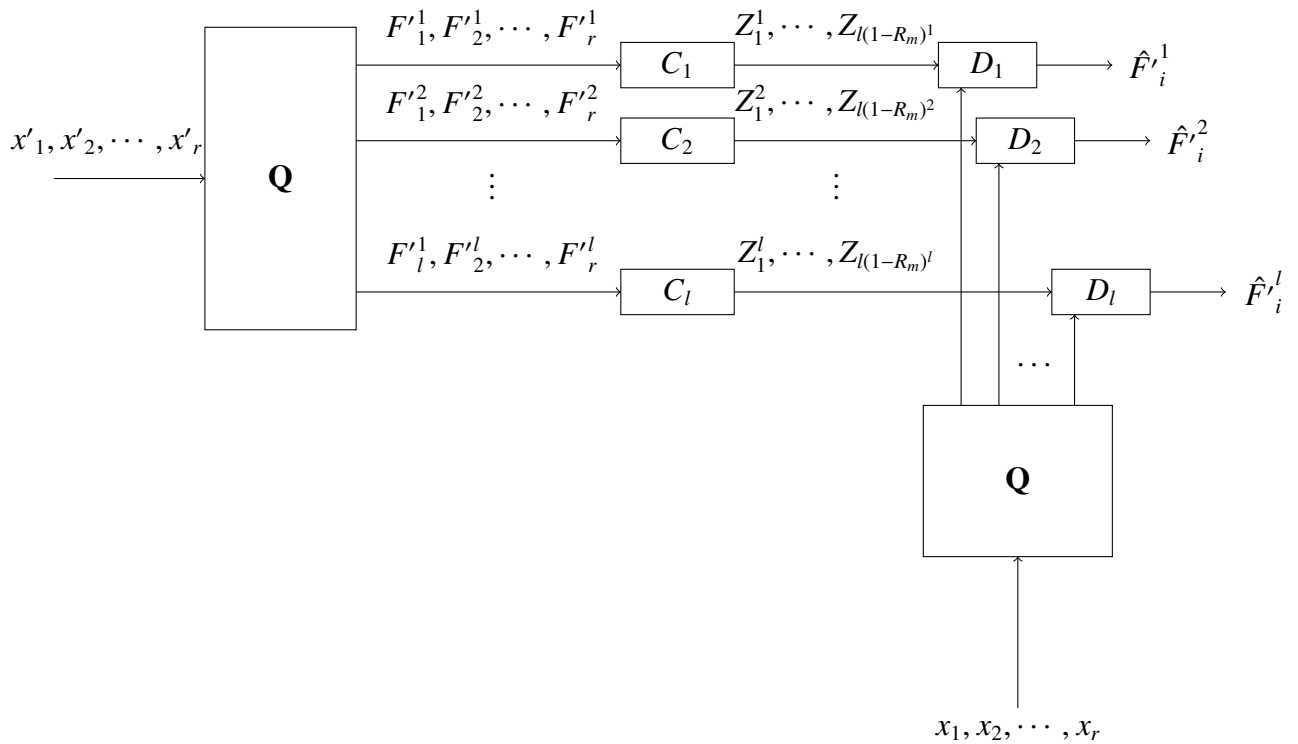


Figura 8 – Esquema de reconciliação reversa considerado para fins de reconciliação das realizações de variáveis gaussianas correlacionadas X e X' .

É assumido, para este trabalho, um processo de reconciliação reversa, em vista disso, a codificação é feita no sentido de comprimir a sequência de Bob com o intuito de restringir ao máximo a informação vazada para Eva através do processo de reconciliação, já que o canal clássico é assumido perfeito.

Codificando independentemente a sequência $F_i'^c$ de Bob com um codificador de fonte que conhece a correlação média entre as fontes X e X' , e assumindo que cada sequência $F_i'^c$ é comprimida para sua entropia de fonte e é conhecida pelo decodificador como informação lateral, o objetivo é comprimir a sequência $F_i'^c$ com uma taxa $R_{X'}$ o mais próxima possível da entropia condicional $R_{X'} \geq H(X'|X)$ alcançando o ponto A na Figura 6 (DANESHGARAN; LADDOMADA; MONDIN, 2009).

O decodificador deve descomprimir a sequência $F_i'^c$, para obter uma estimativa \hat{X}' , através do emprego de F_i^c como informação lateral. Nenhuma informação acerca da taxa é passada ao decodificador, entretanto, este conhece a correlação média de forma implícita a partir da SNR utilizada e estimação dos canais, e do fato que Alice utiliza uma taxa tão próxima quanto possível de $H(p)$.

4.2.1 Codificação

Dada a matriz teste de paridade $H_{i(n-k) \times n}$ de um código LDPC, a codificação de uma sequência binária F_i^c medida por Bob é feita a partir do produto $H_i \cdot F_i^{cT}$ que corresponde à síndrome de F_i^c , Z , de tamanho $n - k$.

4.2.2 Decodificação

A decodificação foi realizada tal qual exposto em (LIVERIS; XIONG; GEORGHIADES, 2002), de modo que a única diferença para o *Belief Propagation* tradicional baseado na razão de verossimilhança logarítmica (LLR – *Logarithmic Likelihood Ratio*)³ é a inclusão do fator $(1 - 2s_j)$, em que s_j corresponde à j -ésima componente da síndrome, no cálculo das razões de verossimilhança enviadas pelos nós de paridade para considerar a informação recebida de Alice através do canal clássico.

³ Decodificação de decisão suave símbolo a símbolo baseada no domínio logarítmico para fins de menor complexidade para códigos muito longos, por substituir operações de multiplicação massivas por somas (ZHIXIN et al., 2010).

Capítulo 5

Materiais e Métodos

Conforme trazido na literatura, o protocolo SEC utiliza de 4 a 5 funções de fatiamento para realizar a reconciliação das sequências de interesse (BLOCH et al., 2006), (NASCIMENTO, 2017). Com base nesse parâmetro, o esquema proposto de quantização foi implementado no MATLAB considerando-se um total de 5 canais e um total de 1.000 realizações das variáveis aleatórias gaussianas correlacionadas, para fins de estimação dos canais. As variáveis foram geradas modelando o canal quântico como um canal com ruído aditivo gaussiano conforme (ZHIXIN et al., 2010), de modo que a sequência contínua de Alice foi gerada a partir de realizações de uma variável aleatória $X \sim N(0, \Sigma)$ e a sequência de Bob gerada pela superposição das realizações de X com realizações do ruído Gaussiano considerado $\epsilon \sim N(0, \sigma)$.

A quantização foi realizada conforme proposto no Capítulo 4: foi tomado o valor da função distribuição de probabilidade para cada realização de X e de X' , correspondendo a um valor no intervalo entre 0 e 1; em seguida, realizou-se a expansão binária deste valor, obtendo valores no formato $0.F_1F_2 \dots F_l$. Os *bits* utilizados foram os valores após o 0. de modo que cada *bit* resultante desse processo é equiprovável. Os canais foram definidos como as realizações de cada variável aleatória de Bernoulli F_1, F_2, \dots, F_l e as sequências binárias ao final da quantização são de comprimento igual a 5.000 *bits*.

A contribuição de cada canal foi analisada para a estimação da informação mútua total $I(X; Q(X'))$ através do método dos vizinhos mais próximos, conforme abordado em (ROSS, 2014), para levar em consideração o limiar adotado na literatura para o protocolo SEC que determina os casos em que se é vantajoso realizar a codificação do canal. Foi realizada ainda, a estimação da informação mútua entre as duas sequências quantizadas, $Q(X)$ e $Q(X')$, de modo a avaliar a quantidade de informação compartilhada entre cada nível de quantização antes do procedimento de codificação dos mesmos.

A codificação foi feita utilizando códigos LDPC com taxas determinadas pelo teorema de Slepian-Wolf para cada canal, multiplicando a sequência binária de Bob pela matriz teste de paridade para obtenção da síndrome a ser enviada a Alice. A decodificação foi realizada através do algoritmo LLR-BP (LIVERIS; XIONG; GEORGHIADES, 2002) considerando X como informação lateral.

Capítulo 6

Resultados e Discussão

Este capítulo destina-se à apresentação e discussão dos resultados obtidos no presente trabalho de dissertação.

6.1 Estimação dos Canais

Cada canal, conforme definidos na Seção 4.1, foi estimado através de suas probabilidades de erro exibidas na Figura 9. Foram geradas 1.000 realizações de X , produzindo 5 sequências binárias de 1.000 *bits* cada às quais foram somados ruídos com distribuição $N \sim (0, \Sigma/\sqrt{SNR})$ para obtenção dos valores discretizados de X' . Os erros encontrados entre as sequências de Alice e Bob para cada canal foram computados e feita a razão pelo número de realizações em um processo repetido 700 vezes para cálculo do valor médio.

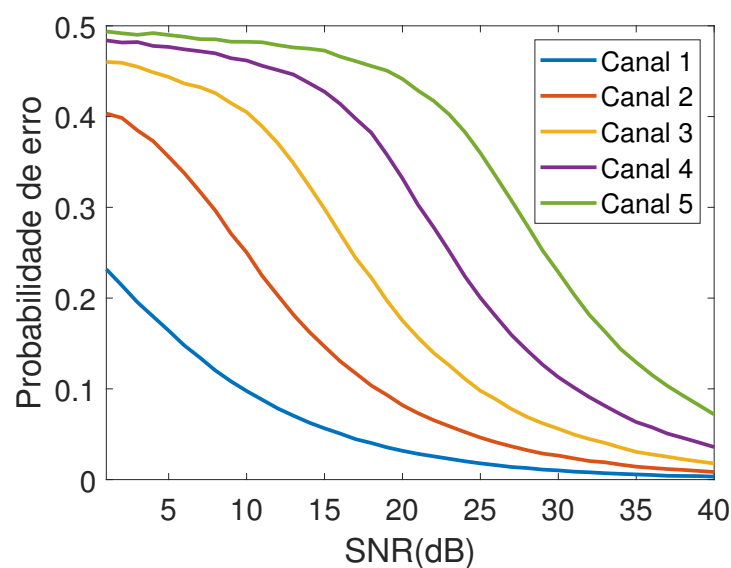


Figura 9 – Probabilidade de erro estimada de cada canal.

Visualmente, os canais 4 e 5 se mostraram bastante ruidosos para baixos valores de SNR, não servindo para fins de compartilhamento de chaves por levarem a elevadas probabilidades de

erro entre as sequências quantizadas. Entretanto, diante da necessidade de uma análise mais detalhada para definir o quão bom se caracteriza o esquema de quantização proposto, foram feitas as estimativas de informação mútua $I(X; \hat{X}'_1)$, $I(X; \hat{X}'_2)$, $I(X; \hat{X}'_3)$ e $I(X; \hat{X}'_4)$ para quantificar a contribuição individual de cada canal para a informação mútua total $I(X; \hat{X}')$. Os resultados para tal estimativa são apresentados na Figura 10.

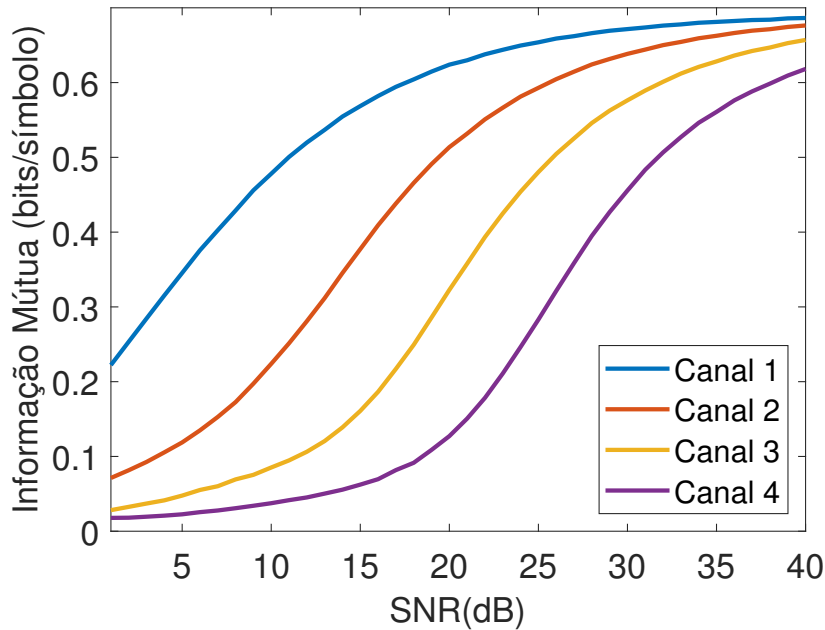


Figura 10 – Contribuição de cada canal para a informação mútua total $I(X, \hat{Y})$.

Os resultados para o regime de baixa SNR foi exposto na forma da Tabela 5 para melhor visualização.

SNR\Canal	Canal 1	Canal 2	Canal 3	Canal 4
1 dB	0,2222	0,0712	0,0282	0,0178
2 dB	0,2534	0,0816	0,0326	0,0181
3 dB	0,2845	0,0927	0,0370	0,0194
4 dB	0,3154	0,1055	0,0413	0,0208
5 dB	0,3455	0,1188	0,0476	0,0226

Tabela 5 – Contribuição de cada canal para informação mútua total para $1 \text{ dB} \leq \text{SNR} \leq 5 \text{ dB}$.

O descarte/divulgação de níveis que contribuem com menos de 0,02 *bit* têm pouco impacto na eficiência do protocolo (BLOCH et al., 2006), (ZHIXIN et al., 2010). Com base nesse limiar estabelecido na literatura para definição dos níveis de quantização a serem utilizados no protocolo de reconciliação, pode-se verificar a partir da Figura 10 e, principalmente, da Tabela 5 que, através do esquema de discretização das variáveis gaussianas proposto neste trabalho, é possível codificar 3 níveis para SNRs até 3 dB e 4 níveis para SNRs mais elevadas, caracterizando um ganho em termos de quantidade de *bits* de chave secreta gerados por cada variável

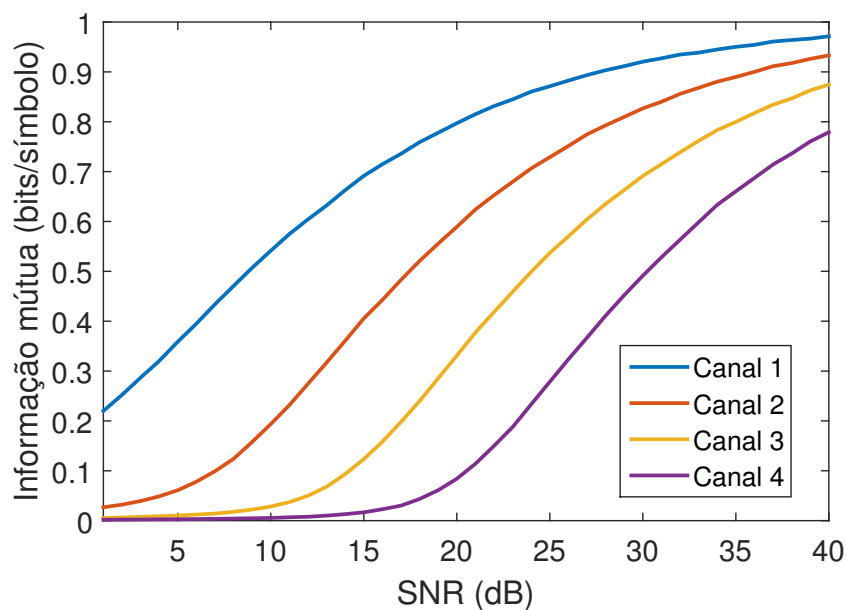
Canal 1	$H(\hat{X}')$	$I(\hat{X}; \hat{X}')$	$H(\hat{X}' \hat{X})$
5 dB	0,9992	0,3589	0,6408
10 dB	0,9991	0,5414	0,4577
15 dB	0,9988	0,6915	0,3078
20 dB	0,9995	0,7971	0,2024

Tabela 6 – Parâmetros obtidos para o canal 1.

contínua distribuída por meios quânticos em comparação com os resultados para o SEC apresentados no Capítulo 3. Apesar do valor estimado para informação mútua do nosso primeiro canal ser inferior àquele demonstrado em (ZHIXIN et al., 2010), todos os demais canais apresentam equivalência ou superioridade em relação aos níveis de quantização mostrados para o SEC.

6.2 Codificação e Decodificação

Os canais 1 e 2 foram usados para compartilhamento da chave secreta sendo que a estes foi aplicado o processo de reconciliação a partir da codificação/decodificação LDPC considerando as sequências binárias de Alice e Bob como realizações de fontes correlacionadas. Para o cálculo das taxas segundo o teorema de Slepian-Wolf, isto é, considerando X disponível sem erro no decodificador ($R_X = 1$), faz-se necessário comprimir X' com uma taxa $R_{X'}$ o mais próxima possível da entropia condicional $R_{X'} \geq H(X'|X)$. Os valores de informação mútua para as versões quantizadas, apresentados na figura 11, foram estimados para fins de obtenção das taxas dos códigos LDPC a serem utilizados, conforme exibido nas Tabelas 6 e 7.

Figura 11 – Informação mútua entre os *bits* não-reconciliados F_i e F'_i .

Canal 2	$H(\hat{X}')$	$I(\hat{X}; \hat{X}')$	$H(\hat{X}' \hat{X})$
5 dB	0,9996	0,0710	0,9286
10 dB	0,9995	0,1937	0,8058
15 dB	0,9997	0,4056	0,5941
20 dB	0,9996	0,5892	0,4104

Tabela 7 – Parâmetros obtidos para o canal 2.

Utilizando códigos LDPC de comprimento de bloco $N = 24576$ e $N = 32000$ com taxas $R = 2/3$ e $R = 0,93$, respectivamente, obtiveram-se os gráficos mostrados na Figura 12, para SNR de 5 dB, para os quais pode-se observar que Bob corrige sua sequência a partir, unicamente, dos *bits* de paridade enviados por Alice e da sua própria sequência obtida na transmissão quântica em menos de 40 iterações, conforme observado também para o protocolo SEC em (LI et al., 2016) para o esquema de decodificação suave que requer 35 iterações para reconciliação.

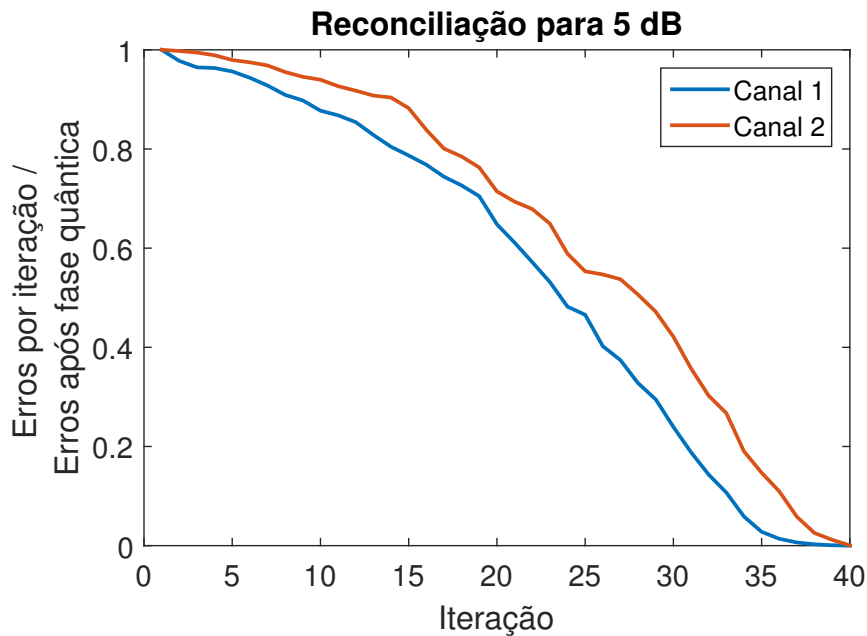


Figura 12 – Reconciliação para os dois primeiros níveis de quantização segundo protocolo proposto.

Um comparativo entre as taxas utilizadas é feito na tabela 8, no qual é feita a equivalência entre o quarto nível de quantização do SEC com nosso primeiro canal, devido a este se tratar do menos ruidoso. As taxas, em geral, são equiparáveis, com a vantagem de ser possível codificar dois níveis a mais a partir da construção de códigos LDPC eficientes para as taxas citadas, podendo elevar as taxas de geração de chave secreta.

	Nível 4	Nível 3	Nível 2	Nível 1
(BLOCH et al., 2006)	0,86	0,25	0	0
(ZHIXIN et al., 2010)	0,73	0,11	0	0
(LI et al., 2016)	0,9	0,3	0	0
(BAI et al., 2017)	0,9725	0,448	0	0
Nosso Esquema	0,66	0,93	0,99	0,998

Tabela 8 – Comparação entre taxas utilizadas para reconciliação no esquema proposto e aquelas apresentadas na literatura.

Capítulo 7

Considerações Finais

Foi apresentado um protocolo de reconciliação de chaves secretas que utiliza uma nova técnica de quantização das variáveis contínuas geradas após a transmissão pelo canal quântico. Para compreensão do esquema proposto, foi apresentado um breve resumo de tópicos essenciais de QKD, com enfoque para a distribuição de chaves quânticas com variáveis contínuas, o protocolo em uso na literatura para reconciliação de chaves gaussianas (SEC) e códigos LDPC para correção de erros com informação lateral para minimizar a informação vazada pelo canal público.

Com base na literatura de diversas implementações experimentais do protocolo SEC aliado a códigos LDPC para fins de comparação, foram mostrados uma solução alternativa para a fase de quantização das variáveis aleatórias contínuas geradas após a comunicação quântica, principal contribuição do trabalho baseada nos resultados da Teoria da Informação apresentados no Apêndice C, e os resultados obtidos para tal implementação, dentre os quais o método proposto se apresentou competitivo com o SEC, visto que, permite o uso de mais níveis de reconciliação (para SNRs acima de 4 dB, é possível codificar 4 canais, o dobro do que se consegue pelo uso do SEC), o que significa que mais *bits* de chave secreta são produzidos a partir de uma única variável contínua, a partir de um algoritmo visivelmente menos complexo. As taxas de compressão obtidas para codificação das sequências binárias também se mostraram bastante próximas àquelas presentes em trabalhos anteriores, apresentando nível satisfatório de compressão da informação e, conseqüentemente, pouca informação vazada para uma possível espiã que observa o canal clássico.

Os códigos LDPC utilizados para reconciliação ficaram restritos a tamanhos pequenos devido à limitação do computador utilizado para as simulações. Assim, uma vez que alta eficiência de reconciliação é alcançável para blocos de grandes comprimentos e códigos construídos aleatoriamente, conforme mostrado em (LODEWYCK et al., 2007) e (BAI et al., 2017), trabalhos futuros incluem a construção de códigos LDPC de construção aleatória (RC – *Random Construction*) na ordem de $N = 10^6$, que permitam decodificação para qualquer nível de SNR respeitados os limites de compressão, com utilização da GPU no processo de decodificação

para reduzir o tempo da computação. É de grande importância também quantificar a informação vazada durante o protocolo de reconciliação para determinar o tamanho prático das chaves geradas após a fase de amplificação de privacidade.

Referências

- ASSCHE, G. V.; CARDINAL, J. Construction of a shared secret key using continuous variables. In: *Proc 2003 IEEE Information Theory Workshop (ITW2003)*. [S.l.: s.n.], 2003. p. Paris, France. ISBN 0-7803-7799-0. Citado nas páginas 19, 24 e 25.
- ASSCHE, G. V.; CARDINAL, J.; CERF, N. J. Reconciliation of a quantum-distributed gaussian key. *IEEE Transactions on Information Theory*, IEEE, v. 50, p. 394 – 400, Fevereiro 2004. Citado nas páginas 13, 15, 16, 18, 19, 21, 22, 23, 24, 26 e 34.
- BAI, Z. et al. High-efficiency reconciliation for continuous variable quantum key distribution. *Japanese Journal of Applied Physics* 56, 044401 (2017), CrossMark, v. 56, p. 044401/1–5, Março 2017. Citado nas páginas 13, 20, 27, 34, 36, 37, 47 e 48.
- BENNETT, C. H.; BRASSARD., G. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, IEEE Press., p. 175—179, Dezembro 1984. Citado na página 16.
- BLOCH, M. et al. Ldpc-based gaussian key reconciliation. *Information Theory Workshop*, IEEE, p. 116–120, Junho 2006. Citado nas páginas 13, 34, 36, 41, 44 e 47.
- CALTECH. *Quantum Information Theory*. 2015. Accessed May. 12, 2018. Disponível em: <<http://www.theory.caltech.edu/people/preskill/ph229/notes/chap5.pdf>>. Citado na página 20.
- CARVALHO, L. M.; LAVOR, C.; MOTTA, V. S. Caracterização matemática e visualização da esfera de bloch: Ferramentas para computação quântica. *TEMA Tend. Mat. Apl. Comput.*, Sociedade Brasileira de Matemática Aplicada e Computacional, v. 8, p. 351–360, 2007. Citado na página 53.
- CHRISTIAN, K.; PIVK, M. *Applied Quantum Cryptography, Lecture Notes in Physics 797*. 1. ed. [S.l.]: Springer, 2010. An optional note. ISBN 9783642048296. Citado nas páginas 16 e 17.
- COVER, T. M.; THOMAS, J. A. *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. [S.l.]: Wiley-Interscience, 2006. ISBN 0471241954. Citado nas páginas 29, 30, 37, 56 e 60.
- DANESHGARAN, F.; LADDOMADA, M.; MONDIN, M. Ldpc-based iterative algorithm for compression of correlated sources at rates approaching the slepian-wolf bound. *2009 First International Conference on Advances in Satellite and Space Communications*, IEEE, p. 74–79, Julho 2009. Citado na página 39.

- FOSSIER, S. et al. Field test of a continuous-variable quantum key distribution prototype. *New Journal of Physics* 11 (2009) 045023, IOP Publishing Ltd and Deutsche Physikalische Gesellschaft, v. 11, p. 045023/1–15, Abril 2009. Citado na página 35.
- GROSSHANS, F. et al. Quantum key distribution using gaussian-modulated coherent states. *Nature (London)*, Macmillan Magazines Ltd., v. 421, p. 238—241, 2003. Citado nas páginas 8, 13, 37, 57, 58 e 59.
- GROSSHANS, F.; GRANGIER, P. Quantum cloning and teleportation criteria for continuous quantum variables. *Physical Review A*, American Physical Society, v. 64, p. (010301)1–4, 2001. Citado na página 56.
- GROSSHANS, F.; GRANGIER, P. Continuous variable quantum cryptography using coherent states. *Physical Review Lett.* 88, 057902 (2002), IEEE Press., p. 1–5, 2002. Citado nas páginas 19, 29, 56 e 57.
- GROSSHANS, F.; GRANGIER, P. Reverse reconciliation protocols for quantum cryptography with continuous variables. *Proceedings of the 6th International Conference on Quantum Communications, Measurement, and Computing*, 2002. Citado nas páginas 20 e 57.
- JOUGUET, P.; ELKOUSS, D.; KUNZ-JACQUES, S. High bit rate continuous-variable quantum key distribution. *Physical Review A* 90, 042329 (2014), IEEE Press., p. 1–9, Setembro 2014. Citado nas páginas 18, 20, 27 e 36.
- JOUGUET, P.; KUNZ-JACQUES, S.; LEVERRIER, A. Long-distance continuous-variable quantum key distribution with a gaussian modulation. *Physical Review A* 84, 062317 (2011), American Physical Society, p. 1–7, Dezembro 2011. Citado nas páginas 15, 18, 27 e 34.
- JOUGUET, P. et al. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, Nature Publishing Group, v. 7, p. 378–381, 2012. Citado nas páginas 13, 34 e 35.
- LI, Q. et al. An improved ldpc-based sec error reconciliation scheme. *2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)*, IEEE, p. 540–544, Julho 2016. Citado nas páginas 13, 34, 36, 46 e 47.
- LIVERIS, A. D.; XIONG, Z.; GEORGHIADES, C. N. Compression of binary sources with side information at the decoder using ldpc codes. *IEEE Communications Letters*, IEEE, p. 440–442, Outubro 2002. Citado nas páginas 29, 40 e 42.
- LODEWYCK, J. et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Physical Review A* 76, 042305 (2007), IEEE Press., v. 76, p. 042305/1–10, Outubro 2007. Citado nas páginas 18, 20, 34, 35 e 48.
- 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 nas páginas 12, 13, 18 e 41.
- NGUYEN, K.; ASSCHE, G. V.; CERF, N. J. Side-information coding with turbo codes and its application to quantum key distribution. *International Symposium on Information Theory and its Applications, ISITA2004*, 2004. Citado na página 13.

- NIELSEN, M. A.; CHUANG, I. L. *Quantum Computation and Quantum Information*. 10. ed. [S.l.]: Cambridge University Press, 2010. An optional note. ISBN 9781107002173. Citado nas páginas 12, 13 e 55.
- PIRANDOLA, S. et al. Direct and reverse secret-key capacities of a quantum channel. *Physical Review Letters*, The American Physical Society, v. 102, p. (050503)1–4, 2009. Citado na página 58.
- RICHARDSON, T. J.; URBANKE, R. L. Efficient encoding of low-density parity-check codes. *IEEE Transactions on Information Theory*, IEEE, v. 47, p. 638–656, Fevereiro 2001. Citado nas páginas 28 e 29.
- RICHARDSON, T. J.; URBANKE, R. L. *Modern Coding Theory*. [S.l.]: Cambridge University Press 2008, 2008. ISBN 9780521852296. Citado nas páginas 26 e 28.
- ROSS, B. C. Mutual information between discrete and continuous data sets. *PLoS ONE*, PLoS ONE, v. 9, p. 1–5, 2014. Citado na página 41.
- SLEPIAN, D.; WOLF, J. Noiseless coding of correlated information sources. *IEEE Transactions on Information Theory*, IEEE, v. 19, p. 471 – 480, 1973. Citado na página 30.
- XUDONG, Q.; GUANGQIANG, H.; GUIHUA, Z. Realization of error correction and reconciliation of continuous quantum key distribution in detail. *Sci China Ser F-Inf Sci*, Springer, v. 52, p. 1598 – 1604, 2009. Citado na página 25.
- ZHIXIN, L. et al. Reverse reconciliation for continuous variable quantum key distribution. *Science China*, Science China Press and Springer-Verlag Berlin Heidelberg 2010, v. 53, p. 100–105, 2010. Citado nas páginas 27, 34, 35, 37, 40, 41, 44, 45 e 47.

APÊNDICE A

Noções Gerais da Mecânica Quântica

A notação padrão para estados em mecânica quântica é $|\cdot\rangle$, intitulada “notação de Dirac”. O mais simples e importante sistema da mecânica quântica é o *qubit*, com espaço de estados bi-dimensional. O estado $|\psi\rangle$ do sistema quântico permite superposições do tipo $\alpha|\psi_1\rangle + \beta|\psi_2\rangle$, com $|\psi_1\rangle$ e $|\psi_2\rangle$ estados ortonormais e $\alpha, \beta \in \mathbb{C}$ satisfazendo $|\alpha|^2 + |\beta|^2 = 1$.

A interpretação física da superposição é de que o *qubit* está simultaneamente nos estados $|\psi_1\rangle$ e $|\psi_2\rangle$, o que faz com que a quantidade de informação armazenada no estado $|\psi\rangle$ possa ser infinita (CARVALHO; LAVOR; MOTTA, 2007). Entretanto, essa quantidade infinita de informação está no nível quântico, de modo que para torná-la acessível, no nível clássico, é necessário fazer uma medição. A mecânica quântica, entretanto, afirma que o processo de medição altera o estado de um *qubit*, fazendo-o assumir o estado $|\psi_1\rangle$, com probabilidade $|\alpha|^2$, ou o estado $|\psi_2\rangle$, com probabilidade $|\beta|^2$ (CARVALHO; LAVOR; MOTTA, 2007).

A.0.1 Postulados básicos da mecânica quântica

Os postulados, descritos a seguir, são resultados de um longo processo de tentativa e erro e fornecem uma conexão entre o mundo físico e o formalismo matemático da mecânica quântica.

Postulado I: Associado a qualquer sistema físico isolado, existe um espaço vetorial complexo com produto interno¹ conhecido como o *espaço de estados* do sistema. O sistema é completamente descrito por seu vetor de estados².

Postulado II: A evolução de um *sistema quântico fechado* é descrita por uma transformação unitária (operador unitário U). O estado $|\psi\rangle$ do sistema no tempo t_1 é relacionado ao estado $|\psi'\rangle$ do sistema no tempo t_2 através de U :

$$|\psi\rangle = U|\psi'\rangle \tag{A.1}$$

¹ Espaço de Hilbert.

² Vetor unitário no espaço de estados do sistema.

Uma versão mais refinada deste postulado descreve a evolução de um sistema quântico em tempo contínuo.

Postulado II': A evolução temporal de um estado de um sistema quântico fechado é descrita pela equação de Schrödinger,

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle \quad (\text{A.2})$$

onde \hbar é a constante de Planck e H um operador Hermitiano conhecido como o Hamiltoniano do sistema fechado.

A solução da equação de Schrödinger dada por

$$|\psi(t_2)\rangle = \exp\left(\frac{-iH(t_2 - t_1)}{\hbar}\right) |\psi(t_1)\rangle = U(t_1, t_2) |\psi(t_1)\rangle \quad (\text{A.3})$$

onde define-se

$$U(t_1, t_2) \equiv \left(\frac{-iH(t_2 - t_1)}{\hbar}\right) |\psi(t_1)\rangle \quad (\text{A.4})$$

Onde U é um operador unitário, uma vez que qualquer operador unitário pode ser escrito na forma $U = \exp(iK)$ para algum operador Hermitiano K . Assim existe uma correspondência direta entre a descrição da dinâmica em tempo discreto usando operadores unitários e a descrição em tempo contínuo a partir de Hamiltonianos.

Postulado III: Medições quânticas são descritas por uma coleção $\{M_m\}$ de operadores de medição. Tais operadores atuam no espaço de estados do sistema e o índice m refere-se à saída do experimento obtida na medição. Se o estado do sistema quântico é $|\psi\rangle$ imediatamente antes da medição então a probabilidade de ocorrer o resultado m é dada por

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

e o estado do sistema após a medição passa a ser

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

Operações de medição satisfazem a equação de plenitude $\sum_m M_m^\dagger M_m = I$ de modo a garantir que a soma das probabilidades seja 1:

$$\sum_m p(m) = \sum_m \langle \psi | M_m^\dagger M_m | \psi \rangle = 1 \quad (\text{A.7})$$

É claro, portanto, que os dispositivos de medição são sistemas quânticos de modo que forma, com o sistema quântico sendo medido, um sistema quântico maior, isolado.

Postulado IV: O estado de espaços de um sistema físico composto é o produto tensorial dos espaços de estados dos sistemas físicos individuais. Para sistemas enumerados de 1 a n e sistema i preparado no estado $|\psi_i\rangle$, então o estado conjunto do sistema total é $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

A.0.2 Estados não-ortogonais e distinguibilidade

Como resultado do postulado III, prova-se em (NIELSEN; CHUANG, 2010) a inexistência de medições quânticas capazes de distinguir estados não-ortogonais.

Considera-se que duas partes, Alice e Bob, desejam trocar informações entre si e definem um conjunto fixo de estados não-ortogonais $|\psi_i\rangle$ ($1 \leq i \leq n$). Alice escolhe um estado $|\psi_i\rangle$ e envia para Bob que deve identificar o índice i do estado enviado por ela. No entanto, $|\psi_j\rangle$ pode ser decomposto em uma componente não-nula paralela a $|\psi_i\rangle$ e uma componente ortogonal a $|\psi_i\rangle$, para valores $i \neq j$. Supondo que s é a saída da medição tal que Bob especula que o estado enviado por Alice era $|\psi_i\rangle$, existe uma probabilidade não-nula de se obter a saída s quando o estado $|\psi_j\rangle$ é preparado, devido à componente de $|\psi_j\rangle$ paralela a $|\psi_i\rangle$, de modo que algumas vezes Bob irá cometer erros ao tentar identificar o estado preparado.

Prova: Supondo existir uma medição capaz de distinguir entre os estados não-ortogonais $|\psi_1\rangle$ e $|\psi_2\rangle$, se o estado $|\psi_1\rangle$ é preparado, então a probabilidade de medir s tal que $f(s) = 1$ deve ser 1 – onde $f(\cdot)$ representa a regra utilizada por Bob para tentar adivinhar o índice $i = 1, 2$.

Definindo o operador $E_i \equiv \sum_{j:f(j)=i} M_j^\dagger M_j$, as medições de $|\psi_1\rangle$ e $|\psi_2\rangle$ podem ser descritas por

$$\langle \psi_1 | E_i | \psi_1 \rangle = 1 \quad \langle \psi_2 | E_i | \psi_2 \rangle = 1 \quad (\text{A.8})$$

Uma vez que $\sum_i E_i \stackrel{(a)}{=} I$, onde (a) deve-se à equação de plenitude, então $\sum_i \langle \psi_1 | E_i | \psi_1 \rangle = 1$ e utilizando a equação A.8, tem-se $\langle \psi_1 | E_2 | \psi_1 \rangle = 0$ ou $\sqrt{E_2} |\psi_1\rangle$.

Como $|\psi_1\rangle$ e $|\psi_2\rangle$ não são ortogonais, então o estado $|\psi_2\rangle$ pode ser decomposto em $|\psi_2\rangle = \alpha |\psi_1\rangle + \beta |\varphi\rangle$, onde $|\varphi\rangle$ é ortonormal a $|\psi_1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$ e $\beta \stackrel{(b)}{<} 1$, e (b) deriva da não-ortogonalidade entre $|\psi_1\rangle$ e $|\psi_2\rangle$. Assim, $\sqrt{E_2} |\psi_2\rangle = \beta \sqrt{E_2} |\varphi\rangle$ que implica

$$\langle \psi_2 | E_2 | \psi_2 \rangle = |\beta|^2 \langle \varphi | E_2 | \varphi \rangle \stackrel{(c)}{<} |\beta|^2 < 1 \quad (\text{A.9})$$

Sendo a desigualdade (c) advinda da observação que $\langle \varphi | E_2 | \varphi \rangle \leq \sum_i \langle \varphi | E_i | \varphi \rangle = 1$.

APÊNDICE B

Reconciliação Direta e Reversa

Uma breve síntese relativa às diferenças entre os processos de reconciliação direta e reversa é abordada neste apêndice, justificando a escolha em se realizar a reconciliação reversa no protocolo apresentado neste trabalho.

B.1 Reconciliação Direta

Na QKD, Alice modula aleatoriamente um feixe gaussiano e o envia, através de um canal ruidoso para Bob, com fase e amplitude modulados com valores aleatórios gaussianos. Bob então mede um desses parâmetros do feixe e informa a Alice a medição realizada. Assim, de posse de variáveis aleatórias gaussianas correlacionadas, Alice e Bob podem extrair uma sequência binária secreta comum com taxa ótima de informação, em *bits/símbolo*, dada pela fórmula de Shannon para um canal de transmissão ruidoso (GROSSHANS; GRANGIER, 2002a). Considerando o ruído gaussiano branco e uma SNR Σ , (COVER; THOMAS, 2006) mostra que

$$I_{AB} = \frac{1}{2} \log_2(1 + \Sigma) \quad (\text{B.1})$$

E a taxa de chave secreta que pode ser construída é de

$$\Delta I = I_{AB} - I_{AE} \quad (\text{B.2})$$

onde I_{AB} e I_{AE} são as taxas de informação entre Alice e Bob e Alice e Eva, respectivamente. I_{AE} deve ser assumido o máximo possível, dadas as leis da física, para garantir a segurança do protocolo até no pior cenário (GROSSHANS; GRANGIER, 2002a).

Um resultado geral demonstrado em (GROSSHANS; GRANGIER, 2001) mostra que para um ruído χN_0 adicionado no lado de Bob, onde N_0 é a variância do ruído do vácuo, o mínimo ruído adicionado no lado de Eva é $\chi^{-1} N_0$, onde $\chi = (1 - \eta)/\eta$ quando a linha tem transmissividade η na ausência da espiã; esse resultado se aplica a ambas as quadraturas e o ruído adicionado pode ser devido às perdas nas linhas, espionagem ou qualquer outra razão.

(GROSSHANS; GRANGIER, 2002a) garantem, a partir desse resultado, que o melhor ataque para Eva, consiste em tomar uma fração de $1 - \eta$ do feixe no lado de Alice e enviar a fração η para Bob através de sua própria linha sem perdas, fazendo-se totalmente indetectável e conseguindo o máximo possível de informação de acordo com o teorema da não-clonagem.

A equação (B.2) mostra que o protocolo é seguro desde que Bob possua mais informação sobre os elementos de chave de Alice do que Eva, isto é, $I_{AB} > I_{AE}$. Como a equação (B.1) é válida tanto para Bob quanto para Eva, (GROSSHANS; GRANGIER, 2002a) apontam que a condição de segurança pode ser vista como

$$\Delta I > 0 \Leftrightarrow \Sigma_B > \Sigma_E \Leftrightarrow \chi < 1 \quad (\text{B.3})$$

onde Σ_B e Σ_E são os ruídos adicionados, respectivamente, no lado de Bob e no lado de Eva.

A condição $\chi < 1$, por sua vez, requer que $\eta > 1/2$. Portanto, para se obter uma chave secreta a partir da técnica de reconciliação direta existe um limite superior nas perdas de transmissão de 3 dB (GROSSHANS; GRANGIER, 2002a), que é um resultado intuitivo conforme mostrado em (GROSSHANS; GRANGIER, 2002b), já que Eva pode simular as perdas por um divisor de feixe e observar uma porta de saída: se ela retém maior parte do feixe enviado por Alice, simulando perdas superiores a 50%, ela pode extrair mais informação do feixe que Bob ($I_{AE} > I_{AB}$), impossibilitando a geração de uma chave secreta comum apenas às partes legítimas do protocolo.

B.2 Reconciliação Reversa

Quando a transmissividade da linha óptica é superior a 50%, isto é, para perdas menores ou iguais a 3 dB, os limites físicos de clonagem quântica para variáveis contínuas garantem a segurança do protocolo contra ataques individuais (GROSSHANS; GRANGIER, 2002a). Entretanto, quando as perdas são elevadas, (GROSSHANS; GRANGIER, 2002b) e (GROSSHANS et al., 2003) mostraram que para um protocolo QKD baseado em estados coerentes, a segurança é alcançada através da reversão do mesmo para qualquer valor de transmissividade da linha.

Na reconciliação direta, mostrada na figura 13, Bob adquire R bits extras de informação de Alice com o objetivo de corrigir os erros de transmissão, permitindo a geração de uma sequência binária comum de $I_{AB} + R$ bits, dos quais Eva conhece $I_{AE} + R$ bits. Ao considerar a reconciliação reversa, apresentada na figura 14, na qual Bob envia R bits de informação para que Alice acrescente os erros de transmissão nos seus dados iniciais, uma sequência binária de $I_{BA} + R$ bits pode ser gerada, da qual Eva conhece $I_{BE} + R$ bits. (GROSSHANS et al., 2003) garantem maior adequação dessa técnica aos protocolos CV-QKD devido a maior dificuldade de Eva em controlar os erros no lado de Bob em detrimento de realizar leituras das modulações de Alice, por não poder conhecer os ruídos internos à configuração de detecção de Bob; Nestes

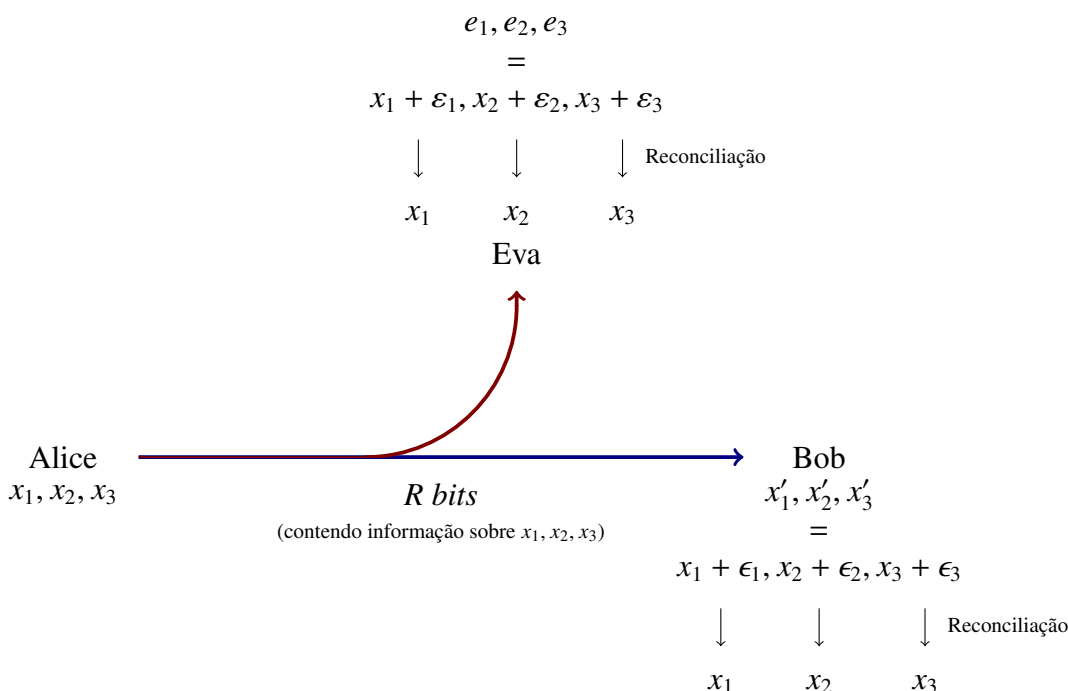


Figura 13 – Esquema de reconciliação direta através de um canal clássico pelo qual Alice envia R bits para ajudar Bob a corrigir sua sequência $x'_1 x'_2 x'_3$ para $x_1 x_2 x_3$.

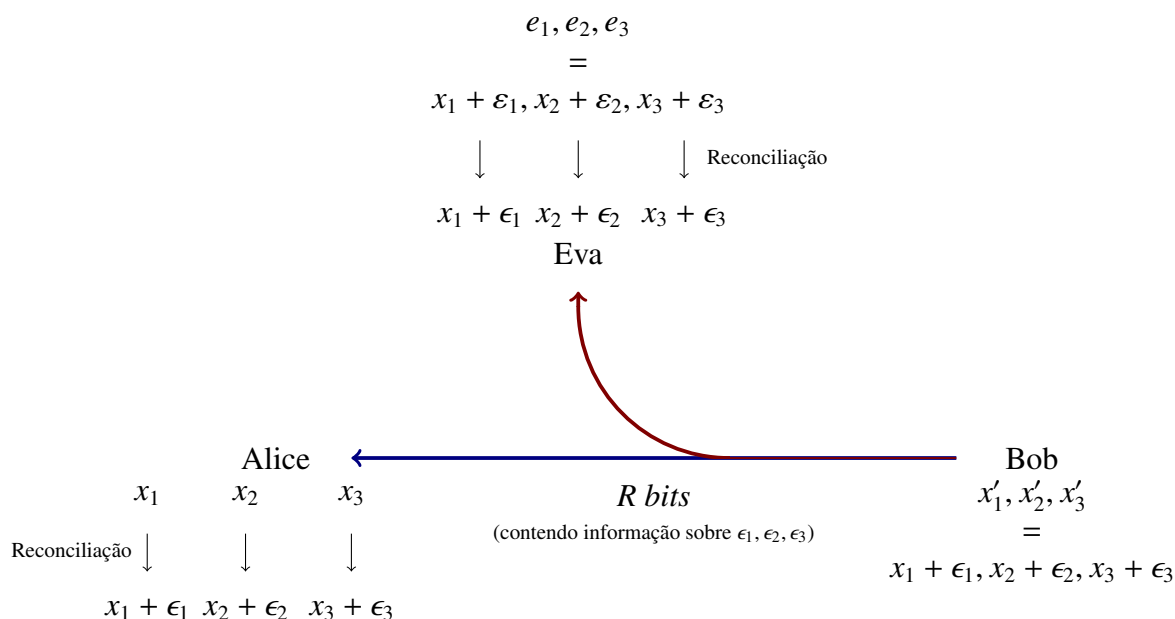


Figura 14 – Esquema de reconciliação reversa através de um canal clássico pelo qual Bob envia R bits para ajudar Alice a corrigir sua sequência $x_1 x_2 x_3$ para $x'_1 x'_2 x'_3$.

esquemas, Alice pode, ainda, explorar a informação que recebe de Bob para condicionar as entradas subsequentes do canal quântico (PIRANDOLA et al., 2009).

O resultado apresentado por (GROSSHANS et al., 2003) na figura 15 esclarece o porquê da reconciliação reversa ser segura para qualquer valor de transmissividade de linha contra ataques individuais gaussianos, de acordo com a equação (B.2) e mesmas considerações feitas para o

caso da segurança de esquemas baseados em reconciliação direta, isto é, $I_{BA} > I_{BE}$ para qualquer valor de transmissividade do canal.

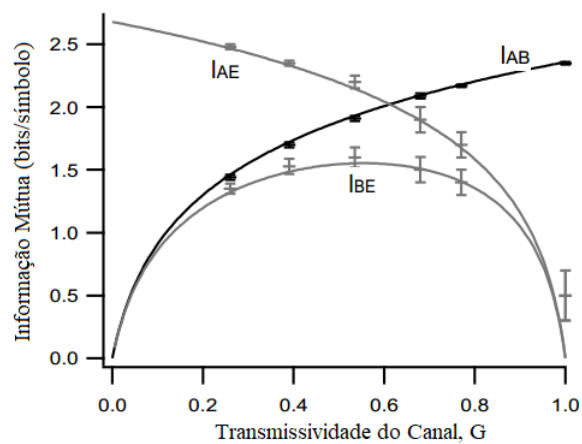


Figura 15 – Valores de I_{AB} , I_{AE} e I_{BE} em função da transmissividade de linha G para $V \approx 40$, onde V representa a variância das quadraturas de Alice. Retirado de (GROSSHANS et al., 2003).

APÊNDICE C

Lema Importante da Codificação Aritmética

Na codificação aritmética, a representação de um símbolo não é feita através de uma sequência de *bits*, mas sim por intermédio de um subintervalo do intervalo unitário.

Dada uma sequência de símbolos, o código é um intervalo cujo comprimento diminui à medida que mais símbolos são adicionados, permitindo um esquema de codificação que é incremental¹.

Uma das motivações para esse esquema de codificação advém do lema a seguir apresentado em (COVER; THOMAS, 2006):

Lema: Seja X uma variável aleatória com função de distribuição contínua $F(x)$, defina $U = F(X)$. Então, U é uniforme em $[0, 1]$.

Prova: Se $F(X) \in [0, 1]$, a imagem de U é $[0, 1]$. Assim, para $u \in [0, 1]$, tem-se

$$F_U(u) = Pr(U \leq u) \tag{C.1}$$

$$= Pr(F(X) \leq u) \tag{C.2}$$

$$= Pr(X \leq F^{-1}(u)) \tag{C.3}$$

$$= F(F^{-1}(u)) \tag{C.4}$$

$$= u \tag{C.5}$$

Para uma sequência infinita de variáveis aleatórias X_1, X_2, \dots , qualquer realização x_1, x_2, \dots de um alfabeto finito $\mathcal{X} = 0, 1, 2, \dots, m$, pode ser escrita no formato $0.x_1, x_2, \dots$, ou seja, acrescentando-se 0. no início da sequência considerando a nova representação como um número real pertencente ao intervalo $[0, 1]$. Logo, considerando X a variável aleatória $X = 0.X_1X_2\dots$,

¹ O código de uma extensão de uma sequência pode ser calculado a partir do código para a sequência original.

a função distribuição de X é:

$$F_X(x) = \Pr[X \leq x = 0.x_1x_2\cdots] \quad (\text{C.6})$$

$$= \Pr[0.X_1X_2\cdots \leq 0.x_1x_2\cdots] \quad (\text{C.7})$$

$$= \Pr[X_1 \leq x_1] + \Pr[X_1 = x_1, X_2 \leq x_2] + \cdots \quad (\text{C.8})$$

Considerando $U = F_X(X) = F_X(0.X_1X_2\cdots) = 0.F_1F_2\cdots$, pelo lema previamente enunciado, U possui distribuição uniforme em $[0, 1]$ e, portanto, os *bits* $F_1F_2\cdots$ na expansão binária de U são Bernoulli($\frac{1}{2}$), de modo que esses *bits* formam uma representação comprimida da sequência $0.X_1X_2\cdots$.