Revista Brasileira de Ensino de Física, vol. 47, e20250373 (2025)
www.scielo.br/rbef
DOI: https://doi.org/10.1590/1806-9126-RBEF-2025-0373

Artigos Gerais

Um tutorial sobre Distribuição Quântica de Chaves: dos fundamentos às tecnologias modernas

A tutorial on Quantum Key Distribution: from fundamentals to modern technologies

Vitor L. Sena[*1], Fernando de Melo[2], Micael A. Dias[1,3], Alexandre B. Tacla[1], Rafael Chaves[4]

[1]SENAI CIMATEC, Centro de Competência EMBRAPII CIMATEC em Tecnologias Quânticas, QuIIN – Quantum Industrial Innovation, Salvador, BA, Brasil.
[2]Centro Brasileiro de Pesquisas Físicas, Rio de Janeiro, RJ, Brasil.
[3]Technical University of Denmark, Department of Electrical and Photonics Engineering, Lyngby, Denmark.
[4]Universidade Federal do Rio Grande do Norte, Instituto Internacional de Física e Escola de Ciências e Tecnologia, Natal, RN, Brasil.

Recebido em 18 de agosto de 2025. Revisado em 09 de outubro de 2025. Aceito em 10 de outubro de 2025.

A física quântica marca um novo paradigma no desenvolvimento de tecnologias – nesse contexto, este trabalho apresenta um panorama acerca da Distribuição Quântica de Chaves (QKD). Partindo dos conceitos clássicos de criptografia e da ameaça iminente de computadores quânticos capazes de quebrar algoritmos de segurança amplamente utilizados, como o RSA, exploramos como a QKD aproveita propriedades intrínsecas da mecânica quântica – superposição, medidas em bases conjugadas e emaranhamento – para gerar chaves criptográficas seguras. Discutimos os primeiros protocolos com modelagem discreta (BB84, E91) detalhando cada etapa de pós-processamento: estimação de parâmetros, correção de erros e amplificação de privacidade; além de elaborarmos sobre as noções básicas de como avaliar segurança nesse contexto. Abordamos também técnicas modernas, como QKD em variáveis contínuas e (semi-)independente de dispositivos, que apresentam algumas vantagens frente às técnicas tradicionais. Com uma linguagem acessível e exemplos práticos, este tutorial convida o leitor a mergulhar na criptografia quântica e dar os primeiros passos para compreender a área de Distribuição Quântica de Chaves. Dessa forma, visamos fomentar a formação de uma nova geração de pesquisadores nesta área, dada as crescentes iniciativas de redes quânticas em desenvolvimento no Brasil.
Palavras-chave: Criptografia Quântica, Protocolos, Tecnologias Quânticas.

Quantum physics establishes a new paradigm for technological advancement. In this context, this work provides an overview of Quantum Key Distribution (QKD). Starting from classical cryptography concepts and the imminent threat of quantum computers capable of breaking security algorithms like RSA, we explore how QKD leverages intrinsic properties of quantum mechanics-superposition, measurement in conjugate bases, and entanglement-to generate secure cryptographic keys. We discuss pioneering discrete-variable protocols (BB84, E91), detailing each post-processing step: parameter estimation, error correction, and privacy amplification, while also delving into fundamental notions for evaluating QKD protocol security. Modern techniques are addressed, including continuous-variable and (semi)device-independent QKD, highlighting their advantages over traditional approaches. With accessible language and practical examples, this tutorial invites readers to dive into quantum cryptography and take their first steps toward understanding Quantum Key Distribution. We thereby aim to foster training for a new generation of researchers in this field, given Brazil's growing quantum network initiatives
Keywords: Quantum Cryptography, Protocols, Quantum Technologies.

1. Introdução

A comunicação é uma das bases das relações humanas, e é através dela que somos capazes de expressar boa parte das nossas intenções e ideias. Mas o que seria "comunicação"? De forma simples, podemos definí-la como uma transmissão de informação de um ponto a outro [1]: um recital de poesia, uma ligação telefônica ou um pedido de socorro de um navio perdido no oceano usando código Morse são todos exemplos de comunicação. E como estudar isso de maneira quantitativa? Claude Shannon, um brilhante engenheiro que viveu no século XX, lançou as bases de uma bela teoria científica que torna possível esse estudo: a Teoria da Informação [2]. Graças a esse desenvolvimento teórico, fomos capazes de chegar à compreensão de que a informação poderia ser quantificada – o que abriu a possibilidade de entendê-la de modo mais fundamental [3].

Neste texto, focamos no estudo da criptografia, que é a área de pesquisa que avalia as possibilidades de enviar informação de maneira segura. Mais especificamente,

[*]Endereço de correspondência: vitorlucasena@gmail.com
Editor-Cheffe: Marcello Ferreira

nosso foco se direciona à Criptografia Quântica, que envolve técnicas de transmissão segura de dados usando princípios da Mecânica Quântica. Aqui, abordamos desde o surgimento dessa área até seus desenvolvimentos mais recentes.

A urgência por comunicações seguras ganhou novos contornos em 1994, quando Peter Shor demonstrou como computadores quânticos poderiam fatorar números inteiros em tempo que cresce polinomialmente com o tamanho do número sendo fatorado [4]. Esse resultado não apenas revelou a vulnerabilidade de protocolos criptográficos amplamente utilizados como o RSA [5], mas também expôs uma dicotomia fundamental: enquanto o melhor algoritmo clássico para fatoração (a "peneira do campo de números" [6]) possui complexidade superpolinomial, exigindo tempos impraticáveis para fatorar números com milhares de bits, mesmo se executado em supercomputadores. O algoritmo quântico de Shor promete realizar a mesma tarefa em bem menos tempo.

Uma estimativa feita por Gidney (2025) [7] demonstra que – sob hipóteses explícitas (taxa uniforme de erro de portas de $0,1\%$, tempo de ciclo do código de superfície de $1\ \mu$s, e tempo de reação do sistema de controle de $10\ \mu$s) – um inteiro RSA de 2048 bits poderia ser fatorado em menos de uma semana por um computador com menos de um milhão de qubits ruidosos[1]. Enquanto isso, já é realidade para grandes empresas de tecnologia como IBM [8] e Atom Computing [9] a produção de chips ultrapassam a barreira dos 1.000 qubits ruidosos.

Contudo, o caminho para computação quântica prática está repleto de desafios. A decoerência (perda das propriedades quânticas de um sistema devido a sua interação com o ambiente) e a necessidade de correção de erros exigem que milhões de qubits físicos sejam combinados para formar qubits lógicos estáveis [10, 11]. Paradoxalmente, mesmo nesse estágio embrionário, a ameaça à segurança atual é real: informações criptografadas hoje poderiam ser armazenadas e decifradas no futuro, quando máquinas quânticas plenamente funcionais surgirem. Além disso, a própria suposição de que certos problemas matemáticos são intratáveis – pedra angular da criptografia clássica – mostra-se frágil diante de possíveis avanços teóricos [12, 13].

Nesse contexto, duas estratégias emergem como respostas à ameaça à segurança de sistemas trazida pelos computadores quânticos. A primeira, a criptografia pós-quântica (PQC, sigla em inglês para *Post Quantum Criptography*), busca desenvolver algoritmos clássicos baseados em problemas matemáticos considerados difíceis até para computadores quânticos, como isogenias entre curvas elípticas ou desafios em redes multidimensionais [14]. Embora o NIST (sigla em inglês para *National Institute of Standards and Technology*[2]) já tenha selecionado padrões promissores [15], essa abordagem ainda repousa sobre suposições matemáticas não comprovadas. A segunda estratégia, e foco deste trabalho, é a criptografia quântica propriamente dita – particularmente a Distribuição Quântica de Chaves (QKD, sigla em inglês para *Quantum Key Distribution*) –, que oferece segurança incondicional fundamentada nas leis da física quântica.

Curiosamente, a origem da QKD antecede a própria ameaça quântica à criptografia. Em 1984, Bennett e Brassard propuseram o protocolo BB84 [16], utilizando estados quânticos não-ortogonais e o teorema da não clonagem [17] para criar chaves secretas invioláveis. Inspirado na ideia de "dinheiro quântico" de Wiesner [18], o BB84 permite detectar qualquer tentativa de espionagem através de perturbações nos estados quânticos transmitidos. Desde então, avanços sucessivos têm expandido as fronteiras da QKD: o protocolo de seis estados [19] introduziu bases adicionais para melhorar a detecção de intrusos; o SARG04 [20] mitigou vulnerabilidades em fontes de fótons múltiplos; e o MDI-QKD [21] tornou a segurança independente dos dispositivos de medição.

Um marco recente foi o desenvolvimento do Twin-Field QKD [22], que utiliza interferência quântica para estender drasticamente as distâncias de transmissão. No Brasil, essa técnica fundamenta a Rede Rio Quântica [23, 24], iniciativa pioneira que demonstra a viabilidade prática dessas tecnologias em cenários reais. Paralelamente, protocolos como o DPS-QKD [25] e COW-QKD [26] exploram propriedades de fase e tempo dos fótons, enquanto abordagens baseadas em emaranhamento quântico, como o BBM92 [27] e E91 [28], vinculam a segurança à violação de desigualdades de Bell [29].

O dinamismo desse campo reflete-se na proliferação de revisões técnicas [30–32] e livros especializados [33–35], porém a escassez de material em português e a complexidade inerente aos conceitos quânticos criam barreiras para estudantes e profissionais. Embora trabalhos introdutórios como o de Rigolin em 2005 [36] tenham sido valiosos, a rápida evolução da área demanda atualizações constantes. Essa lacuna educacional torna-se ainda mais crítica no cenário atual brasileiro, onde iniciativas recentes de grande porte em comunicação e criptografia quânticas vêm sido fomentadas pelo MCTI. Por exemplo, a chamada CNPq/MCTI nº 26/2023 vem apoiando projetos para o desenvolvimento de redes quânticas em Recife (PE), Rio de Janeiro (RJ) e São Carlos (SP). Além disso, inaugurado em dezembro de 2023 o *Quantum Industrial Innovation* (QuIIN) – Centro de Competência EMBRAPII CIMATEC em Tecnologias Quânticas – busca posicionar o país na vanguarda do

[1] Nas estimativas de Gidney (2025), considera-se cerca de 1280 qubits lógicos de entrada, aproximadamente 897864 qubits físicos no arranjo descrito (arredondados para $< 10^6$), o que resulta num tempo total esperado de ≈ 4.96 dias.

[2] Agência do governo dos Estados Unidos responsável por desenvolver padrões, diretrizes e métricas para ciência, tecnologia e segurança.

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2025-0373

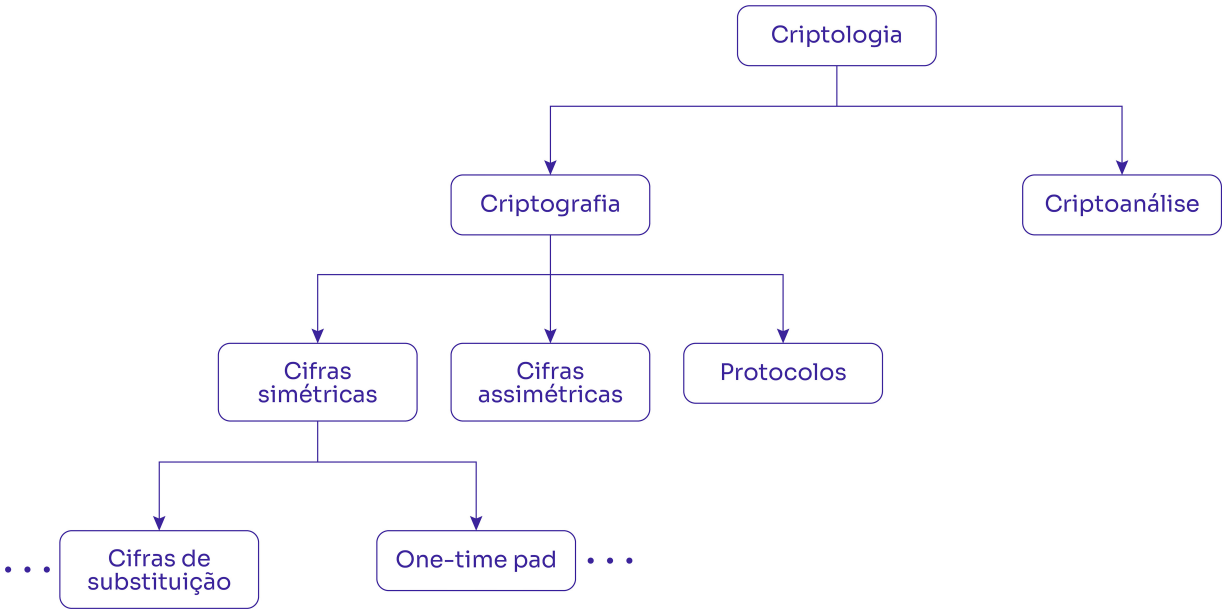

Figura 1: Diagrama das principais áreas de estudo em Criptologia, com destaque para a Criptografia – ciência dedicada à proteção da informação.

desenvolvimento científico e tecnológico também nessas áreas. Nesse contexto, a formação de recursos humanos qualificados torna-se não apenas necessária, mas urgente, o que reforça a motivação para a elaboração deste tutorial.

Este artigo é organizado da seguinte forma. Na Seção 2 apresentamos um panorama histórico e conceitual da criptografia. Na Seção 3 apresentamos o único protocolo criptográfico com segurança incondicional, as chamadas chaves secretas de uso único. Na Seção 4, introduzimos os conceitos básicos sobre teoria quântica necessários para compreender este texto. Na Seção 5, falamos de Criptografia Quântica em si, apresentando alguns dos principais e mais ilustrativos protocolos de QKD. Nas Seção 6 e Seção 7, abordamos as etapas de pós-processamento e análise de de segurança de um protocolo de QKD. Na Seção 8, falamos sobre alguns dos desenvolvimentos conceituais mais recentes da área de QKD e, por fim, na Seção 9, apresentamos nossas conclusões.

2. Um Panorama Sobre a Criptografia

Sob a perspectiva da segurança da informação, o campo no qual este artigo se insere é a Criptologia. O termo deriva do grego, em que kryptós significa "oculto" e lógos significa "estudo"; assim, a criptologia compreende o estudo voltado para a proteção e sigilo da informação.

O problema que nos interessa é o de tornar uma mensagem o mais segura possível, embaralhando seu conteúdo para que não possa ser lida por qualquer pessoa – esse processo é conhecido como cifragem. Quanto mais difícil for desembaralhar a mensagem, mais eficaz é a cifra, ou seja, mais robusto é o algoritmo de criptografia. No jargão técnico, a Criptografia é a ciência dedicada à proteção da informação, englobando métodos de cifragem e decifragem que asseguram que somente destinatários autorizados possam acessar o conteúdo original[3]. Em contrapartida, a Criptoanálise é o estudo e a prática de tentar comprometer a criptografia e acessar informações protegidas, frequentemente testando a robustez dos sistemas de segurança [37].

Na criptografia, podemos considerar dois principais modelos de geração de cifras: as cifras simétricas, em que as partes envolvidas compartilham um método comum de encriptação e decriptação, além de uma chave secreta; e as cifras assimétricas, nas quais são utilizadas duas chaves distintas – uma mantida em um canal privado e outra em um canal público. Dentro desses modelos, temos os protocolos, que consistem em conjuntos de regras ou procedimentos pré-definidos que orientam a comunicação, seja com o uso de chaves simétricas ou assimétricas [34]. A Figura 1 ilustra visualmente esse panorama das áreas de estudo. Neste trabalho, embora façamos algumas referências a cifras assimétricas e à criptoanálise, o foco é a avaliação de criptografia com cifras simétricas, especialmente por meio de protocolos QKD. Entretanto, antes de abordarmos o cenário de QKD, é importante discorrer um pouco mais sobre a criptografia clássica e seus principais conceitos.

As cifras de substituição, por exemplo, são modelos bastante simples de cifragem e são de boa serventia para

[3] Nesse contexto, vale mencionar a Esteganografia, que é a prática de ocultar uma mensagem dentro de um outro objeto, como, por exemplo, um código secreto escondido em palavras específicas de uma poesia. Todavia, este não é o foco de nosso trabalho e tampouco um assunto tradicionalmente abordado em textos de QKD e por isso não o contemplaremos neste tutorial.

ilustrar as ideias básicas de criptografia. Este tipo de cifragem funciona simplesmente trocando os símbolos da mensagem original por algum outro, criando um mapa entre o alfabeto original e o alfabeto cifrado. Por exemplo, se considerarmos o mapa:

$$\begin{aligned} A &\to \# \\ B &\to \& \\ C &\to * \\ D &\to ! \\ E &\to @ \\ &\vdots \end{aligned}$$

a palavra "BECA" seria cifrada como "&@*#". Esse tipo de substituição altera todas as letras do alfabeto por novos símbolos. A desvantagem dessa cifra é que, para decifrar toda a mensagem, o receptor geralmente precisa receber o mapa completo de correspondências, especialmente em textos que utilizam todas ou quase todas as letras do alfabeto.

Em contraponto a esta dificuldade, um tipo de cifra de substituição que mapeia um mesmo alfabeto nele mesmo foi criado – a Cifra de César. Este método de cifragem, que leva o nome do general e ditador romano Júlio César (Roma, 100 a.C. – Roma, 44 a.C.)[4], foi usado na Roma Antiga por volta do século I a.C. para fins militares e de segredos de estado [40]. Na Cifra de César, cada letra do texto original é trocada por outra, deslocada um número fixo de posições no alfabeto. Por exemplo, com um deslocamento de 3 posições para a direita, a letra A seria substituída por D, B por E, C por F e assim sucessivamente, conforme ilustrado na Figura 2. Com esta codificação, a famosa frase atribuída a Júlio César "Vim, vi, venci" se tornaria 'Ylp, yl, yhqfl".

Embora este método de cifragem tenha sido eficaz em seu tempo, o polímata árabe Ismail Al-Kindi (Cufa,

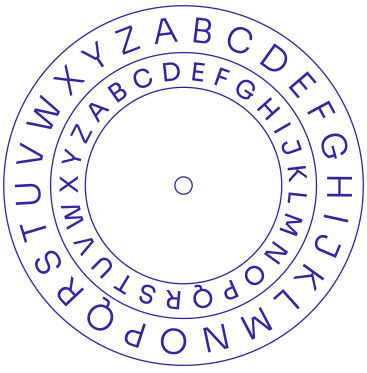

Figura 2: Anel de codificação da Cifra de César. O anel externo representa o alfabeto original e o anel interno o alfabeto cifrado.

[4] Todas os locais e datas de nascimento e falecimento das personalidades citadas neste artigo foram obtidas pelo *Virtual International Authority File* [38], plataforma digital administrada pela *Online Computer Library Center* e pela *Library of Congress* [39] – a biblioteca nacional dos Estados Unidos.

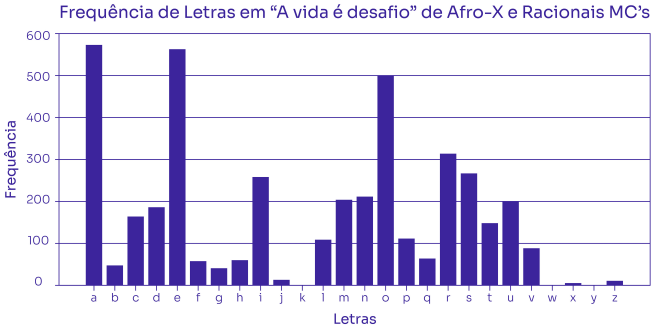

Figura 3: Histograma com a ocorrência de letras na música "A vida é desafio" de Afro-X e Racionais MC's [41].

801 – Bagdá, 873) teve seu nome marcado na história da Criptoanálise como aquele que desenvolveu uma técnica capaz de quebrar a cifra de César. A técnica consiste em um análise de padrões estatísticos de uma dada língua. Essa técnica permite quebrar facilmente a Cifra de César, pois esse método de cifragem não altera a distribuição natural das letras de um idioma.

Para entender como a análise estatística funciona, basta considerar que, em quase qualquer língua, algumas letras aparecem com muito mais frequência do que outras. No caso do português, por exemplo, letras como "A" e "E" são as mais comuns, enquanto letras como "W" e "Y" são bastante raras. Al-Kindi aplicou esse princípio à criptoanálise, partindo da premissa de que a frequência das letras no texto cifrado reflete a frequência das letras no idioma original.

O método envolve contar a ocorrência das letras no texto cifrado e compará-las com as frequências típicas da língua. Se uma determinada letra aparece com mais frequência no texto cifrado, ela provavelmente corresponde à letra mais comum no idioma original. Assim, é possível identificar rapidamente a chave de deslocamento usada na cifra, permitindo a decifração da mensagem. Para ilustrar estas afirmações, basta fazermos uma análise de frequência de letras em um texto suficientemente grande escrito em português – para tanto, analisamos a letra da música "A vida é desafio" [41] e geramos um histograma com a frequência das letras (vide Figura 3).

A fraqueza da Cifra de César e suas variações de substituição simples, decorre do fato que cada as letras do texto original são sempre codificadas nas mesmas letras no texto cifrado. Se o alfabeto é finito, duas estratégias são possíveis: ou testar todas as possíveis combinações de substituição até encontrar a correta (força bruta) ou fazer uma análise de frequência para decifrar qual troca foi feita.

Para contornar este problema, a cifra de Vigenère, que teve seu aprimoramento final dado por Blaise de Vigenère (Saint-Pourçain-sur-Sioule, 1523 – Paris, 1596), utiliza uma chave secreta ao invés de um deslocamento fixo, como na cifra de César. Esta chave nada mais é do que uma sequência de letras que dirá qual substituição deverá ser feita em cada letra da mensagem.

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2025-0373

Por exemplo, considere que queremos cifrar a palavra "criptografia" usando a chave "fisica", primeiro devemos alinhá-las para que fique nítido quais substituições devem ser feitas.

Mensagem:	c	r	i	p	t	o	g	r	a	f	i	a
Chave:	f	i	s	i	c	a	f	i	s	i	c	a

Considerando que a letra a corresponda ao número zero ($a = 0$) na codificação da cifra de Vigenère, a primeira letra da mensagem, "c", corresponde ao número dois, i.e., $c = 2$. Enquanto isso, na chave, $f = 5$. Para computarmos qual letra corresponderá a cifra, basta somarmos estes valores e atribuirmos à letra correspondente: $\mathrm{c} + \mathrm{f} = 2 + 5 = 7 \rightarrow \mathrm{h}$.

Para criptografar uma mensagem, o texto é alinhado com as letras da chave, repetindo-a conforme necessário. Cada letra do texto é deslocada de acordo com a letra correspondente da chave. Essa abordagem torna a criptoanálise mais difícil, pois o comprimento e a aleatoriedade da chave criam um padrão de deslocamento complexo. Assim sendo,

Mensagem:	c	r	i	p	t	o	g	r	a	f	i	a
	+	+	+	+	+	+	+	+	+	+	+	+
Chave:	f	i	s	i	c	a	f	i	s	i	c	a
Cifra:	h	z	a	x	v	o	l	z	s	n	k	a

No último passo, convertemos os números de volta para letras com resultado "hzaxvolzsnka".

Mas mesmo a cifra de Vigenère pode ser quebrada através de uma combinação da análise estatística descrita anteriormente com o chamado método de Kasiski [42] proposto em 1863 pelo militar e criptógrafo prussiano Friedrich Wilhelm Kasiski (Schlochau, 1805 – Neustettin, 1881) com o intuito de desvendar o tamanho da chave secreta utilizada.

Com o tempo, diversos protocolos de criptografia evoluíram em resposta à crescente demanda por segurança nas comunicações. Durante a Segunda Guerra Mundial, a máquina de cifras Enigma se destacou, utilizando rotores para gerar chaves dinâmicas, o que tornava a criptoanálise ainda mais desafiadora [43]. Nesses casos, o destinatário precisava conhecer a chave secreta utilizada pelo remetente; caso contrário, não conseguiria decifrar a mensagem. Foi justamente a necessidade de quebrar a criptografia utilizada pelos nazistas que motivou a construção dos primeiros computadores clássicos.

Os sistemas criptográficos apresentados até aqui são baseados em criptografia de chave simétrica, na qual a mesma chave é utilizada para a cifragem e a decifragem da mensagem. Em 1976, Whitfield Diffie e Martin Hellman propuseram sistemas de criptografia assimétrica [44], que utilizam um par de chaves: uma chave pública, usada para cifrar a mensagem, e uma chave privada, utilizada para decifrá-la. Para que esse método seja prático e seguro, a função de cifragem precisa ser computacionalmente difícil de inverter sem o conhecimento da chave privada, mas de fácil inversão quando a chave privada é conhecida. Inspirados no esquema de Diffie e Hellman, em 1978, Rivest, Shamir e Adleman, fundadores da empresa *RSA Data Security, Inc.*, propuseram um protocolo criptográfico baseado na dificuldade de fatorar números inteiros muito grandes [5], que ficou conhecido como o sistema criptográfico RSA. Isso permitiu a troca segura de mensagens sem a necessidade de uma chave simétrica pré-estabelecida, lançando as bases para os sistemas de segurança modernos. No entanto, o algoritmo de Shor [4], proposto em 1994, ameaça diretamente o RSA ao permitir a fatoração eficiente de números inteiros, quebrando a base matemática que sustenta sua segurança.

A tensão entre criação de modelos criptográficos mais robustos e o desenvolvimento de técnicas de criptoanálise mais sofisticados é constante. Mas seria possível conceber um protocolo de criptografia que fosse fundamentalmente seguro? Isto é, um tipo de lógica de defesa de informação que seja inquebrável? A resposta a esta pergunta é: sim! Discutiremos ela mais a fundo na seção a seguir.

3. Segurança Incondicional: Chaves Secretas de Uso Único

Quando falamos de um sistema de comunicação com "segurança incondicional", estamos nos referindo a uma proteção que não pode ser violada, nem mesmo por um computador hipotético com recursos infinitos. Embora essa ideia possa soar fantasiosa, ela é real e relativamente simples. Em 1926, cerca de dois milênios após o primeiro registro de um sistema criptográfico, foi publicado o trabalho do engenheiro estadunidense Gilbert Vernam (Nova Iorque, 1890 – Hackensack, 1960) [45], que propôs e comprovou um modelo de segurança incondicional da informação.

Este modelo, conhecido como Cifra de Vernam ou, em seu nome mais popular, *One-time pad*, é um tipo de criptografia simétrica que se utiliza chaves de uso único, isto é, a chave é utilizada uma única vez para cifrar e decifrar a mensagem. Em uma comunicação com chaves simétricas, temos um esquema como o ilustrado na Figura 4. Uma parte codifica uma determinada mensagem com a chave, transformando o texto original em uma cifra; a cifra então é enviada para a outra parte; esta segunda parte decifra a mensagem usando uma cópia da chave que foi utilizada na cifragem. Note que a cifra pode ser enviada por um canal aberto sem grandes problemas, pois mesmo que ela seja interceptada por um espião, se ele não possuir a chave para decifrá-la, ele não poderá acessar a mensagem.

Todos esses elementos – mensagem, chave e cifra – podem, em última análise, ser representados por um número binário (uma sequência de zeros e uns). Isso ocorre porque o nível mais fundamental de representação da informação é o binário, permitindo que qualquer informação (clássica) seja expressa em bits. Este princípio

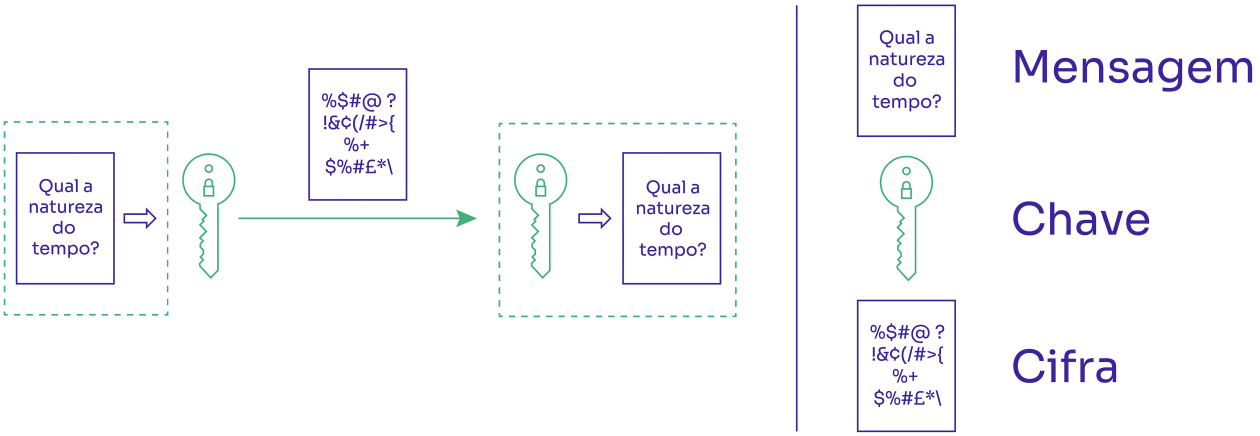

Figura 4: Representação pictórica da criptografia de chave simétrica, destacando seus três elementos principais: mensagem, chave e cifra.

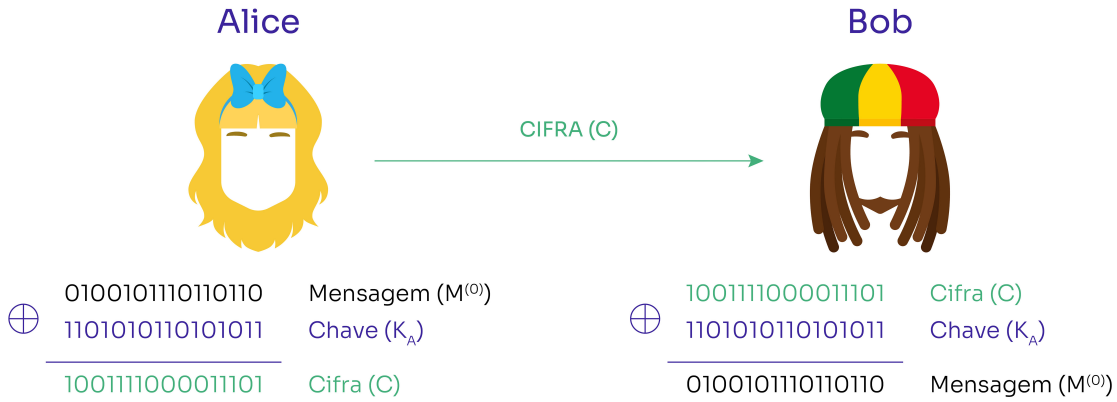

Figura 5: Ilustração do processo de cifragem e decifragem utilizando uma chave secreta de uso único.

foi formalizado em 1948 por Claude Shannon, um dos fundadores da teoria da informação [2].

Sendo assim, consideremos um cenário de comunicação simples para verificar o funcionamento prático do *one-time pad*. A explicação a seguir está ilustrada na Figura 5. Assumamos que uma parte, Alice, quer enviar uma mensagem cifrada para outra parte, Bob. A mensagem inicial $M^{(0)}$ é cifrada por Alice usando uma chave K_A, o que gera uma cifra C, este procedimento é feito utilizando soma binária (ou soma módulo 2). Na soma módulo 2, $0 \oplus 0 = 1 \oplus 1 = 0$ e $0 \oplus 1 = 1 \oplus 0 = 1$. Se consideramos duas sequências de bits, a soma módulo 2 será realizada bit a bit dessas sequências. Em particular, se somamos a mesma sequência, por exemplo as chaves, temos que $K_A \oplus K_A = 0 \ldots 0$. De forma similar, se somamos uma sequência, por exemplo, $M^{(0)}$ com uma sequência de zeros, temos que $M^{(0)} \oplus 0 \ldots 0 = M^{(0)}$. Usando estas propriedades básicas podemos definir a cifra da seguinte forma:

$$C = M^{(0)} \oplus K_A. \tag{1}$$

Já Bob, quando recebe C, utiliza uma chave K_B para decifrá-la usando também soma binária. Em geral, Bob recupera uma mensagem final $M^{(f)}$,

$$M^{(f)} = C \oplus K_B. \tag{2}$$

O interessante do protocolo *one-time pad* é o fato de que, se as chaves de Alice e Bob forem iguais ($K_A = K_B$), é garantido que as mensagens inicial e final serão iguais. A verificação deste resultado pode ser vista como a seguir:

$$\begin{aligned} M^{(f)} &= C \oplus K_B \\ &= [M^{(0)} \oplus K_A] \oplus K_B \\ &= M^{(0)} \oplus \underbrace{[K_A \oplus K_B]}_{\text{tome } K_A = K_B = K} \\ &= M^{(0)} \oplus [K \oplus K] \\ M^{(f)} &= M^{(0)}. \end{aligned} \tag{3}$$

Esta construção nos mostra que, se Alice e Bob compartilham uma mesma chave, eles podem trocar mensagens encriptadas entre si. Pois, se a chave é verdadeiramente aleatória, então a mensagem cifrada C também parece perfeitamente aleatória para quem não tem a chave.

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2025-0373

No entanto, apesar de crucial, apenas a aleatoriedade não garante a segurança do protocolo. Para que o *one-time pad* seja efetivamente seguro, deve atender as seguintes condições:

1. A chave K deve ser verdadeiramente aleatória;
2. A chave só pode ser utilizada uma única vez;
3. A chave K que Alice e Bob compartilham deve ser conhecida apenas por eles.

A condição 1 quer dizer que os bits individuais de uma chave verdadeiramente aleatória não estão correlacionados entre si, nem com outras chaves geradas pelo mesmo sistema. Isto é, para uma chave de tamanho N, os n primeiros bits ($n < N$) não revelam informação alguma sobre os bits $N - n$, nem sobre qualquer bit de outras chaves. Entretanto, gerar números verdadeiramente aleatórios é um enorme desafio. A maioria dos computadores atuais geram números pseudoaleatórios por meio de algoritmos determinísticos, resultando, em última instância, em sequências previsíveis, se a sequência de bits inicial usada para alimentar o algoritmo (chamada de semente) for conhecida. Em contraste, a natureza probabilística da mecânica quântica nos permite não apenas gerar números verdadeiramente aleatórios, mas também certificar sua aleatoriedade [46], nos chamados QRNGs (sigla em inglês para *Quantum Random Number Generator*), fornecendo alta entropia e segurança essencial em aplicações criptográficas.

A condição 2, embora teoricamente possível, apresenta desafios práticos significativos. O uso único de cada chave exige que ela tenha pelo menos o mesmo tamanho da mensagem, pois, segundo essa condição, a mesma chave não pode ser reutilizada para cifrar diferentes partes da mensagem. Isso pode ser gerenciável em textos curtos, mas, por exemplo, para cifrar um arquivo de 1 GB, seria necessário gerar uma chave de pelo menos o mesmo tamanho, o que complica tanto a cifragem quanto a geração e a distribuição dessa chave. Por essas razões, o *one-time pad* raramente é usado na prática, apesar de sua segurança incondicional. Em muitas situações, opta-se por alternativas mais eficientes, como, por exemplo, o AES (Padrão de Criptografia Avançada, do inglês *Advanced Encryption Standard*) [47], o uso de geradores de números pseudoaleatórios criptograficamente seguros [48], entre outros.

A condição 3 implica em um problema crucial em Criptografia: a distribuição de chaves. Veja que, dado o esquema da Figura 4, não há problema se o canal que a cifra será enviada for inseguro, mas a chave precisa ser mantida em máximo segredo, inclusive durante a etapa de distribuição. Esta etapa de um protocolo é tão importante que existe uma área de estudos em Criptografia dedicada a ela, e especificamente quando falamos de utilizar sistemas quânticos para realizar esta tarefa, esta área é denominada Distribuição Quântica de Chaves. A *QKD* é o coração do que discutiremos neste artigo e o foco da Seção 5. Todavia, antes de chegar lá, é instrutivo apresentar alguns conceitos e ideias formais da teoria quântica.

4. As Regras do Jogo Quântico

Para uma abordagem prática, podemos entender a teoria quântica como um conjunto de regras fundamentais que permitem descrever sistemas físicos de maneira consistente. O conjunto mínimo dessas regras, conhecidas como postulados, serve de base para deduzir todas as implicações e fenômenos da mecânica quântica. Embora o número de postulados varie conforme a fonte consultada, neste contexto, voltado para aplicações em criptografia quântica, focaremos em três postulados principais.

4.1. Primeiro postulado

O primeiro postulado diz respeito à forma como descrevemos sistemas quânticos. Na física clássica, costumamos definir o estado de uma partícula por sua posição e momento, representados em coordenadas no espaço tridimensional. Em contraste, na teoria quântica, o estado de um sistema físico é descrito por um vetor de estado, não no espaço de três dimensões usual, mas em um espaço de Hilbert. Esse espaço é um espaço vetorial sobre os números complexos, possivelmente de dimensão infinita, e está equipado com um produto interno, que permite definir normas (comprimentos) e distâncias [49].

De forma resumida, o primeiro postulado estabelece a seguinte correspondência:

$$\begin{array}{lcl} \text{Sistema Quântico} & \longrightarrow & \mathcal{H} \text{ (Espaço de Hilbert)}, \\ \text{Estado Quântico} & \longrightarrow & \psi \in \mathcal{H} \text{ tal que } \|\psi\| = 1, \end{array}$$

onde $\|\psi\| = \sqrt{\langle \psi, \psi \rangle} = 1$ é o produto interno do vetor com ele mesmo. Para vetores $\psi \in \mathcal{H}$ normalizados, $\|\psi\| = 1$, isto é, para estados quânticos, reservamos o símbolo $|\psi\rangle$, leia-se "ket"-ψ. De forma geral, o produto escalar de dois vetores de estados, $|\psi\rangle$ e $|\phi\rangle$ em um espaço de Hilbert $\mathcal{H}$, é expresso como $\langle \phi | \psi \rangle = \langle \phi, \psi \rangle$.

Para ilustrar as diferenças entre a descrição clássica e quântica, consideremos o sistema físico não-trivial mais simples possível, que possa assumir um de dois possíveis valores. Classicamente, estamos falando de um bit, assumindo os valores 0 ou 1. Quanticamente o vetor de estado do chamado qubit, ou bit quântico, pode assumir não apenas os valores correspondentes $|0\rangle$ e $|1\rangle$, mas também qualquer superposição $|\psi\rangle = \alpha\,|0\rangle + \beta|1\rangle$, onde α e β são números complexos que devem satisfazer a condição $|\alpha|^2 + |\beta|^2 = 1$, uma vez que os estados $|0\rangle$ e $|1\rangle$ são ortogonais entre si. Essa restrição aos coeficientes α e β é chamada de condição de normalização, sendo essencial para a interpretação probabilística dos resultados de medições, como discutimos no próximo postulado.

4.2. Segundo postulado

Medições quânticas são representadas matematicamente por uma coleção de operadores que agem sobre o espaço de estados do sistema quântico [49]. No contexto deste tutorial, é suficiente considerarmos o caso particular, e de grande importância, em que os operadores de medição podem ser descritos por um conjunto completo de projetores de posto-um $\{P_i\}$, isto é, satisfazem $\sum_i P_i = \mathbb{1}$, auto-adjuntos ($P_i^\dagger = P_i$) e mutuamente ortogonais, $P_i P_j = \delta_{ij} P_i$. O indíce i rotula as possíveis medidas de uma grandeza física.

Dessa forma, em um espaço de Hilbert em dimensão d, podemos representar uma grandeza física φ por um operador linear auto-adjunto Φ cuja decomposição espectral é,

$$\Phi = \sum_{i=1}^{d} \phi_i \, |\phi_i\rangle\langle\phi_i|, \tag{4}$$

onde os possíveis resultados de medição são os autovalores ϕ_i e a cada ϕ_i corresponde um projetor $P_{\phi_i} = |\phi_i\rangle\langle\phi_i|$ que isola o subespaço próprio associado. A probabilidade de obter ϕ_i em um estado $|\psi\rangle$ é dada por $\langle\psi|P_{\phi_i}|\psi\rangle$, e a condição de completude assegura normalização das probabilidades, ou seja, que: $\sum_{i=1}^{d}\langle\psi|P_{\phi_i}\,|\psi\rangle = 1$.

Seguindo essa lógica, a regra de Born nos exprime a probabilidade de obter o resultado $|\phi\rangle$ em um processo de medição.

$$\begin{aligned}
\Pr\left(\phi_i|\psi\right) &= \|P_{\phi_i}\,|\psi\rangle\|^2, \\
&= \||\phi_i\rangle\langle\phi_i|\psi\rangle\|^2, \\
&= \left(\sqrt{(\langle\phi_i|\psi\rangle^*\langle\phi_i|)(|\phi_i\rangle\,\langle\phi_i|\psi\rangle)}\right)^2, \\
&= \left(\sqrt{|\langle\phi_i|\psi\rangle|^2\langle\phi_i|\phi_i\rangle}\right)^2, \\
&= |\langle\phi_i|\psi\rangle|^2.
\end{aligned} \tag{5}$$

Para ilustrar, considere o estado $|\psi\rangle = \alpha\,|0\rangle + \beta|1\rangle$. Usando a regra descrita acima, vemos que a probabilidade de encontrar $|\psi\rangle$ no estado $|0\rangle$ será $|\alpha|^2$ e similarmente para o estado $|1\rangle$ será $|\beta|^2$. Frisamos que, por consequência da normalização, temos: $|\alpha|^2+|\beta|^2 = 1$.

Um ponto importante é de que uma medição é um processo irreversível que, de modo geral, modifica um estado quântico, quer dizer, se após uma medição de um observável $\Phi \equiv \sum_{i=1}^{d}\phi_i\,P_{\phi_i}$ obtivermos como resultado ϕ_i o estado quântico pós-medição será $|\phi_i\rangle$. Note que, no caso particular em que o estado pré-medição fosse $|\phi_i\rangle$, a medição do observável Φ não alteraria o estado, pois $\{|\phi_i\rangle\}$ são autoestados de Φ. Importante também ressaltar que assumimos que cada valor de φ está associado a um projetor de posto um, quer dizer, um operador que projeta qualquer vetor de um espaço em um subespaço unidimensional gerado por um vetor normalizado $|\phi\rangle$, tendo a forma $|\phi\rangle\langle\phi|$. Neste caso o observável é dito não degenerado [50].

Podemos resumir então o postulado da medição da seguinte forma. A toda propriedade física φ associamos um observável $\Phi = \sum_{i=1}^{d}\phi_i P_{\phi_i}$, tal que ϕ_i sejam números reais, $P_{\phi_i}^2 = P_{\phi_i}$, $\sum_{i=1}^{d} P_{\phi_i} = \mathbb{1}$. Dado um estado $|\psi\rangle$, a probabilidade que obtenhamos o valor ϕ_i na medição será:

$$\Pr(\phi_i|\psi) = \|P_{\phi_i}\,|\psi\rangle\|^2, \tag{6}$$

e o estado após a medição será dado por

$$\frac{P_{\phi_i}\,|\psi\rangle}{\|P_{\phi_i}\,|\psi\rangle\|}. \tag{7}$$

4.3. Terceiro postulado

O último postulado de interesse se relaciona à evolução temporal de um estado quântico $|\psi(t)\rangle$ que é governada pela equação de Schrödinger:

$$\mathrm{i}\hbar\frac{d\,|\psi(t)\rangle}{dt} = H\,|\psi(t)\rangle\,, \tag{8}$$

onde H é o observável associado à energia total do sistema, quer dizer, seu Hamiltoniano.

Para Hamiltonianos independentes do tempo podemos integrar explicitamente a equação de Schrödinger para obter:

$$|\psi(t)\rangle = e^{-\frac{\mathrm{i}H}{\hbar}(t-t')}\,|\psi(t')\rangle\,, \tag{9}$$

que conecta o estado no tempo t com o estado em um tempo t'. Assim, o operador que translada o estado quântico no tempo, o chamado operador de evolução,

$$U(t,t') = e^{-\frac{\mathrm{i}H}{\hbar}(t-t')}, \tag{10}$$

é um operador unitário, tal que $U(t,t')^\dagger U(t,t') = U(t,t')U(t,t')^\dagger = \mathbb{1}$. Essa unitariedade implica que a norma do estado quântico é preservada, quer dizer, $\||\psi(t)\rangle\|^2 = \||\psi(t')\rangle\|^2$. De forma mais geral, mesmo para Hamiltonianos que dependam do tempo, o operador de evolução temporal continuará a ser dado por um operador unitário [5].

4.4. Quarto postulado

O quarto postulado nos aponta como lidar com a composição de sistemas quânticos [49]. O espaço de estados do sistema composto é dado pelo produto tensorial (representado por $\otimes$) dos espaços dos subsistemas. Em termos práticos, se $\{|e_i\rangle\}$ é base do sistema A e $\{|w_j\rangle\}$ é base do sistema B, então $\{|e_i\rangle \otimes |w_j\rangle\}$ é base do sistema composto. A dimensão do espaço de Hilbert do sistema total é o produto das dimensões dos espaços individuais.

[5] Note que por simplicidade didática, restringiremos nossa análise ao caso de sistemas quânticos fechados, descritos por estados puros (sem incerteza estatística), associados a evoluções unitárias e descritos por medições projetivas. Para generalizações para o caso de sistemas quânticos abertos sugerimos a Ref. [49].

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2025-0373

Se o estado composto for um produto tensorial de estados individuais, as partes são independentes; mas se for uma superposição não-separável no espaço tensorial, ele representa um estado emaranhado [49]. Estados desse tipo apresentam correlações quânticas que não têm análogo clássico e justamente por isso, são um recurso chave para a criptografia quântica baseada em violações de desigualdades de Bell (vide Seção 5) e para provar a segurança de protocolos QKD [51, 52].

Para enxergarmos a representação do emaranhamento nas contas, considere um estado $|\psi\rangle \in \mathcal{H}_{AB}$ que descreve um estado de um sistema composto de duas partes, A e B. Se pudermos escrever $|\psi\rangle$ como o produto do estado em $\mathcal{H}_A$ com um estado em $\mathcal{H}_B$, tal que:

$$|\psi\rangle = |\phi\rangle \otimes |\chi\rangle\,, \tag{11}$$

para $|\phi\rangle \in \mathcal{H}_A$ e $|\chi\rangle \in \mathcal{H}_B$, então o estado é dito separável ou não-emaranhado. Caso contrário, se:

$$|\psi\rangle \neq |\phi\rangle \otimes |\chi\rangle\,, \tag{12}$$

ele é dito emaranhado.

Ressaltamos que é comum se usar também uma notação reduzida tal que $|\phi\rangle \otimes |\chi\rangle \equiv |\phi\rangle\,|\chi\rangle \equiv |\phi\chi\rangle$. Uma das consequências do produto tensorial é que a dimensão do espaço combinado cresce de acordo com o produto das dimensões individuais $\dim(\mathcal{H}_{AB}) = \dim(\mathcal{H}_A) \cdot \dim(\mathcal{H}_B)$. Ou seja, ela aumenta muito mais rapidamente do que no caso clássico, em que o espaço associado a variáveis aleatórias combinadas cresce com a soma das dimensões individuais. Isso significa que, no domínio quântico, temos "espaço" para um número muito maior de configurações diferentes quando comparado aos estados clássicos. Essas possibilidades a mais de configurações correspondem justamente aos estados quânticos emaranhados.

4.5. Exemplos e implementações

Para exemplificar, considere o estado:

$$|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle). \tag{13}$$

Seria este um estado separável? A resposta é sim já que podemos reescrevê-lo como

$$|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \tag{14}$$

ou seja, o produto tensorial de dois estados. Entretanto para o estado

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{15}$$

pode-se verificar que esta decomposição é impossível. O estado (15) é conhecido como estado de Bell, sendo também chamado de estado maximamente emaranhado de dois qubits), tendo um papel essencial em toda a computação, comunicação e criptografia quântica. Ele pode ser gerado, por exemplo, a partir de um estado inicialmente separável no qual aplicamos uma transformação unitária emaranhante chamada de CNOT (Negação Controlada) que pode ser definida na base $\{|00\rangle\,, |01\rangle\,, |10\rangle\,, |11\rangle\}$ como

$$CNOT = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|\,, \tag{16}$$

implicando que:

$$\begin{aligned} CNOT\,|00\rangle &= |00\rangle\,;\\ CNOT\,|01\rangle &= |01\rangle\,;\\ CNOT\,|10\rangle &= |11\rangle\,;\\ CNOT\,|11\rangle &= |10\rangle\,. \end{aligned}$$

ou seja, se o primeiro qubit estiver no estado $|0\rangle$, nada é feito; se o primeiro qubit estiver no estado $|1\rangle$, aplicamos a unitária X ao segundo qubit, "flipando" $|0\rangle$ para $|1\rangle$ e vice-versa.

De forma resumida, o emaranhamento é definido pela sua negação, já que um estado será dito emaranhado quando não for separável, ou seja, para um estado emaranhado não existem $|\phi\rangle_A \in \mathcal{H}_A$ e $|\chi\rangle_B \in \mathcal{H}_B$ tal que $|\psi\rangle \overset{!}{=} |\phi\rangle_A \otimes |\chi\rangle_B$.

Uma outra consequência dos postulados da mecância quântica, é o chamado teorema da não clonagem, resultado essencial em criptografia quântica e em particular no protocolo BB84 [16] que será discutido detalhadamente mais adiante. Esse teorema impede a cópia perfeita de estados quânticos desconhecidos, ele também assegura que informações codificadas em superposições quânticas – como as usadas em protocolos de criptografia quântica – não possam ser replicadas por um invasor sem perturbar o sistema.

Teorema 1 (Teorema da não clonagem) *É impossível construir uma copiadora universal de estados quânticos. Isto é, uma máquina que clone perfeitamente um estado quântico arbitrário.*

Podemos provar este teorema seguindo o que foi feito por Nielsen e Chuang em [49].

Prova

Faremos uma prova por contradição. Suponha U_C como uma operação unitária que realiza clonagem de um estado quântico. Assim, queremos criar uma cópia do estado desconhecido $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ em um segundo qubit inicialmente preparado em $|0\rangle$. Se tal unitária existe, esperamos que ela funcione da seguinte forma:

$$\begin{aligned} U_C\,|\psi\rangle \otimes |0\rangle &= |\psi\rangle \otimes |\psi\rangle\,,\\ &= (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\alpha\,|0\rangle + \beta\,|1\rangle)\,,\\ &= |\alpha|^2\,|00\rangle + \alpha\beta\,|01\rangle + \beta\alpha\,|10\rangle + |\beta|^2\,|11\rangle\,. \end{aligned} \tag{17}$$

No entanto, se, por hipótese, U_C clona qualquer estado quântico, em particular também faz: $U_C\,|0\rangle \otimes |0\rangle = |0\rangle \otimes$

$|0\rangle$ *e* $U_C\,|1\rangle \otimes |1\rangle = |1\rangle \otimes |1\rangle$. *Logo, pela linearidade da mecânica quântica temos:*

$$\begin{aligned} U_C\,(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes |0\rangle &= \alpha\; U_C\,|00\rangle + \beta\; U_C\,|10\rangle\,, \\ &= \alpha\,|00\rangle + \beta\,|11\rangle\,. \end{aligned} \tag{18}$$

Ao compararmos as Eq. (17) *e Eq.* (18)*, vemos que elas só são iguais se* $\alpha = 1$ *e* $\beta = 0$*, ou se* $\alpha = 0$ *e* $\beta = 1$*. Ou seja, não é possível construir* U_C *unitária tal que se possa clonar estados* $|\psi\rangle$ *para* α *e* β *arbitrários.*

Tal como vemos na prova do Teorema 1 acima, enquanto cópias dos estados clássicos (como o $|0\rangle$ e o $|1\rangle$) são triviais, qualquer tentativa de clonar um estado de superposição usando o mesmo dispositivo, como $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, resulta não em duas cópias idênticas, mas em estados emaranhados. Essa limitação fundamental é aproveitada em sistemas de comunicação segura, onde a impossibilidade de clonagem age como um selo de autenticidade: se alguém tentar interceptar e copiar a mensagem, a própria tentativa deixará marcas detectáveis, garantindo que a intrusão seja identificada.

Assim sendo, vemos que qualquer protocolo de clonagem só é capaz de copiar perfeitamente um conjunto de estados ortogonais particulares. O que nos assegura que a informação quântica não pode ser copiada, fato que obviamente tem relevância estratégica em protocolos nos quais queiramos proteger a nossa informação.

5. Distribuição Quântica de Chaves

Como apresentado, os sistemas de criptografia clássica de chave pública não garantem que a mensagem cifrada esteja incondicionalmente segura, uma vez que a segurança é baseada na expectativa (ou conjectura) de que certas funções são difíceis de inverter sem o conhecimento da chave privada. A segurança incondicional é possível utilizando chaves simétricas, resultando em problemas práticos para geração e distribuição dessas chaves. Os métodos de Distribuição Quântica de Chaves[6] utilizam as propriedades inerentes de sistemas quânticos para viabilizar a geração e distribuição segura de chaves criptográficas.

Em condições ideais, um protocolo quântico seria inviolável. Entretanto, na prática, imperfeições como ruído, perdas ou falhas no hardware podem ser exploradas por agentes mal-intencionados, comprometendo o sistema sem contrariar a teoria. Analisaremos esses ataques com mais detalhes na Seção 7. Por ora, vamos nos concentrar na versão idealizada da criptografia quântica.

Como ponto de partida, relembremos o que foi discutido no final da Seção 3: para garantir uma comunicação segura, é essencial ser capaz de gerar chaves secretas que codifiquem a mensagem da melhor forma possível. Idealmente, essas chaves devem ser conhecidas apenas pelo emissor e pelo receptor das mensagens. O desafio central, portanto, é como gerar e distribuir essas chaves de maneira segura.

Um típico cenário de comunicação para Distribuição Quântica de Chaves (QKD) envolve três partes: Alice (parte 1) e Bob (parte 2), que tentam estabelecer uma comunicação segura, e Eva (parte 3), uma espiã que busca interceptar as informações compartilhadas. A troca de dados ocorre por meio de dois canais: o canal quântico, utilizado para enviar estados quânticos, e o canal clássico público e autenticado, pelo qual Alice e Bob podem se comunicar sem a possibilidade de que Eva modifique as mensagens enviadas ou se passe por Alice ou Bob durante a execução do protocolo. Na Figura 6, ilustra-se um cenário de comunicação do tipo "prepara e mede" – nesse modelo, uma parte prepara e transmite estados quânticos, enquanto a outra os mede utilizando um canal clássico autenticado, as partes se comunicam para processar, destilar e validar a chave secreta sem expor informações sensíveis.

Os protocolos de QKD podem ser divididos em duas etapas principais: a transmissão da chave e o pós-processamento. O canal clássico desempenha um papel crucial nesta segunda etapa, que será abordada com mais detalhes na Seção 6. A parte quântica do protocolo, que utiliza o canal quântico, é responsável pela geração da chave. Nesta fase, os estados quânticos são transmitidos de Alice para Bob[7], e as medições realizadas sobre esses estados os transformam em bits clássicos que comporão a chave final.

A seguir, introduzimos o protocolo BB84 [16], o primeiro protocolo de criptografia quântica a fazer uso

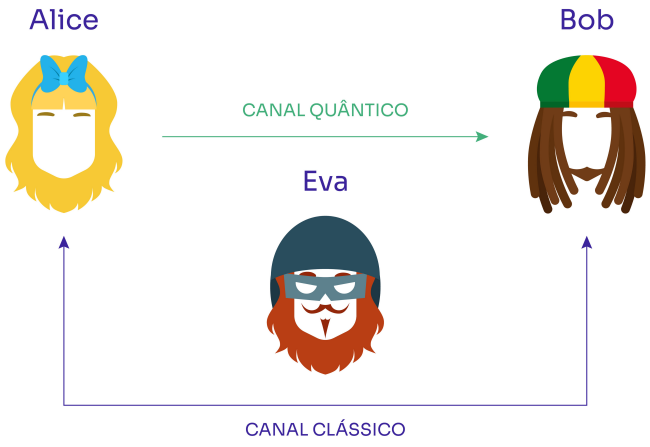

Figura 6: Cenário de comunicação quântica, no qual duas partes distantes, Alice e Bob, utilizam um canal quântico e outro clássico para estabelecer um chave secreta que permite criptografar a informação contra Eva, uma espiã que possa ter acesso a ambos os canais.

[6] Nesse manuscrito, destacamos o estudo de técnicas de distribuição quântica de chaves, mas devemos ressaltar a existência de outros protocolos criptográficas baseados em sistemas quânticos, como a transmissão quântica de chaves oblívias [53] e a comunicação privada quântica sem chave [54].

[7] A transmissão também poderia ocorrer na direção oposta. O importante é que o canal seja unidirecional.

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2025-0373

da impossibilidade de se copiar informação quântica codificada em distintas bases. Em seguida apresentamos o protocolo proposto por Arthur Ekert em 1991 (E91) [28], cuja segurança se baseia no emaranhamento quântico e a violação de uma desigualdade de Bell, formando a base dos protocolos "independentes de dispositivo" mais seguros possíveis e que serão explorados em mais detalhes na Seção 7.

5.1. Protocolo BB84

Este protocolo, desenvolvido por Bennett e Brassard em 1984 [16], parte de uma ideia simples: Alice e Bob empregam a não clonagem e aleatoriedade intrínseca de sistemas quânticos para que um eventual hacker, ao tentar ganhar informação sobre a chave secreta sendo estabelecida, seja facilmente detectado. Mas como isso funciona?

Primeiramente, Alice e Bob devem utilizar duas bases incompatíveis para gerar e medir os qubits que serão empregados na etapa de comunicação quântica. O termo "bases incompatíveis" refere-se a propriedades observáveis que não comutam entre si, como, por exemplo, o spin de um elétron nas direções $\hat{z}$ e $\hat{x}$, ou equivalentemente as orientações de polarização retilínea e diagonal da luz. No que se segue, focaremos no segundo exemplo, o mais comum quando falamos de comunicação quântica e criptografia.

A polarização é uma propriedade das ondas eletromagnéticas, representando a direção na qual o campo elétrico da onda está oscilando. Alternativamente, podemos também falar da polarização das partículas que compõe uma onda eletromagnética, os chamados fótons. No caso do protocolo BB84, iremos lidar com duas direções de oscilação deste campo elétrico, ou seja, com duas direções da polarização. A base $\{|0\rangle, |1\rangle\}$, chamada retilínea, descreve o campo eletromagnético polarizado nas direções 0° e 90°; enquanto a base $\{|+\rangle, |-\rangle\}$, conhecida diagonal, descreve o campo polarizado em 45° e −45°. Estas bases se relacionam da tal forma que:

$$|\pm\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle \pm |1\rangle \right). \tag{19}$$

Cada um dos estados em cada base pode ser associado a um bit de informação, como detalhado no Quadro 1. Dessa forma, se os estados forem preparados na base diagonal, $|+\rangle$ ou $|-\rangle$, e medidos na própria base diagonal, o resultado será totalmente determinístico: obteremos sempre o bit 0 no caso de $|+\rangle$ e sempre o bit 1 no caso de $|-\rangle$. Por outro lado, se estados preparados na base diagonal forem medidos na base retilínea, o resultado é totalmente aleatório: os bits 0 e 1 ocorrem com probabilidade 1/2 em ambos os casos[8]. Algo similar acontece quando preparamos $|0\rangle$ ou $|1\rangle$: se medirmos na base retilínea, os resultados são, respectivamente, 0 e 1, mas

[8] Vide a Equação 19, na qual escrevemos $|\pm\rangle$ na base $\{|0\rangle, |1\rangle\}$.

Quadro 1: Estados quânticos, bases de medição e bits pós-medição.

Estado quântico	Base de medição	Bit codificado
$\|0\rangle$	Retilínea	0
$\|1\rangle$	Retilínea	1
$\|+\rangle$	Diagonal	0
$\|-\rangle$	Diagonal	1
$\|0\rangle$ ou $\|1\rangle$	Diagonal	0 (prob. 50%)
		1 (prob. 50%)
$\|+\rangle$ ou $\|-\rangle$	Retilínea	0 (prob. 50%)
		1 (prob. 50%)

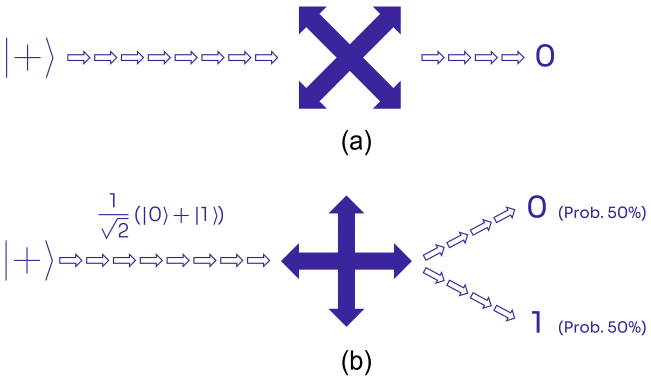

Figura 7: a) Um estado preparado na base diagonal é medido também na base diagonal. Em casos como este, em que há coincidência entre a base de preparação e medição, o bit medido sempre corresponde ao qubit codificado. Esta figura ilustra o caso da terceira linha do Quadro 1. **b)** Um estado preparado na base diagonal é medido na base retilínea. Em casos como este, por as bases de preparação e medição serem incompatíveis, o resultado da medição é aleatório e equiprovável. Esta figura ilustra o caso da última linha do Quadro 1.

se medirmos na base diagonal, há uma probabilidade de 50% de obtermos 0 ou 1. Estas informações estão resumidas no Quadro 1 e ilustrada com exemplos na Figura 7.

Agora voltando ao protocolo em si, seu primeiro passo consiste em Alice escolher aleatoriamente entre uma das duas bases para codificar o bit, ou a base retilínea ou a base diagonal; escolhida a base, ela escolhe, também aleatoriamente, o bit a ser transmitido e codifica ele em um estado quântico, quer dizer, um qubit, conforme ilustrado na Figura 8. Já Bob recebe o qubit codificado por Alice e escolhe, também de forma aleatória, uma das bases para realizar a medição; escolhida a base, ele mede o estado quântico e obtém como resposta ou o bit 0 ou o bit 1, conforme ilustrado na Figura 9.

Quando Alice finaliza o envio de um número n de estados quânticos pré-estabelecido com Bob, ela tem duas informações relevantes: os bits que ela codificou e as bases que foram por ela utilizadas. Imaginemos que cada uma dessas informações esteja armazenada em duas *bitstrings*, uma $a = (a_1, a_2, \ldots, a_n)$ para os bits e outra

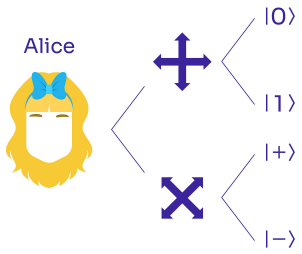

Figura 8: Codificação dos bits em estados quânticos $|0\rangle$, $|1\rangle$, $|+\rangle$ ou $|-\rangle$. Cada bifurcação representa uma escolha aleatória que ela deve fazer, na primeira parte ela escolhe uma base e, dada uma base, ela escolhe o par de estados que codificarão o bit quanticamente.

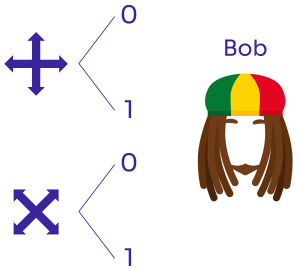

Figura 9: Bob escolhe uma das bases para fazer a medição do estado quântico que Alice envia. Escolhida a base, quando ele mede, obtém um dos dois possíveis resultados, ou o bit 0 ou o bit 1. Aqui, as bifurcações também representam caminhos possíveis para o processo de medição que, naturalmente, sempre culminam em um resultado binário.

$B^{(a)} = (B_1^{(a)}, B_2^{(a)}, \ldots, B_n^{(a)})$ para as bases. De maneira similar, Bob possui as informações de bases que ele usou para a medição $B^{(b)} = (B_1^{(b)}, B_2^{(b)}, \ldots, B_n^{(b)})$ e os bits que ele mediu $b = (b_1, b_2, \ldots, b_n)$.

Na próxima etapa, realizada por meio de um canal de comunicação clássico autenticado, Alice e Bob devem comparar as bases que usaram no procedimento, $B^{(a)}$ e $B^{(b)}$, para verificarem em quais das rodadas elas foram compatíveis. Isso é importante porque eles só terão certeza de que um determinado bit numa i-ésima rodada é igual se as bases nesta rodada foram compatíveis. Sendo assim, Alice e Bob descartam todos os bits correspondentes às bases que não foram compatíveis. A esta etapa damos o nome de *sifting*[9] ou reconciliação de bases. A seguir, mostramos um exemplo de como isso é feito:

a:	0	0	1	0	1	0	1	0	1
$B^{(a)}$:	D	R	D	R	D	R	R	D	R
$B^{(b)}$:	R	R	R	R	D	D	D	D	R
b:	1	0	1	0	1	1	0	0	1
Coincidência?	Não	Sim	Não	Sim	Sim	Não	Não	Sim	Sim

[9] Palavra em inglês para "peneirar".

No exemplo acima, após serem descartados os bits em que as bases foram incompatíveis, teremos a chave bruta de Alice e Bob dada por

$$\begin{aligned} a &= 00101; \\ b &= 00101. \end{aligned} \tag{20}$$

Assumindo que nenhum erro ou outra forma de corrupção da informação ocorreu, e dado que Alice e Bob prepararam e mediram os estados na mesma base, as sequência de bits a e b serão idênticas. A princípio, essa chave já poderia ser usada para cifrar mensagens usando o *one-time pad* ou outras técnicas de cifragem descritas anteriormente.

Até o momento, não levamos em consideração possíveis tentativas de espionagem ou falhas no processo. Como veremos a seguir, utilizando o Quadro 2 como exemplo, uma das grandes vantagens deste protocolo é que, devido à aleatoriedade intrínseca dos sistemas quânticos, qualquer tentativa de espionagem pode ser detectada na análise estatística das rodadas do protocolo.

Quadro 2: Possíveis escolhas de base para Alice, Eva e Bob. Em destaque (linhas 1, 3, 6 e 8) fazem referência às rodadas em que Alice e Bob escolhem as mesmas bases.

	Alice	Eva	Bob
1	D	D	D
2	D	D	R
3	D	R	D
4	D	R	R
5	R	D	D
6	R	D	R
7	R	R	D
8	R	R	R

Como Eva não sabe que base foi escolhida na preparação de Alice, nem pode saber que base Bob vai escolher para sua medição, a melhor estratégia para ela é escolher aleatoriamente uma das duas bases; interceptar o fóton sendo transmitido; medir o fóton na base escolhida; preparar um fóton de acordo com o resultado da medição que ela fez; e enviar esse fóton para Bob.

O Quadro 2 indica todas as possíveis escolhas de base de transmissão e/ou medição de cada uma das partes: Alice, Eva e Bob. As linhas destacadas são aquelas em que Alice e Bob escolheram as mesmas bases (o que estamos chamando de *coincidência*). Na primeira e na última linha, vemos casos em que Eva consegue roubar informação do bit transferido sem ser detectada, isso porque, por acaso, ela também escolheu a mesma base que Alice e Bob. No entanto, nas linhas três e seis da tabela, vemos casos em que, apesar de Alice e Bob escolherem a mesma base entre si, Eva mede o estado quântico em uma base diferente – são casos como estes que possibilitam a detecção de Eva.

Nessa última situação, é possível detectar Eva ao analisarmos a estatística final do experimento. Com

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2025-0373

probabilidade de 50%, Eva escolherá a base errada para medir e preparar o fóton interceptado. E com uma probabilidade de 50% o resultado da medição de Bob vai estar relacionada com um bit diferente do que Alice enviou, mesmo que nesse caso ambos tenham escolhido a mesma base. Sendo assim, se Eva intercepta uma fração f dos fótons, em torno de $f/4$ dos bits da chave final de Alice e Bob diferirão. Para o caso em que Eva manipula o canal qântico em todo o processo, isso representa algo em torno de 25% da chave final. Se Alice e Bob comparam uma substring aleatória dos bits que restaram após o *sifting*, poderão detectar a presença da espiã. Mais detalhes do pós-processamento serão apresentados na Seção 6.1.

5.2. Protocolo E91

Semelhantemente ao protocolo BB84, o nome deste protocolo também deriva de seu principal autor e do ano de sua criação. Desenvolvido por A. Ekert em 1991, ele ficou conhecido como "protocolo E91" [28].

Diferentemente do cenário "prepara e mede", ilustrado na Figura 6, este protocolo fundamenta-se na distribuição de emaranhamento entre Alice e Bob, conforme mostrado na Figura 10. Cada um recebe um subsistema do estado total e realiza uma medição sobre ele. A segurança do protocolo decorre da chamada monogamia do emaranhamento [55, 56] que implica que um estado maximamente emaranhado entre duas partes não pode ter qualquer correlação com uma terceira parte. Quer dizer, se pudermos garantir que Alice e Bob compartilham um estado maximamente emaranhado, temos a garantia que um eventual espião não terá qualquer informação sobre as correlações compartilhadas. Posto de outro forma, qualquer tentativa de Eva de interferir no estado compartilhado perturbaria as correlações entre

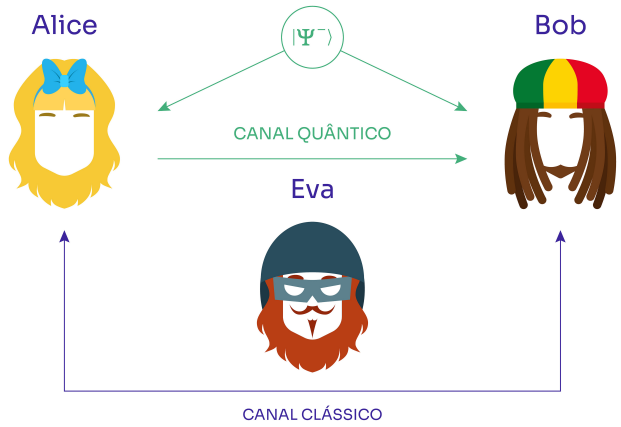

Figura 10: Cenário de comunicação baseado em emaranhamento. O sistema é análogo ao cenário "prepara e mede" (Figura 6), mas com a adição de um estado quântico emaranhado (aqui denotado por $|\Psi^-\rangle$) que se compartilha entre Alice e Bob.

os resultados de Alice e Bob, o que pode ser detectado testando a violação de desigualdades de Bell [57].

Considere, por exemplo, que o estado compartilhado por Alice e Bob seja:

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right), \tag{21}$$

e, dados $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$ e $X = |+\rangle\langle +| - |-\rangle\langle -|$, que seus operadores de medição sejam:

$$A_1 = Z, \quad B_1 = Z,$$
$$A_2 = X, \quad B_2 = \frac{1}{\sqrt{2}}(Z - X),$$
$$A_3 = \frac{1}{\sqrt{2}}(Z + X), \quad B_3 = \frac{1}{\sqrt{2}}(Z + X).$$

Onde A_i correspondem aos operadores de Alice e B_i os de Bob (com $i = 1, 2, 3$).

Nesta situação, a fonte de partículas emaranhadas deverá enviar continuamente estados $|\Psi^-\rangle$ para Alice e Bob, que em cada rodada escolherão de maneira independente e aleatória, uma medição para realizar dentro das três possibilidades $\{A_1, A_2, A_3\}$ e $\{B_1, B_2, B_3\}$, respectivamente. Cada parte obterá como resultado bits 0 e 1, onde usamos a mesma codificação que anteriormente, ou seja, independentemente do observável sendo medido, associamos bit 0 com o autovalor $+1$ e o bit 1 com o autovalor -1.

A fase seguinte envolve comparar os pares de escolhas de medição, de modo análogo à reconciliação de bases do protocolo BB84, porém sem descartar amostras: todas as rodadas em que Alice e Bob registrem configurações compatíveis são aproveitadas, ou para gerar chave ou para estimar a presença de um intruso. Em particular, as medições (A_1, B_1) e (A_3, B_3) apresentam antissimetria (anticorrelação) ideal no protocolo – sempre que Alice obtém 0, Bob obtém 1 (e vice-versa) – de modo que, depois de identificadas essas rodadas, basta que Bob (ou Alice) inverta os bits correspondentes para que ambos disponham de uma sequência de bits compartilhada e aleatória – a chave bruta.

Os demais pares – (A_1, B_3), (A_1, B_2), (A_2, B_3) e (A_2, B_2) – são reservados para a estimação de parâmetro: a partir dos correlatores $\langle A_i B_j\rangle$ calculados nessas configurações constrói-se a combinação de CHSH a partir da Eq. (22) verifica-se a sua violação em relação à cota clássica ($S \leq 2$). Uma violação compatível com a previsão quântica ($2 < S \leq 2\sqrt{2}$) coloca limites quantitativos sobre a informação que Eva poderia ter obtido [58, 59]. O Quadro 3 a seguir resume o papel de cada par de medições no protocolo E91.

Nesta notação, desigualdade CHSH tem a seguinte forma:

$$S \equiv |\,\langle A_1 B_3\rangle + \langle A_1 B_2\rangle + \langle A_2 B_3\rangle - \langle A_2 B_2\rangle\,| \leq 2, \tag{22}$$

onde $\langle A_i B_j\rangle = \frac{1}{N}\sum_r (-1)^{a_r + b_r}$ com a_r o bit obtido por Alice na r-ésima rodada, e similarmente para b_r no

Quadro 3: Resumo dos pares de medições no protocolo E91. Os pares destinados à estimação servem para calcular os correladores $\langle A_i B_j \rangle$ e a combinação linear S pertinente. Se a violação observada for insuficiente, indica-se possível interferência de Eva e procede-se a continuidade ou o cancelamento do protocolo.

Medições	Propriedade	Uso
(A_1, B_1)	Anticorrelação	Geração da chave
(A_3, B_3)	Anticorrelação	Geração da chave
(A_1, B_3)	Correlações experimentais	Estimação (CHSH)
(A_1, B_2)	Correlações experimentais	Estimação (CHSH)
(A_2, B_3)	Correlações experimentais	Estimação (CHSH)
(A_2, B_2)	Correlações experimentais	Estimação (CHSH)

caso de Bob. O valor $S = 2$ representa a cota clássica de um sistema bipartido, ou seja, sempre que $S \leq 2$, significa que Alice e Bob compartilham um estado cujas correlações podem ser explicadas classicamente.

As desigualdades de Bell limitam as correlações clássicas de um determinado estado do sistema, isto é, quando elas são violadas, indicam para nós que as correlações existentes não podem ser explicadas classicamente. Por exemplo, dentro da mecânica quântica, a máxima violação da desigualdade (22) é $S = 2\sqrt{2}$, que é obtida por um estado maximamente emaranhado e por medições não compatíveis, como o estado (21) e medições dadas pelos observáveis A_1, e A_2 de Alice e B_2 e B_3 de Bob. Em termos da QKD, a máxima violação da CHSH significa que Eva não obteve qualquer informação sobre a chave. Se $2 < S < 2\sqrt{2}$, então Eva obteve alguma informação sobre a chave, mas ainda pode ser possível extrair uma chave secreta dos dados compartilhados [60]. Agora se $S \leq 2$, então é impossível gerar uma chave secreta [61].

6. Pós-Processamento

A etapa de transmissão quântica do protocolo QKD, Alice e Bob terão, cada um, uma sequência binária que não necessariamente é uma chave secreta ainda, pois, durante a transmissão pelo canal quântico, os estados quânticos podem ter passado por uma série de interferências, seja problemas no canal, seja ataques de um espião. Desse modo, as sequências obtidas por Alice e Bob são chamadas de chaves brutas, as quais são sequências binárias parcialmente seguras (a espiã pode ter obtido informação sobre a sequência binária enviada por Alice) e parcialmente correlacionadas (as chaves brutas de Alice e Bob não são idênticas). O objetivo do pós-processamento é transformar o par de chaves brutas em um par de chaves idênticas e secretas.

De maneira geral, podemos separar o pós-processamento em três grandes etapas: estimação de parâmetros, correção de erros e amplificação de privacidade, conforme ilustrado na Figura 11. É importante frisar que, nesta seção, discutiremos técnicas matemáticas de manipulação da informação clássica para garantir que a chave final seja simétrica e segura, mas que pouco se relacionam com física quântica. De fato, a parte quântica na Criptografia Quântica se resume a distribuição desta chave bruta e das garantias teóricas sobre sua segurança. O seu pós-processamento é inteiramente clássico.

6.1. Estimação de parâmetros

Após a transmissão pelo canal quântico, Alice e Bob precisam avaliar se o par de chaves brutas pode ser utilizado para gerar uma chave secreta. Essa avaliação é feita verificando se a taxa de chave secreta do protocolo é positiva (Seção 7). A função da taxa de chave secreta pode depender tanto dos parâmetros do canal ou de características das chaves brutas, como a probabilidade de erro de bit, os quais devem ser estimados vazando a menor quantidade possível de informação pelo canal público.

Para realizar a estimação de parâmetros, Alice seleciona de forma aleatória um subconjunto das rodadas em que as duas partes escolheram a mesma base, e comunica publicamente quais foram as rodadas escolhidas bem como os bits que ela quis enviar para Bob nessas rodadas. De posse dessa informação, Bob pode verificar se nas rodadas escolhidas por Alice ele obteve exatamente os bits que ela quis enviar. Desta forma, Alice e Bob podem estimar a taxa de erro de bit da comunicação, ou seja, o número de bits discordantes dividido pelo número de bits comparados. Mais detalhes serão dados na subseção 7.1. Em criptografia, mesmo sabendo que alguns desses erros podem ser por falhas incontroláveis na implementação do protocolo, assumimos sempre o pior cenário possível,

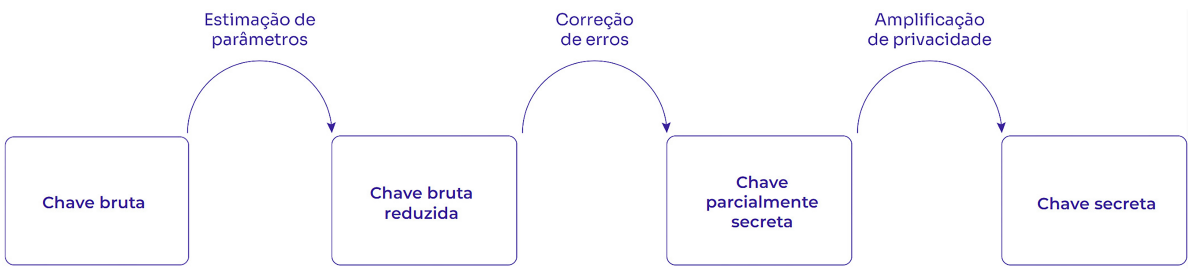

Figura 11: Diagrama das etapas do pós-processamento (sobre as setas) e o estado da chave a cada passo (dentro das caixas). Inicia-se com "Chave bruta", logo após o sifiting e finaliza-se com "Chave secreta".

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2025-0373

ou seja, que esses erros foram causados pela interferência de algum espião.

A depender de quanto for a diferença entre seus dados, Alice e Bob deverão descartar a sequência binária compartilhada, já que, acima de uma certo limiar de erro, não há mais como garantir a segurança da chave. Nesta primeira parte, inspiramo-nos na explicação dada por R. Wolf acerca do assunto em [34].

Nesse contexto, duas perguntas fundamentais surgem: qual fração da chave deve ser comparada? E qual taxa de erro pode ser tolerada antes que o protocolo seja abortado? Ambas podem ser respondidas utilizando o teorema de Serfling [62] sobre somas de amostragens sem reposição. No caso específico da estimação de parâmetros utilizamos o teorema de Serfling, como descrito abaixo, para estabelecer quando as propriedades de um subconjunto aleatório dos dados refletem, dentro de um erro, as propriedades do conjunto total.

Teorema 2 (Teorema de Serfling) *Considere um conjunto $\mathcal{X}$ de tamanho N, cujos elementos são variáveis aleatórias X_i, ou seja, $\mathcal{X} = \{X_1, X_2, \ldots, X_N\}$. Cada variável aleatória X_i assume valores $x_i \in \{0, 1\}$.*

Suponha que selecionemos aleatoriamente uma amostra (sem reposição) de tamanho n de dentro do conjunto $\mathcal{X}$. Essa amostra forma um outro conjunto $\mathcal{Y}_n \subset \mathcal{X}$ de variáveis aleatórias Y_j que assumem valores $y_j \in \{0, 1\}$. Logo, temos que $\mathcal{Y}_n = \{Y_1, Y_2, \ldots, Y_n\}$. A partir disso, define-se as médias:

$$\langle \mathcal{X} \rangle = \frac{1}{N} \sum_{i=1}^{N} X_i,$$

$$\langle \mathcal{Y}_n \rangle = \frac{1}{n} \sum_{i=1}^{n} Y_i.$$

Então, para qualquer $0 \leq \beta \leq 1$, temos que:

$$Pr[\langle \mathcal{Y}_n \rangle \geq \langle \mathcal{X} \rangle + \beta] \leq \exp\left\{ \left(-\frac{2\beta^2 n}{1 - \frac{n-1}{N}} \right) \right\}.$$

Em resumo, o teorema fala que, para um tamanho fixo N do conjunto total, a probabilidade de que a média de uma amostra de tamanho n, $\langle \mathcal{Y}_n \rangle$, seja maior que a média geral, $\langle \mathcal{X} \rangle$, por um valor β, decai exponencialmente com $\beta^2 n$. Ou seja, conforme aumentamos o tamanho do subconjunto selecionado, a probabilidade de uma estimativa ruim para a média do conjunto total se torna muito baixa.

Consideremos agora o problema da estimação de parâmetros em QKD. Neste caso, N é o tamanho da chave bruta compartilhada por Alice e Bob, m é o tamanho da sequência binária selecionada para comparação, e definimos como $n \equiv N - m$ o tamanho da sequência restante. Seja $[N] = \{1, 2, \ldots, N\}$ um conjunto de índices das sequências de tamanho N, podemos construir a sequência para comparação por meio de uma escolha aleatória de um subconjunto $I_{teste} = \{i_1, \cdots, i_m\} \subset [N]$. Dessa forma, as sequências restantes serão formadas através dos índices $I_{chave} = [N] \setminus I_{teste}$. Sendo $K_A^{(N)} = \{a_1, a_2, \cdots, a_N\}$ e $K_B^{(N)} = \{b_1, b_2, \cdots, b_N\}$ as chaves brutas de Alice e Bob antes da estimação de parâmetros, as sequências de teste utilizadas para estimar os parâmetros de interesse serão dadas por $K_A^{(m)} = \{a_{i_1}, \cdots, a_{i_m}\}$ e $K_B^{(m)} = \{b_{i_1}, \cdots, b_{i_m}\}$, com $K_A^{(n)} = K_A^{(N)} \setminus K_A^{(m)}$ e $K_B^{(n)} = K_B^{(N)} \setminus K_B^{(m)}$ sendo as chaves brutas após estimação de parâmetros.

Exemplo 1 *Tome $N = 8$ e $m = 3$. Um possível subconjunto de teste é $I_{teste} = \{3, 5, 8\}$, de modo que $I_{chave} = [N] \setminus I_{teste} = \{1, 2, 4, 6, 7\}$. Dessa forma,*

$$K_A^{(8)} = \{a_1, \cdots, a_8\} \qquad K_B^{(8)} = \{b_1, \cdots, b_8\}$$
$$K_A^{(5)} = \{a_1, a_2, a_4, a_6, a_7\} \qquad K_B^{(5)} = \{b_1, b_2, b_4, b_6, b_7\}$$
$$K_A^{(3)} = \{a_3, a_5, a_8\} \qquad K_B^{(3)} = \{b_3, b_5, b_8\}$$

Em um protocolo de variáveis discretas, como os apresentados na Seção 5, o parâmetro de interesse é a taxa de erro de bit entre as chaves brutas de Alice e Bob, a qual pode ser estimada utilizando uma média amostral:

$$\frac{1}{m} \sum_{i=1}^{m} K_A^{(m)} \oplus K_B^{(m)}. \tag{23}$$

Para utilização na análise do protocolo QKD, se faz necessário estabelecer as condições para as quais a média amostral da Equação 23 resulta em uma estimativa confiável da probabilidade de erro de bit das sequências restantes. Um dos resultados fundamentais da análise estatística de estimadores é que a média amostral converge para o valor real conforme o tamanho da amostra aumenta. Logo, é preciso garantir que a probabilidade de a taxa de erro de bit estimada através das sequências $K_A^{(m)}$ e $K_B^{(m)}$ ser menor do que o parâmetro referente às sequências $K_A^{(n)}$ e $K_B^{(n)}$ seja baixa o suficiente.

Utilizando $\left| K_A^{(n)} \oplus K_B^{(n)} \right| = \sum_{i=1}^{n} K_A^{(n)} \oplus K_B^{(n)}$ para denotar o número de bits incorretos entre duas sequências, podemos definir as taxas de erro como

$$\Lambda_n \equiv \frac{1}{n} \left| K_A^{(n)} \oplus K_B^{(n)} \right|, \tag{24}$$

e

$$\Lambda_m \equiv \frac{1}{m} \left| K_A^{(m)} \oplus K_B^{(m)} \right|. \tag{25}$$

Naturalmente, a taxa de erro total deve ser,

$$\Lambda \equiv \frac{1}{N} \left| K_A \oplus K_B \right|, \tag{26}$$

mas veja que, por construção,

$$\left| K_A \oplus K_B \right| = \left| K_A^{(m)} \oplus K_B^{(m)} \right| + \left| K_A^{(n)} \oplus K_B^{(n)} \right|. \tag{27}$$

Agora lembremos da regra de Bayes que, para dois eventos A e B, pode ser escrita como

$$\Pr(A|B) = \frac{\Pr(B|A)\Pr(A)}{\Pr(B)}. \tag{28}$$

Note que se $\Pr(B|A) \leq 1$, então $\Pr(A|B) \leq \frac{\Pr(A)}{\Pr(B)}$. Assim sendo, ao aplicarmos as Eqs. (24) e (25) na Eq. (28), obtemos que

$$\Pr(\Lambda_n \geq \Lambda_m + \gamma | \Lambda_m \leq \lambda_{\text{máx}}) \leq \frac{\Pr(\Lambda_n \geq \Lambda_m + \gamma)}{\Pr(\Lambda_m \leq \lambda_{\text{máx}})}, \tag{29}$$

onde $\lambda_{\text{máx}}$ é a taxa de erro máxima que um protocolo pode ter e $\Pr(\Lambda_m \leq \lambda_{\text{máx}})$ é, portanto, a probabilidade de que a parte m da bitstring passe pela checagem de erro. Já γ é uma constante pequena em relação aos valores Λ, Λ_n e Λ_m.

Agora basta usarmos o Teorema 2 para reescrevermos o numerador da fração na Eq. (30) como

$$\Pr(\Lambda_n \geq \Lambda_m + \gamma | \Lambda_m \leq \lambda_{\text{máx}}) \leq \frac{\exp\left(-\frac{2m^2 n\gamma^2}{(m+1)N}\right)}{\Pr(\Lambda_m \leq \lambda_{\text{máx}})}. \tag{30}$$

Dessa forma, a Eq. (30) estabelece um limite superior para a probabilidade de que a taxa de erro na parte não verificada da chave (Λ_n) seja maior do que a taxa de erro observada na amostra (Λ_m) acrescida de um pequeno fator γ. Isso é essencial no contexto da estimação de parâmetros na QKD, pois Alice e Bob não podem comparar toda a chave bruta, apenas uma fração dela.

O resultado mostra que a probabilidade de erro decai exponencialmente com o tamanho da amostra m, permitindo que Alice e Bob estimem a segurança da chave total sem comprometer muitos bits. Se a taxa de erro (Λ_m) estiver abaixo de $\lambda_{\text{máx}}$, o protocolo segue para a correção de erros; caso contrário, a chave é descartada. Estas taxas de erro serão discutidas com mais detalhes na Seção 7, quando discutiremos taxa de chave e taxa de erro quântico.

6.2. Reconciliação da informação

Passada a estimação de parâmetros, Alice e Bob compartilham sequências binárias contendo alguns erros (em algumas posições das sequências, $a_i \neq b_i$), sendo a probabilidade de erro de bit o parâmetro estimado. Agora, o objetivo do protocolo QKD é fazer com que as sequências de Alice e Bob sejam idênticas, o qual pode ser alcançado com a utilização de algum protocolo de correção de erros. Uma vez que o objetivo de um protocolo QKD é gerar uma chave final aleatória, não há diferença operacional (ou teórica) se a correção de erros seja realizada no "sentido direto" (a sequência de Bob é corrigida) ou no "sentido reverso" (a sequência de Alice é corrigida). Por esse motivo, é dito que as chaves brutas são *reconciliadas*, tarefa essa realizada por protocolos de reconciliação da informação.

Para corrigir as sequências, Alice e Bob precisam divulgar publicamente alguma informação para possibilitar que o erros sejam corrigidos. Dessa maneira, diferentes métodos de correção de erros permitem realizar a reconciliação de informação, de modo que um protocolo QKD pode utilizar diferentes protocolos de reconciliação. Após a correção de erros, Alice e Bob precisam verificar que as sequências resultantes são idênticas, resultando em uma etapa de verificação.

6.2.1. Correção de erros

A correção de erros é um dos temas centrais da teoria da informação. Em seu artigo seminal, Shannon apresentou quais os limites fundamentais para transmissão confiável de informação por um canal ruidoso de comunicação, os quais podem ser operacionalmente alcançados através da utilização de códigos corretores de erros. Dessa forma, o tópico de correção de erros se tornou um campo de pesquisa com mérito próprio, encontrando aplicações em sistemas de transmissão e armazenamento da informação [63, 64].

Um dos modelos de canal mais utilizados na análise de sistemas de comunicação é o canal binário simétrico com parâmetro p, denotado por BSC(p), conforme apresentado na Figura 12. Nesse modelo de canal, os símbolos binários de entrada são transmitidos sem alteração com probabilidade $1-p$ ou invertidos com probabilidade p.

A utilização de códigos corretores de erro atuam sobre a chave bruta (vide Figura 11) como parte do protocolo de reconciliação em sistemas QKD é possível uma vez que o par de sequências $K_A^{(n)}$ e $K_B^{(n)}$ pode ser interpretado como o resultado da transmissão de $K_A^{(n)}$ por um canal BSC(p). Dessa maneira, o limite inferior da quantidade de informação divulgada pelas *mensagens de reconciliação* é dado pelos resultados da teoria da informação, mais especificamente o Teorema de Slepian-Wolf [65] para codificação de fontes correlacionadas, enquanto a operacionalização da reconciliação pode ser realizada utilizando códigos corretores de erro que atendem às restrições do limite fundamental.

No desenvolvimento dos sistemas de distribuição quântica de chaves, as primeiras aplicações de reconciliação de informação não utilizavam códigos corretores, mas esquemas iterativos que permitiam verificar a existência de um erro binário e corrigí-lo. Esquemas notáveis são os protocolo *Binary* e o *CASCADE* [66],

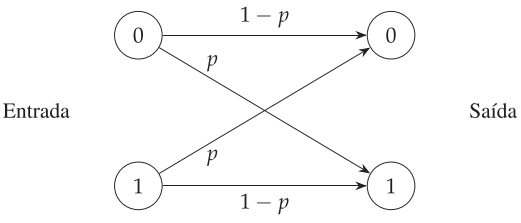

Figura 12: Modelo de um canal BSC(p).

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2025-0373

os quais utilizam estratégias de particionamento das chaves brutas e verificação das partições para encontrar as posições que apresentam erros. Apesar de não apresentar estruturas formais de códigos corretores de erros, protocolos iterativos como o CASCADE podem realizar a correção de erros de maneira eficiente enquanto apresenta baixa complexidade computacional.

Para fins didáticos, mostraremos o funcionamento de um algoritmo básico usando portas XOR. Lembremos que, para bits, a porta XOR funciona como soma módulo dois: se os bits forem iguais o resultado é 0, se diferentes, 1.

O algoritmo funciona da seguinte forma, considere $K_A = (a_1, a_2, \ldots, a_n)$ como sendo a chave de Alice e $K_B = (b_1, b_2, \ldots, b_n)$ a chave de Bob. As etapas são as seguintes:

(I) Alice escolhe dois bits de sua chave, digamos a_i e a_{i+1};
(II) Ela calcula $XOR(a_i, a_{i+1})$;
(III) Alice envia para Bob a posição dos bits, quer dizer, i e $i+1$, bem como o valor de $XOR(a_i, a_{i+1})$;
(IV) Bob seleciona b_i e b_{i+1} e calcula $XOR(b_i, b_{i+1})$;
(V) Ele compara $XOR(a_i, a_{i+1})$ com $XOR(b_i, b_{i+1})$:
  - Se $XOR(a_i, a_{i+1}) = XOR(b_i, b_{i+1})$, Alice e Bob mantém a_i e b_i e descartam a_{i+1} e b_{i+1};
  - Se $XOR(a_i, a_{i+1}) \neq XOR(b_i, b_{i+1})$, Alice e Bob descartam ambos os bits.

Mesmo que Eva intercepte os resultados das operações XOR, ela não consegue recuperar informação alguma sobre a chave, pois a operação XOR é irreversível (vide Tabela 1). O descarte dos bits é feito no intuito de eliminar ao máximo os bits discordantes entre Alice e Bob.

Nas duas primeiras linhas da Tabela 2, vemos casos de correção bem-sucedida: na primeira linha não há erro e na segunda o erro está no segundo bit. A terceira linha mostra descarte equivocado (pois descarta-se o ambos os bits, quando se deveria descartar apenas o primeiro) e a quarta um falso positivo (pois o algoritmo manda descartar apenas o segundo bit, quando se deveria descartar os dois). A seguir mostramos um exemplo simples de execução deste algoritmo.

$$
\begin{aligned}
a^{(inicial)} &= \underline{\mathbf{01}}0111100 \\
b^{(inicial)} &= \underline{\mathbf{01}}0101111 \\
&\downarrow \\
a &= 00\underline{\mathbf{11}}1100 \\
b &= 00\underline{\mathbf{10}}1111 \\
&\downarrow \\
a &= 0011\underline{\mathbf{00}} \\
b &= 0011\underline{\mathbf{11}} \\
&\downarrow \\
a^{(final)} &= 00110 \\
b^{(final)} &= 00111
\end{aligned}
$$

Seguindo essa lógica, vemos que este algoritmo requer iterações múltiplas – a cada execução, cerca de metade dos bits pode ser descartada. Não há garantia de correção completa em uma única rodada, mas múltiplas iterações melhoram progressivamente a precisão, à custa de eficiência[10].

Quando comparamos $\{a^{(inicial)}, b^{(inicial)}\}$ com $\{a^{(final)}, b^{(final)}\}$, vemos que a quantidade de bits diferentes entre as chaves caiu de três para um, mas a custo de descartar quase metade da chave. Por isso, frisamos que este tipo de técnica usando portas XOR não é utilizada em implementações práticas justamente pela sua ineficiência. Protocolos reais, como CASCADE ou LDPC, corrigem erros ativamente (via paridades e busca binária) e minimizam o vazamento de informação, ao contrário deste método baseado em descarte puro.

Tabela 1: Tabela verdade da porta XOR.

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Tabela 2: Comparação entre bitstrings a e b na etapa de correção de erros.

Bitstrings	Equivalência entre XOR
$a = 01\underline{\mathbf{01}}11100$ $b = 01\underline{\mathbf{01}}01111$	$XOR(0,1) = XOR(0,1)$
$a = 010\underline{\mathbf{11}}1100$ $b = 010\underline{\mathbf{10}}1111$	$XOR(1,1) \neq XOR(1,0)$
$a = 0101\underline{\mathbf{11}}100$ $b = 0101\underline{\mathbf{01}}111$	$XOR(1,1) \neq XOR(0,1)$
$a = 0101111\underline{\mathbf{00}}$ $b = 0101011\underline{\mathbf{11}}$	$XOR(0,0) = XOR(1,1)$

6.2.2. Verificação

Após a reconciliação, Alice e Bob verificam a igualdade das chaves usando funções hash dois-universais:

Definição 1 (Funções hash dois-universais) *Seja $\mathcal{F}$ uma família de funções de um alfabeto $\mathcal{X}$ para um alfabeto $\mathcal{Z}$ e seja p_F a distribuição de probabilidade em $\mathcal{F}$. O par $(\mathcal{F}, p_F)$ é chamado dois-universal se:*

$$Pr[f(x) = f(x')] \leq \frac{1}{|\mathcal{Z}|},$$

para qualquer x,$x' \in \mathcal{X}$ com $x \neq x'$ e f escolhida aleatoriamente de $\mathcal{F}$ de acordo com p_F.

[10] Perceba que, neste exemplo, utilizamos a leitura dos bits de maneira sequencial: a_i e a_{i+1}. Mas, em princípio, ela poderia ser qualquer: a_i e a_j com $i \neq j$.

Dada esta definição[11], considere $\mathcal{X}$ o conjunto de possíveis chaves, particularmente K_A, $K_B \in \mathcal{X}$. Sendo $f \in \mathcal{F}$, a probabilidade de que as imagens $f(K_A)$ e $f(K_B)$ sejam iguais, dado que as chaves são diferentes, é limitada pelo tamanho do conjunto das imagens $|\mathcal{Z}|$, uma vez que que $f(x) \in \mathcal{Z}$. Ou seja, se escolhermos uma família de funções apropriada, podemos escolher $|\mathcal{Z}|$ grande para que o erro seja pequeno.

A partir disso, Alice e Bob seguem o seguinte algoritmo para fazer a verificação de funcionamento da correção de erros:

(I) Alice escolhe $f \in \mathcal{F}$;
(II) Ela computa $f(K_A)$;
(III) Alice envia para Bob f e $f(K_A)$;
(IV) Bob avalia sua *bitstring* com f computando $f(K_B)$;
(V) Bob compara $f(K_A)$ e $f(K_B)$:
- Se $f(K_A) = f(K_B)$, quer dizer que existe uma alta probabilidade de as chaves deles serem iguais;
- Se $f(K_A) \neq f(K_B)$, eles abortam o protocolo.

Para protocolos de correção de erros probabilísticos como o exemplo apresentado, introduzimos um parâmetro de segurança ϵ_{cor} que quantifica a máxima probabilidade tolerada de chaves distintas após uma verificação bem-sucedida. Definimos que o protocolo é ϵ-correto se:

$$\Pr[K_A \neq K_B \mid f(K_A) = f(K_B)] \leq \epsilon_{\text{cor}}. \tag{31}$$

Na implementação prática, Alice e Bob selecionam funções hash dois-universais com tamanho de saída $|\mathcal{Z}| = \lceil 1/\epsilon_{\text{cor}} \rceil$. Pela propriedade fundamental dessas funções:

$$\Pr[f(K_A) = f(K_B) \mid K_A \neq K_B] \leq \frac{1}{|\mathcal{Z}|}.$$

A probabilidade condicional desejada é então limitada por:

$$\begin{aligned} &\Pr[K_A \neq K_B \mid f(K_A) = f(K_B)] && (32)\\ &\leq \frac{\Pr[f(K_A) = f(K_B) \mid K_A \neq K_B]}{\Pr[f(K_A) = f(K_B)]} && (33)\\ &\leq \frac{1}{|\mathcal{Z}|} && (34)\\ &\leq \epsilon_{\text{cor}}, && (35) \end{aligned}$$

onde utilizamos que[12]: $\Pr[f(K_A) = f(K_B)] \geq \Pr[K_A = K_B]$. Esta escolha de $|\mathcal{Z}|$ garante diretamente que o protocolo é ϵ-correto.

Essa parte do pós-processamento nos garante portanto a corretude do protocolo, mas ainda não garante o seu sigilo.

6.3. Amplificação de privacidade

A amplificação de privacidade é a última etapa do pós-processamento e funciona como um último filtro que "purifica" a chave. Alice e Bob precisam completar uma última etapa do protocolo: eliminar qualquer informação que Eva, a espiã, possa ter sobre a chave. Para isso, eles utilizam os chamados "extratores de aleatoriedade". Esses extratores são funções que recebem como entrada uma fonte de aleatoriedade[13] e uma pequena sequência de números aleatórios, chamada semente[14].

O objetivo aqui é gerar uma nova sequência que seja amostrada de uma distribuição quase uniforme das *bitstrings*, que seja aproximadamente descorrelacionada com qualquer outra variável aleatória, e que seja maior que a semente original. Concretamente:

- $X \in \{0,1\}^n$ é uma variável aleatória de entrada;
- $S \in \{0,1\}^m$, com $m < n$, é a semente, uma pequena sequência de números aleatórios;
- $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^l$, é uma função extratora de aleatoriedade se $Z = f(X,S)$ é uma variável aleatória com distribuição aproximadamente uniforme sobre as *bitstrings* de tamanho l, e aproximadamente independente de S.

No nosso contexto, Alice amostra uma semente s, e envia publicamente para Bob. Alice então calcula $f(K_A, s)$, enquanto Bob calcula $f(K_B, s)$. Como já sabemos que com alta probabilidade $K_A = K_B$, então, com alta probabilidade $f(K_A, s) = f(K_B, s)$, e $z = f(K_A, s)$ vai ser a chave final. Note que pelas propriedades da função extratora de aleatoriedade, z é praticamente independente de s e de qualquer outra variável aleatória, ou seja, mesmo sabendo s Eva não tem qualquer informação sobre z.

Nos resta saber como determinar a função f. Note que ao fim da amplificação de privacidade, a chave final deve ser aproximadamente descorrelacionada de qualquer informação que Eva possa ter, ainda que ela tenha acesso a recursos quânticos. Felizmente pode ser mostrado que as funções dois-universais da Definição 1 satisfazem todas as propriedades desejadas. A semente aleatória de Alice então serve para determinar qual função de $\mathcal{F}$ será escolhida; essa escolha é comunicada a Bob; os dois aplicam a função em suas chaves corrigidas e já verificadas para obter a chave segura final.

É nesta parte do pós-processamento que garantimos a segurança do protocolo.

[11] Exemplo de família dois-universal: família afim modular. Seja p primo e $\mathcal{X} = \mathcal{Z} = \mathbb{F}_p$. Defina $\mathcal{F} = \{f_{a,b} : x \mapsto ax + b \bmod p \mid a, b \in \mathbb{F}_p\}$ com $f_{a,b}$ escolhido uniformemente. Para $x \neq x'$,

$$f_{a,b}(x) = f_{a,b}(x') \iff a(x - x') \equiv 0 \pmod{p}.$$

Como $x - x' \not\equiv 0$, isso só ocorre se $a = 0$. Logo $\Pr[f(x) = f(x')] = \Pr[a = 0] = 1/p = 1/|\mathcal{Z}|$, satisfazendo a definição de dois-universalidade.

[12] Esta desigualdade é válida, pois todo evento em que $K_A = K_B$ implica necessariamente $f(K_A) = f(K_B)$

[13] O nome "fonte de aleatoriedade" se deve ao fato de essa string possuir algum nível de entropia, ou seja, é uma variável estocástica.

[14] A "semente" é uma pequena sequência de números aleatórios adicionais que é usada como insumo pelo extrator de aleatoriedade para gerar uma saída final (quase) perfeitamente aleatória.

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2025-0373

7. Análise de Segurança

Dado um protocolo (incluindo sua realização e o pós-processamento), podemos nos perguntar qual o nível de segurança que ele nos oferece. No contexto de QKD, alguns parâmetros são centrais: taxa de erro quântico ("Quantum Bit Error Rate", QBER) e taxa de chave secreta.

7.1. Taxa de erro quântico (QBER)

A *QBER* mede a discrepância entre as chaves de Alice e Bob antes do pós-processamento na parte de estimação de parâmetros, ou seja, quando já foram descartadas todas as rodadas onde Bob mediu em uma base diferente da que Alice usou para preparar seu qubit. O QBER, portanto, revela não apenas erros experimentais, mas também possíveis interferências de Eva, sendo definido como

$$QBER = \frac{\text{Número de bits discordantes}}{\text{Número total de bits comparados}}. \quad (36)$$

A QBER surge de três fontes principais: ruídos do canal (perdas ópticas, dispersão, ou imperfeições nos detectores); imperfeições na implementação (bases mal alinhadas, lasers não ideais, etc) e ataques de Eva. Por exemplo, no BB84, quando Eva intercepta e mede um fóton sendo transmitido e prepara um outro de acordo com o resultado de sua medição, com probabilidade de 25% ela induzirá um bit na chave de Bob que vai ser diferente do de Alice mesmo quando esses usaram a mesma base. Sendo assim, a *QBER* funciona como uma espécie de termômetro de segurança ao final da QKD.

7.2. Taxa de chave secreta (R)

Esta quantidade avalia quantos bits secretos podem ser gerados por unidade de tempo (ou por pulso) enquanto mantém a segurança contra ataques. Algebricamente,

$$R = \frac{|k|}{|K_A|}, \quad (37)$$

onde $|k|$ é o número de bits secretos finais após pós-processamento e $|K_A|$ é o tamanho da chave bruta de Alice. Em teoria de informação, a taxa de chave secreta assintótica pode ser definida formalmente como o total de correlação entre as chaves de Alice e Bob, menos a correlação entre a chave de Alice e de uma hipotética Eva. Essa relação é conhecida como a taxa de Devetak-Winter [67], a qual pode ser obtida para cada protocolo. Mesmo sem entrar em detalhes, para o BB84 essa relação estabelece que a taxa (assintótica) de bits seguros por rodada é dada por

$$R_{\text{BB84}} \geq 1 - h(\text{QBER}_Z) - h(\text{QBER}_X); \quad (38)$$

onde QBER_Z e QBER_X, são, respectivamente, a taxa de erro quântico quando Alice e Bob escolhem a base Z ou X, e $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ é a entropia de Shannon binária. Note que se as taxas de erro são tais que $\text{QBER}_Z = \text{QBER}_X = 11\%$ (correspondendo a $h(\text{QBER}_Z) \approx 0.5 = h(\text{QBER}_X) \approx 0.5$) a taxa de bits seguros é aproximadamente zero, ou seja, não podemos garantir a segurança do protocolo e o mesmo deve ser abortado. Esse valor crítico de QBER depende de protocolo para protocolo, e para o E91 por exemplo é de aproximadamente 14.6% [61].

7.3. Tipos de ataque

Formalmente, podemos modelar um ataque quântico de Eva como o procedimento em que um sistema preparado por Eva no estado conhecido $|E\rangle\langle E|$ interage com o(s) sistema(s) que Alice envia a Bob, cujo estado é ϱ_A. A interação mais geral possível pode ser descrita por uma unitária U atuando no sistema composto. Após a interação, o(s) sistema(s) de Alice seguem para Bob, enquanto Eva tem acesso ao seu sistema quântico que é então descrito por:

$$\varrho_E = \text{Tr}_\text{A}\left(U^\dagger \varrho_A \otimes |E\rangle\langle E| U\right). \quad (39)$$

A interação pode gerar alguma correlação entre o(s) sistema(s) sendo compartilhado por Alice e Bob com o sistema de Eva. Medindo o seu sistema Eva pode então tentar obter alguma informação sobre a chave que está sendo estabelecida.

Existem pelo menos três maneiras distintas de Eva realizar seu ataque. A primeira são os ataques individuais nos quais Eva interage com cada qubit enviado por Alice de forma independente, sem criar correlações quânticas entre eles, e realiza medições individuais em cada interceptação. Neste caso a medição de Eva não depende da informação clássica trocada por Alice e Bob, sendo realizada antes das etapas de reconciliação da informação e amplificação de privacidade. Por exemplo, no ataque interceptar-e-reenviar (ilustrado no protocolo BB84 na Seção 5), Eva mede cada qubit em uma base aleatória, prepara um novo estado de acordo com sua medição, e o envia a Bob. Esse método é simples de de implementar, mas introduz erros facilmente detectáveis: se Eva escolher a base errada para medir, o estado reenviado não coincidirá com o original enviado por Alice, aumentando o QBER.

Nos chamados ataques coletivos, Eva interage com cada qubit individualmente, mas armazena seus estados quânticos para medição conjunta posterior às etapas de reconciliação e amplificação de privacidade. Isso traz a necessidade de Eva ter posse de uma memória quântica (um dispositivo que armazene estados quânticos sem perda de coerência). Tal procedimento permite extrair mais informação que em ataques individuais, mas sem criar emaranhamento entre os qubits ou correlações entre as diferentes rodadas do protocolo.

Os ataques coerentes são os mais gerais e garantir segurança contra esse tipo de ataque representa o nível

mais alto de segurança. Em tais ataques coerentes, Eva usa uma operação unitária global que pode emaranhar todos os qubits sendo enviados de Alice para Bob com o sistema em posse de Eva. Além disso, neste cenário também assumimos que Eva pode ter uma memória quântica e que pode fazer medições em seu sistema após o pós-processamento clássico. Protocolos seguros contra ataques coerentes são considerados universalmente seguros, pois descrevem a estratégia mais geral que Eva pode usar. A análise de tais cenários, i.e., provar a segurança de protocolo contra tais ataques, pode ser bastante difícil.

No entanto, pode-se mostrar que no limite assintótico de sinais sendo enviados de Alice para Bob, ataques coerentes são equivalentes a ataques coletivos [68]. É dentro dessa hipótese que a taxa de chave segura, Eq. (38) foi obtida. Portanto, o protocolo BB84 é seguro, no limite assintótico, contra quaisquer ataques que Eva possa fazer, mesmo que ela tenha acesso a memórias e computadores quânticos. Versões para estatística finita, sem a hipótese assintótica também podem ser mostradas [52], porém vão muito além do escopo desse trabalho.

Vale ressaltar ainda os *side-channel attacks*, que são ataques que exploram graus de liberdade físicos não considerados em protocolos ideais e cuja análise depede da implementação experimental. Várias das terminologias utilizadas aqui já estão incorporadas em publicações de normatização, como as do *European Telecommunications Standards Institute* (ETSI), que podem ser encontradas no repositório [69].

8. Técnicas Modernas em Distribuição Quântica de Chaves

8.1. CV-QKD

Entre as abordagens modernas em distribuição quântica de chaves, os protocolos baseados em variáveis contínuas (*Continuous-Variable Quantum Key Distribution*, CV-QKD) se destacam por sua capacidade natural de atingir altas taxas de geração de chaves seguras e compatibilidade com tecnologias ópticas já amplamente utilizadas em sistemas clássicos de comunicação [70–72]. Demonstrações recentes reportam avanços expressivos, como taxas de chaves da ordem de Gbps (Mbps) para distâncias da ordem de 10 km (100 km) [73–75], e coexistência do sinal quântico de CV-QKD com sinais clássicos para distâncias acima de 120 km por fibra optica [76]. Tais avanços são possíveis porque, tanto nos protocolos CV-QKD quanto na comunicação óptica coerente, a informação é codificada em propriedades do campo eletromagnético da luz que variam de forma contínua, como a amplitude e a fase. Dessa forma, protocolos de CV-QKD podem ser implementados utilizando equipamentos comerciais de telecomunicação óptica convencional, como lasers e receptores coerentes, sem a necessidade do uso de fontes ou detectores de fótons únicos – fundamentais para sistemas QKD com variáveis discretas (*Discrete-Variable Quantum Key Distribution*, DV-QKD). Por essa razão, sistemas CV-QKD também podem ser totalmente integrados em chips fotônicos [75], o que abre a possibilidade da construção de sistemas mais compactos, em larga escala e de baixo custo.

Apesar de suas diversas vantagens promissoras, os sistemas CV-QKD também apresentam desafios significativos em sua implementação prática. Enquanto na comunicação clássica utilizam-se sinais ópticos intensos (com muitos fótons), nos sistemas CV-QKD é necessário empregar sinais muito fracos (muitas vezes com menos de um fóton por pulso) para garantir que a informação seja protegida pela natureza quântica da luz. Essa característica torna o sistema substancialmente mais sensível a imprecisões e ruídos, limitando as distâncias viáveis de comunicação e impondo maior complexidade às etapas de pós-processamento clássico – que demandam algoritmos sofisticados e alto poder computacional [77–79]. Do ponto de vista teórico, os sistemas CV-QKD também enfrentam desafios adicionais comparados aos sistemas DV-QKD, como maior dificuldade nas provas de segurança e complexidade ampliada na modelagem de canais e dispositivos. Muitas dessas dificuldades decorrem da dimensionalidade infinita do espaço de Hilbert nesses sistemas, o que, por exemplo, inviabiliza a aplicação direta de técnicas utilizadas em DV-QKD [51, 80].

Assim como nos protocolos DV-QKD, os protocolos CV-QKD consistem em duas fases: uma quântica e outra clássica. A fase quântica compreende a preparação, transmissão e detecção de estados quânticos não-ortogonais da luz, permitindo que Alice e Bob gerem uma chave bruta (assimétrica e insegura). Na fase clássica de pós-processamento, Alice e Bob realizam as etapas de estimação de parâmetros, reconciliação da informação e amplificação de privacidade, resultando em uma chave simétrica e segura. Uma descrição detalhada da teoria de CV-QKD excede o escopo deste tutorial, mas apresentamos sua ideia básica e conceitos fundamentais de óptica quântica essenciais para sua compreensão. Mais detalhes sobre CV-QKD podem ser encontrados, por exemplo, em [51, 71, 80, 81] e sobre óptica quântica em [82–85]. Por simplicidade, discutiremos sucintamente o cenário típico de protocolos "prepara e mede" (P&M) CV-QKD para dispositivos confiáveis, embora também existam protocolos independentes do dispositivo de medição (*Measurement-Device Independent*, MDI-CV-QKD), propostos pela primeira vez em 2015 [86]. A independência de dispositivos será discutida detalhadamente na Seção 8.2.

8.1.1. Conceitos básicos de óptica quântica

Na quantização do campo eletromagnético [82], a amplitude complexa do campo clássico passa a ser descrita por operadores não-hermitianos associados à criação e aniquilação de fótons, de forma análoga à criação e aniquilação de quanta de energia em um oscilador harmônico quântico. Considera-se como sistema mais simples

um único modo do campo de radiação quantizado (com vetor de onda $\vec{k}$, frequência ω e polarização $\vec{\epsilon}$), que pode ser descrito, tal como um oscilador harmônico quântico, pelo hamiltoniano $\hat{H} = \hbar\omega(\hat{a}^\dagger\hat{a} + 1/2)$. Neste, $\hat{a}$ e $\hat{a}^\dagger$ são respectivamente os operadores de aniquilação e criação de fótons nesse modo, os quais satisfazem a relação de comutação bosônica $[\hat{a},\, \hat{a}^\dagger] = \hat{\mathbb{1}}$. Consequentemente, os autoestados de $\hat{H}$ coincidem com os autoestados do operador número $\hat{n} = \hat{a}^\dagger\hat{a}$, definidos por:

$$\hat{n}\,|n\rangle = n\,|n\rangle\,, \tag{40}$$

onde os autovalores n são inteiros não-negativos ($n = 0, 1, 2, \ldots \infty$). Os estados número (ou de Fock) $\{|n\rangle\}$, formam uma base ortonormal no espaço de Hilbert, na qual fica clara a ação dos operadores de aniquilação e criação de fótons

$$\hat{a}\,|n\rangle \;=\; \sqrt{n}\,|n-1\rangle\,, \tag{41}$$

$$\hat{a}^\dagger\,|n\rangle \;=\; \sqrt{n+1}\,|n+1\rangle\,. \tag{42}$$

Tipicamente, na maioria dos protocolos "prepara e mede" (P&M) CV-QKD, Alice prepara aleatoriamente estados coerentes do campo eletromagnético utilizando um laser estabilizado e um modulador de amplitude e fase (ou, equivalentemente, de quadraturas). Esses estados não apenas descrevem com precisão o estado quântico de um laser ideal, como também possuem grande relevância em óptica quântica, sendo amplamente empregados em diversas técnicas de análise e descrição do campo eletromagnético [82–85]. Os estados coerentes são definidos como os autoestados (à direita) do operador de aniquilação $\hat{a}$:

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,, \tag{43}$$

onde os autovalores $\alpha \in \mathbb{C}$ são contínuos e os autoestados $|\alpha\rangle$ podem ser escritos na base de Fock como

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle. \tag{44}$$

Dessa forma, é possível observar que estados coerentes não têm um número de fótons bem definido, mas que flutua em torno do valor médio $\langle n\rangle \equiv \langle\alpha|\hat{a}^\dagger\hat{a}\,|\alpha\rangle = |\alpha|^2$ de acordo com a distribuição de Poisson

$$P(n) = |\langle n|\alpha\rangle|^2 = e^{-\langle n\rangle}\,\frac{\langle n\rangle^n}{n!}, \tag{45}$$

cuja variância $\Delta\hat{n} = \langle n\rangle$ dá origem ao chamado "ruído balístico" (shot noise, em inglês), característico de partículas independentes.

Estados coerentes são os estados quânticos que mais se aproximam de uma onda eletromagnética clássica monocromática (como um laser operando muito acima do limiar), apresentando amplitude e fase mais bem definidas do que os estados número (cuja fase é completamente aleatória). Essa propriedade decorre do fato de que, para um estado coerente, a incerteza conjunta nas medidas de amplitude e fase – ou, mais precisamente, nas medidas das quadraturas do campo eletromagnético – atinge o valor mínimo permitido pelo princípio da incerteza de Heisenberg [83]. As quadraturas $\hat{q}$ e $\hat{p}$ do campo correspondem a variáveis conjugadas associadas às partes real e imaginária dos operadores de criação e aniquilação de fótons, sendo matematicamente análogas aos operadores hermitianos de posição e momento de um oscilador harmônico. Elas são definidas por

$$\hat{q} \;=\; \sqrt{\frac{\hbar}{2\omega}}(\hat{a} + \hat{a}^\dagger), \tag{46}$$

$$\hat{p} \;=\; -i\sqrt{\frac{\hbar\omega}{2}}(\hat{a} - \hat{a}^\dagger). \tag{47}$$

As quadraturas $\hat{q}$ e $\hat{p}$ satisfazem a regra de comutação canônica $[\hat{q}, \hat{p}] = i\hbar$ e, por conseguinte, o produto de suas respectivas variâncias, $\Delta\hat{q}^2$ e $\Delta\hat{p}^2$, são limitados inferiormente de acordo com o princípio de Heisenberg, dado pela relação de incerteza

$$\Delta\hat{q}^2\Delta\hat{p}^2 \geq \frac{\hbar^2}{4}. \tag{48}$$

Para qualquer estado coerente, pode-se mostrar que $\Delta\hat{q}^2 = \Delta\hat{p}^2 = \hbar/2$, resultando na relação de incerteza mínima. Dessa forma, a natureza quântica da luz pode ser observada não apenas nas flutuações do número de fótons, mas também no ruído das quadraturas. É importante ressaltar, que é possível comprimir a incerteza de uma das quadraturas de um estado coerente para valores menores que $\hbar/2$, desde que a incerteza da outra quadratura aumente, conforme a Eq. (48). Esses estados são denominados de estados comprimidos [82–85]. A medição da quadratura $\hat{x}$ (ou de $\hat{p}$) pode ser realizada diretamente por meio de uma detecção homódina [85]. Ambas as quadraturas podem ser medidas simultâneamente por uma detecção homódina dupla, uma combinação de duas detecções homódinas (uma para cada quadratura), também comumente chamada na literatura de CV-QKD de detecção heteródina [81].

8.1.2. Protocolos P&M CV-QKD

O primeiro protocolo CV-QKD foi proposto em 1999 por Timothy C. Ralph [87], em que o transmissor codifica bits de informação (aleatórios) em quatro deslocamentos discretos das quadraturas de feixes de dois modos comprimidos e emaranhados, enquanto o receptor emprega detecção homódina para medir aleatoriamente uma das quadraturas dos feixes incidentes. A partir de então, outros protocolos foram propostos [88–91]. Dentre eles, o de Cerf *et al.* [90] se destaca por ter sido o primeiro a utilizar uma modulação contínua dos estados quânticos do campo eletromagnético, produzindo, assim, variáveis aleatórias contínuas. Sua ideia central foi codificar uma chave aleatória gaussiana no valor médio de uma das

duas quadraturas de um estado comprimido de um modo.

Pouco depois, em 2002, Frédéric Grosshans e Philippe Grangier propuseram um protocolo QKD baseado na modulação das amplitudes das quadraturas de estados coerentes de um modo, com o receptor realizando detecção homódina (com escolha aleatória da quadratura detectada) [92]. Essa abordagem garantiu maior praticidade experimental e a possibilidade de emprego de dispositivos comerciais de telecomunicações ópticas. Por essa razão, o protocolo GG02, como ficou conhecido, tornou-se a base para o desenvolvimento teórico e experimental subsequente dos protocolos CV-QKD.

Posteriormente, em 2004, um protocolo análogo ao GG02 foi proposto mas aplicando um esquema de detecção heteródina [93]. A mudança no esquema de detecção permite medir simultaneamente as duas quadraturas do campo eletromagnético, removendo a necessidade de escolha aleatória da quadratura medida pela detecção homódina, motivo pelo qual ficou conhecido como o protocolo *no-switching*. Notavelmente, os protocolos GG02 e *no-switching* compõem a classe de protocolos de estados coerentes com modulação gaussiana (*Gaussian Modulated Coherent States*, GMCS).

As implementações de sistemas CV-QKD ficaram mais próximas dos sistemas convencionais de comunicações ópticas com a proposta de protocolos CV utilizando modulações discretas, ou seja, modulando as quadraturas do campo eletromagnético de acordo com um conjunto finito de fases e amplitudes (conhecido como constelação, no jargão das telecomunicações) [94–99]. Os esquemas de modulação discreta são amplamente utilizados nos sistemas modernos de comunicação digital, estando presentes nos padrões de comunicações móveis, televisão digital, entre outros. O uso dessa estratégia em CV-QKD foi motivada em grande parte pela possibilidade de redução da complexidade do algoritmo de reconciliação de informação, o qual tem sido o gargalo dos protocolos GMCS [71, 79].

Os desenvolvimentos teóricos dos protocolos CV compreendem, em grande parte, aos avanços nas provas de segurança dos esquemas propostos. Marcos notáveis são: (*i*) o teorema da extremalidade de estados gaussianos [100], que estabelece que estados gaussianos fornecem um limite inferior para a taxa de chave secreta destilável contra ataques coletivos, e (*ii*) a demostração de que ataques gaussianos são ótimos no contexto de ataques coletivos para protocolos com modulação gaussiana [101, 102]. Para a demonstração de segurança incondicional contra ataques arbitrários (coerentes), as técnicas utilizadas para estabelecer a equivalência aos ataques coletivos, como teoremas quânticos de de Finetti [103, 104] e *postselection* [105], não são diretamente aplicáveis aos sistemas CV, uma vez que o comprimento final da chave é função da dimensão do espaço de Hilbert, que neste caso é infinita. Adpatações do teorema de de Finneti quântico para dimensões infinitas foram propostas em [106, 107], as quais podem ser utilizadas em conjunto com provas de segurança componível para ataques coletivos [108]. Além disso, a segurança contra ataques arbitrários no regime finito foi desenvolvida em [109] explorando simetrias no espaço de fase e a técnica de *postselection*. Uma versão gaussiana do teorema de de Finetti foi proposta em [110], permitindo estabelecer a equivalência entre a segurança contra ataques arbitrários e a segurança contra ataques coletivos gaussianos. Com isso, demonstrou-se que os ataques gaussianos representam o pior caso para esses protocolos, sendo, portanto, suficiente comprovar a segurança apenas contra ataques coletivos.

8.1.3. Pós-processamento em protocolos CV

As diferenças entre protocolos DV e CV também são significativas nas etapas clássicas do protocolo, especificamente para estimação de parâmetros e reconciliação da informação. Nessas etapas, o modelo de segurança do protocolo, bem como a natureza contínua dos resultados das medições, devem ser levadas em consideração. A seguir, serão destacados os aspectos principais que diferenciam as tarefas clássicas entre protocolos CV e DV, tomando o GG02 como protocolo CV base.

Desenvolver o modelo teórico de protocolos CV está fora do escopo desse artigo, mas é possível assumir, sem perda de generalidade, que a taxa de chave secreta de um protocolo CV com modulação gaussiana pode ser escrita como

$$K = f(\tilde{V}_m, \beta, \tau, \xi, \eta), \tag{49}$$

em que $\tilde{V}_m$ é a variância de modulação, β é a eficiência do protocolo de reconciliação, τ a transmitância do canal quântico, ξ o ruído de excesso do sistema ponta-a-ponta e η a eficiência dos detectores de Bob. Dentre os parâmetros da Equação 49, η é fixo e $\tilde{V}_m$ é otimizado para maximizar a taxa de chave, enquanto o protocolo de reconciliação é projetado para maximizar o valor de $\beta \in [0, 1]$, de modo que esses três parâmetros são conhecidos. Por sua vez, τ e ξ são parâmetros referentes apenas ao canal e precisam ser estimados para limitar a quantidade de informação possivelmente vazada durante a comunicação quântica.

Analogamente ao caso DV, uma amostra aleatória da chave bruta é utilizada para estimar os valores de τ e ξ. Utilizando um modelo de canal gaussiano, os pares (x_i, y_i) são relacionados por um modelo linear normal [111],

$$y_i = tx_i + z_i \tag{50}$$

em que $t = \sqrt{\tau}$ e $z_i \sim \mathcal{N}(0, 1 + \tau\xi)$ e os estimadores de máxima verossimilhança irão resultar em uma região de confiança que indica os limites estatísticos de confiabilidade sobre o valor estimado [112]. Isso significa que, para uma amostra de tamanho m, é possível calcular os valores de t_{min} e ξ_{max} que configuram o pior caso dentro do intervalo de confiança do estimador. A utilização de

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2025-0373

diferentes técnicas de estimação podem resultar em diferentes regiões de confiança e diferentes velocidades de convergência do estimador para o valor esperado do parâmetro. Essas características da "qualidade" da estimação de parâmetros influencia diretamente a taxa de chave secreta no regime de comprimento finito.

A etapa de reconciliação da informação, por sua vez, apresenta a maior distinção conceitual entre as tarefas clássicas do pós-processamento da chave. Ao contrário dos protocolos DV, em que as chaves brutas são vetores binários, após a comunicação quântica e estimação de parâmetros de protocolos CV, Alice e Bob compartilham vetores gaussianos correlacionados. Logo, o objetivo do protocolo de reconciliação deve ser (i) aplicar algum método de discretização para transformar os vetores $X_n, Y_n \in \mathbb{R}^n$ em sequências binárias $X_l, Y_l \in \{0,1\}^{n\cdot b}$, sendo $b \in \mathbb{Z}^+$ e $l = n \cdot b$, e (ii) realizar a correção de erros entre os vetores discretizados.

Como a etapa de discretização pode ser descrita como uma função $\mathcal{Q} : R^n \to \{0,1\}^{n\cdot b}$, é sabido que, pela desigualdade de processamento de dados, $I(X_n;Y_n) \geq I(X_l;Y_l)$, onde $I(X;Y)$ é a informação mútua clássica entre as variáveis aleatórias X e Y definida como,

$$I(X;Y) = -\sum_{x,y} p(x)p(y)\log\frac{p(x)p(y)}{p(x,y)}. \tag{51}$$

Logo, a função de discretização deve ser projetada para "preservar" a informação mútua inicial da chave bruta, e a eficiência da função da discretização será dada por

$$\beta_{disc} = \frac{I(X_l;Y_l)}{I(X_n;Y_n)}. \tag{52}$$

Vale destacar que a eficiência de discretização da Equação 52 considera o caso simplificado em que Alice e Bob aplicam a função $\mathcal{Q}$ nas suas chaves brutas. Os esquemas de reconciliação podem considerar a discretização de apenas um dos lados para utilizar a "informação suave" das verossimilhanças como dado de entrada nos algoritmos de decodificação iterativos para algumas classes de códigos corretores de erro [113, 114].

A eficiência do protocolo de reconciliação também depende do tipo de estratégia de correção de erros utilizada. Desenvolver a relação entre as características do código corretor de erros e a eficiência de reconciliação está fora do escopo deste trabalho. O leitor interessado pode encontrar uma análise mais completa em [115–117]. Contudo, vale destacar que o problema de reconciliação de informação para sequências binárias correlacionadas pode ser tratado como uma codificação de fontes correlacionadas [118–120], e os limites fundamentais para a quantidade de informação enviada no canal público para realização da reconciliação são estabelecidos pelo teorema de Slepian-Wolf [65, 121]. Operacionalmente, códigos corretores de erro podem ser projetados para possuir taxa próxima ao limite de Slepian-Wolf, minimizando a quantidade de informação vazada durante as etapas clássicas do protocolo QKD. Denotando por β_{cod} a eficiência do código corretor de erros, têm-se que a expressão geral para a eficiência de um protocolo de reconciliação de informação para sistemas CV-QKD é dada por,

$$\beta = \beta_{disc} \cdot \beta_{cod}. \tag{53}$$

Historicamente, o primeiro protocolo de reconciliação especializado para sistemas CV foi a reconciliação por fatiamento [122], que utiliza funções de particionamento da reta real para realizar a atribuição de palavas binárias a cada partição. Adicionalmente, também utiliza estratégias de codificação de várias camadas e decodificação de vários estágios [116, 117]. Posteriormente, a estratégia de reconciliação multidimensional permitiu a reconciliação de chaves a longas distâncias [115].

8.1.4. O protocolo GG02

Para entender como funcionam os protocolos CV-QKD na prática, vamos examinar o protocolo GG02 [92], que inspirou o desenvolvimento da maioria dos protocolos desenvolvidos posteriormente. A versão "prepara e mede" do protocolo GG02 se dá da seguinte maneira.

(i) Alice gera N amostras i.i.d. $Q, P \sim \mathcal{N}(0, \tilde{V}_m)$, onde $\tilde{V}_m$ é a variância de modulação, formando as sequências $Q_N = \{q_1, \cdots, q_N\}$ e $P_N = \{p_1, \cdots, p_N\}$. Alice então prepara N estados coerentes $|q_1 + ip_1\rangle, \cdots, |q_N + ip_N\rangle$ e os envia a Bob por um canal quântico.

(ii) Bob gera um vetor aleatório $B = \{b_1, \cdots, b_N\}$ em que cada b_i é equiprovável. Na i-ésima rodada do protocolo, Bob realiza a medição homódina da quadratura q se $b_i = 0$ ou mede a quadratura p se $b_i = 1$, e armazena o resultado na i-ésima posição do vetor $Y = y_1, \cdots, y_N$. Ao final das N rodadas, Bob informa a Alice o vetor B contendo informação das quadraturas medidas, de modo que Alice forma a sequência X_L da seguinte maneira:

$$x_i = \begin{cases} q_i, \text{ se } b_i = 0 \\ p_i, \text{ se } b_i = 1 \end{cases}$$

(iii) Para a estimação de parâmetros, Alice e Bob sorteiam um conjunto aleatório de m índices $I_{teste} = \{i_1, \cdots, i_m\} \subset [N]$ e divulgam publicamente as amostras $x_{i_1}, \cdots, x_{i_1}$ e $y_{i_1}, \cdots, y_{i_1}$ para estimar os parâmetros do canal, transmitância τ e ruído de excesso ξ.

(iv) Após a estimação de parâmetros, Alice e Bob compartilham dois vetores com os dados restantes X_l e Y_l, Alice e Bob aplicam quantização e executam um protocolo de reconciliação da informação, obtendo uma sequência binária comum $U \in \{0,1\}^{l\cdot b}$. Tipicamente, utiliza-se reconciliação reversa, onde Bob envia informações para que Alice corrija sua sequência e ambas fiquem idênticas.

(v) Por fim, Alice e Bob aplicam amplificação de privacidade utilizando funções de *hash*, gerando a chave final K a partir de U, com comprimento determinado pelos parâmetros estimados.

A taxa de chave secreta para o protocolo GG02 é dada pela fórmula de Devetak-Winter para o cenário de ataques coletivos no regime assintótico [123], dada por

$$K = \beta I(X;Y) - \chi(E,B), \tag{54}$$

indicando que a quantidade média de bits seguros por estado quântico transmitido é, em média, dada pela diferença entre a quantidade de informação clássica compartilhada por Alice e Bob, $I(X;Y)$ (a informação mútua clássica de Shannon), e o limite superior para a quantidade de informação acessível de Eva, $\chi(E,B)$, (limitante de Holevo).

Para o protocolo GG02 em que as sequências compartilhadas por Alice e Bob são vetores Gaussianos, a informação mútua é função da razão-sinal-ruído [81],

$$I(X;Y) = \frac{1}{2}\log_2(1+SNR), \tag{55}$$

sendo

$$SNR = \frac{\tau 4\tilde{V}_m}{1+\xi}. \tag{56}$$

A expressão para calcular o termo $\chi(E,B)$ para protocolos com modulação gaussiana depende da definição do protocolo equivalente baseado em emaranhamento, bem como da escolha de se atribuir ou não o ruído gerado pelos equipamentos dos laboratórios de Alice e Bob (moduladores, conversores analógico-digital, detectores, etc.) como uma ação de espionagem de Eva. Por esse motivo, para o leitor que queira se aprofundar no tema, indicamos os seguintes artigos de revisão que apresentam as expressões da taxa de chave secreta para diversas situações para protocolos Gaussianos [71, 81, 124].

8.2. Processamento de informações independente de dispositivo

No protocolo BB84, o teorema da não clonagem garante que a preparação e medição de estados quânticos em bases não ortogonais permitem detectar a presença de um espião, assegurando assim o estabelecimento de uma chave secreta entre pontos distantes. Contudo, esse protocolo depende implicitamente do pressuposto de que os dispositivos executam fielmente as operações quânticas teóricas. Na prática, essa condição nem sempre é satisfeita: como verificar se um dispositivo de medição efetivamente realiza medições do operador de Pauli X? Como confirmar que o estado quântico preparado é $|0\rangle$ e não $\sqrt{1-\epsilon}\,|0\rangle + \sqrt{\epsilon}\,|1\rangle$? Essa problemática torna-se particularmente crítica quando os dispositivos são obtidos de fornecedores externos, nos quais não se pode depositar confiança absoluta. Conforme demonstrado [125], sistemas comerciais de criptografia quântica podem ser vulneráveis a ataques quando não há garantias sobre a correta operação dos dispositivos de preparação e medição. Surge então a questão: é possível estabelecer uma criptografia quântica fundamentalmente segura, independente da confiança ou conhecimento detalhado do aparato experimental? Como veremos, a resposta afirmativa fundamenta-se no teorema de Bell [57].

A violação de desigualdades de Bell (como no Protocolo E91) mostra que medições em sistemas emaranhados são incompatíveis com teorias de realismo local. A localidade exige que eventos distantes (fora do cone de luz) não influenciem-se causalmente, enquanto o realismo assume que propriedades físicas existem independentemente de medições.

Essa violação evidencia a incompatibilidade sem depender de detalhes dos dispositivos, usando apenas correlações estatísticas observadas. Isso fundamenta o paradigma de processamento de informação independente de dispositivos.

Aplicado à criptografia quântica, esse paradigma assegura privacidade da chave mesmo com dispositivos fabricados por adversários ou com falhas desconhecidas. Essa robustez é crucial em cenários sem confiança nos dispositivos, tornando essa abordagem a mais avançada e segura em QKD [126, 127].

Como ilustração, considere a máxima violação da desigualdade CHSH. Resultados de auto-teste [56] garantem que, a menos de unitárias locais, apenas o estado maximamente emaranhado (Eq. (15)) atinge o valor $2\sqrt{2}$. A monogamia do emaranhamento implica que tal estado bipartido não pode correlacionar-se com outros sistemas. Portanto, para o sistema total compartilhado por Alice, Bob e Eva:

$$|\psi\rangle_{AB} \otimes |\phi\rangle_E \tag{57}$$

onde $|\psi\rangle_{AB}$ é o estado emaranhado Alice-Bob e $|\phi\rangle_E$ o estado de Eva. Esta separabilidade na partição $AB|E$ elimina quaisquer correlações entre os subsistemas. Se $p(a,b|x,y)$ descreve a distribuição de probabilidades de Alice e Bob (resultados a,b para medições x,y) e $p(e)$ a distribuição de Eva, então para quaisquer medições locais:

$$p(a,b,e|x,y) = p(a,b|x,y)p(e). \tag{58}$$

Consequentemente, Eva não obtém informação sobre os resultados de Alice e Bob usados na geração da chave secreta.

De forma geral, diferentes quantificadores de aleatoriedade avaliam a segurança da chave estabelecida entre Alice e Bob. Um exemplo é a probabilidade de adivinhação:

$$G(a,b|e,xy) = \sum_{a,b} p(a,b,e=(a,b)|xy), \tag{59}$$

que quantifica a capacidade de Eva prever os resultados de Alice e Bob. Quando Eva tem acesso total,

 DOI: https://doi.org/10.1590/1806-9126-RBEF-2025-0373

$G(a,b|e,xy) = 1$; sem acesso, $G(a,b|e,xy) = 1/4$ para variáveis binárias a, b – indicando que sua melhor estratégia é adivinhar aleatoriamente (25% de sucesso). Outra quantidade relevante é a entropia mínima:

$$H_{\min} = -\log_2(G(a,b|e,xy)). \tag{60}$$

Dado um cenário de Bell e correlações observadas, a melhor probabilidade de adivinhação de um espião é obtida resolvendo:

$$\begin{aligned} \max \quad & G(a,b|e,x,y) \\ & \text{tal que} \\ p(a,b,e|x,y) &= \mathrm{Tr}(\varrho_{ABE} \cdot (A_{a|x} \otimes B_{b|y} \otimes E_e)), \\ p(a,b|x,y) &= \sum_e p(a,b,e|x,y). \end{aligned} \tag{61}$$

Aqui, $A_{a|x}$, $B_{b|y}$ e E_e são operadores de medição para Alice, Bob e Eva, e ϱ_{ABE} descreve o estado quântico compartilhado. Embora este problema seja computacionalmente difícil, técnicas aproximadas como a hierarquia de Navascues-Pironio-Acín [128] fornecem cotas eficientes via programas semidefinidos [129].

A criptografia quântica baseada em violação de desigualdades de Bell oferece segurança máxima, mas é experimentalmente desafiadora [29]. Por isso, surgiram variações denominadas protocolos semi-independentes de dispositivo, que admitem hipóteses adicionais para facilitar implementações, ainda que com segurança reduzida.

Considere, por exemplo, um canal seguro entre um banco e seu cliente. Os dispositivos do banco podem ser considerados confiáveis e bem caracterizados, mas não os do cliente – quanto menos suposições sobre estes, maior a segurança. Nesse cenário assimétrico, a segurança é garantida pelo direcionamento quântico [130] (do inglês *quantum steering* [131]). Outra abordagem envolve assumir dimensões fixas para sistemas quânticos [132, 133].

Protocolos como BB84 são implementáveis mas vulneráveis a ataques em dispositivos, enquanto os baseados em violação Bell oferecem segurança absoluta porém impraticáveis. Um paradigma intermediário, que assume segurança apenas nos dispositivos de preparação de estados (não nos de medição), tem atraído atenção. Tais protocolos são denominados independentes do dispositivo de medição (MDI-QKD, do inglês *measurement device independent*) [21, 33, 34], conforme ilustrado na Fig. 13.

A ideia central destes protocolos deriva parcialmente dos completamente independentes de dispositivos: garantir pelas estatísticas de medição que, para um espião, o estado conjunto de Alice e Bob comporta-se como maximamente emaranhado. No MDI-QKD, contudo, Alice e Bob enviam sinais independentemente – sem emaranhamento entre os fótons. Ainda assim, a medição por Charlie (potencialmente controlado por espião) projeta probabilisticamente o estado conjunto em um estado maximamente emaranhado.

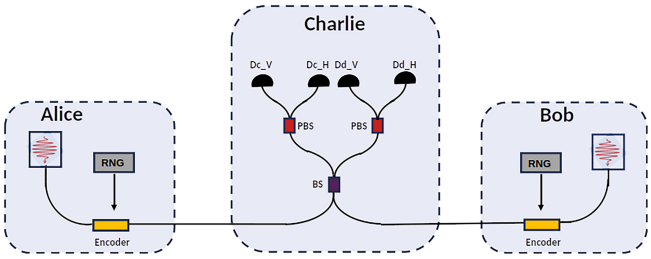

Figura 13: Em um protocolo MDI-QKD, Alice e Bob preparam fótons individuais enviados a Charlie – responsável por todas as medições. A codificação de bits ocorre na polarização: $|H\rangle$ e $|+\rangle$ representam o bit 0, enquanto $|V\rangle$ e $|-\rangle$ representam o bit 1. Essa codificação é realizada pelo dispositivo *encoder*, constituído por placas de onda e meia-onda. A seleção de estados é aleatória, determinada por um gerador de números aleatórios (RNG, do inglês *random number generator*). Os fótons são enviados simultaneamente e chegam ao mesmo tempo ao divisor de feixe (BS, do inglês *beam splitter*), que apaga a informação sobre a origem (Alice ou Bob). Em seguida, passam por divisores de feixes polarizantes (PBS, do inglês *polarized beam splitter*) para detecção de polarização nos detectores Dc_V, Dc_H, Dd_V e Dd_H. Como estabelecido, *clicks* em dois detectores distintos correspondem a uma projeção em estado maximamente emaranhado, permitindo que Alice e Bob estabeleçam seguramente os bits para a chave criptográfica.

A heurística do protocolo é simples: ao detectar dois fótons (um em Dc_V e outro em Dd_H), Charlie (potencialmente controlado por espião) infere que ocorreu:

- Alice enviou $|H\rangle$ e Bob enviou $|V\rangle$, ou
- Alice enviou $|V\rangle$ e Bob enviou $|H\rangle$,

assumindo bases lineares conhecidas (pós-*sifting*) com ambos enviando $|H\rangle$ ou $|V\rangle$. Contudo, Charlie desconhece qual cenário ocorreu. Associando bit 0 a $|H\rangle$ e bit 1 a $|V\rangle$, ele conhece apenas a soma dos bits (não seus valores individuais). Quando Bob inverte seu bit para igualar ao de Alice, a probabilidade de Charlie adivinhar corretamente é 50%, não obtendo informação.

Para demonstrar a segurança do protocolo e sua conexão com o emaranhamento, aplicamos uma técnica comum na área: mapear um protocolo em outro. Especificamente, mapeamos o protocolo MDI-QKD (Fig. 13) no protocolo BB84 com distribuição de emaranhamento (Fig. 10). Para isso, consideramos que Alice e Bob possuem em seus laboratórios um qubit local com acesso completo e estático – um artifício matemático que não precisa existir fisicamente na implementação. Alice cria um estado emaranhado entre seu qubit local (subespaço a) e o fóton enviado a Charlie (subespaço A):

$$|\Psi\rangle_{aA} = \frac{1}{\sqrt{2}} \left(|0\rangle_a \otimes |H\rangle_A + |1\rangle_a \otimes |V\rangle_A \right).$$

Quando Alice mede seu qubit na base Z, ela envia a Charlie $|H\rangle$ ou $|V\rangle$, cada com probabilidade 1/2. Se medir na base X, prepara $|+\rangle$ ($+45°$) ou $|-\rangle$ ($-45°$),

igualmente com probabilidade 1/2. Assim, ao escolher aleatoriamente entre as bases Z ou X (probabilidade 1/2 para cada), cada um dos quatro estados de polarização é preparado com probabilidade 1/4, replicando o protocolo original. Bob produz um estado equivalente entre seu qubit local e seu fóton.

Agora imaginemos que Alice e Bob não medem seus qubits locais, e enviam os fótons para Charlie. Como podemos alterar a ordem da medição de Charlie com a de Alice e Bob, vejamos o estado total do sistema após os fótons passarem pelo divisor de feixes. Este é dado por [15]:

$$|\Phi_{BS}\rangle = \frac{1}{2}\left[|\psi^+\rangle_{ab}\left(\frac{|1\rangle_{c_H}|1\rangle_{c_V} - |1\rangle_{d_H}|1\rangle_{d_V}}{\sqrt{2}}\right) - |\psi^-\rangle_{ab}\left(\frac{|1\rangle_{c_H}|1\rangle_{d_V} - |1\rangle_{c_V}|1\rangle_{d_H}}{\sqrt{2}}\right) + |00\rangle_{ab}\left(\frac{|2\rangle_{c_H} - |2\rangle_{d_H}}{2}\right) + |11\rangle_{ab}\left(\frac{|2\rangle_{c_V} - |2\rangle_{d_V}}{2}\right)\right], \tag{62}$$

onde $|\psi^\pm\rangle = (|01\rangle_{ab} \pm |10\rangle_{ab})/\sqrt{2}$ são estados maximamente emaranhados entre os qubits físicos de Alice e Bob; e a notação $|n\rangle_{c_H}$ significa que temos n fótons no modo c com polarização H, e similarmente para os demais.

Note que existem casos onde Charlie não tem "click" em dois detectores distintos. Dizemos que Charlie não mede coincidências. Por exemplo, no caso onde só detecção no detector D_{c_H} é registrada, Charlie projeta os estados dos qubits físicos em $|00\rangle_{ab}$. Portanto, quando, no processo de sifting, ele souber qual base foi escolhida por Alice e Bob, ele saberá exatamente quais foram os bits escolhidos. Todos esses casos devem ser então descartados.

Contudo, sempre que Charlie detecta dois fótons com polarizações opostas – seja no mesmo modo de saída do divisor de feixes ou em modos distintos – os qubits locais de Alice e Bob são projetados em um estado maximamente emaranhado. Nesses casos, Alice e Bob podem empregar um protocolo BB84 baseado em emaranhamento. Como esses qubits são artefatos matemáticos, estabelece-se que, nessas situações, Alice e Bob podem gerar uma chave criptográfica segura, dada a equivalência com um protocolo comprovadamente seguro.

Assim, demonstra-se que mesmo com o detector controlado por um espião, a segurança do protocolo quântico de distribuição de chaves é garantida. Outros protocolos MDI-QKD existem, incluindo um em implementação na Rede Rio Quântica – rede metropolitana de distribuição quântica de chaves no Rio de Janeiro [23, 24].

[15] Para obter esse estado é conveniente utilizarmos o formalismo de segunda quantização, onde a estatística bosônica dos fótons é intrinsecamente levada em conta.

9. Conclusões

A Criptografia Quântica representa um novo paradigma para a segurança de informação, fundamentando-se nos princípios da física quântica ao invés de depender da complexidade computacional de algoritmos específicos. Neste tutorial, apresentamos uma introdução acessível aos conceitos fundamentais da área, construindo um panorama desde o básico da criptografia clássica até os princípios da teoria quântica e suas aplicações em protocolos QKD.

Os protocolos QKD apresentados, desde o pioneiro BB84 até desenvolvimentos mais recentes em variáveis contínuas, demonstram a diversidade de abordagens possíveis e suas respectivas vantagens. Para ilustrar esse tipo de sistemas, detalhamos alguns dos primeiros protocolos DV-QKD desenvolvidos (BB84 e E91) e os principais protocolos CV-QKD com modulação gaussiana (GG02 e *No-switching*). Além disso, descrevemos suas respectivas etapas de pós-processamento que transformam chaves brutas ruidosas em sequências secretas e idênticas: estimação de parâmetros, reconciliação de informação (correção de erros) e amplificação de privacidade. Discutimos brevemente a segurança desses protocolos e apresentamos algumas das técnicas mais modernas de QKD, incluindo sistemas de variáveis contínuas, que podem ser implementados em circuitos fotônicos, e protocolos independentes de dispositivos, que apresentam um maior nível de segurança.

A QKD representa hoje uma das aplicações mais maduras das tecnologias quânticas, com sistemas comerciais já disponíveis e redes de comunicação quântica em operação. Contudo, desafios significativos permanecem tanto no campo teórico quanto nas aplicações práticas, incluindo o aumento das distâncias de transmissão, a melhoria das taxas de geração de chaves e a integração com infraestruturas de comunicação existentes. Para o cenário brasileiro, acreditamos que este tutorial chega em momento oportuno, quando iniciativas nacionais, como o Quantum Industrial Innovation (QuIIN) – Centro de Competência EMBRAPII CIMATEC em Tecnologias Quânticas, a Rede Rio Quântica, entre outras, visam posicionar o país na vanguarda do desenvolvimento de tecnologias de comunicação e criptografia quânticas. A formação de recursos humanos qualificados e a democratização do conhecimento em língua portuguesa tornam-se, portanto, urgentes para consolidar essa posição. Nesse sentido, este tutorial visa contribuir para a formação de uma nova geração de pesquisadores especializados em QKD.

Agradecimentos

Este trabalho foi parcialmente financiado pelo projeto Certificação de Aleatoriedade Quântica, suportado pelo QuIIN – Quantum Industrial Innovation, Centro de Competência EMBRAPII CIMATEC em Tecnologias

Quânticas, com recursos do PPI IoT/Manufatura 4.0 do MCTI, através do Termo de Cooperação 053/2023 com a EMBRAPII. FdM agradece financiamento do CNPq (409611/2022-0), FAPERJ (APQ1 E-26/210.576/2024) e FAPESP (Temático 2021/06823-5). RC agradece à Simons Foundation (1023171), CNPq (307295/2020-6, 403181/2024-0) e FINEP (1699/24 IIF-FINEP). MD agradece financiamento da União Europeia (HORIZON-MSCA-2023 Postdoctoral Fellowship, 101153602 – COCoVaQ). Agradecemos também a Johene Amorim e Pedro Henrique da Silva pelo design das figuras deste artigo.

Disponibilidade de Dados

Todos os dados necessários para avaliar as conclusões deste estudo estão apresentados no artigo.

Referências

[1] MICHAELIS ON-LINE, *Dicionário brasileiro da língua portuguesa*, disponível em: https://michaelis.uol.com.br, acessado em: 10/07/2024.

[2] C.E. Shannon, The Bell System Technical Journal **27**, 379 (1948).

[3] J. Von Neumann, *Mathematical foundations of quantum mechanics: New edition* (Princeton University Press, Princeton, 2018).

[4] P.W. Shor, em: *35th Annual Symposium on Foundations of Computer Science* (Santa Fe, 1994).

[5] R.L. Rivest, A. Shamir e L. Adleman, Communications of the ACM **21**, 120 (1978).

[6] A.K. Lenstra e H.W. Lenstra, *The development of the number field sieve* (Springer Science & Business Media, Berlin, 1993), v. 1554.

[7] C. Gidney, arXiv:2505.15917 (2025).

[8] J. Gambetta, *Ibm's roadmap for scaling quantum technology*, disponível em: https://www.ibm.com/quantum/blog/ibm-quantum-roadmap.

[9] M.A. Norcia, H. Kim, W.B. Cairncross, M. Stone, A. Ryou, M. Jaffe, M.O. Brown, K. Barnes, P. Battaglino, T.C. Bohdanowicz et al., PRX Quantum **5**, 030316 (2024).

[10] J. Ha, J. Lee e J. Heo, Quantum Information Processing **21**, 60 (2022).

[11] S.J. Devitt, W.J. Munro e K. Nemoto, Reports on Progress in Physics **76**, 076001 (2013).

[12] C.P. Schnorr, *Fast factoring integers by svp algorithms, corrected*, disponível em: https://eprint.iacr.org/2021/933.

[13] B. Yan, Z. Tan, S. Wei, H. Jiang, W. Wang, H. Wang, L. Luo, Q. Duan, Y. Liu, W. Shi et al., arXiv:2212.12372 (2022).

[14] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F.D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables e R. Hansen, Nature **605**, 237 (2022).

[15] G. Alagic, G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.K. Liu, C. Miller et al., *Status report on the third round of the nist post-quantum cryptography standardization process*, disponível em: https://www.nist.gov/publications/status-report-third-round-nist-post-quantum-cryptography-standardization-process.

[16] C.H. Bennett e G. Brassard, Theoretical Computer Science **560**, 7 (2014).

[17] W.K. Wootters e W.H. Zurek, Nature **299**, 802 (1982).

[18] S. Wiesner, ACM Sigact News **15**, 78 (1983).

[19] D. Bruß, Physical Review Letters **81**, 3018 (1998).

[20] V. Scarani, A. Acin, G. Ribordy e N. Gisin, Physical Review Letters **92**, 057901 (2004).

[21] H.K. Lo, M. Curty e B. Qi, Physical Review Letters **108**, 130503 (2012).

[22] M. Lucamarini, Z.L. Yuan, J.F. Dynes e A.J. Shields, Nature **557**, 400 (2018).

[23] G. Temporão, F. Melo e A. Khoury, em: *I Workshop de Redes Quânticas* (Niteroi, 2024).

[24] M. Ribeiro, R. Vallejos, G. Temporão, A. Khoury e F. Melo, em: *II Workshop de Redes Quânticas* (Natal, 2025).

[25] K. Inoue, E. Waks e Y. Yamamoto, Physical Review Letters **89**, 037902 (2002).

[26] N. Gisin, S. Fasel, B. Kraus, H. Zbinden e G. Ribordy, Physical Review A—Atomic, Molecular, and Optical Physics **73**, 022320 (2006).

[27] C.H. Bennett, G. Brassard e N.D. Mermin, Physical Review Letters **68**, 557 (1992).

[28] A.K. Ekert, Physical Review Letters **67**, 661 (1991).

[29] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.Z. Liu, Q. Zhang, H. Weinfurter e M. Curty, npj Quantum Information **9**, 10 (2023).

[30] N. Gisin, G. Ribordy, W. Tittel e H. Zbinden, Reviews of Modern Physics **74**, 145 (2002).

[31] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus e M. Peev, Reviews of Modern Physics **81**, 1301 (2009).

[32] H.K. Lo, M. Curty e K. Tamaki, Nature Photonics **8**, 595 (2014).

[33] F. Grasselli, *Quantum cryptography* (Springer, Cham, 2021).

[34] R. Wolf, *Quantum key distribution* (Springer, Cham, 2021).

[35] T. Vidick e S. Wehner, *Introduction to quantum cryptography* (Cambridge University Press, Cambridge, 2023).

[36] G. Rigolin e A.A.L. Rieznik, Revista Brasileira de Ensino de Física **27**, 517 (2005).

[37] C. Paar, J. Pelzl e T. Güneysu, *Understanding Cryptography: From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms* (Springer, Berlin, Heildelberg, 2024), 2 ed.

[38] VIAF – Virtual International Authority File, disponível em: https://viaf.org/.

[39] LIBRARY OF CONGRESS, disponível em: https://www.loc.gov/.

[40] J.F. Dooley, *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms* (Springer, Cham, 2018), 1 ed.

[41] Racionais MC's e Afro-X, *A vida é desafio* (Cosa Nostra Fonográfica, São Paulo, 2002).

[42] D. Kahn, *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet* (Simon and Schuster, New York, 1996).

[43] F.H. Hinsley e A. Stripp, *Codebreakers: the inside story of Bletchley Park* (Oxford University Press, Oxford, 2001).

[44] W. Diffie e M. Hellman, IEEE Transactions on Information Theory **22**, 644 (1976).

[45] G.S. Vernam, Journal of the American Institute of Electrical Engineers **45**, 109 (1926).

[46] A. Acín e L. Masanes, Nature **540**, 213 (2016).

[47] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Advanced encryption standard* (National Institute of Standards and Technology, Gaithersburg, 2001).

[48] U.V. Vazirani e V.V. Vazirani, em: *Workshop on the Theory and Application of Cryptographic Techniques* (Paris, 1984).

[49] M.A. Nielsen e I.L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2010).

[50] C. Cohen-Tannoudji, B. Diu e F. Laloe, Quantum Mechanics **1**, 898 (1986).

[51] S. Pirandola, U.L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani et al., Advances in Optics and Photonics **12**, 1012 (2020).

[52] R. Renner, International Journal of Quantum Information **06**, 1 (2008).

[53] M.B. Santos, P. Mateus e A.N. Pinto, Entropy **24**, 945 (2022).

[54] A. Vázquez-Castro, D. Rusca e H. Zbinden, Physical Review Applied **16**, 014006 (2021).

[55] M. Koashi e A. Winter, Physical Review A **69**, 022309 (2004).

[56] I. Šupić e J. Bowles, Quantum **4**, 337 (2020).

[57] J.S. Bell, Physics Physique Fizika **1**, 195 (1964).

[58] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani e S. Wehner, Reviews of Modern Physics **86**, 419 (2014).

[59] J.F. Clauser, M.A. Horne, A. Shimony and R.A. Holt, Physical Review Letters **23**, 880 (1969).

[60] S. Pironio, A. Acín, S. Massar, A.B. de La Giroday, D.N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T.A. Manning et al., Nature **464**, 1021 (2010).

[61] M. Curty, M. Lewenstein e N. Lütkenhaus, Physical Review Letters **92**, 217903 (2004).

[62] R.J. Serfling, The Annals of Statistics **2**, 39 (1974).

[63] F.J. MacWilliams e N.J.A. Sloane, *The theory of error-correcting codes* (Elsevier, Amsterdam, 1977).

[64] R.W. Hamming, *Coding and information theory* (Prentice Hall, Hoboken, 1986).

[65] D. Slepian e J. Wolf, IEEE Transactions on Information Theory **19**, 471 (1973).

[66] G. Brassard e L. Salvail, em: *Workshop on the Theory and Application of of Cryptographic Techniques* (Lofthus, 1993).

[67] I. Devetak e A. Winter, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **461**, 207 (2005).

[68] M. Christandl, R. König, G. Mitchison e R. Renner, Communications in Mathematical Physics **273**, 473 (2007).

[69] ETSI – European Telecommunications Standards Institute, *Industry Specification Group (ISG) on Quantum Key Distribution (QKD)*, disponível em: https://www.etsi.org/committee/qkd.

[70] E. Diamanti, H.K. Lo, B. Qi e Z. Yuan, npj Quantum Information **2**, 16025 (2016).

[71] Y. Zhang, Y. Bian, Z. Li, S. Yu e H. Guo, Applied Physics Reviews **11**, 011318 (2024).

[72] A.A.E. Hajomer, I. Derkach, R. Filip, U.L. Andersen, V.C. Usenko e T. Gehring, Light: Science & Applications **13**, 291 (2024).

[73] H. Wang, Y. Li, T. Ye, L. Ma, Y. Pan, M. Wu, J. Li, Y. Bian, Y. Pi, Y. Shao et al., arXiv:2503.14843 (2025).

[74] A.A.E. Hajomer, I. Derkach, N. Jain, H.M. Chin, U.L. Andersen e T. Gehring, Science Advances **10**, eadi9474 (2024).

[75] A.A.E. Hajomer, A. Bomhals, C. Bruynsteen, A. Sidhique, I. Derkach, U.L. Andersen, X. Yin e T. Gehring, arXiv:2504.09308 (2025).

[76] A.A.E. Hajomer, I. Derkach, V.C. Usenko, U.L. Andersen e T. Gehring, arXiv:2502.17388 (2025).

[77] H.M. Chin, N. Jain, U.L. Andersen, D. Zibar e T. Gehring, Quantum Science and Technology **7**, 045006 (2022).

[78] Z. Chen, X. Wang, S. Yu, Z. Li e H. Guo, npj Quantum Information **9**, 28 (2023).

[79] S. Yang, Z. Yan, H. Yang, Q. Lu, Z. Lu, L. Cheng, X. Miao e Y. Li, EPJ Quantum Technology **10**, 40 (2023).

[80] V.C. Usenko, A. Acín, R. Alléaume, U.L. Andersen, E. Diamanti, T. Gehring, A.A.E. Hajomer, F. Kanitschar, C. Pacher, S. Pirandola et al., arXiv:2501.12801 (2025).

[81] F. Laudenbach, C. Pacher, C.H.F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther e H. Hübel, Advanced Quantum Technologies **1**, 1800011 (2018).

[82] L. Mandel e E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, Cambridge, 1995).

[83] D.F. Walls e G.J. Milburn, *Quantum Optics* (Springer, Berlin, Heidelberg, 2008).

[84] S. Barnett e P.M. Radmore, *Methods in Theoretical Quantum Optics* (Clarendon Press, Oxford, 2002).

[85] M.O. Scully e M.S. Zubairy, *Quantum Optics* (Cambridge University Press, Cambridge, 1997).

[86] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S.L. Braunstein, S. Lloyd, T. Gehring, C.S. Jacobsen e U.L. Andersen, Nature Photonics **9**, 397 (2015).

[87] T.C. Ralph, Physical Review A **61**, 010303 (1999).

[88] M. Hillery, Physical Review A **61**, 022309 (2000).

[89] M.D. Reid, Physical Review A **62**, 062308 (2000).

[90] N.J. Cerf, M. Lévy e G. Van Assche, Physical Review A **63**, 052311 (2001).

[91] D. Gottesman e J. Preskill, Physical Review A **63**, 022309 (2001).

[92] F. Grosshans e P. Grangier, Physical Review Letters **88**, 57902 (2002).

[93] C. Weedbrook, A.M. Lance, W.P. Bowen, T. Symul, T.C. Ralph e P.K. Lam, Physical Review Letters **93**, 170504 (2004).

[94] Y.B. Zhao, M. Heid, J. Rigas e N. Lütkenhaus, Physical Review A **79**, 012307 (2009).

[95] A. Leverrier e P. Grangier, arXiv:1002.4083 (2010).

[96] A. Denys, P. Brown e A. Leverrier, Quantum **5**, 540 (2021).

[97] S. Ghorai, P. Grangier, E. Diamanti e A. Leverrier, Physical Review X **9**, 021059 (2019).

[98] P. Papanastasiou, C. Lupo, C. Weedbrook e S. Pirandola, Physical Review A **98**, 012340 (2018).

[99] I.B. Djordjevic, IEEE Photonics Journal **11**, 4500610 (2019).

[100] M.M. Wolf, G. Giedke e J.I. Cirac, Physical Review Letters **96**, 080502 (2006).

[101] M. Navascués, F. Grosshans e A. Acín, Physical Review Letters **97**, 190502 (2006).

[102] R. García-Patrón e N.J. Cerf, Physical Review Letters **97**, 190503 (2006).

[103] M. Christandl, R. König, G. Mitchison e R. Renner, Communications in Mathematical Physics **273**, 473 (2007).

[104] R. Renner, Nature **3**, 645 (2007).

[105] M. Christandl, R. König e R. Renner, Physical Review Letters **102**, 020504 (2009).

[106] R. König e M.M. Wolf, Journal of Mathematical Physics **50**, 012102 (2009).

[107] R. Renner e J.I. Cirac, Physical Review Letters **102**, 110504 (2009).

[108] A. Leverrier, Physical Review Letters **114**, 070501 (2015).

[109] A. Leverrier, R. García-Patrón, R. Renner e N.J. Cerf, Physical Review Letters **110**, 030502 (2013), arXiv:1208.4920.

[110] A. Leverrier, Physical Review Letters **118**, 200501 (2017).

[111] R.D. Yates e D.J. Goodman, *Probability and Stochastic Processes: A Friendly Introduction for Electrical and Computer Engineers* (Wiley, Hoboken, 2014), 3 ed.

[112] A. Leverrier, F. Grosshans e P. Grangier, Physical Review A **81**, 062343 (2010).

[113] M.N. Notarnicola, S. Olivares, E. Forestieri, E. Parente, L. Potì e M. Secondini, IEEE Transactions on Communications **72**, 375 (2024).

[114] M. Origlia e M. Secondini, em: *14th International ITG Conference on Systems, Communications and Coding (SCC)* (Karlsruhe, 2025).

[115] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor e P. Grangier, Physical Review A **77**, 42325 (2008).

[116] P. Jouguet, D. Elkouss e S. Kunz-Jacques, Physical Review A **90**, 42329 (2014).

[117] Z. Bai, S. Yang e Y. Li, Japanese Journal of Applied Physics **56**, 44401 (2017).

[118] A.D. Liveris, Z. Xiong e C.N. Georghiades, IEEE Communications Letters **6**, 440 (2002).

[119] K.C. Nguyen, G. Van Assche e N.J. Cerf, em: *International Symposium on Information Theory and Its Applications* (Parma, 2004).

[120] M. Bloch, A. Thangaraj, S.W. McLaughlin e J.M. Merolla, em: *IEEE Information Theory Workshop* (Punta del Este, 2006).

[121] Joy A. Thomas Thomas M. Cover, *Elements of Information Theory* (Wiley John + Sons, 2006).

[122] G. Van Assche, J. Cardinal e N.J. Cerf, IEEE Transactions on Information Theory **50**, 394 (2004).

[123] I. Devetak e A. Winter, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **461**, 207 (2005).

[124] V. Usenko e R. Filip, Entropy **18**, 20 (2016).

[125] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar e V. Makarov, Nature Photonics **4**, 686 (2010).

[126] U. Vazirani e T. Vidick, Communications of the ACM **62**, 133 (2019).

[127] V. Scarani, Acta Physica Slovaca **62**, 347 (2012).

[128] M. Navascués e T. Vértesi, Physical Review Letters **106**, 060403 (2011).

[129] S.P. Boyd e L. Vandenberghe, *Convex optimization* (Cambridge University Press, Cambridge, 2004).

[130] D.J. Joch, S. Slussarenko, Y. Wang, A. Pepper, S. Xie, B.B. Xu, I.R. Berkman, S. Rogge e G.J. Pryde, Physical Review A **106**, L050401 (2022).

[131] R. Uola, A.C.S. Costa, H.C. Nguyen e O. Gühne, Reviews of Modern Physics **92**, 015001 (2020).

[132] M. Pawłowski e N. Brunner, Physical Review A—Atomic, Molecular, and Optical Physics **84**, 010302 (2011).

[133] T. Lunghi, J.B. Brask, C.C.W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden e N. Brunner, Physical Review Letters **114**, 150501 (2015).