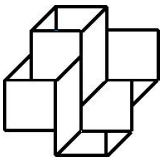


Laboratório Nacional de Computação Científica

Programa de Pós-Graduação em Modelagem Computacional

Distribuição quântica de chaves:

Um estudo sobre a geração quântica de chaves criptográficas clássicas

Gabriel Moysés Delfino

Petrópolis, RJ - Brasil

Fevereiro de 2024

Gabriel Moysés Delfino

Distribuição quântica de chaves:

Um estudo sobre a geração quântica de chaves criptográficas clássicas

Dissertação submetida ao corpo docente do Laboratório Nacional de Computação Científica como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências em Modelagem Computacional.

Laboratório Nacional de Computação Científica

Programa de Pós-Graduação em Modelagem Computacional

Orientador(es): Renato Portugal

Petrópolis, RJ - Brasil

Fevereiro de 2024

Ficha catalográfica elaborada por Patrícia Vieira Silva - CRB7 5822

D349d Delfino, Gabriel Moysés.
Distribuição quântica de chaves: um estudo sobre a geração quântica de chaves criptográficas clássicas / Gabriel Moysés Delfino. – Petrópolis, RJ: Laboratório Nacional de Computação Científica, 2024.
123 f.: il.; 30 cm.
Referências: f. 102-105.

Dissertação (Mestrado em Modelagem Computacional) – Laboratório Nacional de Computação Científica, 2024.
Orientador: Renato Portugal

1. Computação quântica. 2. Distribuição quântica de chaves. 3. Criptografia. 4. Criptografia quântica. I. Portugal, Renato. II. LNCC/MCTI. III. Título.

CDD – 004.1

Laboratório Nacional de Computação Científica
UNIDADE DE PESQUISA DO MCTI

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

GABRIEL MOYSÉS DELFINO

DISTRIBUIÇÃO QUÂNTICA DE CHAVES: UM ESTUDO SOBRE A GERAÇÃO QUÂNTICA DE CHAVES CRIPTOGRÁFICAS CLÁSSICAS

Dissertação submetida ao corpo docente do Laboratório Nacional de Computação Científica como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências em Modelagem Computacional.

Aprovada por:

Prof. Renato Portugal, D.Sc.
(Presidente)

Prof. Antônio Tadeu Azevedo Gomes, D.Sc.

Prof. Guilherme Penello Temporão, D.Sc.

Documento assinado eletronicamente por **Antônio Tadeu Azevedo Gomes**, **Tecnologista**, em 29/02/2024, às 16:46 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Renato Portugal**, **Pesquisador Titular**, em 29/02/2024, às 16:51 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **guilherme penello temporao (E)**, **Usuário Externo**, em 01/03/2024, às 09:09 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.mcti.gov.br/verifica.html, informando o código verificador **11704077** e o código CRC **0F9D110A**.

Referência: Processo nº 01209.000098/2020-83 SEI nº 11704077

Dedicatória

Aos familiares e professores
sem os quais nada disso seria possível.

Agradecimentos

Ao Professor Renato Portugal cuja profunda erudição no campo da computação quântica foi uma fonte inestimável de conhecimento e valiosa orientação. Sua dedicação exemplar à pesquisa ao longo da vida juntamente de sua habilidade em comunicar conceitos complexos de maneira clara e perspicaz foram fundamentais para uma compreensão mais profunda dos princípios subjacentes à criptografia quântica, necessários para conclusão do trabalho em tela. A orientação precisa com indicação vasta de recursos acadêmicos ampliaram em muito meu entendimento da computação quântica e me capacitaram a enfrentar os desafios inerentes à pesquisa, campo tão dinâmico e complexo. Com discussões sempre enriquecedoras, questionamentos desafiadores e críticas valiosas, suas diretrizes metodológicas foram fundamentais para a elaboração deste trabalho.

À prestigiosa instituição do LNCC, que ressoa com significado profundo para todos aqueles que tiveram o privilégio de conhecê-la. Fui acolhido por sua impressionante estrutura acadêmica e também por sua comunidade vibrante e dedicada e, por isso, sou muito grato. Com sua tradição de busca incessante por conhecimento e sua dedicação ao avanço científico, abrangendo desde a exploração de fronteiras em pesquisa até a formação de mentes curiosas e ávidas por contribuir para o progresso da sociedade, sinto-me honrado em contribuir para a narrativa contínua de sua história fascinante de excelência acadêmica e busca pelo saber.

À IBM por disponibilizar acesso remoto a computadores quânticos, tendo sido uma notável contribuição para diversas pesquisas na área, incluindo esta. Sua iniciativa é, indubitavelmente, um marco significativo no avanço da pesquisa em computação quântica, não somente promovendo o desenvolvimento individual dos pesquisadores, mas também fomentando uma comunidade global de aprendizado e descoberta. Tal feito democratiza o acesso a uma tecnologia frequentemente vista como complexa e de alto custo, permitindo que pesquisadores, independentemente de suas afiliações institucionais, explorem as nuances da computação quântica, enriquecendo o cenário global da pesquisa na área.

Ao Exército Brasileiro cujo apoio foi imprescindível para conclusão dos estudos. Ao dar suporte para o projeto, o Exército Brasileiro não apenas demonstrou seu compromisso com o avanço do conhecimento e da investigação científica, mas também tornou possível a exploração aprofundada das nuances da computação quântica e da criptologia. O investimento evidenciou de maneira inquestionável seu comprometimento com o desenvolvimento intelectual e científico da sociedade brasileira como um todo, exemplificando seu papel social imprescindível no tocante aos avanços de tecnologia e ciência do nosso país.

"What quantum mechanics takes away with one hand,
it gives back with the other: a procedure known as
quantum cryptography or quantum key distribution."
Nielsen e Chuang (2011)

Resumo

A criptografia clássica utiliza suposições de dificuldade computacional, como a fatoração de grandes números, para garantir segurança na comunicação. Tal uso pode ser comprometido por avanços de hardware ou software, como a implementação do algoritmo de Shor pela computação quântica. O trabalho em tela explora a segurança da criptografia quântica atrelada inteiramente às leis da mecânica quântica, em um contexto no qual busca-se gerar, de forma segura, chaves clássicas por meios quânticos com a Distribuição Quântica de Chaves para posterior uso em algoritmos como o one-time-pad. A pesquisa teve foco na QKD dependente de equipamentos, mais especificamente dentro da categoria de preparação e medição, contemplando implementações práticas do protocolo de seis estados feitas no IBM Quantum Experience platform. Explora-se cenários ideais, ruidosos, com e sem adversários, analisando os resultados através do QBER. O trabalho abrange ainda conceitos sobre os procedimentos de pós-processamento de reconciliação da informação e amplificação privada, mencionando eventuais ataques quânticos e suas contramedidas, citando a distribuição quântica de chaves independente de dispositivos como uma das possíveis abordagens de solução.

Palavras-chave: Distribuição quântica de chave. Computação quântica. Criptografia. QKD dependente de dispositivos. Protocolo de seis estados.

Abstract

Classical cryptography relies on assumptions of computational difficulty, such as the factorization of large numbers, to ensure security in communication. This reliance becomes vulnerable to advancements in hardware or software, exemplified by the implementation of the Shor algorithm in quantum computing. The present work delves into the security of quantum cryptography, entirely anchored in the laws of quantum mechanics. It operates in a context where is sought to securely generate classical keys through quantum means using Quantum Key Distribution for subsequent use in algorithms like the one-time-pad. The research focused on device-dependent QKD, specifically within the prepare and measure category, encompassing practical implementations of the six-state protocol conducted on the IBM Quantum Experience platform. Ideal, noisy, adversarial, and non-adversarial scenarios are explored, analyzing the results through QBER. The work also encompasses concepts regarding post-processing procedures for information reconciliation and private amplification, in addition to mentioning potential quantum attacks and their countermeasures, citing independent device quantum key distribution as one of the possible solution approaches.

Keywords: Quantum Key Distribution. Quantum Computing. Cryptography. Device-Dependent QKD. Six states protocol.

Lista de figuras

Lista de tabelas

Lista de abreviaturas e siglas

AES	Advanced Encryption Standard
DES	Data Encryption Standard
DIQKD	Device-Independent Quantum Key Distribution
LNCC	Laboratório Nacional de Computação Científca
MDC	Maior Divisor Comum
MDIQKD	Measurement-Device-Independent Quantum Key Distribution
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
RSA	Rivest-Shamir-Adleman

Lista de símbolos

ϕ	Letra grega Phi minúscula
Φ	Letra grega Phi maiúscula
ψ	Letra grega Psi minúscula
Ψ	Letra grega Psi maiúscula
H	Porta de Hadamard
$\otimes$	Produto de Kronecker
$\dagger$	Dagger

Sumário

1 Introdução

1.1 O surgimento da criptografia clássica

Desde os tempos antigos a comunicação entre pessoas é um tópico de grande interesse para o homem. Nos primórdios, durante a pré-história, as sociedades humanas enfrentaram uma série de desafios inerentes a um ambiente naturalmente hostil. A falta de tecnologia, como conhece-se hoje, tornava extremamente desafiadoras práticas rotineiras de obtenção de alimentos e proteção contra ameaças ambientais e predatórias. A tenacidade e adaptabilidade dos ancestrais torna-se notória, porém destaca-se um grande aliado na luta pela sobrevivência: a possibilidade de compartilhar conhecimento; de se comunicar.

Diversas habilidades novas, como a domesticação do fogo, permitiam aos nossos antepassados uma maior chance de sobrevivência, fosse pela proteção a potenciais predadores ou pela melhora na qualidade do alimento ingerido. A utilização dessas habilidades e a evolução humana propriamente dita, contudo, foram possíveis devido à capacidade humana de passar o conhecimento obtido para as gerações futuras. Em um cenário no qual não houvesse comunicação tornaria-se inviável qualquer tentativa de utilizar o fogo ou até mesmo de produzi-lo, por exemplo. Milhares de anos seriam necessários em cada nova iteração de aprendizado e teria-se que, repetidamente, reinventar o que já fora feito anteriormente (HARARI, 2014). Todo esse contexto invalidaria a possibilidade de avanços tecnológicos ou de conhecimento na magnitude ocorrida.

A história da comunicação, portanto, é uma narrativa que se entrelaça intrinsecamente com a evolução da sociedade humana, transcendendo fronteiras geográficas e moldando os fundamentos da nossa existência em constante evolução. A habilidade de trocar informações e ideias tem sido o veículo por meio do qual as civilizações floresceram, os impérios se expandiram e as fronteiras do conhecimento humano foram constantemente redefinidas. No entanto, à medida que as conexões entre as mentes humanas se tornaram mais complexas, o mundo se tornou globalizado e as informações passaram a ter um viés de distribuição individualizado, emergiu uma necessidade crítica de garantir que as comunicações permanecessem seguras e protegidas contra acessos indesejados

Nesse contexto, a criptografia, palavra de origem grega que remete à escrita escondida, emerge almejando garantir confidencialidade das informações que fluem através dos canais de comunicação. A criptografia, através de diferentes técnicas e algoritmos, passou a oferecer então, em teoria, uma camada de segurança que garante que apenas os destinatários pretendidos tenham acesso ao conteúdo das mensagens. Sua importância, portanto, é profundamente entrelaçada com a própria essência da comunicação humana.

A criptografia, mais especificamente o campo da comunicação segura, permite que as sociedades expressem suas opiniões livremente, compartilhem segredos estratégicos e preservem sua privacidade pessoal, o que é garantido pela encriptação de e-mails e mensagens de texto, também utilizada em termos de segurança bancária, comunicações militares, governamentais e até no mercado de ações.

> An important subfield of cryptography is secure communication, which nowadays mainly involves electronic data such as encrypting emails and other plain-text messages, online banking security, and communication related to the military, governments, and the financial market.(RENNER, 2022).

A participação da criptografia em transações bancárias e sua íntima relação com o sistema financeiro, citado aqui com mais destaque, é fundamental no mundo contemporâneo no qual o patrimônio de uma vida inteira pode estar representado unicamente por dígitos virtuais dentro do sistema financeiro. Na hipótese de uma falha tecnológica grave envolvendo os dados e as transações, ocasionado, por exemplo, por uma quebra de confiabilidade das mesmas, o mundo enfrentaria uma total ruptura de seu sistema financeiro. A criptografia, então, passou a fazer parte do cotidiano das pessoas, sendo um conjunto de técnicas essencial para o correto funcionamento da troca de informações do mundo contemporâneo.

Entretanto, embora extremamente relevante no mundo contemporâneo, o surgimento da criptografia remonta a tempos antigos, estando entrelaçado com a necessidade de manter comunicações confidenciais e proteger informações sensíveis. Desde civilizações antigas há indícios de seu uso, sendo um dos exemplos mais notáveis da história da criptografia a utilização pelo imperador romano Júlio César, que empregava a Cifra de César para proteger mensagens militares (SINGH, 2000).

1.1.1 A cifra de César

A Cifra de César, também conhecida como Cifra de Troca ou Código de César, é uma das mais simples e antigas técnicas de criptografia conhecidas. Atribuída a Júlio César, renomado líder militar e estadista romano, essa técnica envolve a substituição de cada letra em um texto pelo caractere que se encontra um número fixo de posições adiante no alfabeto. Esse número é conhecido como "*chave*" ou "*deslocamento*" (SINGH, 2000).

No caso do imperador romano, a chave utilizada era o número 3, resultando em um deslocamento fixo de 3 letras seguintes do alfabeto. Era, portanto, uma cifra de substituição monoalfabética. Nesse sentido, a letra "A" seria substituída por "D", ao passo que a letra "D" seria substituída pela letra "G", e assim por diante, em um processo que pode ser entendido como o acréscimo da letra "C" na cifragem e o decréscimo da mesma letra "C" na decifragem. Essa técnica simples, embora primitiva, já quebra a estrutura do texto original, dificultando a compreensão imediata por parte de alguém que não conheça a chave de deslocamento.

A título de exemplo, o texto cifrado

"R vlvwhpd ilqdqfhlur dwxdo qãr halvwluld vhp d fulswrjudild".

significaria

"O sistema financeiro atual não existiria sem a criptografia".

Enquanto a Cifra de César era eficaz contra ameaças da época, com sistemas de quebra de criptografia pouco rebuscados ou inexistentes, como mensagens interceptadas por espiões sem conhecimento da chave, ela é facilmente decifrada através de algoritmos atualmente conhecidos, como tentativa e erro, especialmente considerando as limitações do alfabeto latino e a pequena quantidade de chaves possíveis. Um exemplo de quebra criptográfica de um texto escrito em português com deslocamento de caracteres a partir de um número fixo poderia ser feito testando todas as 26 possibilidades do alfabeto, dado a existência de 26 letras: em algum dos casos acertaria-se a combinação pretendida com a decodificação do texto e poder-se-ia ler a mensagem em claro, decriptografada. No entanto, a cifra de César é um exemplo seminal na história da criptografia, ilustrando o princípio básico de substituição de caracteres e fornecendo um ponto de partida para o desenvolvimento de técnicas mais sofisticadas. (SINGH, 2000).

1.1.2 Outras técnicas clássicas simétricas

Ao longo da história muitas foram as cifras implementadas por diferentes países e culturas. Em uma análise intuitiva a respeito daquilo que sucederia a cifra de César, poderia-se pensar em uma cifra cujo deslocamento não fosse a partir de um número fixo, mas variando letra a letra. Nesse sentido, ao invés de sempre codificar a mensagem com o deslocamento de 3 letras, poderia-se deslocar primeiro com 3 letras, depois com 6, depois com 7, com 2, com 4, enfim, gerando uma criptografia muito mais forte a partir de uma "palavra senha" e não uma "letra senha". Essa estratégia de fato existiu e ficou conhecida como Substituição polialfabética e tem, como um dos exemplos mais notórios da história, a Cifra de Vigenère, cuja implementação é uma sequência de Cifras de César (SINGH, 2000).

Em uma análise preliminar, pode-se pensar que o resultado final é um texto cifrado seguro, cuja decodificação seria difícil de ser obtida. O pensamento origina-se da ideia que testar diferentes combinações de letras é mais trabalhoso do que tentar apenas uma letra, caso trivial. Entretanto, a repetição da palavra senha, que pode ou não ter um significado a ela associado, cria certos padrões na escrita. É importante ressaltar que a palavra senha não necessariamente é uma palavra presente no dicionário, podendo ser um conjunto de caracteres totalmente randômico. Apesar disso, quando a mensagem a ser codificada é

longa em relação à chave ocorrem repetições que levam à geração de padrões. As vogais no português, por exemplo, aparecem com muito mais frequência do que letras como “x”, “y” ou “z” (SOUSA; PIRES, 2018). Além disso, a utilização de artigos curtos como “a”, “o” ou palavras monossilábicas no geral, como “de”, “ou”, “ao” podem facilitar o trabalho de decodificação das mensagens, por criarem pequenos padrões.

> Given an encrypted sequence, a key and a decryption of that sequence, can we reconstruct the decryption function? We might begin by looking for small patterns shared by the two sequences. When we find these patterns, we can piece them together to create a rough model of the unknown function. Next, we might use this model to predict the translations of other sequences. Finally, we can refine our model based on whether or not these guesses are correct(GREYDANUS, 2017).

Tal estratégia foi adotada na quebra criptográfica mais importante da história bélica da humanidade: a decriptografia da máquina Enigma. A máquina Enigma foi uma máquina criptográfica baseada em rotores utilizada amplamente pela Alemanha nazista e seus aliados durante a Segunda Guerra Mundial. Apesar de semelhante as estratégias de criptografia polialfabéticas supracitadas, a máquina Enigma possuía o grande diferencial de utilizar diferentes alfabetos nas suas codificações. A codificação a ser realizada dependia da escolha de diferentes rotores, diferentes configurações de anéis e diferentes posições iniciais. O seu funcionamento era transparente para o operador que, ao pressionar uma tecla na máquina, semelhante a uma máquina de escrever conforme ilustrado na Figura 1, percebia ser ascendida uma lâmpada associada a uma outra letra, provavelmente diferente da letra digitada: seria a letra criptografada. A máquina, por possuir diferentes rotores em movimentação, faria com que uma nova letra criptografada fosse acesa em seguida mesmo no caso da mesma letra em claro ser pressionada, já que suas partes móveis alterariam a posição. O processo de decriptografia era similar e utilizaria o inverso da chave de criptografia, por ela ser simétrica, devendo ao operador a tarefa de realizar a configuração inicial e datilografar a mensagem, em claro ou criptografada a depender da tarefa pretendida (REJEWSKI, 1981).

Mais de uma versão da máquina existiu e foi para o mercado, com diferentes possibilidades de criptografia associadas. Na versão M3, por exemplo, escolhia-se três rotores diferentes dentre cinco opções disponíveis, uma posição de início com qualquer uma das letras do alfabeto para cada rotor e também uma configuração de anel para o qual o rotor mais à direita forçaria a mudança do rotor do meio e uma configuração de anel para o rotor do meio. Ao posicionar o primeiro rotor, portanto, escolheria-se entre cinco disponíveis, havendo 5 possibilidades. Para o segundo rotor, deve-se escolher um dentre os quatro remanescentes, e para o último rotor, deve-se escolher um entre os três restantes, levando a um total de $5 \times 4 \times 3 = 60$ possibilidades para os rotores. Em relação à posição inicial de cada rotor cada um poderia escolher uma letra de ínicio dentre as 26 disponíveis,

Figura 1 – Máquina Enigma

Fonte: Computing (2023)

sem preocupações com repetições. Nesse sentido, teria-se um total de $26 \times 26 \times 26 = 17.576$ possibilidades. Por fim, a configuração do rotor mais a direita poderia ser uma dentre 26 diferentes, uma para cada letra do alfabeto. O mesmo valia para o rotor do meio, levando a um resultado de $26 \times 26 = 676$ possibilidades. Por fim, as máquinas enigmas ainda permitiam a combinação de letras par a par através de dez cabos diferentes no qual a conexão de uma letra "a" a uma letra "b" faria com que ao se pressionar a letra "a" a criptografia seguisse o caminho como se houvesse sido pressionada a letra "b". Dentro do contexto de 26 letras diferentes, escolher 10 pares significa uma combinação superior a 150 trilhões de combinações (REJEWSKI, 1981).

Em resumo, pode-se dizer que a quantidade de combinações possíveis para a criptografia da máquina enigma era exorbitante, então, mesmo que o exército que fazia oposição ao Alemão possuísse uma máquina enigma seria extremamente improvável que ele conseguisse configurar a máquina de maneira a realizar uma criptografia assertiva. Entretanto, sabe-se que a criptografia da máquina foi quebrada. Tal resultado foi obtido através de uma grande cooperação internacional de engenheiros, criptógrafos e matemáticos, analisando diversos padrões das mensagens alemãs, aproveitando-se do fato de diversas mensagens diferentes serem enviadas ao longo do dia com as mesmas configurações iniciais e utilizando exaustivamente de meios eletromecânicos, que poderiam ser entendidos

como máquinas de decriptografar ou máquinas de calcular, um nome alternativo para computadores (REJEWSKI, 1981).

1.2 A relação entre a criptografia e o tempo

Ao longo do detalhamento do funcionamento da máquina Enigma ficou evidente o poder teórico alcançado em termos de criptografia pela sua utilização, o que é notoriamente comprovado pela história dada a extensa gama de mensagens que foram trafegadas em canais públicos durante meses pelo exército Alemão sem qualquer possibilidade de decodificação pelo exército inimigo. Apenas através de uma conjuntura de fatores específicos e pela cooperação entre diversos países, reunindo grandes mentes brilhantes ao redor do mundo, foi possível almejar a quebra da máquina (REJEWSKI, 1981). Entretanto, um fato da história ganha destaque: a utilização das máquinas de calcular, citadas através da utilização dos meios eletromecânicos. Essa ferramenta de decriptografia, entendida aqui como um computador, foi fundamental para o sucesso da decriptografia.

Existem, contudo, limites para aquilo que um computador pode fazer, principalmente quando fala-se em problemas matemáticos e o número de operações necessários para resolvê-lo. Mesmo já diante do contexto de funcionamento da máquina Enigma, tendo tido a exploração quase completa de suas configurações, não seria nada trivial para os matemáticos e engenheiros, por mais brilhantes que fossem, fazer, em um tempo razoável, a quebra da criptografia sem o apoio de uma máquina de calcular robusta. No contexto atual, de supercomputadores que realizam quatrilhões de operações por segundo, o tempo de decriptografia seria ainda menor, promovendo uma eficiência que poderia ser crucial no desenrolar da guerra.

Tal afirmação deriva do fato do tempo ser um parâmetro extremamente relevante quando se fala de criptografia. Isso fica evidenciado devido à utilidade das mensagens poder ser real apenas durante um intervalo de tempo limitado, um escopo de contexto bem definido e demarcado. No contexto da Segunda Guerra Mundial, por exemplo, de nada adiantaria a decriptografia de uma mensagem de ataque a determinado ponto geográfico após o ataque já ter sido executado e percebido: seria uma informação tardia e essencialmente inútil; a informação deixa de ser relevante no momento em que já temos o fato concluído. Um exemplo seria a decodificação de um token de acesso após a validade do mesmo ter expirado: de nada vale a informação de como teria sido possível ganhar acesso no passado.

Nesse contexto, dentro do qual é extremamente relevante realizar decodificação de mensagens em um tempo razoável, pode-se pensar em estimar a segurança de determinado algoritmo pelo tempo que seria gasto na decodificação da chave associada. Assume-se, portanto, a hipótese de que alguns problemas são difíceis em termos da complexidade

computacional associada. Diversos algoritmos recaem nessa categoria cuja estratégia, em resumo, seria criar problemas difíceis de serem resolvidos, demandando tempo excessivo para a quebra e garantindo uma comunicação segura enquanto a decifragem ainda está sendo calculada. A expectativa, nesse contexto, é que, no momento no qual a resolução do problema aconteça levando à quebra de sigilo do algoritmo, a informação não será mais útil, tendo se tornado já obsoleta.

> The security of classical protocols is usually based on the assumption that certain problems are hard in terms of their computational complexity. Widely used algorithms that fall into this category are the Diffie-Hellman key exchange method, which relies on the hardness of the discrete logarithm problem, and the RSA cryptosystem, whose security depends on the practical difficulty of factoring the product of two large prime numbers.(RENNER, 2022).

1.2.1 Criptografia Assimétrica e o RSA

Dentro do contexto de desenvolver problemas difíceis, cujo cálculo computacional levaria um tempo exaustivo, surgiu a ideia de utilizar o problema da fatoração de números grandes em seus fatores primos, mais especificamente através do algoritmo RSA (Rivest-Shamir-Adleman). Sendo um dos algoritmos de criptografia assimétrica mais amplamente usados para comunicação segura e assinatura digital, foi proposto por Ron Rivest, Adi Shamir e Leonard Adleman em 1978, tendo representado uma revolução em termos do que se conhecia a respeito de algoritmos de criptografia seguros(STALLINGS, 2021).

Diferentemente da Cifra de Cesar ou da própria máquina Enigma, citadas anteriormente como chaves simétricas, o algoritmo RSA é, como dito, um algoritmo de chaves assimétricas, possuindo portanto um par de chaves: uma chave pública e uma chave privada. A ideia é que apenas o dono do par de chaves possua a chave privada, cabendo apenas a ele o poder de decriptografar mensagens que tenham sido criptografadas utilizando sua chave pública. Nesse sentido, garante-se que qualquer pessoa que esteja de posse da chave pública do usuário conseguirá encaminhar para ele mensagens em sigilo, já que apenas detentores da chave privada poderiam decifrar a mensagem. Em contrapartida, qualquer mensagem criptografada com a utilização da chave privada, a chamada assinatura digital, poderia ser lida utilizando a chave pública do par de chaves, ficando garantida a autenticidade da mensagem feita pelo dono original do par de chaves, dado que apenas esse dono teria acesso à chave privada e, portanto, apenas ele poderia gerar tal mensagem criptografada, ou seja, apenas ele poderia ter assinado a mensagem (STALLINGS, 2021).

1.2.2 Implementação do RSA

Na implementação do algoritmo RSA, algumas etapas são necessárias para gerar as chaves e realizar operações de criptografia e descriptografia. Abaixo, descrever-se-á cada

etapa em detalhes, seguindo o originalmente exposto em (RIVEST; SHAMIR; ADLEMAN, 1978).

1.2.2.1 Geração de Chaves

Para começar, um usuário gera um par de chaves RSA. Isso envolve dois passos principais:

1. Escolher dois números primos grandes, p e q.
2. Calcular o produto $n = p \cdot q$. O número n é usado como parte da chave pública e da chave privada. Dado o fato que p e q são números primos grandes a fatoração de n não é um cálculo trivial.

1.2.2.2 Cálculo da Função Totiente de Euler

A função $\phi(n)$ de Euler é calculada. Ela representa o número de inteiros positivos menores que n e coprimos com n. Para o RSA, $\phi(n)$ é calculado como $(p-1) \cdot (q-1)$. Estando de posse dos valores de p e q é imediato o cálculo de $\phi(n)$. Entretanto, no caso de não possuir os valores de p e q, apenas de n, o cálculo de $\phi(n)$ é extremamente complexo.

1.2.2.3 Escolha da Chave Pública

Um número inteiro e positivo e é escolhido como a chave pública. O número e deve ser escolhido de forma que seja coprimo com $\phi(n)$, ou seja, o maior divisor comum entre e e $\phi(n)$ seja 1.

1.2.2.4 Cálculo da Chave Privada

A chave privada é calculada usando o expoente privado d, que é a inversa multiplicativa de e modulo $\phi(n)$, ou seja, $(d \cdot e) \equiv 1 \pmod{\phi(n)}$. Percebe-se, então, que só é trivial calcular d dado o fato de que é sabido o valor de $\phi(n)$. Para alguém que não seja proprietário do par de chaves, sem conhecimento de p e q torna-se extremamente custoso calcular o $\phi(n)$, tornando inviável a descoberta de d.

1.2.2.5 Criptografia

Para criptografar uma mensagem M usando a chave pública (n, e), ela é elevada à potência e e depois reduzida modulo n. O resultado é a mensagem criptografada C: $C = M^e \pmod{n}$.

1.2.2.6 Descriptografia

Para descriptografar a mensagem criptografada C usando a chave privada (n, d), ela é elevada à potência d e depois reduzida modulo n. O resultado é a mensagem original M: $M = C^d \pmod{n}$.

Percebe-se então que para decriptografar a mensagem é necessário ter d, cujo cálculo não é trivial a partir de e e n dada a escolha em segredo de p e q como primos grandes.

1.2.3 Segurança associada ao RSA

A segurança do algoritmo RSA repousa na complexidade computacional da fatoração de n em seus fatores primos p e q. Essa tarefa é amplamente reconhecida como um problema computacionalmente difícil, que requer uma quantidade significativa de tempo e recursos computacionais para ser resolvida (STALLINGS, 2021).

1.2.3.1 Ausência de medida de segurança definitiva

Um problema associado à definição de tempo gasto para resolução de problemas complexos seria a dificuldade em corretamente mapear uma medida de segurança associada. Em outras palavras, não é possível mapear diretamente a medida de segurança associada a uma chave dado que a conclusão basearia-se apenas em estimativas do custo computacional envolvido na quebra e na capacidade atual dos computadores mais modernos conhecidos (RENNER, 2022). Outro problema, derivado da forma como são feitos os cálculos de segurança prevista, englobariam o surgimento de computadores mais poderosos e também o surgimento de algoritmos mais eficientes, sendo um ponto extremamente negativo da criptografia clássica assimétrica e exemplo notório de suas limitações.

1.3 Limites da criptografia clássica

O gasto envolvido na fatoração de números em primos, conforme anteriormente citado, promove, de fato, uma proteção ao segredo pretendido. Entretanto, a segurança promovida está intrinsecamente relacionada ao tempo gasto para fatorar n, conforme visto. Em outras palavras, quanto mais poderoso fosse o equipamento utilizado na fatoração de n, mais cálculos por segundo seriam feitos e, em um âmbito geral estatístico do resultado esperado, menor tempo seria gasto na fatoração do número n. Consequentemente, menos tempo seria esperado para quebrar o algoritmo. De maneira similar, caso houvesse um algoritmo eficiente para a fatoração de números nos seus primos poderia-se, de maneira menos custosa e consequentemente mais rápida, calcular p e q a partir de n, dado que esses são produtos imediatos de sua fatoração. Nesse contexto, teria-se o cálculo de $\phi(n)$ e, em

seguida, de d feitos de maneira direta, o que ocasionaria a quebra do algoritmo RSA em tempo potencialmente curto o suficiente para que a informação da senha e da mensagem criptografada fossem relevantes. A existência de um supercomputador rápido o suficiente para executar os cálculos de fatoração, mesmo se feitos da maneira clássica como temos hoje, ou o surgimento de um algoritmo com potencial de realizar a fatoração de maneira mais eficiente fariam, portanto, com que o algoritmo RSA passasse a ser entendido como inseguro.

> Basing the security of a cryptographic system on the difficulty of mathematical problems has its issues: Although it is widely believed to be true that factoring large number on a classical computers is hard, it has not yet been proven despite decades of exhaustive research in this area. As long as the hardness of this and other problems that cryptography is based on is only a conjecture, it is always possible that an efficient algorithm is found to solve them, making cryptographic schemes built on them effectively unsafe.(RENNER, 2022).

De uma maneira geral, pode-se dizer que a segurança dos algoritmos clássicos, como o RSA, está enfrentando um desafio constante devido à evolução contínua do hardware de computação e às descobertas algorítmicas. A crescente capacidade computacional, aprimoramentos em técnicas de ataque e descoberta de novos algoritmos estão, gradualmente, expondo vulnerabilidades em algoritmos que, até então, eram considerados seguros (SMITH, 2020; JONES, 2019; BROWN, 2021).

> Classical algorithms (including post-quantum ones) become increasingly insecure over time due to evolution of hardware and algorithmic discoveries.(RENNER, 2022).

1.4 Estrutura do trabalho em tela

Ao longo do capítulo 2, almejando fornecer maior detalhamento sobre o contexto de utilização de algoritmos criptográficos clássicos que, assim como o RSA, confiam exclusivamente em uma complexidade computacional associada, o estudo abordará uma possível solução alternativa resiliente a ataques de força-bruta, apresentando o one-time-pad. Ainda nesse capítulo, discutir-se-á a dificuldade logística de distribuição de chaves associada ao one-time-pad e mencionar-se-á os algoritmos de Shor e de Grover como potenciais riscos a segurança clássica baseada em complexidade computacional.

Adiante, dentro do capítulo 3, o trabalho discutirá a possibilidade de contornar o problema logístico associado a utilização do one-time-pad com a implementação da distribuição quântica de chaves. O estudo tem foco em uma distribuição quântica de chaves dependente de equipamentos e que utiliza protocolos de preparação e medição, mais especificamente o protocolo de seis estados. Ainda neste capítulo, serão feitas também

menções breves aos protocolos BB84, B92, que também são protocolos de preparação e medição, e ao protocolo de Ekert, um protocolo de emaranhamento.

No capítulo 4, o trabalho apresentará um estudo prático utilizando o IBM Quantum Experience platform de implementação do protocolo de seis estados simulado. Busca-se analisar o problema da quantidade de ruído associada a medições em um computador quântico explorando cenários ideais, ruidosos, com e sem adversários simulados. O objetivo final é diferenciar os resultados percebidos quando há ocorrência de medições indevidas dos casos onde existe apenas o ruído do meio-ambiente, visando responder se o impacto das medições poderia, por exemplo, ser pequeno o suficiente para que um eventual atacante conseguisse camuflar sua presença em meio ao ruído mesmo realizando medições em todos os qubits. Espera-se que o ruído associado aos casos com medições indevidas seja grande o suficiente para evidenciar a presença de um atacante que não teve sucesso em camuflar seus vestígios, sendo esse resultado uma das contribuições associadas ao trabalho em tela.

Ainda no contexto do capítulo 4, será apresentada também uma comparação entre os resultados associados a execução de um dado circuito em um computador quântico real e a sua execução em um ambiente simulado com a adição de um modelo de ruídos construído com erros de backend ligados ao referido computador quântico utilizando a biblioteca do QisKit. A contribuição associada à comparação é evidenciar se, para tais experimentos, a simulação apresentou resultados próximos o suficiente da execução real. Espera-se que a simulação com adição de um modelo de ruídos construído com erros de backend apresente resultados próximos da execução real no computador quântico. A análise de resultados realizada ao longo de todo o capítulo utilizou como parâmetro de avaliação a Taxa de Erro de Bit Quântico. O capítulo também engloba menções aos casos nos quais ocorre erro de decodificação da base de medição por *Bob* e uma citação à possibilidade de geração de números verdadeiramente aleatórios utilizando o computador quântico.

Ao longo do capítulo 5, mais descritivo, discutir-se-á de forma breve a importância dos procedimentos executados após a comunicação, citando os procedimentos de pós-processamento de reconciliação da informação e amplificação privada, associados aos cenários de implementação de uma distribuição quântica de chaves. Além disso, o capítulo mencionará os ataques hackers quânticos de photon number splitting attack, time-shift attack, detector blinding attack, trojan-horse attack e a possibilidade de ataques coerentes, dada a tecnlogia teoricamente infinita do adversário. Cita-se, ao final, possíveis contramedidas associadas aos ataques, mencionando, por fim, as estratégias de DI-QKD e MDI-QKD como potenciais soluções às vulnerabilidades dos protocolos de QKD dependentes de equipamentos geradas por falhas no comportamento dos dispositivos.

No capítulo 6, de conclusão, contextualizar-se-á o trabalho e abordar-se-á de forma sucinta conclusões associadas aos resultados obtidos ao longo do trabalho, principalmente associadas aos experimentos discutidos no capítulo 4. O capítulo 6 ainda possui uma breve

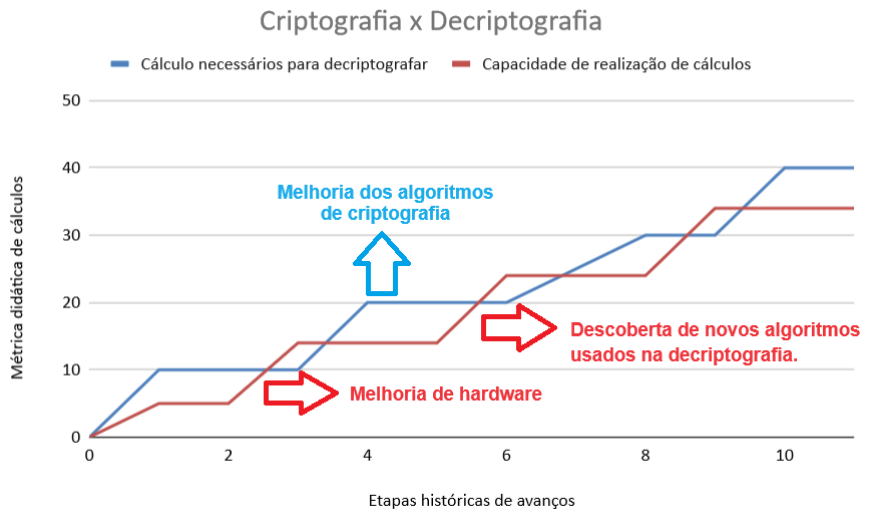
citação de estudos futuros, indicando os modelos de Distribuição Quântica de Chaves baseados na comunicação via satélites como um campo fértil de pesquisa. A indicação do tópico como possibilidade de estudos futuros baseia-se na capacidade teórica desses modelos transcenderem as limitações impostas por uma infraestrutura terrestre, estabelecendo, assim, a possibilidade de comunicação segura também a longas distâncias.

2 Os riscos de utilizar a complexidade computacional como parâmetro de segurança

Em resumo, os desafios que afetam a segurança dos algoritmos clássicos, exemplificados pelo RSA, são uma realidade em constante evolução. A contínua melhoria na capacidade computacional, bem como as constantes inovações nas técnicas de ataque e as descobertas de novos algoritmos estão, como dito, gradualmente expondo vulnerabilidades em sistemas criptográficos que, anteriormente, eram considerados robustos e seguros (SMITH, 2020; JONES, 2019; BROWN, 2021).

A ideia pode ser representada como uma corrida entre os avanços dos algoritmos de criptografia ou nos seus requisitos que, a cada momento, exigem maior número de cálculos computacionais para serem quebrados e os avanços de hardware ou de algoritmos de quebra propriamente ditos, que tornam os cálculos mais rápidos por maior processamento ou por maior eficiência (RENNER, 2022). Sempre que ocorre alguma evolução de hardware ou a descoberta de um novo algoritmo mais eficiente no tangente à decriptografia, uma nova melhoria nos algoritmos de criptografia deve ser proposta para manter a segurança das mensagens dos utilizadores dos algoritmos. A Figura 2 ilustra a supracitada eterna disputa entre os dois lados principais da criptologia, a criação de algoritmos cada vez mais robustos e resistentes e a elaboração de estratégias de quebra cada vez mais elaboradas e eficientes.

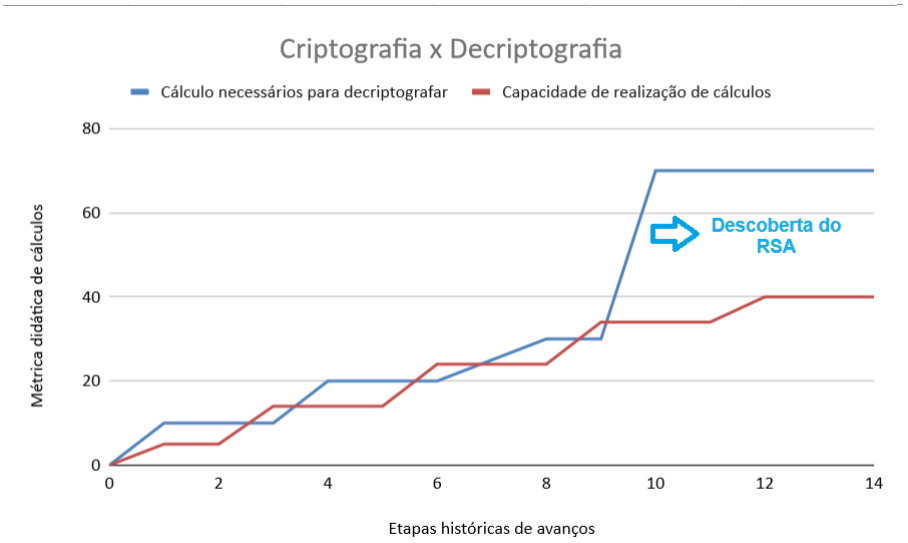
Figura 2 – Criptografia x Decriptografia



Fonte: autoria própria inspirada em (RENNER, 2022)

Conforme mencionado anteriormente, o algoritmo RSA é amplamente reconhecido como um dos pilares da criptografia moderna. Sua robustez e segurança são notáveis devido à complexidade envolvida na fatoração de números inteiros grandes em seus fatores primos. O RSA, durante seu surgimento e durante muitos anos, ofereceu um sistema de chave pública confiável que desempenha ainda hoje um papel fundamental na segurança da comunicação digital e na autenticação de informações. Seu uso, generalizado em aplicativos que exigem alta segurança, como transações financeiras e comunicação segura, é um testemunho de sua eficácia e resiliência ao longo do tempo (STALLINGS, 2021). Nesse sentido, a representação gráfica de sua descoberta poderia ser didaticamente ilustrada conforme feito na Figura 3.

Figura 3 – Criptografia x Decriptografia com RSA



Fonte: autoria própria inspirada em (RENNER, 2022)

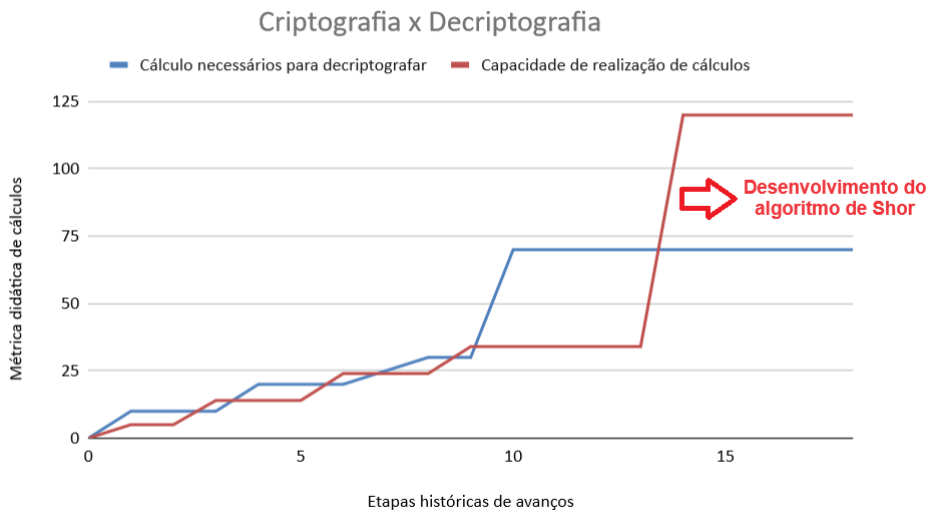
Entretanto, um fato novo surgiu devido aos avanços de pesquisa associados à computação quântica: a descoberta de algoritmos que ameaçam, em muito, a segurança associada às estratégias de criptografia utilizadas pelo RSA. No caso da fatoração de números em primos propriamente dito, problema matemático computacionalmente custoso utilizado pelo RSA, um algoritmo mais recente com potencial de eficientemente realizar tal fatoração e a consequente quebra da segurança do RSA já existe no contexto quântico: o algoritmo de Shor (SHOR, 1994).

> With the imminent advent of quantum computing devices comes another complication that can arise when relying on the hardness of specific tasks: There are types of computations, such as quantum computation, that cannot be sorted into classical complexity classes. Although integer factorization and the discrete logarithm problem are believed to be hard for classical computers, there exists a quantum algorithm that can solve them in polynomial runtime, namely Shor's algorithm.(RENNER, 2022).

A descoberta do algoritmo de Shor é tão impactante que, por si só, já exemplifica o título adotado neste capítulo: a implementação prática do algoritmo e a consequente possibilidade de eficientemente fatorar números grandes em primos é sim uma grande ameaça à confiabilidade associada ao RSA, representando uma quebra de segurança desse que é um dos mais notórios algoritmos clássicos de chaves assimétricas. A representação gráfica de sua descoberta poderia ser didaticamente ilustrada conforme feito na Figura 4.

Os dados utilizados na geração das Figuras 2, 3 e 4, presentes neste capítulo, estão registrados, para fins de documentação, no Apêndice B.

Figura 4 – Criptografia x Decriptografia com Shor



Fonte: autoria própria inspirada em (RENNER, 2022)

2.1 Algoritmo de Shor

O algoritmo de Shor é um marco na computação quântica. Proposto por Peter W. Shor em 1994 (SHOR, 1994), este algoritmo desafia a segurança de sistemas de criptografia baseados na dificuldade de fatoração de números inteiros grandes em seus primos constituintes, como mencionado. O processo de fatoração é conhecido por ser computacionalmente demorado em sistemas clássicos, tornando, como dito, o RSA e outros sistemas de criptografia similares teoricamente robustos contra ataques através da fatoração. No entanto, Shor demonstrou que a computação quântica tem o potencial de fatorar números inteiros grandes de forma eficiente.

> Shor's algorithms were presented at a conference in 1994, the full paper was published in 1997, and reviewed in 1999. It describes two quantum algorithms for integer factoring and discrete logarithm exponentially

> faster than the best-known classical algorithms. It is a remarkable and celebrated scientific contribution to quantum computing. (PORTUGAL, 2022).

Dada sua irrefutável importância, o algoritmo de Shor foi amplamente discutido e apresentado em muitos livros ao longo dos anos (PORTUGAL, 2022; HIDARY, 2019; KAYE; LAFLAMME; MOSCA, 2007; MERMIN, 2007; NAKAHARA; OHMI, 2008; RIEFFEL; POLAK, 2011; SCHERER, 2019; STOLZE; SUTER, 2008; YANOFSKY; MANNUCCI, 2008). Apresentando o algoritmo de forma sucinta, pode-se dividi-lo em três etapas principais: um pré-processamento clássico, um processamento quântico e, por fim, um pós-processamento, também clássico. Espera-se que, dada a entrada de um número N composto, ocorra a saída pretendida de um fator não trivial de N, entendido aqui como fatores triviais de N o número 1 e o próprio número N.

A saída pretendida de um fator não trivial de N, contudo, não é alcançada em todas as execuções do algoritmo, existindo casos nos quais é necessário uma nova execução do mesmo. Combinando as probabilidades de sucesso das etapas de processamento quântico e de pós-processamento clássico, dado que o pré-processamento clássico não apresenta problemas de eficiência, obtêm-se o caso geral de probabilidade de sucesso, cujo valor pode ser ainda multiplicado por $\frac{3}{4}$ ao entender o algoritmo como um algoritmo Monte Carlo, sem o retorno aos passos anteriores do algoritmo (PORTUGAL, 2022). Entendendo r como a ordem multiplicativa de a módulo N, com a sendo um número natural aleatório tal que $1 < a < N$, a probabilidade de sucesso de todas as etapas em conjunto pode ser descrita como:

$$p_{\text{sucesso}} = \frac{3}{4\pi^2 ln(ln(r))} \tag{2.1}$$

O número médio de execuções necessárias do algoritmo para encontrar um fator não trivial de N é $\frac{1}{p_{\text{sucesso}}}$ (PORTUGAL, 2022). Em seu trabalho, Shor mostrou que o número de execuções necessárias do algoritmo para encontrar uma solução é $\mathcal{O}(\log \log r)$ (SHOR, 1994).

2.1.1 Consequências da implementação do algoritmo de Shor para o RSA

Dado a eficiência comprovada do algoritmo de Shor em computadores quânticos para realização da fatoração de um número N em seus fatores não triviais, ocorre a possibilidade de fatorar eficientemente um número n composto pela multiplicação de dois números primos p e q grandes. Em outras palavras, conforme antecipado no inicio do capítulo, o resultado imediato de uma eventual implementação do algoritmo de Shor é a possibilidade de quebrar a segurança de sistemas de criptografia baseados em fatoração de números primos, como é o caso do RSA.

> If there exists an efficient quantum algorithm for breaking it (which is the case for RSA), the scheme will immediately become insecure once the first universal quantum computer is built (RENNER, 2022).

Caso houvesse disponibilidade de se ter um computador quântico com 20 milhões de qubits físicos (ruidosos) para uso, por exemplo, o tempo estimado para fatorar um inteiro de 2048 bits, tamanho usualmente associado ao RSA, seria de 8 horas assumindo que apenas uma execução da parte quântica do algoritmo é necessária (GIDNEY; EKERA, 2021). Caso o número de qubits ruidosos disponíveis estivesse na casa das dezenas de milhares, com 13436 qubits físicos disponíveis, a expectativa é que, utilizando uma memória multímodo, a fatoração de inteiros de 2048 bits levaria aproximadamente 177 dias (GOUZIEN; SANGOUARD, 2021). Entretanto, no contexto atual, a implementação prática em um computador quântico do algoritmo de Shor para quebrar o RSA em um tempo razoável ainda não é possível. Até o ano de 2023, um dos computadores quânticos com maior número de qubits era o Osprey da IBM, tendo 433 qubits (KAM et al., 2023).

2.2 Algoritmo de Grover

Embora o trabalho em tela tenha até aqui abordado apenas os impactos que os avanços da computação quântica podem trazer para a criptografia assimétrica, com foco na ameaça que o algoritmo de Shor traz para os algoritmos que utilizam da dificuldade em fatorar números grandes em seus primos, como o RSA, é válido mencionar também o algoritmo de Grover devido a possibilidade de utilizá-lo em ataques de força bruta visando quebrar a criptografia simétrica.

O algoritmo de Grover, também conhecido como algoritmo de busca quântico (NIELSEN; CHUANG, 2011), é um algoritmo referência da computação quântica quando se fala de busca, tendo sido proposto por Lov Grover em 1996 (GROVER, 1996). Em seu trabalho, Grover tinha como objetivo encontrar com alta probabilidade um número específico dentre N possíveis sem ter qualquer conhecimento prévio sobre o conjunto total de números. Em termos clássicos, esse problema precisaria de $\mathcal{O}(N)$ operações para ser resolvido (NIELSEN; CHUANG, 2011), porém Grover conseguiu fazê-lo em $\mathcal{O}(\sqrt{N})$ passos (GROVER, 1996), fornecendo uma aceleração quadrática para a busca.

2.2.1 Consequências da implementação do algoritmo de Grover para criptografia simétrica

O resultado da aceleração quadrática para a busca trazido pelo algoritmo de Grover para a criptografia está na possibilidade de utilizar o algoritmo de busca em ataques de força bruta a esquemas criptográficos de chave simétrica. Segundo (MAVROEIDIS et al., 2018), foi defendido por (BONE; CASTRO, 1997) a possibilidade de utilizar o algoritmo

de Grover para quebrar o algoritmo Data Encryption Standard (DES), que baseia sua segurança em uma chave de 56-bits, tendo afirmado que foram necessárias apenas 185 buscas para encontrar a chave.

O resultado da utilização do algoritmo de Grover para quebrar algoritmos criptográficos de chave simétrica, contudo, não é tão impactante quanto a utilização do algoritmo de Shor para quebrar algoritmos que utilizam da complexidade computacional atrelada à fatoração de números grandes, já que o algoritmo de Grover não é tão surpreendentemente rápido quanto o de Shor e dado que os os criptógrafos podem compensar a ameaça escolhendo chaves maiores (BERNSTEIN; DAHMEN; BUCH, 2010).

Para a criptografia simétrica, portanto, a computação quântica não é vista como uma ameaça tão grande neste momento para (MAVROEIDIS et al., 2018), que cita ainda o Advanced Encryption Standard (AES) como resiliente à computação quântica desde que sejam usadas chaves de 192 ou 256 bits. A contramedida de aumentar as chaves é tida como eficiente também por (RENNER, 2022), que cita que o esquema AES com chave de 256 bits é considerado resiliente a computação quântica pois, considerando ataques de força bruta, esquemas com chave de 256 bits seriam, para o computador quântico, tão difíceis de serem quebrados quanto é para um computador clássico quebrar o esquema que utiliza chave de 128 bits.

> Since Grover's algorithm provides only a quadratic speedup, an attack based on Grover's algorithm may be circumvented using longer keys. (H.; PATHAK, 2018).

2.3 O algoritmo clássico resiliente a ataques de força bruta

A partir do momento que temos a possibilidade de implementação de algoritmos como o de Shor e as consequências apresentadas de quebra de confiabilidade de algoritmos clássicos como o RSA, surge o questionamento do que fazer para se ter uma troca de informações confiável. A dúvida, portanto, concentra-se na existência ou não de um algoritmo a prova de falhas. Um algoritmo que, independentemente da evolução estratégica de quebra por força bruta utilizada, dos novos algoritmos que poderiam ser desenvolvidos ou das evoluções de hardware que poderiam ocorrer, permaneceria seguro. Embora pareça uma utopia pensar na existência de tal algoritmo de criptografia, resiliente a eventuais avanços de tecnologia ainda não mapeados, a existência dos mesmos não é ficção e, um exemplo de protocolo de informação teoricamente seguro seria o *one-time-pad*.

> If the key is uniformly random, kept perfectly secret to everyone except the two parties, and no part of it is ever reused, it can be employed in an encryption scheme called one-time-pad (OTP), which is an example of an information-theoretically secure encryption protocol (RENNER, 2022).

2.3.1 One-time-pad

O primeiro ponto de destaque em relação ao *one-time-pad*, também conhecido como cifra de uso único em português, está no fato dele utilizar criptografia simétrica. Como visto anteriormente, um esquema de chaves assimétricas pressupõem a utilização de um par de chaves, uma pública e uma privada. Dado o fato que uma das chaves é pública, esta chave, em tese, pode sempre ser revertida e, portanto, não está segura independentemente das ações de quebra na teoria, mesmo que no contexto tecnológico de criação do algoritmo essa reversão seja excessivamente custosa e contextualmente impossível. O resumo, então, seria que é fundamentalmente impossível encontrar sistemas de criptografia assimétricos de informação teoricamente segura, tornando necessária a utilização de algoritmos simétricos no caso clássico (RENNER, 2022).

Adentrando na explicação do que é o algoritmo de cifra de uso único, o seu detalhamento é muito próximo ao que se espera de seu nome: constitui um algoritmo de chave simétrica cujo tamanho da chave é maior ou igual ao da mensagem e cuja utilização não é repetida. Nesse sentido, o remetente da mensagem acrescenta o valor da chave na mensagem, fazendo $criptografada = mensagem + chave$. De modo similar, o destinatário da mensagem realiza a operação inversa, subtraindo o valor da chave da mensagem recebida para obter a mensagem original: $criptografada - chave = mensagem$. O estudo de decriptografia, feito por um criptoanalista sem ter conhecimento da chave, poderia ser entendido como $criptografada - supostaChave = supostaMensagem$. Entretanto, a partir do momento que não se tem definido o que está sendo buscado, qualquer valor obtido na $supostaMensagem$ pode ser entendido como válido, fazendo com que a descoberta do valor real da $mensagem$ não possa ser obtido mesmo quando todos os valores possíveis de $supostaChave$ são testados.

2.3.1.1 Mensagem de carácter único

A cifra de César foi apresentada como um exemplo extremamente simples de substituição. Nesse algoritmo, todas as letras seriam acrescidas de um número previamente definido, com a substituição de cada letra por aquela que estivesse 3 posições à frente, por exemplo. A teoria e a prática mostram que tal esquema é quebrado facilmente mesmo sem o auxílio de uma máquina de calcular. Entretanto, há uma maneira de tornar esse algoritmo resiliente a ataques de força bruta e o entendimento dessa situação é a base para compreender o *one-time-pad*. Assume-se aqui dois requisitos para a utilização da cifra de César para que a mesma se torne segura contra ataques de força bruta:

- A chave de substituição será um número aleatório e não necessariamente o número 3.
- A mensagem a ser criptografada terá apenas uma letra, ou seja, mensagem de tamanho 1.

A partir da descrição que envolve o problema pode-se explorar diversas situações diferentes, conforme explicitado na Tabela 1. No caso 1, por exemplo, utilizou-se uma chave de valor 6, que também pode ser entendida como uma chave de valor f. Ao somar o valor da chave com o valor da mensagem temos uma mensagem criptografada g. Entretanto, algo simular ocorre em todos os outros casos: em todos a mensagem criptografada final é g. Nesse sentido, um criptoanalista que esteja em posse da mensagem criptografada, ou seja, que tenha conhecimento da mensagem g, não consegue descobrir qual é a mensagem original dado que ele não tem a chave e que todo e qualquer resultado é possível.

Caso	Mensagem original	Chave criptográfica	Mensagem criptografada
1	a	6 == 'f'	g
2	b	5 == 'e'	g
3	c	4 == 'd'	g
4	d	3 == 'c'	g
5	e	2 == 'b'	g
6	f	1 == 'a'	g

Tabela 1 – Diferentes aplicações da Cifra de César para mensagens de tamanho um

Assume-se, por exemplo, que a chave real e correta é o valor 3, a semelhança do que César fazia. O destinatário final da mensagem, de posse da chave criptográfica simétrica, pode fazer $g - 3 = d$, encontrando assim, facilmente, a mensagem original que é d. O criptoanalista, contudo, por não ter o valor da chave não pode afirmar que o valor dela é três e, assim sendo, teria que recorrer a um teste de força bruta, ou seja, teria de testar todos os valores possíveis, de 1 até 25. Apesar de ser possível realizar esse teste, contudo, o criptoanalista encontraria como resultado dessa operação todas as letras do alfabeto, ou seja, todos os resultados possíveis. O problema é que, sem conseguir testar ou validar qual é o valor correto, ele não teria encontrado nenhuma informação verdadeiramente útil. Se o valor d da mensagem original corresponder a nota de um aluno, por exemplo, os valores dos Casos 1 ao 6 são possíveis, tanto o aluno pode ter tirado uma nota A, máxima, como uma nota mínima, F. O criptoanalista, mesmo tendo encontrado todos esses valores a partir da mensagem criptografada g, não conseguirá determinar qual é o valor correto: ele não chegará a nota verdadeira, que é D. Apenas de posse da chave pode-se ter certeza que a mensagem original foi encontrada.

A segurança desse algoritmo é resguardada pelos fatores:

- A chave utilizada é verdadeiramente randômica, estando de posse dela apenas o remetente e o destinatário da mensagem, sendo, portanto, privada.
- A chave simétrica escolhida é usada uma única vez.
- O tamanho da mensagem é menor ou igual ao tamanho da chave, fazendo com que não haja repetição de qualquer parte da chave.

Ao garantir que a chave permanece privada e secreta, fica impossível reverter a mensagem criptográfica para a mensagem original de forma direta. Como a chave é usada uma única vez e nenhuma parte da mesma é re-utilizada, tendo a chave sido gerada de forma aleatória e sem seguir qualquer tipo de padrão, nenhuma análise pode ser feita na identificação de repetições, como é o caso do que foi feita na quebra da Máquina enigma, por exemplo. Caso a mesma chave de criptografia fosse usada para todos os alunos de uma turma, por exemplo, saber a nota de um único aluno faria com que a chave criptográfica pudesse ser descoberta e, como implicação direta, seria possível a partir daí descobrir a nota de todos os demais alunos estando de posse das notas criptografadas.

No caso de utilização correto, contudo, a chave é utilizada uma única vez e, como qualquer chave é possível, poderia-se escolher qualquer número entre 0 e 25 (ou entre 1 e 26), e todos os resultados finais de mensagem criptografada seriam possíveis. Do mesmo modo, a partir de uma mensagem criptografada qualquer, como todos os valores de chave poderiam ter sido utilizados, todos os valores de Mensagem original são possíveis. A consequência final é que mesmo um teste de força bruta não é capaz de identificar o valor da mensagem original: apesar de corretamente identificá-la em um dos casos possíveis, não consegue-se especificar qual é o valor final correto. O algoritmo, quando utilizado da forma descrita, portanto, é resiliente a ataques de força bruta.

2.3.1.2 Mensagem longa

Embora suficientemente detalhada a utilização do *one-time-pad* para criptografar mensagens de caractere único, tal caso possui aplicações práticas extremamente limitadas: é raro encontrar situações nas quais a mensagem pode ser suficientemente descrita com apenas um caractere. Entretanto, em termos de uso do algoritmo propriamente dito, o caso de uso para mensagens longas tem os mesmos requisitos e o mesmo panorama geral: basta que a chave randômica seja maior ou igual a mensagem e que seja utilizada apenas uma vez.

Para abordar tal utilização utilizar-se-á uma mensagem de n caracteres com uma chave de k caracteres. A chave só será utilizada uma única vez e respeitar-se-á $k \geq n$. Adotando um exemplo didático, ter-se-á uma base militar na iminência de ser atacada por um inimigo. O comandante dessa base militar, chamado de *Alice*, precisa seguir as ordens do seu superior, chamado de *Bob*, sejam as ordens de correr do inimigo e procurar refúgio em outra base próxima ou a ordem de não abandonar o local, lutando por aquele posto estratégico. Entende-se que o Quartel General central, origem da ordem, terá maiores condições de realizar uma escolha assertiva e, portanto, sua ordem deve ser seguida. O inimigo, chamado de *Eve*, contudo, não pode obter conhecimento prévio dessa ordem visto que, caso seja uma ordem de recuar ele poderia preparar uma emboscada e, no caso da ordem ser para lutar, ele poderia repensar seu movimento, dada uma elevada suspeita de

que ele não possui força bélica suficiente para derrotar o inimigo, o que comprometeria uma elevada chance de vitória para *Alice* e *Bob*.

Nesse contexto abordado, *Alice*, que representa a base militar que está na iminência de ser atacada, está de posse da chave criptográfica que o Quartel General Central, *Bob*, utilizou na criptografia da mensagem. Todos os envolvidos no ataque estão de posse da mensagem criptografada, inclusive o inimigo, *Eve*.

Eve, contudo, não tem o valor da chave e precisa tentar adivinhar um valor para a chave, dentre todos aqueles possíveis. Pensando em uma chave criptográfica essencialmente composta por caracteres maiúsculos, de 4 dígitos e uma mensagem também com 4 dígitos apenas, teria-se um total de 26^4 possibilidade de chaves para *Eve* testar. Dentre essas chaves a serem testadas muitas resultariam em palavras totalmente descontextualizadas para a situação. Outras poderiam ou não ter sido utilizadas. Por fim, a maior parte dessas chaves resultaria em caracteres totalmente aleatórios, que não formariam uma palavra conhecida da língua portuguesa. Em um contexto de senhas de acesso, por exemplo, essas *strings*, essas sequências de caracteres, poderiam ser entendidas como mensagens possivelmente corretas. No caso em questão, contudo, não seriam válidas.

Assume-se que *Eve* testou todas as chaves existentes, e está, portanto, de posse das diversas mensagens decriptografadas em potencial. A mensagem enviada por *Bob* foi *AAAA*. *Alice* sabe que a chave utilizada por *Bob* foi *KTSD*. A Tabela 2 mostra 4 casos de estudo dentre os quase quinhentos mil casos analisados por *Eve*.

Caso	Mensagem criptografada	Chave criptográfica testada	Mensagem obtida
1	AAAA	ETIZ	FUJA
2	AAAA	KTSD	LUTE
3	AAAA	FZKN	GALO
4	AAAA	EKVY	FLWZ

Tabela 2 – Resultados obtidos por Eve a partir da mensagem de Bob

O caso 4 é um típico exemplo de uma mensagem que não tem significado algum dentro da língua portuguesa, é uma sequência de caracteres totalmente aleatórios. Esses casos seriam extremamente prováveis em um teste de força bruta já que todas as sequências alfabéticas de 4 letras seriam obtidas, indo do *AAAA* ao *ZZZZ*. O caso 3 mostra um exemplo de uma palavra da língua portuguesa que, embora exista, não está contextualizada com o problema. Todas as palavras da língua portuguesa que possuem 4 letras seriam encontradas em algum momento da análise de *Eve*, já que estão dentro do grupo maior descoberto, que inclui, como dito, qualquer sequência com 4 letras. O caso 1 e o caso 2, contudo, são ambos mensagens extremamente prováveis de estarem corretas; ambas poderiam, de fato, representar a mensagem que *Bob* quis passar. *Alice*, por ter conhecimento da chave *KTSD* sabe que a mensagem é para que ele LUTE e, portanto, já se prepara para o contra-ataque. *Eve*, contudo, não sabe ainda qual das mensagens é a correta, ou

seja, o inimigo continua sem saber se a ordem foi para a base que está pra ser atacada lute ou corra. A conclusão é que, mesmo tendo passado por todas as mensagens possíveis, *Eve* não ganhou informação nenhuma: *Eve* está no mesmo ponto inicial, sem conseguir decriptografar a mensagem. Mesmo que seja possível para *Eve* ler a mensagem correta, caso 2, por não saber que esse é o caso de sucesso a informação é, essencialmente falando, tão relevante quanto todas as outras mensagens incorretas que surgiram pela decriptografia com utilização de chaves erradas.

Conforme dito anteriormente, portanto, a partir do momento que não se tem definido o que está sendo buscado, qualquer valor obtido na suposta mensagem decriptografada encontrada pode ser entendido como válido, fazendo com que a descoberta do valor real da mensagem não possa ser obtido mesmo quando todos os valores possíveis são testados. O *one-time-pad* é, portanto, resiliente ao teste de força bruta e, consequentemente, inquebrável supondo a ação dessa técnica quando utilizado da maneira definida acima. A única forma de obter a mensagem original a partir da mensagem criptografada neste contexto é, de fato, estando de posse da chave simétrica utilizada na criptografia, fato imutável seja pela evolução de hardware ou pela descoberta de novos algoritmos.

2.4 Dificuldades associadas ao uso do one-time-pad

Após evidenciar a eficácia associada ao uso do *one-time-pad* o questionamento que poderia surgir é o por quê do algoritmo não estar sendo amplamente utilizado em todas as comunicações que requerem criptografia do mundo globalizado. Caso ele fosse implementado pelo sistema financeiro, por exemplo, não haveria possibilidade de quebras por meio de força-bruta mesmo após o algoritmo de Shor ser implementado em um computador quântico, evento que ameaçaria o uso do RSA.

Apesar de nenhum sistema estar imune a possibilidade de side-channel attacks, ou seja, apesar de sempre existir a possibilidade de ataques de canal laterais ligados a aspectos de implementação do algoritmo e não às suas características teóricas, explorando portanto aspectos não modelados na prova de segurança (PIRANDOLA, 2019), não haveria receio de quebra do *one-time-pad* devido a avanços de hardware ou de algoritmos mais eficientes pois, mesmo testando todas as possibilidades possíveis de chave, o algoritmo permanece seguro segundo as suas características teóricas. Caso se testasse todos os números existentes menores que N em uma utilização do RSA, por exemplo, chegaria-se, necessariamente, em um fator não trivial de N, o que leva à fatoração do mesmo e consequente obtenção da chave privada.

A resposta da não utilização do *one-time-pad* está em um ponto muito relevante do uso do algoritmo que ainda não foi explorado com destaque: remetente e destinatário devem já estar de posse da chave criptográfica utilizada. No caso de mensagem longa, por

exemplo, tanto *Alice* quanto *Bob* tinham o valor da chave utilizada e, devido a isso, *Alice* conseguiu corretamente decriptografar a mensagem de *Bob*. Esse acordo de qual chave seria utilizada foi feito previamente entre *Alice* e *Bob*. Caso *Alice* não estivesse de posse da chave, a comunicação não seria efetiva pois *Bob* não poderia enviá-la através de um canal público, já que *Eve* passaria a ter acesso à chave também, o que fere os requisitos de segurança. A chave não poderia também ser enviada através de um canal seguro que apenas *Alice* e *Bob* tivessem acesso pois, se tal canal já existisse, não haveria necessidade de utilizar uma chave de criptografia: a mensagem final poderia ser enviada nesse mesmo canal, já que ele é seguro.

Nesse contexto, portanto, com a ressalva de que a chave não pode ser re-utilizada e deve ter o mesmo tamanho da mensagem, *Alice* e *Bob* deveriam ter de maneira premeditada trocado entre si diversas chaves simétricas a serem utilizadas, uma por vez, sempre que quisessem trocar alguma mensagem. *Bob*, que representa um Quartel General centralizado, teria que trocar chaves com cada subordinado cuja comunicação tivesse chance de ocorrer em algum momento futuro, como *Carol*. Caso *Alice* quisesse se comunicar com *Carol*, por sua vez, novas chaves simétricas deveriam ser trocadas entre as partes previamente.

Em um contexto bélico, durante uma guerra, por exemplo, cada comandante teria que trocar com cada subordinado chaves o suficiente para trocar mensagens criptográficas até que os visse novamente, o que poderia demorar anos. Cada subordinado que quisesse comunicar com outra pessoa que não o seu comandante teria que realizar o mesmo procedimento, levando à criação de um número inviável de chaves a serem trocadas previamente e seguramente armazenadas, longe de qualquer inimigo. O problema associado ao *one-time-pad*, portanto, fica evidenciado: é muito custoso realizar a distribuição prévia de todas as chaves a serem utilizadas nas diferentes comunicações, representando um desafio logístico gigantesco.

2.5 Uma possível solução para a distribuição segura de chaves simétricas

Apesar dos problemas de logística encontrados na geração e distribuição prévia de chaves simétricas, o algoritmo do *one-time-pad* funciona. Caso existisse, então, um modo de criar chaves e as distribuir sob demanda entre duas partes de forma eficiente e segura todos os problemas logísticos estariam resolvidos. Sempre que *Alice* quisesse comunicar com *Bob*, por exemplo, bastaria que eles executassem tal método e ambos receberiam uma chave randômica, que apenas eles teriam acesso e que, portanto, poderia ser utilizada para criptografar uma mensagem.

Como esse método de geração e distribuição poderia ser usado mais de uma vez, uma nova chave poderia ser gerada sempre que necessário: não haveria, portanto, limites

para a comunicação segura. Como cada chave gerada seria secreta, sendo de posse apenas de *Alice* e *Bob*, *Eve* não conseguiria usufruir das mensagens mesmo que interceptasse a comunicação. De uma forma mais direta, a partir do momento que *Alice* e *Bob* realizaram a criptografia da mensagem com uma chave randômica, utilizada apenas uma vez e de comprimento maior ou igual à mensagem original, adotando a implementação do *one-time-pad*, o texto cifrado poderia circular livremente por um canal de comunicação público. A possibilidade de existir tal método de geração e distribuição de chaves aleatórias parece utópica, mas, respeitadas certas condições, existe uma estratégia confiável para executá-lo: o *Quantum Key Distribution*; a Distribuição Quântica de Chave.

3 A distribuição quântica de chaves

Conhecido como *Quantum Cryptograph* e também como *Quantum Key Distribution*, QKD, o método de distribuição quântica de chave garante, de maneira comprovadamente segura, a distribuição de informação privada. O trabalho em tela focará na distribuição quântica de chave utilizando protocolos de preparação e medição dependente de equipamentos, citando o Protocolo BB84, o Protocolo B92 e o Protocolo de seis estados. Embora não seja foco do trabalho em tela protocolos de distribuição quântica de chave focados em emaranhamento, contudo, citar-se-á o protocolo E91 dada sua relevância para a Distribuição Quântica de Chave.

Como o próprio nome já adianta, o método da distribuição quântica de chave possui etapas quânticas. Nesse contexto, embora a mecânica quântica tenha ameaçado a segurança da comunicação mundial pela possibilidade, por exemplo, de fatorar eficientemente números grandes em primos, com implementação do algoritmo de Shor, e assim quebrar esquemas criptográficos amplamente utilizados no mundo atual, como aqueles que dependem do RSA, a mecânica quântica, por outro lado, criou também um procedimento que garante a possibilidade de realizar comunicação segura (NIELSEN; CHUANG, 2011).

3.1 Conceitos básicos

O *Quantum Key Distribution*, QKD, é um protocolo comprovadamente seguro no qual *bits* de uma chave privada podem ser gerados entre duas partes a partir de um canal público (NIELSEN; CHUANG, 2011). A conceituação inicial é que o canal no qual ocorre a comunicação é público é extremamente relevante pois não seria possível assumir o canal como privado: um canal de comunicação privado implicaria que as duas partes comunicantes, chamadas aqui de *Alice* e *Bob*, já teriam condições de se comunicar de forma segura, uma hipótese incoerente dado que esse é justamente o objetivo a ser alcançado.

A partir do momento, então, que *Alice* e *Bob* realizam a comunicação em um canal público e executam de forma correta o algoritmo, ocorre a potencial geração de *bits* de uma chave privada. Esses bits de uma chave privada farão a composição final de uma chave simétrica, sendo uma sequência de bits aleatórios detida por *Alice* e *Bob*. Aplica-se o algoritmo exaustivamente até que o número de *bits* gerados sejam numerosos o suficiente para que a chave simétrica final tenha um tamanho igual ou maior que a mensagem a ser criptografada, respeitando em cada execução um limite máximo de ruído permitido. Considerando os casos de sucesso, nos quais o ruído foi dentro do tolerado e as partes comunicantes estão de posse de uma chave simétrica grande o suficiente, aplica-se o protocolo do *one-time-pad* e realiza-se a comunicação de maneira segura. Assim sendo, os

problemas logísticos associados ao armazenamento das chaves simétricas longas estariam vencidos sempre que a geração de chaves fosse bem-sucedida.

> The main reason for our interest in QKD is that secure communication can be built by combining key distribution with the one-time pad protocol. If two protocols are proven secure according to a composable security definition, then the security of their combination can be argued based on their individual functionalities and without the need to give a separate security proof for the combined protocol(PIRANDOLA, 2019).

O requisito inicial associado ao protocolo QKD quando se trata de protocolos de preparação e medição, como o BB84, é que o canal quântico de comunicação utilizado tenha um ruído gerado menor que um limiar previamente definido. A percepção de que o canal de comunicação deve ser relativamente pouco suscetível a falhas é de extrema importância para o correto funcionamento do protocolo e ficará mais evidente após as explicações que se seguem. A segurança associada à chave final gerada é garantida pelas propriedades da informação quântica, algo muito poderoso.

> The only requirement for the QKD protocol is that qubits can be communicated over the public channel with an error rate lower than a certain threshold (NIELSEN; CHUANG, 2011).

O resultado associado a segurança ser garantida pelas propriedades da informação quântica significa dizer que a condição para que o protocolo permaneça seguro está associado unicamente ao fato das leis fundamentais da física quântica estarem corretas.

> For the first time, it became clear how quantum physical laws can provide unconditional security, impossible classically(H.; PATHAK, 2018).

Diferentemente dos algoritmos de chave assimétrica, como o RSA, portanto, que se baseavam em complexidade computacional, o QKD não se torna mais frágil devido a avanços de algoritmos ou de equipamentos computacionais. Mesmo no caso de se tornar possível resolver problemas matemáticos de maneira mais eficiente, com evolução de *software*, e mesmo sendo possível executar cálculos matemáticos em máquinas mais poderosas, evolução de *hardware*, o protocolo QKD ainda é, portanto, comprovadamente seguro.

> Cryptographic scheme information-theoretically secure. This term encompasses the fact that this kind of security can be expressed in terms of purely information-theoretic concepts, in contrast to computational security (which requires the notion of computational complexity(RENNER, 2022).

3.2 Ideia básica do algoritmo

Diferentemente do que a leitura prévia pode levar a se pensar, a Distribuição Quântica de Chave não é uma fórmula mágica a partir do qual sempre será gerada uma chave simétrica de forma segura em cada execução independentemente das condições de cada execução. A justificativa para essa frase é que nem sempre a execução do algoritmo levará ao resultado pretendido, dependendo para o caso de sucesso de fatores inerentes à configuração prática de implementação do método e também da ocorrência de interferência externa indesejada. O brilhantismo do protocolo, entretanto, permanece, residindo na possibilidade de se detectar falhas durante a tentativa de geração da chave. A ideia básica, portanto, não é que *Alice* e *Bob* poderão sempre gerar chaves simétricas de maneira segura, mas que eles podem tentar gerar essa chave e, se algo der errado, eles terão meios suficientes para determinar que a chave final não é segura. Nesse sentido, a partir do momento que *Alice* e *Bob* tem totais condições de avaliar se a chave final é segura ou não, basta que eles executem o algoritmo até que o resultado de sucesso seja obtido.

Fazendo uma analogia com uma transmissão clássica, pode-se pensar em três crianças brincando de compartilhar segredos. A primeira das crianças, *Alice*, quer enviar um recado para seu amigo, *Bob*. O conteúdo do recado, contudo, é sigiloso e, assim sendo, *Alice* que garantir que apenas *Bob* consiga ler o recado. Para tal, *Alice* realizará criptografia simétrica do recado, escrevendo a chave em um pedaço de papel. Entre *Alice* e *Bob*, contudo, existe a presença de *Eve*, que quer, a todo custo, descobrir qual é o conteúdo da mensagem que será enviada. Sempre que possível, portanto, *Eve* tenta obter o pedaço de papel que *Alice* escreveu antes dele chegar até *Bob*. O fato aqui, porém, é que *Alice* possui observação visual de todos os comportamentos de *Eve* e de tudo aquilo que ocorre com o papel, como se todas as três crianças estivessem em um espaço aberto. Nesse sentido, ao escrever em uma folha de papel o conteúdo de uma senha, *Alice* pode observar se esse papel chegou até *Bob* diretamente ou se, em algum momento do percurso, *Eve* ganhou acesso ao mesmo. Nessa brincadeira, *Alice* pode tentar enviar o recado para *Bob* diretamente diversas vezes, estando escrito no papel sempre uma senha randômica diferente. Caso *Eve* consiga pegar o papel ao invés de *Bob*, essa senha é descartada. Entretanto, no momento que *Bob* for capaz de pegar o recado de papel com a senha antes de *Eve*, *Alice* saberá que apenas ela e *Bob* tem o conhecimento sobre a senha, podendo tentar para isso realizar a comunicação quantas vezes for necessário. Nesse momento, *Alice* pode criptografar então o recado com a senha detida tanto por ela quanto por *Bob* e escrever o texto cifrado em um pedaço de papel. Caso *Eve* ganhe acesso ao recado final não fará diferença, pois esse está cifrado e, portanto, legível apenas para *Alice* e *Bob*.

No caso da QKD de preparação e medição tal resultado será obtido pela transmissão de estados quânticos não ortogonais entre *Alice* e *Bob*. Após transmissão dos estados, verificar-se-á o nível de perturbação nos estados transmitidos, estabelecendo um limite para

ruído que ocorra no canal. É de suma importância que *Alice* e *Bob* tenham conhecimento prévio das características do canal e tenham, previamente, estabelecido corretamente limites para o ruído, assumindo a existência dos mesmos devido ao ambiente e não devido a uma bisbilhotagem que ocorra no canal devido à intromissão de *Eve*. Sabe-se que qualquer interferência que ocorra na transmissão deixará vestígios, dado que não é possível distinguir dois estados quânticos não ortogonais sem gerar perturbação (NIELSEN; CHUANG, 2011). Em paralelo a isso, *Eve* só pode consultar a informação original, dado que não é possível clonar a informação para consultar uma cópia, uma réplica, que serviria para ganhar dados sobre a mensagem sem alertar *Alice* e *Bob*. Como *Alice* e *Bob* tem conhecimento do canal que eles estão usando, caso ocorra um ruído acima do previsto eles inferem que houve interferência e abortam a operação.

3.2.1 Ganho de informação gera perturbação

Uma conclusão não muito distante de que a interferência de um agente externo, como *Eve* poderia ser percebida é a de que o sistema de comunicação possui sensibilidade às interações recebidas por ele. Em outras palavras, qualquer atuação no canal como tentativa de distinguir dois estados quânticos não ortogonais, gerando portanto ganho de informação, só é possível mediante introdução de perturbação no sinal, ou seja, mediante geração de ruído (NIELSEN; CHUANG, 2011).

Para demonstrar a proposição, parte-se da ideia de que *Eve*, principal interessada em realizar medições, tem um estado inicial qualquer denotado como $|u\rangle$. A partir desse estado comum, *Eve* realizará interação com dois estados quânticos distintos e não ortogonais, denotados por $|\psi\rangle$ e $|\phi\rangle$. Como hipótese, assumimos que a interação unitária com cada estado não gerará qualquer pertubação, dado que essa é justamente a intenção de *Eve*: ganhar informação, mas passar despercebida; não gerar ruído. Assim sendo, os estados finais continuarão a ser $|\psi\rangle$ e $|\phi\rangle$. Contudo, o resultado final de *Eve* deve ser alterado de $|u\rangle$ para outros dois estados, chamados aqui de $|v\rangle$ e $|v'\rangle$. É necessário que esses últimos estados detidos por *Eve* sejam diferentes entre si para que ela seja capaz de definir o que foi resultado de uma interação com $|\psi\rangle$ e o que foi resultado de uma interação com $|\phi\rangle$, adquirindo informações sobre a identidade do estado interagido. O resultado é:

$$|\psi|u\rangle \rightarrow |\psi|v\rangle \tag{3.1}$$

$$|\phi|u\rangle \rightarrow |\phi|v'\rangle \tag{3.2}$$

Entretanto, dado que os produtos internos são preservados sob transformações unitárias, observa-se:

$$\langle v|v'\rangle\langle\psi|\phi\rangle = \langle u|u\rangle\langle\psi|\phi\rangle \tag{3.3}$$

Do qual, conclui-se que:

$$\langle v|v'\rangle = \langle u|u\rangle = 1 \tag{3.4}$$

$$\langle v|v'\rangle = 1 \tag{3.5}$$

A implicação direta de $\langle v|v'\rangle = 1$ é que $|v\rangle$ e $|v'\rangle$ são iguais e, assim sendo, não foi possível identificar diferenças entre os estados $|\psi\rangle$ e $|\phi\rangle$. A conclusão final, então, é que distinguir entre $|\psi\rangle$ e $|\phi\rangle$ deve, inevitavelmente, perturbar ao menos um desses estados.

3.2.2 O teorema da não clonagem

Como visto, não é possível para *Eve* realizar medições no estado original detido por *Alice* e *Bob* sem gerar perturbação, sem criar ruído e tornar sua interferência perceptível. Entretanto, caso *Eve* realizasse medições em outro estado que não o de *Alice* ou *Bob*, porém com as mesmas propriedades, *Eve* poderia realizar medições a vontade. Bastaria, então, que *Eve* fizesse uma cópia das informações antes de realizar qualquer tipo de medição. Tal estratégia, extremamente comum na computação clássica, não funcionaria na computação quântica, contudo. A justificativa para tal afirmativa é que não é possível copiar informação de estados não ortogonais sem perda de fidelidade.

Suponhamos que exista uma máquina quântica com dois compartimentos identificados como A e B. O compartimento A, chamado de compartimento de dados, inicia em um estado quântico puro, porém desconhecido, $|\psi\rangle$. Este é o estado que se deseja copiar para o compartimento B, chamado de compartimento alvo. Assume-se que o compartimento alvo começa em algum estado puro padrão, $|s\rangle$. Portanto, o estado inicial da máquina de cópia é dado por:

$$|\psi\rangle \otimes |s\rangle \tag{3.6}$$

Agora, uma evolução unitária U efetua o procedimento de cópia, idealmente:

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} U|\psi\rangle \otimes |s\rangle = |\psi\rangle \otimes |\psi\rangle \tag{3.7}$$

Suponha que esse procedimento de cópia funcione para dois estados puros específicos, $|\psi\rangle$ e $|\phi\rangle$. Logo, observa-se que:

$$U|\psi\rangle \otimes |s\rangle = |\psi\rangle \otimes |\psi\rangle \tag{3.8}$$

$$U|\phi\rangle \otimes |s\rangle = |\phi\rangle \otimes |\phi\rangle \tag{3.9}$$

Tomando o produto interno dessas duas equações, é obtido:

$$\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2 \tag{3.10}$$

Mas a equação $x = x^2$ tem apenas duas soluções, $x = 0$ e $x = 1$. Portanto, ou $|\psi\rangle = |\phi\rangle$ ou $|\psi\rangle$ e $|\phi\rangle$ são ortogonais. Assim, um dispositivo de clonagem só pode clonar estados que sejam ortogonais entre si, e, portanto, um dispositivo de clonagem quântica geral é impossível. Um potencial clonador quântico não pode, por exemplo, clonar os estados qubit $|\psi\rangle = |0\rangle$ e $|\phi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, já que esses estados não são ortogonais.

> Even if one allows non-unitary cloning devices, the cloning of non-orthogonal pure states remains impossible unless one is willing to tolerate a finite loss of fidelity in the copied states (NIELSEN; CHUANG, 2011).

3.3 Protocolos de preparação e medição associados à distribuição quântica de chave

Conforme antecipado, na distribuição quântica de chave que utiliza protocolos de preparação e medição o resultado de geração de chave será obtido pela transmissão de estados quânticos não ortogonais entre *Alice* e *Bob* através de um canal quântico público. Após transmissão dos estados, verificar-se-á o nível de perturbação nos estados transmitidos, estabelecendo um limite para ruído que ocorra no canal. Assumindo que *Alice* e *Bob* têm conhecimento prévio das características do canal, será possível estabelecer corretamente limites para o ruído, identificando assim as situações nas quais ocorreu interferência de *Eve*, abortando a operação nesse caso.

3.3.1 Protocolo BB84

O primeiro dos protocolos de distribuição quântica de chave de preparação e medição é o Protocolo BB84, desenvolvido por Charles Bennett e Gilles Brassard em 1984. Esse protocolo desempenha um papel fundamental na área de criptografia quântica

(NIELSEN; CHUANG, 2011). Descrever-se-á brevemente o protocolo, sendo sugerida a leitura do material original, (BENNETT; BRASSARD, 1984), caso seja desejado maior aprofundamento.

Alice, personagem 1 na comunicação, possui duas sequências de bits clássicos aleatórias denotadas por a e b. Cada uma dessas sequências possui $4n + \delta$ bits, onde δ é grande o suficiente para estatisticamente garantir uma chave final com n bits. A primeira das sequências, denotada por a, representará a opção 1 ou a opção 2 relativas aos valores permitidos em uma dada configuração, ao passo que a sequência b fará alusão à base de codificação escolhida por *Alice*, bases essas X ou Z, que representam a configuração supracitada.

Pode-se entender, então, que $b = 0$ representaria uma codificação que resulta nos estados possíveis $|0\rangle$ ou $|1\rangle$ e $b = 1$ representaria uma codificação que resulta nos estados possíveis $|+\rangle$ e $|-\rangle$. Nesse sentido, a primeira opção de cada uma dessas codificações seria escolhida nos casos em que $a = 0$ e, consequentemente, a segunda opção de cada codificação seria escolhida nos casos em que $a = 1$. A Tabela 3 apresenta os estados quânticos possíveis.

a	b	$\|\psi_{a_k,b_k}\rangle$
0	0	$\|0\rangle$
1	0	$\|1\rangle$
0	1	$\|+\rangle$
1	1	$\|-\rangle$

Tabela 3 – Combinações possíveis de a e b e estados quânticos associados

Conforme demonstrado na Tabela 3, então, os estados possíveis são:

$$|\psi_{a_0,b_0}\rangle = |0\rangle \tag{3.11}$$

$$|\psi_{a_1,b_0}\rangle = |1\rangle \tag{3.12}$$

$$|\psi_{a_0,b_1}\rangle = |+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \tag{3.13}$$

$$|\psi_{a_1,b_1}\rangle = |-\rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \tag{3.14}$$

Alice, então, tendo as sequências a e b definidas de forma randômica, obtém um estado quântico $|\psi\rangle$:

$$|\psi\rangle = \bigotimes_{k=1}^{(4+\delta)n} |\psi_{a_k,b_k}\rangle \tag{3.15}$$

O efeito desse procedimento é codificar a na base X ou Z, conforme determinado por b. Os quatro estados possíveis não são todos mutuamente ortogonais, e, portanto, nenhuma medição pode distinguir todos eles com certeza. Em seguida, *Alice* envia $|\psi\rangle$ para *Bob*, por meio de seu canal quântico de comunicação público.

Bob recebe $E(|\psi\rangle\langle\psi|)$, onde E descreve a operação quântica devido ao efeito combinado do canal e das ações de Eve, podendo ser entendido como a informação enviada originalmente por *Alice* com adição de um ruído de transmissão. *Bob* anuncia publicamente o recebimento da informação. Neste ponto, *Alice*, *Bob* e *Eve* têm estados separados, descritos por matrizes de densidade diferentes.

Bob, então, procede a realização de medidas dos qubits recebidos. Entretanto, ele precisa definir em qual base ele realizará a medição. Para definir se a medição será realizada na base X ou na base Z, *Bob* terá sua própria sequência randômica *b'* de $4n + \delta$ bits clássicos a partir da qual, a exemplo do que fora feito por *Alice*, ele definirá a base de medição. Quando *Bob* utiliza na sua medição do k-ésimo termo uma base igual à que fora feita por *Alice* originalmente, ele consegue obter um resultado a'_k que tende a ser igual ao valor original que *Alice* tinha para seu a_k. No caso de *Bob* realizar uma transformação linear indevida para medir o estado quântico utilizando uma base diferente da que *Alice* fez inicialmente, contudo, o resultado final não é confiável. Em outras palavras, só é possível aproveitar o resultado das medições nas quais b'_k de *Bob* é igual ao b_k de *Alice*. Até esse momento, *Bob* não tem conhecimento do que era a sequência b original detida por *Alice*. De maneira similar, *Eve* não possui informação alguma e, caso tenha tentado realizar alguma medição, teve de realizá-la apostando na sorte qual a base correta a ser utilizada.

Somente nesse momento, então, *Alice* anuncia publicamente b, e, por meio de discussão em um canal público autenticado, ela e *Bob* descartam todos os bits em a, a' exceto aqueles para os quais os bits correspondentes de b e b' são iguais. Os bits restantes satisfazem, em teoria, $a = a'$, já que, para esses bits, *Bob* mediu na mesma base que *Alice* preparou. Anunciar publicamente o valor b não revela nada sobre a ou os bits resultantes da medição de *Bob*, dado que as sequências originais são randômicas e não há correlação proposta entre a e b. É importante que *Alice* não publique b até depois que *Bob* anuncie a recepção dos qubits impedindo assim que *Eve* receba qualquer tipo de informação privilegiada.

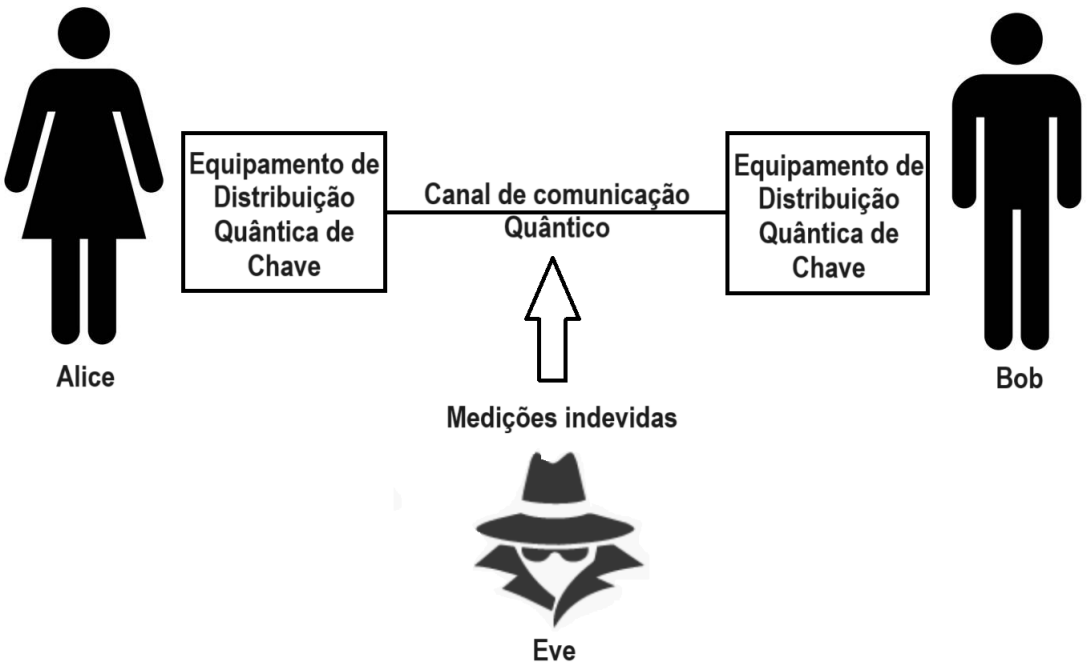
Como para *Bob* existiam duas opções de escolhas de base, X ou Z, pode-se entender que ele escolheu a base correta, que seria a mesma escolhida por *Alice*, ou que escolheu uma base incorreta, diferente do que fora escolhido por *Alice*. *Bob* tem, portanto, 50% de

chance de acertar a escolha da base. A conclusão é que, estatisticamente falando, em torno de metade dos valores obtidos pela combinação a, a' podem ser aproveitados. O δ presente na quantidade inicial serve justamente para garantir que, após descartar todos os pares oriundos de $b'_k \neq b_k$, ter-se-á uma sequência final com $2n$ valores, representada tanto por a quando por a', nas quais se espera uma alta correlação. No caso ideal, ter-se-ia $a = a'$.

Nessa última etapa, *Alice* e *Bob* realizam testes para determinar o quanto de ruído ou espionagem ocorreu durante sua comunicação. *Alice* seleciona n bits aleatoriamente de seus $2n$ bits restantes da cadeia de caracteres a e anuncia publicamente a seleção. *Bob* e *Alice*, então, publicam e comparam os valores desses bits de verificação. Os valores, em um caso ideal, deveriam ser iguais. De posse das características do canal quântico utilizado na comunicação é esperado algum ruído a ele associado. Apesar disso, é possível definir um limite para o qual entende-se que as divergências entre a e a' são, de fato, oriundas do meio-ambiente, ou seja, devidas ao fato do canal de comunicação utilizado não ser perfeito.

Contudo, caso note-se um erro exagerado, se mais de t bits discordarem, por exemplo, *Alice* e *Bob* entendem que houve ruído em excesso, possivelmente gerado por medições ao longo da comunicação. As possíveis medições, indevidas, seriam atribuídas à *Eve*. A figura 5 ilustra o esquema de comunicação entre *Alice* e *Bob* suscetível a bisbilhotagem de *Eve*.

Figura 5 – Desenho da comunicação entre Alice e Bob com Eve



Fonte: autoria própria

No caso onde um ruído exagerado foi percebido, *Alice* e *Bob* abortam o processo e reiniciam o protocolo. O limite t é escolhido de tal forma que, se o teste for aprovado,

eles ficam de posse de n bits não divulgados, feitos a partir de a e a'. Essa sequência final é secreta, tendo origens puramente randômicas e sendo detida unicamente por *Alice* e por *Bob*. Essa cadeia de dígitos final, portanto, é uma cadeia de 0's e 1's que combinadas formam um conjunto de valores secretos detidos exclusivamente pelas partes envolvidas na comunicação: *Alice* e *Bob* agora possuem uma chave compartilhada. O adendo final é que, conforme explicitado, a chave gerada é formada por bits 0s e 1s sendo, portanto, uma chave clássica.

Ao final da transmissão, algoritmos de pós-processamento de reconciliação de informação e de amplificação de privacidade devem ser aplicados. Tais algoritmos serão discutidos ao longo do Capítulo 5. O protocolo BB84 pode ser generalizado para usar outros estados e bases, e conclusões semelhantes se aplicam (NIELSEN; CHUANG, 2011).

3.3.2 Protocolo B92

O Protocolo B92 é uma variação simplificada do Protocolo BB84, tendo sido proposto por Charles Bennett, um dos autores do BB84, em 1992 (BENNETT, 1992). O B92 demonstra que a essência da segurança quântica não requer quatro estados quânticos, mas pode ser alcançada com apenas dois estados. Descrever-se-á brevemente o protocolo, sendo sugerida a leitura do material original, (BENNETT, 1992), caso seja desejado maior aprofundamento.

De maneira similar ao que fora definido no protocolo BB84, aqui *Alice* começa a preparação de seu estado quântico tomando como base uma sequência de bits randômicos. Entretanto, *Alice* está de posse de uma sequência única, denotada por a. Cada valor de a pode ser ser 0 ou 1. No caso de $a_k = 0$, *Alice* prepara o estado quântico $|\psi_k\rangle = |0\rangle$. No caso de $a_k = 1$, *Alice* prepara o estado quântico $|\psi_k\rangle = |+\rangle$.

a	$\|\psi_{a_k}\rangle$
0	$\|0\rangle$
1	$\|+\rangle$

Tabela 4 – Combinações possíveis de a e estados quânticos associados

Bob também possui sua sequência de números aleatórios a', a utilizando para escolher a base na qual realizará a medição, realizando medição na base Z quando $a' = 0$ e fazendo medição na base X quando $a' = 1$. Nesse sentido, caso *Bob* realize a medição na base correta, a tendência é que ele encontre um resultado igual a 0, ou seja, ao medir $|0\rangle$ na base Z ele encontrará 0 e, ao medir $|+\rangle$ na base X ele também encontrará resultado 0. Entretanto, caso ele realize a medição na base indevida, o resultado será imprevisível pois há execução de uma transformação linear indevida. Nesse caso, *Bob* pode encontrar o resultado 0 com probabilidade de 0.5 e pode encontrar o valor 1 com probabilidade de 0.5.

A consequência direta disso é que *Bob* tem certeza que, ao encontrar o valor 1, ele mediu na base errada e, portanto, seu a'_k é o oposto do valor de a_k de *Alice*.

Com base nessa conclusão, *Bob* descarta todos os resultados nos quais obteve resultado 0 e permanece com aqueles que ele obteve resultado 1. *Bob* pode então divulgar todos os resultados que ele obteve e, de posse deles, *Alice* manterá um subconjunto da sua string original a mantendo apenas os valores associados aos resultados 1 de *Bob*. *Bob* pode inverter os valores de sua sequência, $a''_k = 1 - a'_k$, momento no qual ele e *Alice* terão uma sequência compartilhada da qual nada fora revelado. *Alice* e *Bob* detêm uma cadeia de 0's e 1's que combinadas formam um conjunto de valores secretos detidos exclusivamente pelas partes envolvidas na comunicação: eles agora possuem uma chave compartilhada.

De posse dessa chave eles podem escolher bits para, em uma discussão pública autenticada, verificar a correlação da chave, divulgando metade dos bits e utilizando a outra metade como chave somente nos casos que o número de erros for inferior a um valor limite t, a exemplo do que fora feito no Protocolo BB84. Caso seja encontrado um número de erros superior ao valor limite, eles entendem que houve ruído em excesso, possivelmente gerado por medições ao longo da comunicação. Tais medições, indevidas, seriam atribuídas à *Eve*. Nesse caso, *Alice* e *Bob* abortam o processo e reiniciam o protocolo. Tal procedimento poderia ser feito diversas vezes, até a execução na qual as condições de aceitação fossem completamente atendidas. Algoritmos de pós-processamento de reconciliação de informação e de amplificação de privacidade, a serem discutidas no Capítulo 5, devem ser aplicados ao final da transmissão nesse protocolo (NIELSEN; CHUANG, 2011).

O protocolo B92 em sua definição original, contudo, não tem uma performance tão boa quando a do protocolo BB84, dado que a presença de somente dois estados linearmente independentes faz com que seja possível para *Eve* executar uma poderosa medição de discriminação de estado não-ambígua (Unambiguous State Discrimination) nos estados quânticos preparados por *Alice* (PIRANDOLA, 2019). O resultado disso é uma menor tolerância a ruído no protocolo B92, próxima a 0.034 (TAMAKI; KOASHI; IMOTO, 2003). Em comparação, no Protocolo BB84 com one-way entanglement distillation protocol, a tolerância é próxima de 0.165 (SHOR; PRESKILL, 2000) ao passo que, no protocolo de seis estados, apresentado a seguir, o limite de segurança para a taxa de erro de bit quântico é 0.126 (SHU, 2023).

3.3.3 Protocolo de seis estados

Conforme visto, a diferença ente os Protocolos BB84 e B92 tem como base o número de estados utilizados, havendo redução pela metade entre o que o BB84 utiliza quando comparado ao que é utilizado pelo protocolo B92. Entretanto, o caminho inverso também poderia ser escolhido, no qual escolhe-se mais estados do que os quatro estados originais no BB84.

Tal escolha foi feita no protocolo de seis estados, no qual as bases de codificações escolhidas são X, Z e Y. Nesse sentido, são permitidos os estados $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, $|+i\rangle$ e $|-i\rangle$. Esse protocolo, por ser uma variação direta do protocolo BB84, pode de ser entendido como o protocolo BB84 de seis estados ou uma variação do BB84 utilizando 3 bases de codificação (WARKE; BEHERA; PANIGRAHI, 2019).

a	base	$\|\psi_{a_k,base}\rangle$
0	Z	$\|0\rangle$
1	Z	$\|1\rangle$
0	X	$\|+\rangle$
1	X	$\|-\rangle$
0	Y	$\|i\rangle$
1	Y	$\|-i\rangle$

Tabela 5 – Estados quânticos associados ao protocolo de seis estados

Uma consequência direta da adição de uma base de codificação extra é que *Bob* agora terá mais dificuldade de acertar a mesma base escolhida por *Alice*, dado o maior número de possibilidades, conforme ilustrado na tabela 5. Antes, como só havia duas opções, ele poderia acertar ou errar com probabilidade igual a meio. Agora, porém ele tem chance de acertar a base apenas em 1 caso de um total de três, reduzindo a probabilidade de sucesso para 0.33. Em contrapartida, também fica muito mais difícil para *Eve* acertar a base correta de *Alice* nas mesmas iterações que *Bob* acertou, reduzindo drasticamente os casos nos quais a informação seria de fato útil, aumentando a robustez do protocolo (KERN; RENES, 2008).

O reflexo direto da base extra é uma maior tolerância a ruído no protocolo de seis estados. Como comparativo, usualmente, define-se como medida conservadora um limite de segurança de taxa de erro de bits quântico, qubit error rate (QBER), próxima a 11% para o protocolo BB84, mas de até 12.6% para o protocolo de seis estados (SHU, 2023). Uma quantidade maior de qubits, contudo, precisam ser trafegados até obter uma chave de mesmo tamanho quando comparado à utilização do protocolo BB84. Ao final da transmissão, algoritmos de pós-processamento de reconciliação de informação e de amplificação de privacidade, a serem discutidas no Capítulo 5, devem ser aplicados, a semelhança do que fora feito para os outros protocolos de QKD.

3.4 Protocolos de emaranhamento associados à distribuição quântica de chave

Conforme antecipado, a distribuição quântica de chaves possui a categoria de protocolos associados a preparação e medição, foco do trabalho em tela, mas é possível também para *Alice* e *Bob* o fazerem utilizando estados quânticos emaranhados, conforme

proposto por Ekert em 1991 (EKERT, 1991) em sua abordagem alternativa para o QKD (NIELSEN; CHUANG, 2011; PIRANDOLA, 2019).

3.4.1 Protocolo E91

O protocolo E91, também conhecido como Protocolo EPR (NIELSEN; CHUANG, 2011), foi concebido por Arthur Ekert em 1991 (EKERT, 1991). A ideia fundamental do protocolo é que *Alice* e *Bob* irão compartilhar um conjunto de pares de qubits emaranhados, cada um tendo a metade de cada par. Tais pares emaranhados devem estar no estado de Bell, sendo denominados de pares EPR. A origem desses pares emaranhados não é relevante, podendo o conjunto ter sido criada por *Alice*, por *Bob* ou até mesmo por uma terceira entidade.

Alice e *Bob*, então, escolhem um subgrupo desses pares de estados quânticos emaranhados e realizam testes fidelidade visando garantir que os pares emaranhados são ainda suficientemente puros. Pode-se argumentar, baseado no limite de Holevo, que a fidelidade dos pares EPR pode ser utilizada para estabelecer um limite superior na informação acessível para *Eve* (NIELSEN; CHUANG, 2011).

No momento, então, que *Alice* e *Bob* estão de posse de metade de cada par emaranhado, assumindo que o teste de fidelidade obteve sucesso, ambas as partes comunicantes realizarão medidas em cada uma de suas partículas utilizando bases randômicas (PIRANDOLA, 2019; NIELSEN; CHUANG, 2011). Ao final, o resultado das medições é que tanto *Alice* quanto *Bob* terão obtido strings de bits clássicos correlacionadas, a semelhança do que fora obtido nos protocolos BB84 e B92.

3.5 Adendo sobre a nomenclatura e tradução do QKD

Após explicações de alguns dos algoritmos principais associados ao *Quantum Key Distribution* algumas conclusões se fazem evidentes. A primeira a ser mencionada é que, de fato, existe uma grande participação da computação quântica no processo, dado que no caso de protocolos de preparação e medição o canal de comunicação para transmissão dos estados criados por *Alice* e enviados para *Bob* é quântico, sendo requisito indispensável o tráfego de estados quânticos não ortogonais pelo mesmo e, no caso de protocolos de emaranhamento, também está se falando de estados quânticos que estão emaranhados. Entretanto, a chave final é clássica e não quântica. Em outras palavras, a chave final formada é uma sequência de bits, uma composição totalmente randômica de 0s e 1s.

Adicionalmente, tanto *Alice* quanto *Bob* participam do processo de criação da chave, porém nenhum deles tem de fato qualquer domínio sobre o resultado final da chave: nenhum deles tem o poder de controlar qual será o resultado final obtido. Um dos alicerces de eficiência e segurança dos algoritmos, inclusive, reside justamente nessa aleatoriedade.

Nesse sentido, no contexto da chave formada, o processo é muito mais próximo de uma geração de chave com uma distribuição executada em paralelo do que o de uma distribuição pura propriamente dita, dado que a chave é formada durante o processo e não detida previamente por uma das partes que simplesmente à compartilha através do canal quântico, o que poderia ser entendido quando a palavra utilizada é distribuição. A ressalva, portanto, é que a chave é produzida e distribuída durante a execução do método.

Outra observação é que, em um contexto puramente linguístico, a tradução livre de *Quantum Key Distribution* do idioma inglês para o português poderia ter como resultado a expressão *Distribuição de chave quântica*, dada a ambiguidade que reside na tradução pela proximidade entre as palavras *Key*, que significa *Chave*, e *Quantum*, associada à palavra *Quântica*. Tal expressão de tradução livre é frequentemente encontrada em notícias ou sites com viés de comprometimento acadêmico menos rigorosos, como a Wikipedia, cujo aprofundamento teórico tende a ser menos profundo do que em materiais de dissertações ou artigos científicos. As citações abaixo exemplificam a utilização de tal expressão que, em uma análise subjetiva do autor do trabalho em tela, tende a não rotular o método da maneira mais precisa.

> A Toshiba anunciou o lançamento do primeiro sistema de distribuição de chave quântica (QKD) integrado em um único chip.
>
> *Disponível em https://www.inovacaotecnologica.com.br, id de notícia 010150211022, acessado em 27 de outubro de 2023.*

> A distribuição de chave quântica (QKD) é um método de comunicação seguro que implementa um protocolo criptográfico envolvendo componentes da mecânica quântica.
>
> *Disponível em https://pt.wikipedia.org, artigo Distribuição de chave quântica, acessado em em 27 de outubro de 2023.*

A ressalva, portanto, é que a chave final gerada é clássica e não quântica: ela é composta por uma sequência de *bits* e não uma sequência de *qubits*. Devido a isso, o trabalho em tela defende fortemente a tradução do método para a língua portuguesa como **Distribuição Quântica de Chave**, respeitando a escolha de palavras originais do método, mas organizando a tradução de tal forma a deixar evidente a associação da parte quântica com a palavra distribuição, não associando a parte quântica do nome com a palavra chave.

4 Implementação do Protocolo de Seis Estados

Conforme visto nas seções anteriores, assumir a confiabilidade de protocolos criptográficos baseados em matemática computacional pode trazer problemas futuros para a segurança dos sistemas, assumindo que a computação quântica fornecerá poder computacional suficiente para superar a robustez de protocolos como o RSA. Dentro do contexto teórico da distribuição quântica de chaves, fundamentado nos princípios da não clonagem quântica e na perturbação inerente causada pela medição, abordou-se os protocolos BB84, B92 e de seis estados, que emergem como possibilidades sólidas para a distribuição segura de chaves quânticas dependente de dispositivos e, nos casos de sucesso com correta aplicação do protocolo, possibilitariam a posterior utilização da chave gerada em uma implementação do one-time-pad resultando em uma comunicação teoricamente segura.

Este capítulo almeja dar ainda maior profundidade naquilo que tange os protocolos e teorias apresentadas como foco do trabalho, propondo uma imersão na esfera prática da QKD dependente de dispositivos, concentrando-se na implementação do protocolo de seis estados. A introdução de uma terceira base de codificação e decodificação, em relação ao proposto pelo BB84, não apenas enriquece o conjunto de estados quânticos utilizados, mas também eleva a complexidade e a segurança do protocolo, possibilitando resultados práticos potencialmente mais relevantes.

O cerne da abordagem reside na apresentação de estudos práticos, realizando simulações e execuções práticas em computadores quânticos reais com o auxílio da infraestrutura da IBM. Os estudos abrangem três cenários distintos: a idealidade de uma comunicação quântica sem interferências do meio-ambiente ou de uma entidade bisbilhoteira; a comunicação em sistemas reais, com presença de ruídos de meio-ambiente, porém também sem a presença de uma entidade bisbilhoteira; e as situações desafiadoras impostas pela presença potencial de uma entidade maliciosa, personificada por *Eve*, em um ambiente real ou ideal.

Analisar-se-á, portanto, os resultados e potencial desempenho associado ao protocolo de seis estados em face de interferências externas, explorando suas limitações e comparando sob diferentes condições experimentais o que de fato acontece após *Alice* e *Bob* realizarem a comunicação. O experimento prático, diferentemente dos resultados esperados em um mundo ideal, estão inseridos em um contexto de ruídos do meio-ambiente e imperfeições de hardware. Nesse sentido, busca-se medir o impacto dos ruídos do meio ambiente e compará-los com a interferência de *Eve*, visando responder se as medições indevidas dessa entidade adversária, quando realizada em todos os qubits transmitidos, poderiam ser camufladas por imperfeições externas ou se, de fato, os rastros deixados por *Eve* nesse

caso seriam explícitos para *Alice* e *Bob*, personagens envolvidos na comunicação.

Ao explorar as nuances da implementação prática com códigos de autoria própria, portanto, o estudo objetiva não apenas aprofundar a compreensão de protocolos QKD de preparação e medição de uma forma geral, mas também fornecer uma base sólida para avaliar sua eficácia no contexto de comunicações mais próximas da realidade. Este estudo empírico, então, visa mapear os desafios e as oportunidades inerentes à aplicação de protocolos de preparação e medição em ambientes dinâmicos e propensos à presença de ruídos e adversários, ilustrando de fato as diferenças entre os resultados teóricos esperados de uma implementação perfeita e aquilo que é possível ser atingido com a tecnologia atual neste cenário de implementação simulado.

Destaca-se que em uma implementação prática de QKD as partes comunicantes *Alice* e *Bob* estariam distantes entre si, o que não foi coberto nos estudos a seguir, no qual tudo ocorre dentro do mesmo sistema. Assim sendo, os experimentos têm um viés muito maior de análise de ruído em uma geração de chave do que um processo de distribuição propriamente dito. Contudo, apesar de não haver uma simulação da distribuição entre as partes comunicantes, busca-se evidenciar a viabilidade de detecção das interferências de *Eve* mesmo quando essas ocorrem em conjunto a estruturas não ideais de implementação. O Apêndice A possui os códigos mais relevantes associados aos experimentos deste capítulo.

4.1 Implementação QKD ideal

A primeira implementação consiste na criação de um circuito idealizado no qual *Alice* definiu aleatoriamente bases de codificação e as implementou. Neste circuito e nas demais implementações assumir-se-á o estudo como feito em um subconjunto dos qubits transmitidos nos quais *Bob* escolheu bases de decodificações iguais as utilizadas por *Alice* na codificação. Nesse sentido, buscar-se-á um resultado de fato perfeito para este circuito entre aquilo que foi transmitido e o que foi posteriormente medido. As demais implementações também adotarão como foco o estudo de um subconjunto de transmissão e consequente medição no qual não há erros de decodificação.

A principal justificativa para estudar exclusivamente os casos de sucesso entre as escolhas de *Bob* e as de *Alice* está nas próprias definições do protocolo de seis estados: todos os dados obtidos a partir de medições em base incorretas feitas por *Bob* devem ser descartados. Em outras palavras, seria pouco otimizado para o objetivo proposto estudar exaustivamente os casos nos quais *Bob* realizou uma decodificação diferente daquela escolhida por *Alice* dado que os resultados finais dessa medição não poderiam ser aproveitados de fato.

Como adendo, existe uma limitação total de qubits disponíveis pelo IBM Quantum Experience platform em sua versão utilizada para o trabalho em tela. Visando, então,

utilizar os qubits disponibilizados da maneira entendida como a mais eficiente e rica experimentalmente, reforçou-se a escolha de analisar apenas os casos associados a uma decodificação correta. Entetanto, objetivando ilustrar os casos de erros de decodificação de *Bob*, a seção 4.4 foi criada, abordando o que ocorre na prática nos casos em que o descarte do resultado é necessário: uma medição final totalmente imprevisível.

A ideia associada, de resultados verdadeiramente imprevisíveis, com geração aleatória de dados, foi abordada sucintamente na seção 4.5. Poderia-se inclusive ter implementado tal geração randômica de números, característica marcante da computação quântica, nos estados inicialmente criados por *Alice*, adotando portas de Hadamard no lugar de certas portas Not, por exemplo. Entretanto, visando simplificar os circuitos e o experimento de uma forma geral, adotou-se um input padrão igual a "00111" em todas as gerações de *Alice*, ou seja, geração inicial de estados antes da codificação com portas Not no primeiro, segundo e terceiro qubits. O circuito é apresentado na Figura 6. As demais implementações também adotarão o padrão de "00111" no input dos dados.

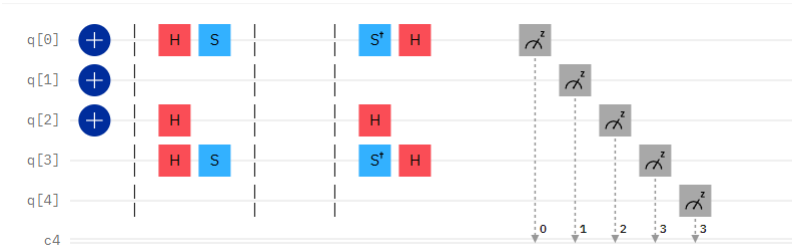
Na Figura 6 o circuito foi exposto organizando-o com barreiras. Tais barreiras são completamente ilustrativas e almejam única e exclusivamente facilitar o entendimento do que está ocorrendo dividindo a exibição do circuito em diferentes partes. A primeira das partes é a presença ou não de uma porta Not. A definição se *Alice* usará ou não a porta Not é definida pelo protocolo como randômica, oriunda da informação de uma das strings. No estudo em questão, contudo, conforme antecipado, adotou-se para fins de simplificação um input constante.

A segunda divisória do circuito apresenta a base de medição escolhida por *Alice*, podendo conter a porta H, nenhuma porta ou a porta H em combinação com a porta S. A escolha de qual combinação utilizar definirá o uso de codificação pela base X, base Z ou base Y, respectivamente, algo que deve ser decidido também de forma aleatória, o que o protocolos de QKD assumem que é possível para as partes comunicantes, tendo elas acesso livre a números verdadeiramente randômicos (PORTMANN, 2021). Em todos os experimentos, contudo, também adotou-se, para fins de simplificação, a mesma escolha de bases, com HS no primeiro e no quarto qubit, H no terceiro qubit e nenhuma porta no segundo e no quinto qubit.

A terceira divisória seria a transmissão dos dados, sem interferências nesse circuito. A quarta divisória representaria a correta decodificação associada exercida por *Bob* e as respectivas medições. Conforme adiantado, em todos os experimentos assume-se que se trata de um subconjunto de dados no qual *Bob* acertou todas as bases de decodificação.

Nos três primeiros registradores mostrados na Figura 6, conforme antecipado, foram inseridas portas Not, invertendo o sinal resultante nesses casos. Realizando um paralelo com o que fora mencionado na Tabela 5, ter-se-ia, portanto, uma sequência a = [1, 1, 1, 0, 0] e bases associadas [Y, Z, X, Y, Z]. Nenhuma medição foi realizada na terceira divisória,

Figura 6 – Circuito ideal

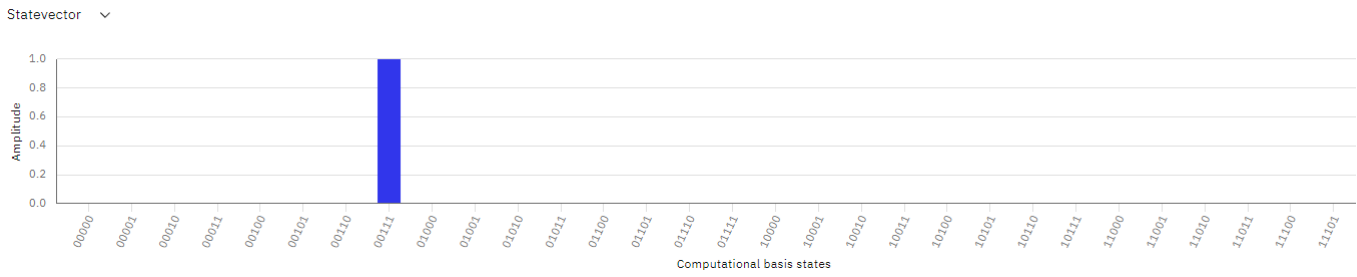


Fonte: autoria própria utilizando IBM Quantum Experience platform

entre as bases de codificação e as bases de decodificação. O resultado dessas sequências de codificação e decodificação é o equivalente da presença de portas identidades ou, em outra perspectiva, uma medição muito simples sem qualquer utilização de portas. Nenhuma mudança ou alteração de resultados, portanto, é esperada em relação o que *Alice* inseriu.

Nesse contexto, realizando a leitura de dados de cima para baixo, indo do q[0] até o q[4], a sequência de bits esperada é 11100, os três primeiros valores tendo sido invertidos devido à presença das três portas Not. O resultado esperado foi corretamente obtido, conforme ilustrado na Figura 7. Não houve, portanto, qualquer ruído ou fato inesperado associado à medição, tendo ela tido um valor final de amplitude igual a 1, ou seja, ocorreu uma medição sem erros ou imperfeições associados a uma correta representação do caso ideal.

Figura 7 – Resultados Circuito ideal



Fonte: autoria própria utilizando IBM Quantum Experience platform

A observação associada à correta interpretação dos resultados ilustrados na Figura 7 é a de que os valores precisam ser lidos da direita para a esquerda, assumindo uma associação correspondente de cima para baixo em relação às linhas do circuito. Caso queira-se ler os resultados da esquerda para a direita é necessário associá-los com as linhas de baixo para cima, ou seja, indo de q[4] até q[0]. O bit de resultado de medição mais à direita, portanto, equivale ao resultado na linha q[0] enquanto o bit de medição mais

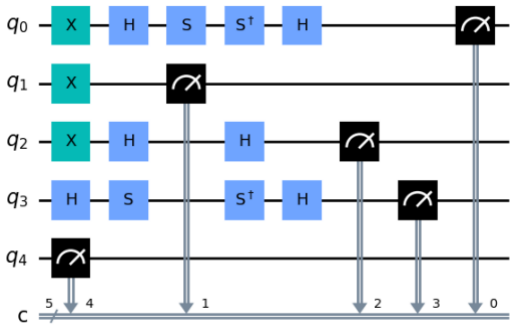
à esquerda está associado ao q[4], quinta linha do circuito. O trabalho em tela adota a leitura dos resultados da esquerda para a direita tratando o valor correto esperado como "00111".

4.1.1 Representações alternativas para o circuito

4.1.1.1 Sem barreiras de visualização

Conforme mencionado, a Figura 6 é uma representação do circuito com barreiras que visam facilitar o entendimento do que está ocorrendo em cada etapa do processo. Entretanto, é possível e até mais usual a representação dos circuitos sem tais barreiras, que foram inseridas com propósitos puramente didáticos. A Figura 8 ilustra o mesmo circuito sem a separação por linhas, com um alinhamento forçado à esquerda.

Figura 8 – Circuito ideal com alinhamento à esquerda



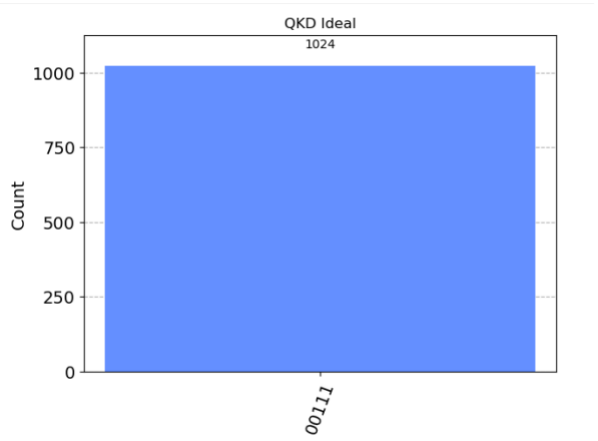
Fonte: autoria própria

O resultado final da medição, contudo, não é alterado pela presença ou ausência das barreiras. Nesse sentido, a medição do circuito ilustrado pela Figura 8 terá o mesmo resultado final com leitura da esquerda para a direita equivalente ao valor "00111". A representação dos resultados mostrada na Figura 7 em termos de amplitude pode também ser alterada para uma representação via histograma, no qual insere-se graficamente o número de resultados obtidos para cada valor. A figura 9 mostra o histograma dos resultados associados à esse circuito após realizar 1024 execuções do circuito. Como o resultado é perfeito, sem erros ou ruídos, nenhum resultado diferente do previsto foi medido e, consequentemente, o resultado correto esperado foi obtido 1024 vezes.

4.1.1.2 Sem portas de codificação ou decodificação

Sabe-se que a presença de portas identidades não altera a medição dos resultados, dado que elas não modificam seus valores. De maneira equivalente, o correto uso de portas para codificação e a consequente decodificação do circuito utilizando as bases

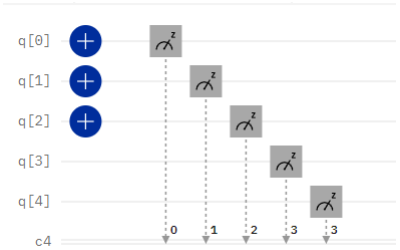
Figura 9 – Resultados Circuito ideal - Histograma



Fonte: autoria própria utilizando IBM Quantum Experience platform

corretas também não acarretará mudanças assumindo que não houve medições no meio da transmissão. Conforme ilustrado nas Figura 6 e 8 e nos resultados associados das Figuras 7 e 9, portanto, o resultado final é exatamente aquele originalmente criado por *Alice*. A criação do circuito foi realizada com a presença das portas para exemplificar o que de fato ocorre na implementação do seis estados para os casos de correta decodificação e sem entidades bisbilhoteiras. O resultado final obtido, contudo, é o equivalente de não termos nenhuma codificação ou decodificação associada. Como o estudo desta seção é sobre o caso ideal de comunicação, no qual não há presença de um bisbilhoteiro, *Eve*, pode-se obter o mesmo resultado de maneira simplificada, conforme ilustrado na Figura 10.

Figura 10 – Circuito simplificado



Fonte: autoria própria utilizando IBM Quantum Experience platform

Na figura 10 de um circuito simplificado omite-se todas as codificações e decodificações realizadas respectivamente por *Alice* e por *Bob*. Embora seja um circuito extremamente simples e a principio pouco representativo, a omissão das codificações e decodificações ilustra com precisão aquilo que o circuito ideal de fato representa: uma medição direta daquilo que fora criado sem qualquer ruído, interferência ou incorreto uso de bases de

medição atrapalhando. O resultado é igual ao inicialmente obtido, com uma amplitude máxima associada ao valor esperado.

4.2 Implementação QKD com ruídos sem Eve

As simulações descritas anteriormente corroboram com toda a teoria previamente definida e explicitada ao longo do trabalho em tela. Entretanto, a computação quântica não está isenta de erros, fazendo com que seja de extrema relevância o estudo do ruído associado. A presença do ruído pode ter origem em diferentes componentes, como falhas de hardware, dificuldades na geração dos dados, na transmissão dos mesmos ou na recepção propriamente dita, indicando um erro de medição neste último caso. Em qualquer uma das situações o ruído acumulado geral pode ser estudado como um distanciamento da idealidade, sendo representado um valor final semelhante ao original, valor esperado, mas com a interferência do meio-ambiente, criando divergências e um distanciamento do inicialmente previsto.

4.2.1 Implementação QKD com ruídos customizados

Visando ilustrar didaticamente o que seria uma implementação mais realista, com taxas de erros menores e resultados finais mais próximos do aceitável, utilizar-se-á a biblioteca de ruídos do Qiskit, denominada Noise Models. Inicialmente, criar-se-á um ruído genérico, adotando erros de depolarização e um erro combinado de amortecimento de fase e de amplitude.

> The NoiseModel class is used to represent noise model for the QasmSimulator. It can be used to construct custom noise models for simulator, to to automatically generate a basic device noise model for an IBMQ backend (Qiskit, 2023).

A elaboração do modelo de erro compreende três etapas fundamentais. Primeiramente, ocorre a definição dos erros que serão incorporados ao modelo. Posteriormente, atribui-se uma probabilidade a cada tipo de erro. Por fim, estabelecem-se as bases de medidas associadas a cada tipo de erro. Essas fases constituem a base para a construção do modelo de erro customizado. No exemplo a seguir, que visa exclusivamente ilustrar o que seria um resultado hipotético que poderia ter dados úteis, adotou-se uma escolha arbitrária de probabilidade associada a cada um dos erros a ser inseridos.

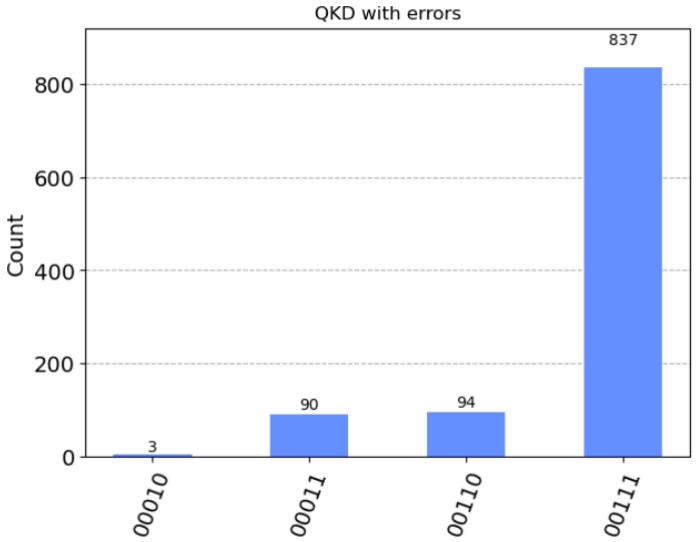
A Tabela 6 mostra os diferentes valores escolhidos livremente, próximos à 0.2. A documentação oficial da biblioteca possui valores de probabilidade em seus códigos de exemplo com valores 0.01 e 0.001 (Qiskit, 2023). De forma proposital, contudo, adotou-se valores com maior probabilidade de erro buscando única e exclusivamente ilustrar graficamente com maior destaque o crescimento de valores incorretos. Os erros foram escolhidos de

tal forma a se ter menos valores totais gerados, visando facilitar o entendimento a respeito do que está acontecendo em uma situação com menos casos de análise. Os resultados encontrados podem ser visualizados na Figura 11.

Probabilidade	**Tipo**
0.2	prob_1
0.25	prob_2
0.2	param_amp
0.2	param_phase

Tabela 6 – Valores e parâmetros para criação de erro customizado

Figura 11 – Resultados circuito sem Eve com erro customizado



Fonte: autoria própria utilizando IBM Quantum Experience platform

Os resultados demonstram o surgimento de três valores alternativos ao valor correto esperado, ou seja, três casos de erros. Os dois valores incorretos com maior destaque, ou seja, com maior ocorrência, consistem na flipagem de um bit específico. Lendo os bits de resultado da esquerda para direita, houve troca do terceiro bit de 1 para 0 em 90 casos e houve troca do quinto bit de 1 para 0 em 94 casos. Houve ocorrência de troca dos dois bits mencionados simultaneamente em 3 casos de um total de 1024 execuções, valor padrão de medições utilizando o simulador "*qasm_simulator*". Os principais códigos utilizados na criação das implementações estão descritos no Apêndice A.

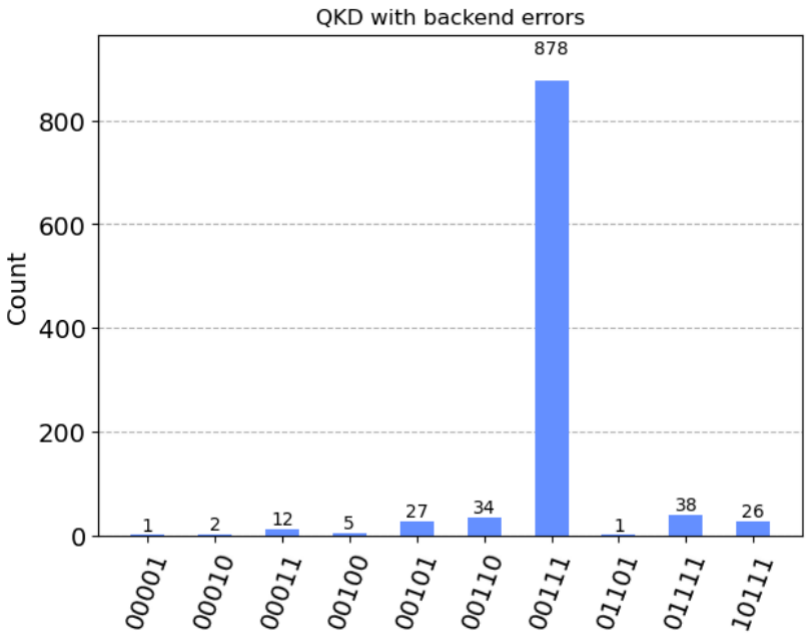
4.2.2 Implementação QKD com ruídos de backend

Embora experimento com ruído customizado forneça uma ideia didática inicial do que seria um resultado não ideal, fica evidente a necessidade de visualizar resultados associados a erros mais próximos da realidade e não criados apenas para fins ilustrativos. Nesse sentido, buscou-se estabelecer um paralelo com os erros de fato existentes em um computador quântico ao executar o circuito em foco com a inserção de um modelo de ruídos mais fidedigno, adotando as características de ruído estabelecidas pela função *NoiseModel.from_backend*, utilizando dados do computador "*ibmq_belem*".

> A simplified approximate NoiseModel can be generated automatically from the properties of real device backends from the IBMQ provider using the NoiseModel.from_backend() method. (Qiskit, 2023).

Nesse contexto, adota-se todas as características do computador quântico de verdade, simulando a execução com os erros estaticamente mais prováveis de ocorrer na máquina física e adotando a frequência com a qual eles ocorrem. Os resultados podem ser visualizados na Figura 12.

Figura 12 – Resultados circuito sem Eve simulação de erros do ibmq_belem



Fonte: autoria própria utilizando IBM Quantum Experience platform

Os resultados ilustrados na Figura 12 mostram o que era esperado para *Bob* obter caso ele realizasse os procedimentos de medição de dados fornecidos por *Alice* no contexto de estudo utilizando o computador da IBM "*ibmq_belem*". É interessante notar

primeiramente que o valor correto, o valor de sucesso “00111”, ocorreu em 878 das 1024 tentativas, levando a uma ocorrência estatística superior a 85%, o que mostra que o resultado do conjunto total de bits mais provável é o valor esperado.

Ao todo, 10 valores novos ocorreram, levando a um experimento muito mais rico que o anterior, deixando explícito também o resultado intuitivo de que erros associados à flipagem de um bit são bem mais prováveis do que a flipagem de dois bits de maneira simultânea, ou seja, é menos frequente a ocorrência de um erro “duplo” em uma mesma medição. Os casos de flipagem de um único bit, da esquerda para a direita, ocorreram 26, 38, 12, 27 e 34 vezes, resultando em uma média próxima a 27 contagens em cada caso. A soma geral dos casos de erro com um bit incorreto somou 137 contagens. Todos os demais casos obtiveram 2 erros, não havendo ocorrência de nenhum caso com 3 bits errados. A soma dos resultados com 2 bits errados simultaneamente foi igual a 9.

Visando caracterizar de maneira mais formal a eficiência de um sistema QKD, dois critérios importantes devem ser considerados: a taxa de erros de bits quânticos (Quantum Bit Error Rate - QBER) e a velocidade de geração da chave (keyrate) (MUSKAN; MEENA; BANERJEE, 2024). No exemplo em tela, contudo, a taxa de geração da chave não seria um bom parâmetro de análise dado que, conforme antecipado no início do capítulo, não há uma transmissão de estados quânticos entre as partes comunicantes, ou seja, nas simulações do experimento a geração e respectiva medição de cada um dos estados quânticos ocorre no mesmo local, algo válido para todos os cenários do experimento. Nesse sentido, avaliar-se-á a taxa de erros de bits quânticos como principal parâmetro de comparação entre os diferentes resultados.

> The QBER serves as an indicator of security and is crucial for evaluating the performance of the link after error correction (MUSKAN; MEENA; BANERJEE, 2024).

A taxa de erros de bits quânticos, QBER, é calculada como a fração entre a taxa de erros e a taxa de geração da chave. Em outras palavras, pode-se calcular o QBER como a razão entre o número total de erros plotados, analisados individualmente bit a bit, pelo total de bits obtidos após a transmissão e medição de todos os estados quânticos inicialmente gerados.

Nos resultados apresentados na Figura 12, o total de contagens de todos os resultados é 1024, sendo cada resultado formado por 5 bits. Em cada contagem de resultado, portanto, foi necessária a geração e medição de 5 estados quânticos, que seriam transmitidos pelo canal quântico de *Alice* até *Bob* em uma implementação prática. Nesse sentido, o valor total de qubits gerados é $5 \times 1024 = 5120$. Conforme antecipado, a soma geral dos casos de erro com um bit incorreto somou 137 contagens, ou seja, teve-se 137 bits errados nesse cenário. A soma dos resultados com 2 bits errados simultaneamente foi igual a 9, levando

portanto ao número de 18 bits errados. A soma total dos erros, então é $137 + 18 = 155$. O resultado final, portanto, é $QBER = \frac{155}{5120} = 0.0302734375 \approx 3.027\%$. Caso fosse desejado calcular a taxa de bits finais corretos ter-se-ia o complemento do resultado, com taxa bits corretos $= \frac{4965}{5120} = 0.9697265625 \approx 96.973\%$.

O valor final obtido de $QBER \approx 3.027\%$ indica que, neste experimento de QKD simulado, no qual a geração de estados quânticos e posterior medição ocorrem no mesmo sistema, a implementação estaria dentro do limite seguro de QBER estabelecido para o protocolo de seis estados.

> It is well-known that the secure bound of qubit error rate (QBER) of BB84 protocol is about 11% while it can be increased to 12.6% by six-state protocol (SHU, 2023).

4.2.3 Implementação QKD sem ruídos adicionais e sem Eve em uma execução real

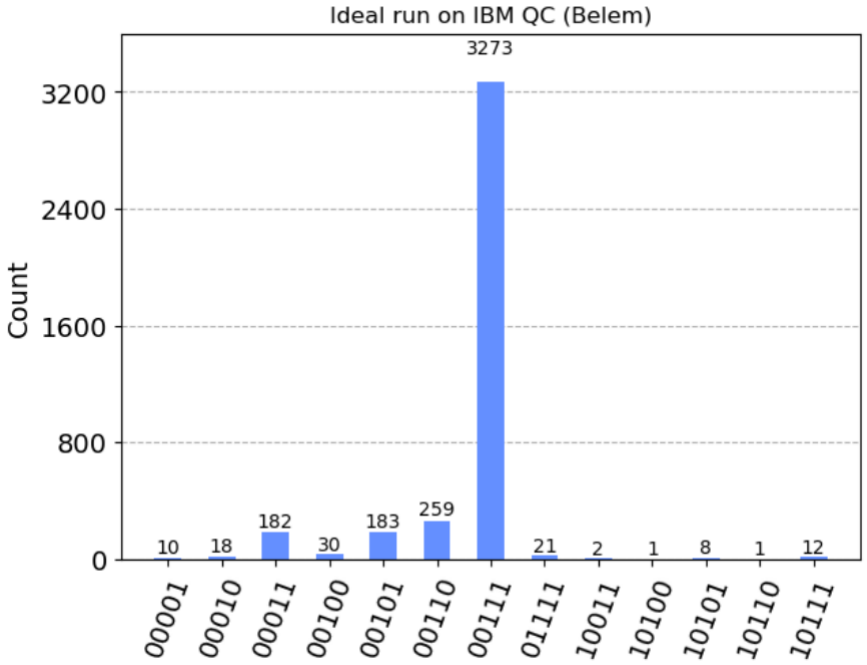
Utilizando a simulação com erros oriundos do *backend* tornou-se evidente a possibilidade de obter valiosas perspectivas iniciais mesmo através de uma simulação. No entanto, é essencial transcender os limites da simulação com criação de modelos de ruídos e adentrar a esfera da execução real, onde as complexidades do ambiente físico e as interações dinâmicas podem revelar nuances cruciais que vão além da abordagem simulada. A transição para a execução real, portanto, representa um passo crucial para validar e enriquecer as descobertas teóricas, fornecendo uma compreensão mais profunda e abrangente do desempenho do sistema em condições o mais próximo da realidade quanto possível.

Quando se trata da execução real em um ambiente não controlado, há diversos motivos pelos quais uma execução no computador quântico propriamente dito é mais vantajosa. O principal ponto, associado à fidelidade aos detalhes do mundo real, é a medição explícita dos fenômenos propriamente ditos, incluindo nuances e eventuais imprevisibilidades. A abordagem simulada com modelo de erros almeja representar da melhor forma possível tais ocorrências, promovendo uma alta correlação do resultado final, mas a execução prática do experimento é, de fato, a fonte original e primária dos resultados mais valiosos. Ressalta-se, novamente, a ideia de todo o experimento se trata de um QKD simulado no qual não há na prática transmissão de estados quânticos para entidades comunicantes distantes entre si.

Na implementação a seguir, os dados foram realizados utilizando um computador quântico verdadeiro, visando dar maior riqueza ao experimento e maior fidedignidade nos resultados. Utilizou-se no experimento o "*ibmq_belem*", backend disponibilizado no IBM Quantum Experience platform. Os resultados podem ser visualizados na Figura 13. Informações a respeito da codificação de construção do experimento estão inseridos no

Apêndice A. A Tabela 19, presente no Apêndice B, apresenta os dados dos resultados em formato tabular.

Figura 13 – Resultados circuito sem Eve executados no ibmq_belem



Fonte: autoria própria utilizando IBM Quantum Experience platform

Diferentemente da simulação anterior, na qual tinha-se 1024 contagens ao todo, no experimento em um computador quântico propriamente dito têm-se 4000 contagens. Além dessa diferença, a representação dos resultados utilizando o computador quântico real mostra divergências relevantes quando comparado aos resultados da simulação com erros comuns pelo modelo de ruído. A primeira grande diferença está no número de resultados diferentes do ideal, um total de 13 resultados existentes ao todo.

Apesar da frequência de ocorrência dos outros casos de erros ser baixa, a presença de um maior número de valores explícita a maior variedade de erros que permeiam situações reais, ou seja, ilustram em detalhes a riqueza de interferências que o meio-ambiente exerce no experimento. Outro detalhe extremamente relevante é a presença de um resultado com 3 bits finais trocados, ou seja, um valor com mais divergência para o valor correto do que divergência, tendo acontecido para o valor “10100” no qual, lendo da esquerda para a direita, temos a troca de bits no primeiro, no quarto e no quinto bit quando em relação ao “00111”.

Apesar das diferenças supracitadas, contudo, o valor final foi obtido em mais de 80% das ocorrências, em proximidade ao que foi percebido na simulação. Nesse sentido, é possível

afirmar categoricamente que, tendo em foco apenas o número de ocorrências de sucesso completo do valor esperado, a simulação com utilização de modelo de ruídos inspirado no computador dá noções preliminares excelentes do que se esperar do computador quântico real. É necessário, contudo, uma análise mais minuciosa do resultado, o que será feito, a exemplo do caso anterior, com o cálculo do QBER associado ao experimento.

A Tabela 7 apresenta de forma detalhada o total de bits errados para cada valor, calculado pela frequência de cada um desses valores multiplicada pelo número de bits errados em cada um deles. Ao todo, obteve-se um total de bits incorretos em 798 dos casos. A soma de todas as frequências, como adiantado, está em 4000, levando a um total de bits equivalente a $5 \times 4000 = 20000$, valor também obtido pela soma entre o total de bits incorretos e o total de bits corretos, como esperado: $798 + 19202 = 20000$. O resultado final, portanto, é $QBER = \frac{798}{20000} = 0.0399 = 3.99\%$.

Tabela 7 – Análise de bits errados para cálculo QBER

Valor	Freq	Nº bits errados	Total bits errados	Nº bits corretos	Total bits corretos
00001	10	2	20	3	30
00010	18	2	36	3	54
00011	182	1	182	4	728
00100	30	2	60	3	90
00101	183	1	183	4	732
00110	259	1	259	4	1036
00111	3273	0	0	5	16365
01111	21	1	21	4	84
10011	2	2	4	3	6
10100	1	3	3	2	2
10101	8	2	16	3	24
10110	1	2	2	3	3
10111	12	1	12	4	48
Total	4000	–	798	–	19202

Adotando um raciocínio equivalente ao que foi registrado anteriormente, considerando 12.6% o limite de segurança para o protocolo de seis estados (SHU, 2023), o valor final obtido de $QBER = 3.99\%$ indica, então, que, neste experimento de QKD simulado, no qual a geração de estados quânticos e posterior medição ocorrem no mesmo sistema, a implementação estaria dentro do limite seguro de QBER estabelecido para o protocolo de seis estados.

4.2.4 Implementação QKD com ruídos adicionais e sem Eve em uma execução real

A partir dos resultados apresentados, então, conclui-se que é possível estabelecer, de forma bem definida, a possibilidade de executar a distribuição quântica de chave e

obter resultados altamente satisfatórios quando não se tem a presença de *Eve* utilizando um esquema de geração e medição em um computador quântico real para esta implementação proposta no experimento. Entretanto, conforme enunciado, foi utilizado um único computador quântico no experimento. A comunicação entre *Alice* e *Bob*, contudo, tende a acontecer com ambos distantes um do outro na utilização prática.

A principal utilidade da distribuição quântica de chaves, conforme feito anteriormente pelo trabalho, é, justamente, resolver o problema logístico da distribuição de chaves simétricas, fazendo tal procedimento de maneira segura, sob demanda e a distância. Nesse sentido, poderia-se ter, por exemplo, uma distância final maior do que 40 quilômetros entre ambos os comunicantes, o que representaria um uso mais útil da distribuição quântica de chaves (NIELSEN; CHUANG, 2011). Assim sendo, mesmo executando o experimento em um computador quântico real, a situação como um todo da distribuição quântica de chaves continua sendo, em termos práticos, apenas uma simulação, dado que omite-se, por exemplo, a geração de ruído da transmissão dos qubits ao longo do canal de comunicação quântico que ligaria *Alice* até *Bob*.

> Quantum key distribution over distances exceeding 40 kilometers, and also in installed telecommunication fiber (under Lake Geneva) has been demonstrated. (NIELSEN; CHUANG, 2011).

Em uma implementação prática, contudo, *Alice* e *Bob* teriam conhecimento do ruído associado ao canal utilizado. Pode-se imaginar, em uma analagia do que a simulação apresentou, que o QBER anteriormente encontrado estaria associado aos processos de geração do estado quântico por *Alice* e de medição por *Bob*, abstraindo o ruído gerado no canal eventualmente associado à transmissão de longas distâncias. Caso o canal quântico fosse ideal, os experimentos anteriores dariam uma noção mais próxima da realidade. Diversos avanços comerciais ocorreram ao longo dos anos e é possível adquirir diversas ferramentas de QKD comercialmente.

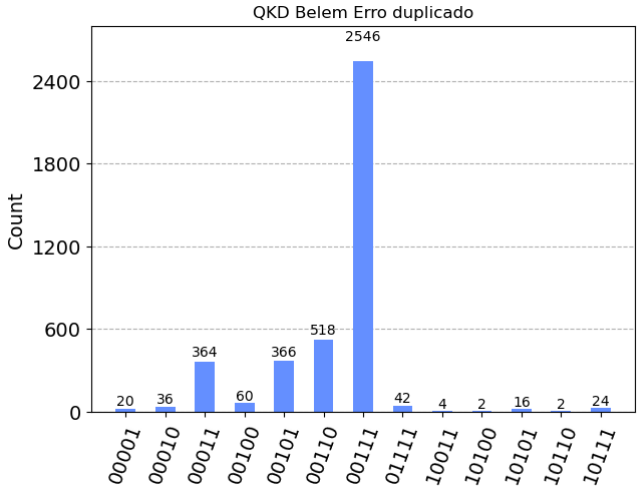
> Several quantum cryptographic tools have now been commercialized. ID-Quantique, a major player in the quantum cryptography industry, sells complete cryptographic solutions. Their products include network encryption systems, quantum cryptographic systems especially designed for industry and government, a quantum random number generator, a state-of-art photon counting device, single photon source, etc (H.; PATHAK, 2018).

Entretanto, ter um canal de comunicação quântico ideal para grandes distâncias ainda é utópico. No experimento proposto a seguir, visando simular eventuais erros extras que poderiam ocorrer ao longo da transmissão, todos os valores incorretos obtidos na execução anterior terão sua contagem dobrada. O objetivo final do estudo prático, como já dito, é a comparação final entre aquilo obtido com a presença de *Eve* realizando medições

em todos os qubits e sem a sua presença, avaliando os impactos da interferência de uma entidade bisbilhoteira indesejada. Nesse contexto, faz sentido aumentar o QBER com essa duplicata de erros que visa dar alguma representatividade dos eventuais erros que ocorreriam no canal de transmissão quântico para que a comparação final seja mais próxima da realidade.

O número total de resultados obtidos permanecerá em 4000, facilitando a comparação com o resultado anterior. O resultado "10100", que teve uma ocorrência única, por exemplo, passará, nesse novo resultado, a ter uma contagem igual a dois. A contagem extra para esse valor sairá do valor correto "00111", que passará de 3273 contagens para 3272 nessa mudança. O mesmo ocorrerá com todos os outros valores encontrados anteriormente. Os resultados podem ser visualizados na Figura 14.

Figura 14 – Resultados circuito sem Eve erros duplicados



Fonte: autoria própria utilizando dados customizados

Conforme o esperado, a contagem do resultado correto diminui em relação ao resultado anterior, dobrando a diferença existente entre a frequência do valor correto e o número total de execuções, conforme esperado. A exemplo do caso anterior, fazer-se-á o cálculo do QBER associado ao experimento.

A Tabela 8 apresenta de forma detalhada o total de bits errados para cada valor, calculado pela frequência de cada um desses valores multiplicada pelo número de bits errados em cada um deles. Ao todo, obteve-se um total de bits incorretos em 1596 dos casos, o dobro do caso anterior, conforme esperado. A soma de todas as frequências, como adiantado, permanece em 4000, levando a um total de bits equivalente a $5 \times 4000 = 20000$. O resultado final, portanto, é $QBER = \frac{1596}{20000} = 0.0798 = 7.98\%$, o dobro do caso anterior.

Adotando um raciocínio equivalente ao que foi registrado anteriormente, considerando 12.6% o limite de segurança para o protocolo de seis estados (SHU, 2023), o valor

Tabela 8 – Análise de bits errados para cálculo QBER

Valor	Freq	Nº bits errados	Total bits errados
00001	20	2	40
00010	36	2	72
00011	364	1	364
00100	60	2	120
00101	366	1	366
00110	518	1	518
00111	2546	0	0
01111	42	1	42
10011	4	2	8
10100	2	3	6
10101	16	2	32
10110	2	2	4
10111	24	1	24
Total	4000	–	1596

final obtido de $QBER = 7.98\%$ indica, então, que, neste experimento de QKD simulado, no qual a geração de estados quânticos e posterior medição ocorrem no mesmo sistema, a implementação estaria dentro do limite seguro de QBER estabelecido para o protocolo de seis estados.

Por analogia, caso o número total de bits errados em cada valor tivesse sido multiplicado por 3, o que indicaria uma taxa de erro atribuída ao canal quântico, inexistente no experimento, como o dobro daquilo obtido devido aos erros associados a preparação e medição, ter-se-ia $QBER = 3 \times 3.99\% = 11.97\%$, ainda dentro do limite seguro de QBER estabelecido para o protocolo de seis estados neste estudo.

4.3 Implementação QKD com a presença de Eve

Nas implementações anteriores, onde a presença de uma terceira entidade bisbilhoteira estava ausente, foi possível estabelecer fundamentos sólidos e compreender o desempenho ideal do protocolo QKD em condições mais próximas daquelas encontradas na prática. Tais simulações proporcionaram conclusões valiosas sobre as capacidades intrínsecas do sistema em condições controladas e com ruídos de meio-ambiente. A análise comparativa entre as implementações de distribuição quântica de chave sem a presença de *Eve* e aquelas que incorporam a presença dessa entidade adversária, contudo, é crucial para entender a robustez do procedimento diante de potenciais ameaças. Nesse sentido, introduzir-se-á a presença simulada de *Eve* nessa seção. Adentrar-se-á, assim, em um cenário ainda mais relevante no qual ocorre a tentativa de obtenção indevida de informações.

Esta seção, portanto, busca investigar como o sistema reage à presença de uma

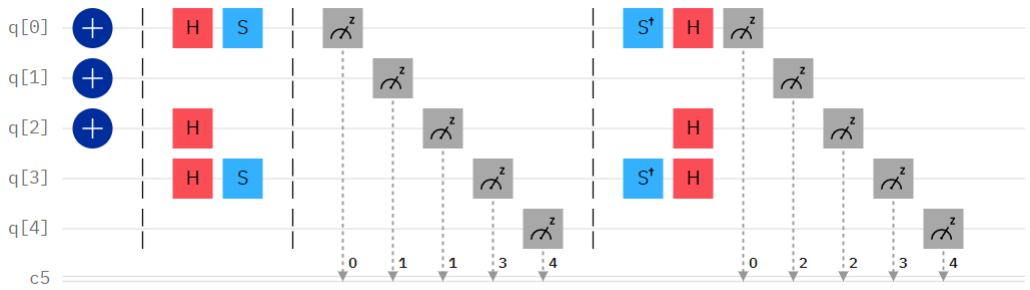
entidade adversária que realiza medições em todos os qubits transmitidos, avaliando a eficácia das medidas de segurança implementadas. Ao contrastar os resultados das simulações com e sem *Eve*, pretende-se validar a rápida detecção associada as vestígios deixados por *Eve* e validar se é possível ocultá-los de maneira eficiente ao tentar mascará-los com ruídos do meio-ambiente.

4.3.1 Implementação QKD com a presença de Eve em ambiente ideal

O resultado do circuito com a presença de *Eve* pode ser visto na Figura 15 na qual o circuito foi exposto organizando-o com barreiras, a semelhança do que fora feito na Figura 6, na apresentação do circuito ideal sem a presença de *Eve*. Tais barreiras são completamente ilustrativas e almejam única e exclusivamente facilitar o entendimento do que está ocorrendo dividindo a exibição do circuito em diferentes partes.

A primeira, a segunda e a quarta parte do circuito foram mantidas conforme feito anteriormente, respeitando a já mencionada padronização estabelecida para todos os experimentos associados. A terceira divisória apresenta diferenças, pois essa seria a etapa de transmissão dos dados, com interferências nesse circuito sendo simulada pela presença de medições em todos os qubits, dada a presença de *Eve*.

Figura 15 – Circuito com a presença de Eve

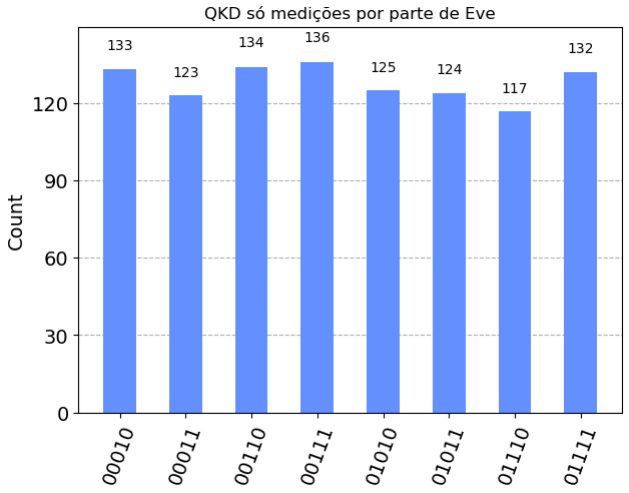


Fonte: autoria própria utilizando IBM Quantum Experience platform

Medições foram realizadas entre as bases de codificação e as bases de decodificação, cujo impacto esperado é elevado. O resultado dessas sequências é o equivalente da presença de um bisbilhoteiro entre *Alice* e *Bob*. Uma simulação associada a esse circuito foi executada sem adição de qualquer ruído customizado, visando um cenário ideal. Os resultados estão disponíveis na Figura 16.

O impacto imediato e bem perceptível é a inexistência de um valor mais frequente em destaque: todos os resultados foram obtidos com contagens extremamente próximas, tanto os valores incorretos como no caso do valor correto, mesmo dentro do contexto do experimento, uma simulação sem a presença de ruído do meio-ambiente. A primeira

Figura 16 – Resultados do circuito apenas medições em ambiente ideal simulado



Fonte: autoria própria utilizando IBM Quantum Experience platform

conclusão visual que surge, então, é que, de fato a presença de *Eve* deixa vestígios bem relevantes de suas medições. Para uma conclusão metódica e replicável, calcular-se-á o QBER associado.

A Tabela 9 apresenta de forma detalhada o total de bits errados para cada valor, calculado pela frequência de cada um desses valores multiplicada pelo número de bits errados em cada um deles. Ao todo, obteve-se um total de bits incorretos em 1512 dos casos. A soma de todas as frequências para a simulação é 1024, levando a um total de bits equivalente a $5 \times 1024 = 5120$. O resultado final, portanto, é $QBER = \frac{1512}{5120} = 0.2953125 \approx 29.53\%$.

Tabela 9 – Análise de bits errados para cálculo QBER

Valor	Freq	Nº bits errados	Total bits errados
00010	133	2	266
00011	123	1	123
00110	134	1	134
00111	136	0	0
01010	125	3	375
01011	124	2	248
01110	117	2	234
01111	132	1	132
Total	1024	–	1512

Adotando um raciocínio equivalente ao que foi registrado anteriormente, considerando 12.6% o limite de segurança para o protocolo de seis estados (SHU, 2023), o valor final obtido de $QBER \approx 29.53\%$ indica o primeiro caso no qual se estaria fora do limite seguro de QBER estabelecido para o protocolo de seis estados, ou seja, a interferência de

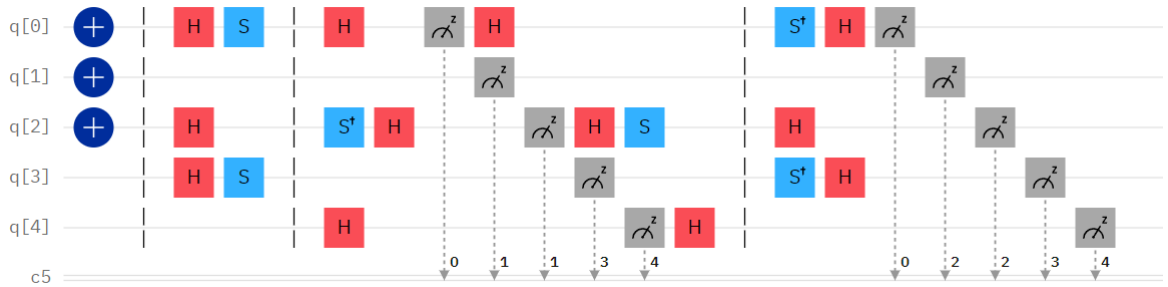
Eve resultaria em abortação desta referida execução do protocolo. Em resumo, pode-se dizer que *Alice* e *Bob* teriam tido dados suficientes para corretamente detectar a presença de *Eve*.

4.3.1.1 Implementação QKD com a presença de Eve e com decodificações em ambiente ideal

Visando dar ainda maior fidedignidade ao que poderia ocorrer na prática, adicionou-se tentativas de decodificações realizadas por *Eve*, o que simularia a entidade bisbilhoteria tentando acertar a codificação realizada por *Alice*. Nesse contexto, adicionou-se uma portas de decodificação H no primeiro qubit e também no quinto, q[0] e q[4], bem como uma combinação das portas H e $S^{\dagger}$ no terceiro qubit. Após realizar a medição, *Eve* procura reverter sua ação.

O circuito que representa tal contexto está na Figura 17. A figura 18 apresenta os resultados associados a esse circuito em uma medição simulada sem ruídos de meio-ambiente, favorecendo a ideia de que *Eve* teria, por exemplo, tecnologia suficiente para corrigir os antigos erros existentes no sistema e ganhar maior margem de erros ocasionados por suas medições. A Tabela 15, presente no Apêndice B, apresenta os dados dos resultados em formato tabular. A Tabela 18 apresenta os resultados em formato tabular tendo sido multiplicados por 4, visando facilitar a comparação com os resultados de outras tabelas.

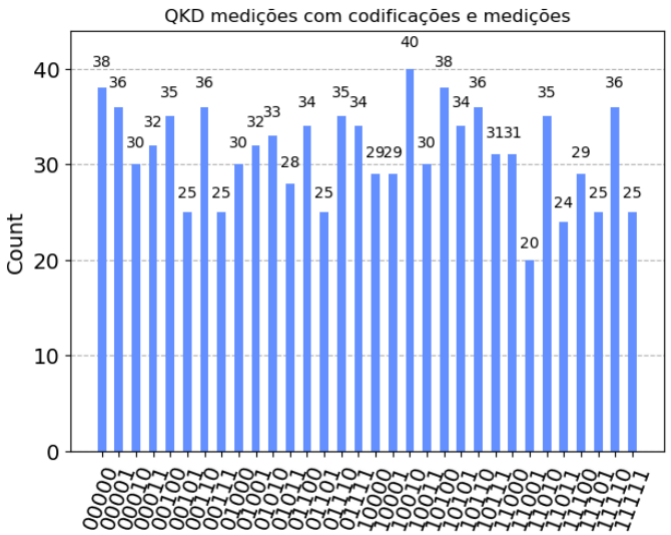
Figura 17 – Circuito com decodificações



Fonte: autoria própria utilizando IBM Quantum Experience platform

O resultado exibido no gráfico é extremamente impactante dado a diferença notável do que havia sido percebido nos circuitos anteriores sem a presença de *Eve*. Mesmo se tratando de uma simulação, sem erros específicos de um computador quântico e também sem a adição de qualquer tipo de ruído, fica perceptível a diferença notável entre os gráficos. A semelhança do que também ocorreu no caso anterior, com *Eve* realizando medições, não é mais possível encontrar um valor de destaque. Existe um total de 32 valores possíveis sendo registrados.

Figura 18 – Resultados do circuito com decodificações medições



Fonte: autoria própria utilizando IBM Quantum Experience platform

A Tabela 20, inserida no Apêndice B, apresenta, a semelhança do que fora feito nas seções anteriores, os dados para o cálculo do QBER que, neste experimento, foi $QBER = 0.5 = 50\%$, pior caso possível e fora do limite seguro de QBER estabelecido para o protocolo de seis estados. Novamente, pode-se dizer que *Alice* e *Bob* teriam tido dados suficientes para corretamente detectar a presença de *Eve* e abortar a geração de chave.

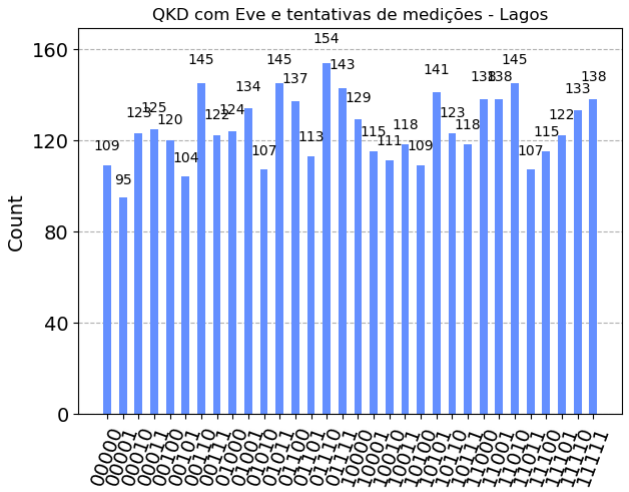
4.3.2 Implementação QKD com a presença de Eve ambiente real

Executa-se, agora, o e experimento com a presença de *Eve* em ambiente com ruídos de meio-ambiente, ou seja, no computador quântico real. Para realizar tal implementação, utilizou-se o computador quântico da IBM "*ibmq_lagos*". Assume-se aqui que os resultados apresentados por ele serão compatíveis e suficientemente semelhantes àqueles apresentados anteriormente pelo computador quântico Belém, permitindo assim uma comparação satisfatória entre ambos os experimentos. Os resultados estão disponíveis na Figura 19. A Tabela 16, presente no Apêndice B, apresenta os dados dos resultados em formato tabular.

Conforme evidenciado na Figura 19, permanece o contraste drástico em relação ao que fora anteriormente percebido na execução real sem a presença de *Eve*: não é possível visualizar o resultado mais provável.

A Tabela 21, inserida no Apêndice B, apresenta, a semelhança do que fora feito nas seções anteriores, os dados para o cálculo do QBER que, neste experimento, foi $QBER = 0.50105 = 50.105\%$, praticamente o pior caso possível e fora do limite seguro de QBER estabelecido para o protocolo de seis estados. Novamente, pode-se dizer que *Alice* e

Figura 19 – Resultados do circuito com Eve em computador quântico real



Fonte: autoria própria utilizando IBM Quantum Experience platform

Bob teriam tido dados suficientes para corretamente detectar a presença de *Eve* e abortar a geração de chave.

4.3.3 Implementação QKD com a presença de Eve ambiente simulado com ruído

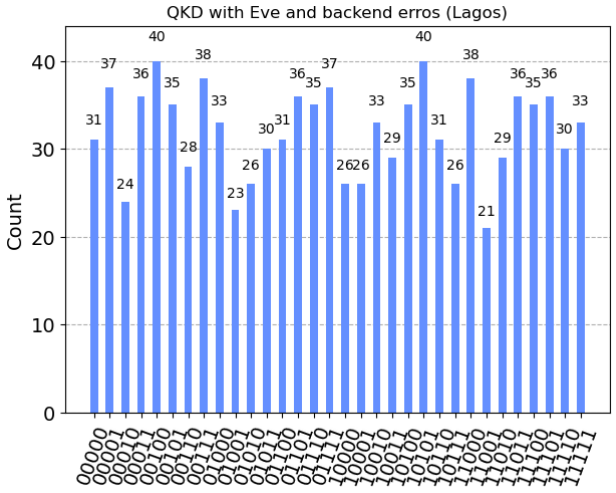
O resultado mais rico e de maior relevância foi apresentado na seção anterior, tendo sido a realização do experimento em um computador quântico real. Nem sempre, contudo, é possível realizar experimentos diversos utilizando os computadores quânticos de verdade na categoria de utilização grátis do serviço. O tempo até a execução e obtenção dos resultados propriamente ditos também pode ser elevado a depender das circunstâncias de momento.

Nesse sentido, visando obter um comparativo do que seria possível obter de resultados em uma simulação, adotando para tanto os erros de backend do computador de Lagos e utilizando a função já mencionada anteriormente de construção de ruído pelo *NoiseModel.from_backend* do Qiskit, executou-se o mesmo circuito neste ambiente simulado. Os resultados estão representados na Figura 20. A Tabela 17, presente no Apêndice B, apresenta os dados dos resultados em formato tabular.

Conforme evidenciado na Figura 20, a semelhança do resultado anterior, permanece o contraste drástico em relação ao que fora anteriormente percebido na execução real sem a presença de *Eve*: não é possível visualizar o resultado mais provável.

A Tabela 22, inserida no Apêndice B, apresenta, a semelhança do que fora feito nas seções anteriores, os dados para o cálculo do QBER que, neste experimento, foi

Figura 20 – Resultados do circuito com Eve em simulação com erros do computador quântico real



Fonte: autoria própria utilizando IBM Quantum Experience platform

$QBER = 0.4919921875 \approx 49.199\%$, praticamente o pior caso possível novamente e também fora do limite seguro de QBER estabelecido para o protocolo de seis estados. Outra vez, pode-se dizer que *Alice* e *Bob* teriam tido dados suficientes para corretamente detectar a presença de *Eve* e abortar a geração de chave.

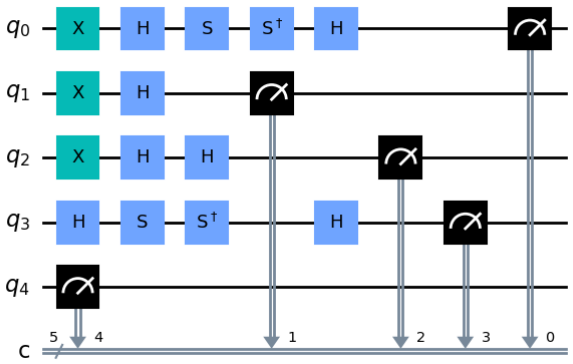
4.4 Casos em que Bob erra a base de decodificação

Conforme enunciado anteriormente, os casos nos quais *Bob* adota uma base de decodificação incompatível com aquela adota por *Alice* na codificação devem ser descartados. Embora a teoria que justifica tal ação já tenha sido abordada ao longo das seções anteriores, optou-se por realizar um experimento simulado no qual foi acrescida uma decodificação de base X indevida antes da medição de *Bob* para o segundo qubit, q1, visando ilustrar experimentamente o que ocorre nesses casos. O circuito que contempla tal implementação pode ser visualizado na Figura 21.

Diferentemente daquilo apresentado nos resultados ideais, então, nesse novo experimento espera-se que uma base incorreta de medição implique em alteração dos resultados associados. O experimento foi executado em simulação com os resultados sendo apresentados na Figura 22.

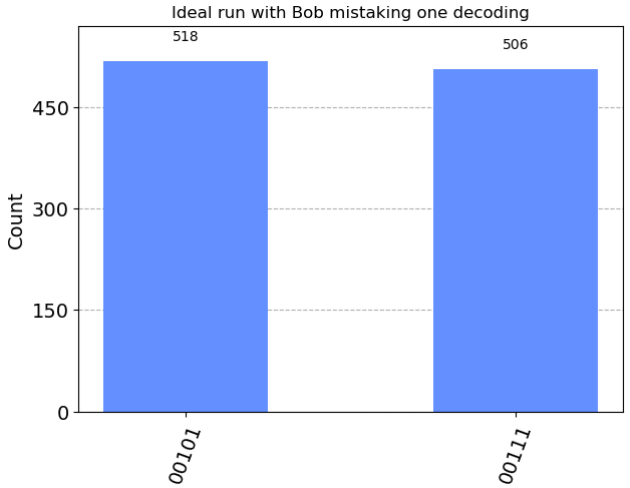
Percebe-se que ocorreu um novo resultado “00101”, com flipagem de bit no segundo bit da direita para a esquerda, justamente o bit associado ao qubit que teve a decodificação incorreta. Os bits do resultado final foram corretamente mensurados para todos os bits cuja medição associada ocorreu utilizando a base de decodificação correta. Em praticamente

Figura 21 – Resultados do circuito com erro de decodificação de Bob no q1



Fonte: autoria própria

Figura 22 – Resultados do circuito com erro de decodificação de Bob no q1



Fonte: autoria própria utilizando IBM Quantum Experience platform

metade dos casos nos quais a base de medição foi a incorreta para determinado qubit, contudo, o bit final medido estava incorreto, fazendo com o que o resultado final medido fosse totalmente imprevisível para o mesmo.

Tal imprevisibilidade associada a uma medição posterior a decodificação incorreta corrobora com a justificativa teórica de descarte necessário de todos os dados atrelados a decodificações incompatíveis e ilustra a aleatoriedade possível de ser obtida em experimentos realizados no contexto da computação quântica. A seção a seguir detalha um pouco mais a aleatoriedade característica do computador quântico que fora perceptível neste último exemplo.

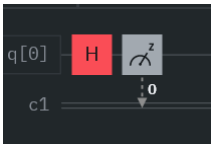
4.5 Geração de número randômico

Conforme mencionado ao longo do capítulo 3, o processo de QKD envolve não só a distribuição, mas também a geração da chave, que acaba por ser uma string final de bits clássicos randômicos detida por *Alice* e *Bob*. A aleatoriedade da chave reside no fato de que nenhuma das partes comunicantes possui domínio sobre o resultado final obtido, sendo esse totalmente imprevisível.

Nesse contexto, essa string final gerada ao final do processo de QKD pode também ser entendida como um número verdadeiramente aleatório que foi gerado pelo processo, algo muito difícil de se obter classicamente, mas extremamente valioso para a ciência e engenharia, com importantes aplicações em simulações e criptografia (HERRERO-COLLANTES; GARCIA-ESCARTIN, 2017). A capacidade de gerar números aleatórios com relativa facilidade, em comparação ao caso clássico, é uma das características mais marcantes do computador quântico, podendo inclusive ser obtida com uma ideia semelhante ao que foi apresentado na seção anterior quando *Bob* errou a base de decodificação. Observa-se que, ao aplicar, em um dado circuito, uma porta de Hadamard antes de realizar a medição em base Z, um bit aleatório é obtido dado que pode ou não ocorrer uma flipagem de bits que possui uma probabilidade de ocorrer equivalente a 0.5. A Figura 23 ilustra tal circuito.

> The inherent randomness of a quantum system makes it a promising platform for generating faithful random numbers. (MENG et al., 2024).

Figura 23 – Ruído de flipagem de bits com porta de Hadamard

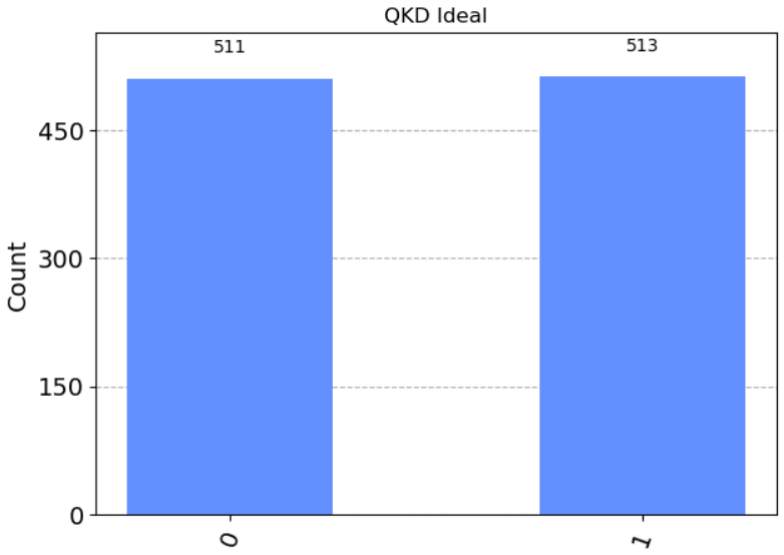


Fonte: autoria própria utilizando IBM Quantum Experience platform

O resultado final obtido de uma simulação pode ser visto na Figura 24, muito próximo ao resultado obtido quando *Bob* errou a base de decodificação.

Observa-se uma ligeira maior incidência do valor 1 neste exemplo da Figura 24: o valor 1, mais frequente, poderia ser adotado como valor final de saída. Tal resultado é totalmente aleatório quando executado em um computador quântico e imprevisível para o dono original do circuito que não tem qualquer controle sobre o bit de saída: não é possível, antecipadamente, determinar se o bit de saída será 0 ou 1, levando, assim, à geração de um bit randômico, o que fora representado pela estatística de resultados de saída. Pode-se repetir o processo inúmeras vezes e, alinhando os bits de saída, seria possível obter um

Figura 24 – Resultados associados à decodificação incorreta



Fonte: autoria própria utilizando IBM Quantum Experience platform

número randômico tão grande quanto se queira, bastando, na prática, um qubit para cada bit desejado. Destaca-se que diferentes geradores quânticos de números randômicos já estão comercialmente disponíveis nos dias atuais (H.; PATHAK, 2018).

4.6 Discussão dos resultados

O primeiro ponto de destaque associado aos resultados obtidos se concentra na necessidade de descarte de todos os bits associados às medições de *Bob* que utilizaram portas de decodificações incorretas. A medição em uma base diferente da correta gera um conjunto de resultados não confiável. O contraste entre os gráficos apresentados pelas Figuras 9 e a 22 ressaltam essa diferença. Sempre que *Bob* mede incorretamente um qubit ele gera uma incerteza associada.

Fazendo o cálculo do QBER associado a esse caso de erro de medição de *Bob* apresentado na seção 4.4, ter-se-ia um $QBER = \frac{518}{5120} = 0.101171875 \approx 10.117\%$, uma taxa representativa. Somando isso ao erro QBER original encontrado devido aos ruídos de meio-ambiente, apresentado na subseção 4.2.3 como 3.99%, ter-se-ia uma taxa superior a 14% que acarretaria inclusive na decisão de abortar o protocolo. Deve-se, portanto, respeitar o descarte obrigatório de dados associados a decodificações incorretas. Deve-se buscar sempre a menor taxa QBER possível, dado que isso resultará em uma maior segurança para o processo.

A higher QBER means that the eavesdropper can gather more information

> about the transmitted key, compromising the security of the legitimate recipient (MUSKAN; MEENA; BANERJEE, 2024).

Dentro contexto de descarte dos dados associados a medições incorretas, faz sentido pensar que *Alice* e *Bob* devem gerar e medir $4 \times n + \delta$ qubits quando aplicarem o protocolo BB84 utilizando duas portas de codificação, assumindo que em um número próximo a metade dos casos *Bob* errará a base de medição, sobrando $2 \times n$ bits finais, dos quais n podem ser utilizados para validar a quantidade de erros existente no procedimento. Caso seja feito um experimento como o implementado pelo trabalho em tela, utilizando três bases de codificação diferente, *Alice* e *Bob* devem gerar e medir $6 \times n + \delta$ qubits, já que nesse caso *Bob* acertará a base em apenas um terço dos casos, levando a um remanescente de $2 \times n$ bits a partir dos quais se repete o procedimento detalhado anteriormente de validar a quantidade de erros existentes divulgando n bits.

O segundo ponto de destaque extraído dos resultados está na possibilidade de utilizar simulações para antecipar os resultados que seriam obtidos na execução de um computador quântico real. Os computadores quânticos reais nem sempre estão disponíveis gratuitamente, estando o pesquisador sujeito a um tempo limite de execução e à ocorrência de filas para executar seu experimento. Conforme visto, contudo, a utilização de simulações com a adoção de erros oriundos do backend permite resultados extremamente próximos da realidade, permitindo o teste de circuitos e até mesmo a tirada de conclusões preliminares importantes.

A Tabela 10 consolida bem os resultados mais indicados para esta análise, facilitando a comparação pelos QBERs calculados: tanto no contexto sem *Eve* quanto naquele com *Eve* seria possível ter uma noção preliminar bastante razoável de qual ruído seria esperado. No casos Sem *Eve*, por exemplo, adicionar os ruídos de backend leva a um QBER de 0.0303 muito mais próximo do valor real de 0.0399 do que se teria ao realizar o cálculo no cenário isento de ruídos, onde o QBER é zero.

Tabela 10 – Análise de resultados: Simulação x Real

Experimento	QBER
Sem Eve sem ruídos	0.000
Sem Eve com ruídos de backend	0.0303
Sem Eve no computador quântico	0.0399

A conclusão mais relevante contudo, é aquela objeto fim do estudo propriamente dito: a comparação entre os resultados do mundo real ou ideal com e sem a presença de *Eve*. Os dados de QBER associados ao experimentos mais relevantes para tal comparação estão condensados na Tabela 11.

Tabela 11 – Análise de resultados: Simulação x Real

Experimento	QBER
Sem Eve e sem ruídos	0.000
Sem Eve no computador quântico	0.0399
Com Eve no computador quântico	0.501
Com Eve - apenas medições e sem ruídos	0.295

Em um contexto de mundo ideal, onde não há ruídos ou bisbilhotagem, a execução retorna dados perfeitos, corroborando com aquilo que fora proposta pela teoria, resultando em um $QBER = 0$. A execução do experimento em um computador quântico, conforme esperado, é acompanhada de erros que se refletem em um $QBER \neq 0$, porém um valor reduzido, dentro do limiar de aceitação para o protocolo implementado adotado no estudo, onde $QBER = 0.0399 < 0.126$. Em uma análise ainda mais conservadora, vantajosa dentro do contexto da QKD, poderia-se dobrar o QBER, simulando um possível erro associado a transmissão dos estados, não contemplado na implementação. Mesmo após esse movimento, ainda seria possível reduzir a taxa de limite permitida. Entretanto, quando ocorre interferência de *Eve*, através de suas medições, os resultados são bem diferentes.

> Any information obtained by an illegitimate third party about the exchanged key leads to a corresponding increase in the quantum bit error rate (QBER) of the transmitted data (MUSKAN; MEENA; BANERJEE, 2024).

O $QBER = 0.501$ quando *Eve* realiza tentativas de decodificações e medições é praticamente o pior caso possível e indica que *Alice* e *Bob* teriam meios para identificar sua presença. O mesmo ocorre no exemplo simulado onde *Eve* realizaria apenas medições, sem tentativas de decodificações, dado que resultou em um $QBER = 0.295$, muito superior ao valor limite utilizado como referência ao longo do trabalho, de 12.6%.

Nesse sentido, a conclusão é que, de fato, para esse caso de estudo específico no qual se teve geração de estados quânticos e medições no mesmo sistema com *Eve* realizando medições indevidas em todos os qubits trafegados, *Alice* e *Bob* seriam capazes de detectar sua presença, não sendo possível para a entidade bisbilhoteira camuflar sua presença no ruído de meio-ambiente. Reforça-se, portanto, o proposto pela teoria do QKD que os vestígios deixados pela entidade maliciosa seriam perceptíveis em todas as combinações propostas pelo trabalho em tela.

A presença de ruído inerente à utilização dos computadores quânticos interfere nos resultados, mas de tal modo a ainda possibilitar a implementação do protocolo nesse caso de estudo, estando abaixo do valor limite estipulado. Ao adicionar medições indevidas ao longo do circuito, existindo ou não mudanças de bases de medição, o resultado é que o

protocolo deveria ser abortado dado a evidência cristalina de presença de *Eve* pela elevação substancial do QBER.

Eve, portanto, não tem o poder de medir toda a sequência de qubits enviados por *Alice* sem que isso deixe vestígios na medição de *Bob*. Entretanto, vale ressaltar que a entidade maliciosa poderia, em um ataque de negação de serviço, impedir a distribuição quântica de chaves caso tivesse acesso ao canal quântico: as suas medições constantes resultariam na decisão dos comunicantes de sempre abortarem aquela execução do protocolo e, nesse contexto, nunca conseguiriam gerar a chave. *Eve* também possui outros meios de interromper a distribuição quântica de chave, como simplesmente danificando o canal de comunicação entre eles (PORTMANN, 2021). Entretanto, assumindo que *Alice* e *Bob* adotaram métricas seguras de limiar de tolerância a erros, *Eve* não conseguiria ganhar dados completos de uma chave em potencial que foi gerada pelos comunicantes.

5 Pós-transmissão

A entidade maliciosa, *Eve*, conforme explicitado no capítulo anterior, pode sempre, em teoria, impedir a comunicação entre *Alice* e *Bob* uma vez que tenha acesso ao canal de comunicação, seja embaralhando as linhas de comunicação, realizando as medições propriamente ditas ou simplesmente atacando o canal quântico utilizando da sua criatividade. Embora tal atividade possa ser extremamente vantajosa para *Eve* em muitos casos, o foco do trabalho é, de fato, analisar o caso onde o desejável é ir além, ganhando acesso à chave final gerada, permitindo uma futura decriptografia da comunicação final e comprometendo assim a distribuição de chave quântica.

Entretanto, conforme apresentado pela teoria e corroborado pelos experimentos práticos, *Eve* acaba por deixar vestígios na sua medição se feita diretamente, tornando extremamente difícil a sua missão. A discussão que se segue é se tais fatos são, por si só, suficientes para garantir uma comunicação segura entre *Alice* e *Bob* ou se, de fato, seria necessário ou minimamente desejável que ocorresse um processo de pós-transmissão no qual, após *Alice* e *Bob* já deterem uma sequência de bits compartilhados com alta correlação, essa informação fosse ainda mais trabalhada, visando garantir um resultado final ainda melhor, com menos erros e com maior segurança associada. Tal procedimento é extremamente desejável e previsto pelos protocolos de QKD dependentes de dispositivos do tipo preparação e medição, citados pelo trabalho. O processo é realizado através da Reconciliação da Informação e da Amplificação privada, conceitos apresentados de forma sucinta ao longo das próximas seções.

5.1 A importância dos procedimentos de pós-transmissão

O primeiro ponto a ser considerado é que a correlação final entre os dados de *Alice* e *Bob* não é perfeita, ou seja, a sequência de bits detidas individualmente por ambas as partes não são idênticas entre si, embora muito próximas. Ressalta-se, portanto, o fato previamente apresentado de que a comunicação não será isenta de erros. Conforme visto, o QBER só é 0 no caso ideal, em um contexto simulado. Adotando erros do meio-ambiente, apresentados pelo trabalho em tela como os erros do computador quântico real, entende-se que seria vantajoso um aumento de correlação entre as sequências detidas individualmente por *Alice* e por *Bob* dado o $QBER \neq 0$. Esse processo, de redução de erros em relação às chaves finais geradas, é denominado Reconciliação da Informação e é importantíssimo para que, ao final do processo, a criptografia e decriptografia da mensagem possam ocorrer conforme defende a teoria do *one-time-pad*, utilizando uma chave simétrica que, em ambas as etapas do procedimento de criptografia e decriptografia, é, verdadeiramente, a mesma.

O segundo aspecto analisado remete ao tamanho da interferência que *Eve* causará. Assumindo que *Eve* medirá toda a sequência de qubits transferidos entre *Alice* e *Bob*, pode-se entender, conforme explicitado ao longo do trabalho, que os vestígios deixados pela entidade bisbilhoteira serão profundos o suficiente para comprometer, como um todo, a distribuição quântica de chaves. Contudo, não necessariamente *Eve* realizará medições em todos os qubits transmitidos. Nas execuções do capítulo 4, por exemplo, analisou-se a medição de 5 qubits e como isso comprometeria a correta medição dessa amostragem específica. O contexto prático da distribuição, porém, teria um número de qubits trafegados substancialmente maior.

Nesse sentido, a tese é de que caso *Eve* realizasse medições em apenas uma parte pequena dos dados sua presença poderia não ser notada por estar dentro de um limiar de erro previsto. Caso *Eve* medisse 5 qubits de cada 1000 transmitidos pelo canal, por exemplo, a porcentagem de dados comprometidos seria de 0,5%, um número que poderia sim ser camuflado, dado que a execução no mundo real não foi perfeita nos experimentos.

Analisando, por exemplo, os "Resultados do circuito sem Eve" executados no *ibmq_belem*, pode-se assumir um QBER associado igual a $\frac{798}{20000} = 0.0399$. Caso fosse do interesse incluir nessa amostra a interferência de *Eve*, que mediu 5 qubits a cada 1000 totalizando interferência em 100 qubits, ter-se-ia $QBER_2 = \frac{798+100}{20000} = \frac{898}{20000} = 0.0449$, um QBER muito próximo do original e ainda bem abaixo do limite adotado pelo trabalho em tela. Nesse caso, *Eve* teria, em tese, adquirido a possibilidade de obter informações a respeito da chave sem ser notada: *Alice* e *Bob* teriam tolerado esse erro inserido.

Em um adendo relacionado a interferência reduzida de *Eve*, caso as partes comunicantes aceitassem um limite de 10% para o caso de estudo, por exemplo, podería-se ter 2000 bits incorretos a cada 20000 qubits transmitidos, um valor extremamente alto que resultaria em $2000 - 798 = 1202$ qubits que *Eve* poderia interferir e causar erros sem que *Alice* e *Bob* abortassem o protocolo, mais de 6% do valor total!

Explicita-se, portanto, a necessidade das partes comunicantes conhecerem bem o canal e adotarem um limiar de erro compatível com as características do sistema de implementação. Assumindo uma mensuração prévia do $QBER = 0.399$ para o sistema, por exemplo, poderia-se pensar em uma taxa de erro máxima que circularia próxima dos 4%. Uma taxa limite próxima do QBER medido previamente resulta em mais segurança para o sistema dado que qualquer informação que uma entidade externa ganhe sobre a chave resulta em aumento do QBER (MUSKAN; MEENA; BANERJEE, 2024).

O caso supracitado de *Eve* ter acesso a quase 6% dos qubits é alarmante, mas mesmo em um exemplo didático limitado no qual a quantidade de informação detida pela entidade fosse 20 bits ter-se-ia dados muito valiosos, diferentemente do que um pensamento preliminar e pouco profundo poderia sugerir. Supõem-se, portanto, que *Eve* conseguiu acesso a 20 qubits sem que *Alice* e *Bob* percebessem sua interferência.

Pode-se pensar, dado todo esse contexto, que das 20 medições realizadas em apenas metade dos casos *Bob* acerta a base de medição, assumindo duas bases de codificação, conforme estipula originalmente o protocolo BB84, levando a 10 bits finais que irão fazer parte da chave. Nesse caso, assume-se a possibilidade de *Eve* ter a capacidade de armazenar os estados quânticos e só medi-los após a divulgação das bases por *Alice*, o que pode ser considerado quando se entende-se *Eve* como detentora de uma tecnologia infinita (H.; PATHAK, 2018).

Embora a utilidade dos 10 bits de informação possa ser preliminarmente questionada através de uma análise superficial, conforme mencionado, a verdade é que a importância da informação detida agora por *Eve* não pode ser menosprezada. O primeiro ponto é que agora *Eve* possui a certeza de alguns bits e, assim sendo, ganha algum referencial de qual é a chave a ser buscada.

Saber parte da chave pode gerar grande impacto caso seja possível decriptografar parte de uma mensagem, por exemplo, podendo levar a estimativas mais direcionadas do que foi transmitido. No contexto da Tabela 2, por exemplo, caso *Eve* estivesse, didaticamente falando, em dúvida apenas entre os casos 1 e 2, descobrir parte da chave que fornecesse certeza da primeira ou da última letra resultaria em descobrir a mensagem original.

Adicionalmente, em um eventual ataque de força bruta para decriptografia da chave, cada bit final que *Eve* tem certeza sobre a chave não precisa ser testado, reduzindo efetivamente o número de tentativas pela metade para cada bit conhecido, dado que ao invés de testar ambas as possibilidades, com o valor 0 ou testar com o valor 1, *Eve* poderia, ao invés disso, apenas inserir o valor correto.

Caso *Eve* soubesse, por exemplo, o último bit, ter-se-ia análise apenas dos casos ímpares ou pares, a depender do valor. Independentemente do valor escolhido ou do bit escolhido, ter-se-ia o número de casos a serem testados reduzido pela metade. Analogamente, caso soubesse o valor de outro bit, o valor de casos de teste novamente seria reduzido pela metade. Nesse sentido, saber dois bits leva a redução do valor pela metade da metade, ou à 2^2. A iteração é contínua, levando a redução de testes totais pela metade para cada bit descoberto, conforme adiantado. Em uma análise de pior caso, no qual testa-se todas as possibilidades, assumindo que o tempo gasto em cada tentativa é o mesmo, o resultado final é:

$$Tempo\_Final\_Com\_Informação = \frac{(Tempo\_Originalmente\_Gasto)}{2^{(bits\_adquiridos)}} \tag{5.1}$$

Esse fato realça a relevância das informações adquiridas por *Eve*, mesmo que seja uma fração dos dados totais transmitidos. A precisão dessa informação, por menor que seja, representa uma vantagem significativa para um possível atacante. Na situação apresentada inicialmente na qual *Eve* teria certeza sobre 10 bits do resultado final, diminuiria-se em

$2^{10} = 1024$ vezes o número de tentativas totais necessárias para encontrar a chave. O resultado dessa redução, em medidas de tempo com 1 segundo para cada operação, seria gastar menos de dois minutos para o que originalmente levaria um dia, 86.400 tentativas sendo reduzidas para menos de 90 tentativas.

Torna-se, portanto, imperativo considerar e mitigar qualquer conhecimento indevido adquirido durante o processo de distribuição quântica de chaves. Nesse contexto, a estratégia a ser adotada por *Alice* e *Bob* seria tal de aumentar o valor do segredo por eles detido, um processo denominado Amplificação privada, explicitado após contextualização da etapa de Reconciliação da informação.

5.2 Reconciliação da informação

A reconciliação da informação emerge como uma etapa crítica nos sistemas de Distribuição Quântica de Chaves desempenhando um papel crucial na garantia da coerência da chave criptográfica gerada entre as entidades envolvidas. Este processo visa mitigar discrepâncias e erros que possam surgir durante a troca de informações quânticas entre *Alice* e *Bob*, sendo fundamental para assegurar que ambas as partes obtenham uma chave secreta idêntica.

De forma resumida, portanto, a reconciliação da informação é uma correção de erros que almeja corrigir discrepâncias resultantes das eventuais interferências que ocorram durante a comunicação, sejam imperfeições do canal, gerando ruídos atribuídos ao meio-ambiente, ou falhas devido à interferência de *Eve*. Um aspecto extremamente relevante desse procedimento é que ele é realizado focado na chave gerada que, conforme explicitado ao longo do trabalho, se trata de uma chave formada por bits, ou seja, é um procedimento clássico de correção de erros.

Adicionalmente, o procedimento de reconciliação da informação é entendido como uma correção de erros que ocorre em um canal público autenticado. Essa suposição inicial preserva o propósito da Distribuição Quântica de Chave que almeja, como foco principal, a geração de uma chave que permita uma comunicação segura. Assume-se, portanto, que até esse momento chegar no qual *Alice* e *Bob* compartilhem uma mesma chave segura, que a comunicação entre ambos deve ocorrer em um canal público sem criptografia.

Nesse sentido, a estratégia clássica de correção de bits a ser adotada deve promover uma correção de erros entre as strings detidas por ambas as partes comunicantes divulgando a menor quantidade de informação possível para eventuais entidades maliciosas. Dentre as diferentes abordagens para resolução do problema de aumentar a correlação entre as chaves de *Alice* e *Bob* divulgando tanto menos quanto possível para *Eve*, rotineiramente aborda-se testes de paridade em subpartições da cadeia de bits detida por uma das partes.

> Information reconciliation is nothing more than error-correction conducted over a public channel, which reconciles errors between X and Y to obtain a shared bit string W while divulging as little as possible to Eve. After this procedure, suppose Eve has obtained a random variable Z which is partially correlated with W (NIELSEN; CHUANG, 2011).

A estratégia a ser utilizada para os testes de paridade não é um consenso na comunidade científica, embora muitos considerem como algoritmo padrão o protocolo Cascade, desenvolvido por Brassard e Salvail. No entanto, algumas limitações associadas ao algoritmo o tornam não tão vantajoso em certas situações, não havendo, até então, um consenso generalizado de qual a melhor escolha associada aos algoritmos de correção de erros (ELKOUSS, 2010).

Poderia-se, portanto, a título de exemplo de um teste de paridade, escolher um dos comunicantes, *Alice* ou *Bob*, para criar uma mensagem clássica u contendo um subgrupo de seus bits, X. A string u tem, então, algumas características divulgadas para o outro comunicante relativas a suas especificações e paridade, permitindo que seja o recebedor dessas informações consiga corrigir bits em sua string Y. A ideia é que, ao final do processo, tanto *Alice* quanto *Bob* compartilhem da mesma string, denominada, por exemplo, de W. O número final de bits detidos por *Alice* e *Bob* é reduzido ao longo do processo e existe a divulgação de conhecimento adicional para *Eve*, que poderia, por exemplo, sair de uma string $Z1$ para uma string $Z2$ na qual a correlação de $Z2$ com W é maior do que a correlação entre $Z1$ e X ou entre $Z1$ e Y.

> Information reconciliation further reduces the number of bits that Alice and Bob can obtain (NIELSEN; CHUANG, 2011).

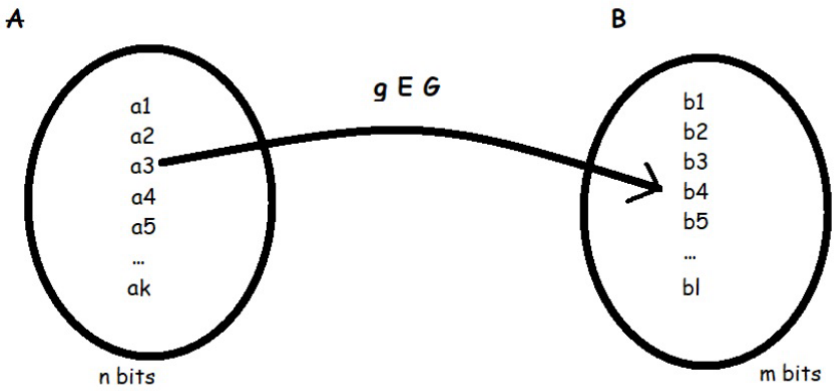
5.3 Amplificação privada

Conforme mencionado, o procedimento de reconciliação da informação acaba por incrementar o conhecimento que *Eve* detém sobre a chave compartilhada por *Alice* e *Bob*. Visando sistematicamente reduzir a informação detida pela entidade maliciosa, as partes comunicantes destilam então de seus bits um conjunto menor de bits cuja correlação com a chave detida por *Eve* está abaixo de uma valor limite: esse procedimento é a chamada amplificação privada.

> Privacy amplification is a process that allows two parties to distil a secret key from a common random variable about which an eavesdropper has partial information. The two parties generally know nothing about the eavesdropper's information except that it satisfies a certain constraint. The results have applications to unconditionally secure secret-key agreement protocols and quantum cryptography, and they yield results on wiretap and broadcast channels for a considerably strengthened definition of secrecy capacity (BENNETT et al., 1995).

Dentre as diferentes maneiras de ganhar maior privacidade associada a chave detida existe a utilização da classe de funções hash universais G que mapeiam strings de n bits de A em strings de m bits de B através de uma função g, escolhida randomicamente, que pertence à G. A figura 25 ilustra a aplicação da função $g \in G$ em $a_3 \in A$ levando até $b_4 \in B$, na qual a_3 possui n bits e b_4 possui m bits.

Figura 25 – Exemplo aplicação hash



Fonte: autoria própria

Dentro do contexto da distribuição quântica de chaves, *Alice* e *Bob* poderiam publicamente selecionar uma função g pertencente à G e aplicá-la à string compartilhada detida por eles, chamada de W, após realização da reconciliação da informação. Tal aplicação levaria a uma nova string destilada S, que poderia ser utilizada como sua chave. Nesse contexto, mesmo *Eve* detendo conhecimento parcial sobre W através de sua string $Z2$, ela não conseguiria chegar em S, diminuindo a correlação daquilo que ela possui com a chave final escolhida. A menção relevante é que a chave destilada possui uma quantidade menor de bits sendo inclusive escolhida de tal forma a maximizar a incerteza de *Eve* sobre a chave final (NIELSEN; CHUANG, 2011).

5.4 Entendendo os processos pós-comunicação como uma decodificação CSS

Outra abordagem a respeito dos procedimentos de pós-comunicação como um todo seria entender a aplicação de reconciliação da informação com posterior amplificação privada como a decodificação de um código CSS randômico. Considerar-se-á para essa comparação dois códigos clássicos lineares, C_1 e C_2, satisfazendo a condição de corrigirem até t erros. Têm-se, então, um código CSS: $C_2 \subset C_1$ e C_1 e $C_2^{\perp}$ ambos corrigindo t erros.

O pensamento reside em entender a string detida por *Alice*, X, e a string detida por *Bob*, Y, de tal forma que $Y = X + ERRO$, seja esse erro qual for, meio-ambiente ou *Eve*, menor que t. Nesse sentido, sendo o erro menor que o dado limiar poderia-se ter uma correção para a palavra-código pertencente ao código linear clássico C_1 mais próxima de X e Y, levando em x' e y' tal que $x' = y' = W \in C_1$. Finalizada a correção de erros, *Alice* e *Bob* poderiam calcular a classe lateral de $W + C_2$ em C_1, resultando em uma string de m bits: a chave s final. Como *Eve* não detém conhecimento sobre C_2 ou sobre suas propriedades, reduziria-se assim a informação mútua por ela detida (NIELSEN; CHUANG, 2011).

5.5 Suposições padrão

De uma maneira genérica, pode-se dizer que a segurança de protocolos criptográficos estão intimamente ligadas a suposições que dizem respeito sobre os componentes físicos utilizados na sua implementação, ou seja, está atrelada aos dispositivos utilizados. Naquilo que diz respeito à Distribuição Quântica de Chaves dependente de dispositivos, existe um conjunto de suposições necessárias para o correto funcionamento do protocolo. De forma antecipada, adianta-se o fato de que nem sempre é possível atingir tais suposições em implementações reais, o que tem como consequência a geração de vulnerabilidades que podem ser explorados por ataques quânticos (PORTMANN, 2021).

A segurança dos protocolos de QKD dependente de dispositivos geralmente se baseia nas seguintes suposições:

1. Todos os dispositivos usados por *Alice* e *Bob*, assim como os canais de comunicação que os conectam, são correta e completamente descritos pela teoria quântica.
2. O canal que *Alice* e *Bob* utilizam para trocar mensagens clássicas é autêntico, ou seja, é impossível para um adversário modificar mensagens ou inserir novas.
3. Os dispositivos que *Alice* e *Bob* utilizam localmente para executar as etapas do protocolo, como preparar e medir sistemas quânticos, fazem exatamente o que são instruídos a fazer.

A primeira das suposições é necessária até mesmo para iniciar a descrição do modelo de implementação do protocolo: todo o esquema criptográfico tem como requisito a correta descrição dos mesmos pela teoria quântica. Vale a ressalva de que um dos alicerces fundamentais para que os protocolos de distribuição quântica de chave sejam de fato efetivos repousa em teoremas como a não-clonagem e o ganho de informação estar atrelado a perturbação do sinal com geração de ruído. Nesse contexto, dizer que um dado adversário, como *Eve*, não está limitado pelas leis da teoria quântica invalidaria todo o

esquema criptográfico proposto por protocolos como o BB84. Entende-se que a suposição 1 é amplamente aceita, dado que provar o contrário representaria um avanço significativo na física.

> Assumption 1 is widely accepted — and proving it wrong would represent a major breakthrough in physics.(PORTMANN, 2021).

A suposição número 2 diz respeito do canal clássico, sendo garantido que ele é autêntico. Sabe-se que adotar a ideia de um canal privado e seguro entre *Alice* e *Bob* recairia no problema do ovo e da galinha, ou seja, utilizaria uma premissa de comunicação segura que é justamente o que o protocolo se propõem a fazer. Nesse sentido, a suposição a respeito do canal, mesmo que ele seja público, é de difícil aceitação inicialmente. Entender que *Eve* não poderia inserir novas mensagens no canal, por exemplo, seria assumir que as configurações de comunicação por meios clássicos entre *Alice* e *Bob* são muito bem protegidas.

Apesar disso, a justificativa principal para que protocolos de QKD sejam úteis de fato é a possibilidade de criar chaves simétricas fortes de utilização única que permitirão uma comunicação segura, ao passo que, para apenas garantir a autenticidade de um canal público, pode-se utilizar chaves fracas. Nesse sentido, embora não seja uma tarefa fácil para a criptografia clássica a garantia de autenticidade, essa é uma tarefa factível e de baixo custo associado quando comparado à geração e distribuição de longas chaves simétricas randômicas para implementação do one-time-pad, ou seja, repousa-se sobre a ideia de garantir um canal clássico autêntico com a utilização de chaves fracas compartilhadas entre *Alice* e *Bob* e, a partir daí, após ter a suposição 2 atendida, implementar-se-ia protocolos de Distribuição Quântica de Chave (PORTMANN, 2021).

A suposição 3 é relativamente intuitiva. Dizer que espera-se que os dispositivos se comportem conforme o esperado é uma premissa necessária para quase qualquer esquema computacional ou criptográfico, incluindo nesse aspecto inclusive procedimentos clássicos. Em um exemplo hiperbólico, seria o mesmo que, em um algoritmo de controle de finanças, por exemplo, esperar que uma dada calculadora utilizada execute operações de soma e subtração corretamente. Apesar disso, atender essa suposição de correta funcionalidade dos equipamentos físicos é bastante desafiador no contexto quântico, o que abre espaço para geração de vulnerabilidades indesejáveis potencialmente exploráveis por ataques hackers quânticos (PORTMANN, 2021), mencionados na subseção a seguir.

> Numerous quantum hacking experiments, which have been conducted over the past few years, have shown that many implementations of QKD failed to satisfy this assumption (PORTMANN, 2021).

5.6 Ataques hackers quânticos e contramedidas

Em um contexto mais amplo de definição, um ataque hacker poderia ser descrito como ações deliberadas e maliciosas de indivíduos ou grupos para comprometer sistemas de computadores, redes, dispositivos eletrônicos ou dados. Tais ações maliciosas podem ter diferentes objetivos, indo desde a obtenção de acesso não autorizado a informações sensíveis até a alterações de dados propriamente dita. Em alguns casos, o ataque pode inclusive ter como foco primário a demonstração de habilidades técnicas, embora os casos mais preocupantes incluam, conforme antecipado, ações mais danosas, a citar como exemplos a interrupção de serviços, a espionagem cibernética ou a disseminação de malwares.

Dentro de ataques hackers pode-se ter a exploração de vulnerabilidades como uma atividade específica. Esta consiste em identificar e aproveitar falhas de segurança de um dado sistema, software ou rede, ganhando acesso não autorizado, contornando medidas de segurança ou simplesmente executando qualquer tipo de ação prejudicial. Tais vulnerabilidades podem surgir de diversos fatores, como erros de programação, configurações inadequadas, falta de atualizações de segurança ou uso de software obsoleto.

No contexto abordado na seção anterior, a causa principal de vulnerabilidade mencionada seria o funcionamento de dispositivos físicos de uma maneira diferente do esperado, ou seja, limitações de hardware criariam brechas, vulnerabilidades, a serem potencialmente exploradas por em ataques laterais, por exemplo. Tais conceitos estão intimamente relacionados ao contexto da cibersegurança, no qual a proteção contra ataques e a correção de vulnerabilidades são aspectos críticos para manter a integridade e a segurança dos sistemas de informação em um contexto global de segurança da informação.

As subseções a seguir descrevem brevemente alguns dos ataques hackers quânticos mais comuns dentro do contexto da Distribuição Quântica de Chaves de preparação e medição dependente de equipamentos que exploram, em muitos casos, as supracitadas limitações de hardware.

5.6.1 Photon number splitting attack

Dentre as diferentes abordagens sugeridas para implementação prática do Protocolo BB84 existe uma na qual utiliza-se uma implementação óptica com fótons individuais como portadores de informação quântica. A IBM, por exemplo, realizou a implementação de um sistema comercial de fibra ótica citado em (NIELSEN; CHUANG, 2011) no qual *Alice* e *Bob* realizam comunicação em uma distância de 10 quilômetros de distância entre si. Nesse esquema supracitado, *Bob* inicialmente gera, através de um lazer de diodo, luz que será posteriormente atenuada por *Alice* até atingir um fóton único. Além disso, *Alice* polariza o fóton único em algum dos estados previamente estabelecidos e o encaminha para *Bob* que tem a função de medi-lo utilizando um analisador de polarização.

No contexto apresentado, descreve-se a implementação explícita do Protocolo BB84. Entretanto, assume-se que apenas um fóton é, de fato, enviado por vez. Dentro do escopo de explorar vulnerabilidades geradas por equipamentos não ideais pode-se ter a ocorrência, por exemplo, de dois fótons serem transmitidos. O problema principal é que ambos terão a mesma polarização associada (PORTMANN, 2021).

Nesse caso ocorre o ataque de separação do número de fótons, em uma tradução livre para o Photon Number Splitting attack descrito em (BRASSARD et al., 2000). Esse ataque é comumente referenciado pelas iniciais das palavras que o nomeiam, sendo denotado por "*PNS attack*". A consequência direta do canal quântico transmitir esse qubit extra, indesejado, é que *Eve* agora pode medi-lo sem receios de gerar ruído no canal, dado que ela toma para si um qubit que não era esperado. Nesse caso, *Bob* não perceberia, em tese, a ausência do qubit roubado por *Eve* dado que ele não deveria existir. *Eve*, assim sendo, teria posse de uma valiosa fonte de informação.

> The essential idea behind the attack is that Eve can perform a quantum non-demolition measurement to determine the number of photons in a run and when it is greater than 1, she could steal one of the excess photons while forwarding the others to Bob. (PIRANDOLA, 2019).

Por explorar uma característica que não foi modelada na prova de segurança, ou seja, por abordar a vulnerabilidade associada à geração e transmissão de um fóton duplo não prevista originalmente, o ataque PNS é considerado um exemplo de ataque de canal lateral.

> Attacks that exploit features not modeled in the security proof are known as side-channel attacks (PIRANDOLA, 2019).

5.6.2 Time-shift attack

Embora o ataque PNS atue diretamente em uma vulnerabilidade gerada pelo comunicante gerador do sinal também é possível realizar ataques que estão vinculados ao recebimento do sinal, atuando diretamente no processo de medição. Esse é o caso do Time-shift attack, por exemplo, que, em uma tradução livre, seria um ataque de distorção do tempo. O ataque explora as peculiaridades dos detectores de fótons que, almejando evitar contagens escuras, são configurados de tal modo a somente contar fótons que chegam dentro de uma pequena janela de tempo pré-definida dentro da qual espera-se, de fato, a chegada de um fóton.

Nesse sentido, a parte comunicante que recebe o sinal, *Bob*, tem o seu sistema de medição formado por mais de um equipamento. A configuração poderia, por exemplo, ser de um medidor para cada estado polarizado possível. As janelas de tempo de cada detector são diferentes e nunca sincronizados, o que implica que existem intervalos de tempo nos quais o

receptor com um todo é mais sensível a sinais de determinada polarização (PORTMANN, 2021). Utilizando desse contexto, o atacante, *Eve*, atrasa de forma proposital os sinais enviados por *Alice*, realizando uma distorção do tempo que estes chegariam até *Bob*, gerando assim uma maior chance estatística do sinal recair em algum dos medidores específicos, que possuem uma determinada polarização, ganhando assim informação sobre o que foi medido.

> For instance, if the detector corresponding to the outcome 0 has a higher efficiency at some given time than the detector corresponding to the outcome 1, Eve can know that if the time of arrival of the pulse is shifted such that it arrives at the detector at that particular time, and the pulse is detected by one of the detectors, it is more likely that the outcome was 0 than that it was 1 (PIRANDOLA, 2019).

5.6.3 Detector blinding attack

Embora ganhar informação seja um dos objetivos primários de *Eve*, em determinadas situações apenas impedir a comunicação pode ser vantajoso. Existem diferentes maneiras de gerar ruídos na medição, por exemplo, o que acabaria por prejudicar o protocolo de Distribuição Quântica de Chaves ao ponto dele ter de ser abortado. Apesar disso, nem sempre é fácil ganhar acesso àquilo que está trafegando no canal de comunicação quântico.

Dado esse contexto, uma solução possível para *Eve* prejudicar a comunicação entre *Alice* e *Bob* seria através da geração de um raio de luz direcionado para o receptor de fótons de *Bob*. A justificativa de eficácia para esse ataque está no fato do receptor de fótons ser acionado para detectar um pulso único de fóton, "clicando" ao recebê-lo. Dado o tempo de relaxação do receptor há um intervalo de tempo entre um clique o próximo. O caso, porém, é que o receptor pode, em determinadas situações, sempre clicar quando expostos a uma luz de uma intensidade específica. Nesse sentido, quando *Eve* iluminasse o receptor de *Bob* com a correta polarização e intensidade o dispositivo de *Bob* clicaria, assumindo que recebeu um fóton, e ficaria impedido de corretamente medir aquilo que fosse oriundo de *Alice* posteriormente (PORTMANN, 2021).

Adentrando ainda mais no ataque de cegamento de detector, *Eve* poderia elaborar uma estratégia ainda mais complexa e potencialmente mais prejudicial ao comunicantes, que seria interceptar os fótons enviados por *Alice*, os medindo em uma dada base, conforme seria esperado que *Bob* fizesse. *Eve*, então, enviaria o raio de luz para *Bob* forçando o seu receptor a clicar, como se ele tivesse recebido fótons de *Alice* (PORTMANN, 2021). A consequência direta em uma ataque bem sucedido dessa forma seria o controle remoto do dispositivo de *Bob*, principalmente nos casos onde o equipamento é responsável por definir a escolha base de medições. Nesse caso, *Eve* poderia inclusive forçar o receptor a somente clicar quando a polarização escolhida fosse a mesma que a sua, forçando um resultado, nesse caso, de igual valor ao obtido pela entidade maliciosa (PIRANDOLA, 2019).

5.6.4 Trojan-horse attacks

Conforme visto, é possível realizar ataques tanto na geração de sinal, afetando diretamente *Alice*, quanto realizar ataques na medição do sinal, interagindo com eventuais vulnerabilidades permitidas por *Bob*. O grande potencial de poder atuar em ambos os lados da comunicação é, para *Eve*, o potencial de poder de escolher a brecha deixada pela parte menos segura da comunicação. Nesse sentido, mesmo que um dos lados tivesse equipamentos perfeitos e um protocolo suficientemente seguro, enquanto a outra parte apresentasse falhas o protocolo como um todo poderia ficar comprometido. Estes ataques, contudo, não são a única categoria existente, sendo possível realizar, por exemplo, ataques no estilo cavalo-de-troia.

Assim como na história, na qual os gregos se esconderam em um cavalo para adentrar no território de Troia, no contexto de ataques hackers um ataque de cavalo-de-troia se parece como algo inofensivo e tem como objetivo primário enfraquecer as defesas da entidade que está sendo atacada. No contexto quântico, a ideia seria enviar raios de luz dentro dos componentes de alguma das partes comunicantes para obter informações de suas configurações.

> Depending on the sender and receiver hardware which is used, measuring the reflection of the pulse can allow Eve, for instance, to determine the basis choices made by Alice and Bob. (PORTMANN, 2021).

Tais informações são potencialmente muito valiosas no sentido de descobrir vulnerabilidades a serem explorados. O ataque, portanto, não gera informação sobre a chave gerada propriamente dita, porém acaba por reduzir a segurança das partes comunicantes através do ganho de informações sobre o sistema de implementação do protocolo, como qual das entidades, *Alice* ou *Bob*, possuiria mais brechas. O adendo final é que, por não necessariamente gerar qualquer distorção de sinal, o ataque pode passar completamente despercebido e, assim como no caso de Troia, só ser percebido após ter cumprido seu propósito (PIRANDOLA, 2019).

5.6.5 Outros tipos de ataques

Ao realizar estudos associados ao QKD é importante adotar a hipótese de que o adversário tem tecnologia ilimitada. Assim sendo, considera-se que *Eve* consegue realizar na prática tarefas extremamente difíceis, fato extremamente relevante na hora de confeccionar provas de segurança. É o caso do que fora citado na seção 5.1, ao afirmar que *Eve* poderia armazenar os estados quânticos por ela detidos até que *Alice* divulgasse quais foram as bases de decodificação associadas. Nesse sentido, *Eve* não precisaria se preocupar em acertar a base escolhida, tendo sempre 100% de acertos.

> More generally, Eve may use sophisticated attacks going beyond the above intercept-resend method. A rigorous proof for security must be able to cover not only general attacks on individual qubits, but also coherent attacks on all qubits, with Eve's final manipulations deferred until after basis reconciliation (H.; PATHAK, 2018).

Nesse mesmo contexto, pode-se entender também que *Eve* não realiza apenas ataques individuais, fóton a fóton, mas que ela é capaz de atacá-los em conjunto, os chamados ataques coerentes. Tais ataques são inclusive mais poderosos do que ataques individuais em certos cenários, conforme demonstrado em (SANDFUCHS; WOLF, 2023). É permitido a *Eve*, portanto, enquanto detentora de tecnologia infinita, adotar a melhor estratégia de ataque em cada cenário.

Visando mitigar a atuação da entidade maliciosa, contudo, certas contramedidas podem ser adotadas, auxiliando a implementação dos protocolos de QKD com maior segurança. A subseção a seguir cita algumas das possíveis contramedidas.

5.6.6 Contramedidas

A primeira das contramedidas que visa mitigar o poder de atuação de *Eve*, embora óbvia, é extremamente eficaz: melhorar os equipamentos. Conforme visto, limitações dos dispositivos criam diversas vulnerabilidades, sejam devido à geração de fótons duplicados ou por ineficiências associadas aos dispositivos de medição. Melhorar os equipamentos reduziria em muito as possibilidades de ataque a serem executados por uma entidade maliciosa quando se trata da implementação de Distribuição Quântica de Chaves dependente de equipamentos: quanto menor o QBER, melhor é a para as entidades comunicantes.

Entretanto, atingir a idealidade é, com a tecnologia atual, algo irreal: ter uma fonte perfeita de geração de fóton único ou um equipamento de medição que só clique em um regime de parametrização específico, por exemplo, é utópico. Não seria possível, portanto, melhorar os dispositivos até a idealidade.

> The devices used in experiments will always, at least slightly, deviate from these specifications. (PORTMANN, 2021)

Contudo, apenas conhecer bem as falhas dos equipamentos previamente pode ser extremamente benéfico para *Alice* e *Bob*. Uma situação que evidencia o poder de ter informações sobre o próprio sistema de implementação é, por exemplo, saber que a geração de sinais gerará fótons duplos. Isso pode ser realizado inclusive de maneira intencional em algumas situações, com *Alice* enviando pulsos de vários fótons em uma estratégia denominada método de estado-isca (decoy-state method), no qual verificaria-se estatisticamente a presença desses pulsos com vários fótons. A ideia é que *Bob* espera receber erros, ou seja, é esperado ter pulsos com mais de um fóton. Caso isso não ocorra,

a hipótese a ser adotada é que existe uma entidade maliciosa no meio do caminho, *Eve*, interceptando os pulsos que possuem mais de um fóton. *Alice* e *Bob*, portanto, seriam capazes de detectar a presença de um adversário (PORTMANN, 2021).

Adotando ideias semelhantes, pode-se através de diferentes maneiras buscar a detecção de um potencial adversário na comunicação. A ressalva válida é que a segurança do protocolo não está atrelada a uma comunicação sempre eficaz e segura, mas na garantia de potencialmente detectar aquelas gerações cuja segurança não pode ser garantida.

Nesse sentido, conhecer bem o canal e com base nisso escolher um bom limite de ruído é uma excelente contramedida. Adotaria-se, assim, um limite máximo de ruído próximo do QBER previamente estabelecido, a exemplo do que fora sugerido na seção 5.1, abortando a comunicação caso, em uma dada execução, o QBER medido se distanciasse do valor de referência.

Outro ponto de escolha importante seria definir um viés máximo de escolha de base de decodificação por parte de *Bob*, o protegendo de ataques na modalidade distorção de tempo, por exemplo, que levariam a uma escolha estatisticamente maior de determinada base de decodificação. Por fim, o monitoramento de fotocorrente possibilitaria a detecção de ataques de cegamento, permitindo a ele minimamente definir que o seu receptor está tendo o clique acionado de maneira indevida (PORTMANN, 2021).

Apesar das contramedidas supracitadas, contudo, permanece o fato da dificuldade prática de desenvolver equipamentos que se comportem exatamente conforme o esperado. Tal fato leva a possibilidade de execução de ataques laterais aos protocolos de QKD dependentes de equipamentos, como o BB84 ou o E91, dado que, nesses casos, são especificados quais estados devem ser preparados e quais medidas devem ser feitas nesses estados preparados. A prova de segurança, portanto, depende das características exatas dos dispositivos utilizados por *Alice* e *Bob*, fazendo com que a segurança do protocolo seja comprometida caso o funcionamento dos equipamentos não ocorra como esperado (RENNER, 2022). Nesse contexto, é válido mencionar a Distribuição Quântica de Chave Independente de Dispositivo, Device-Independent QKD (DIQKD), como uma das possíveis alternativas para o problema de equipamentos não-ideais, mais especificamente fontes imperfeitas (MAYERS; YAO, 1998).

5.7 Distribuição Quântica de Chave Independente de Dispositivo

Como o próprio nome já sugere, a DIQKD é uma abordagem para geração de chaves que independe dos equipamentos utilizados por *Alice* e *Bob*, uma diferença significativa em relação ao QKD tradicional em seus protocolos BB84 ou o protocolo de seis estados, por exemplo. A DIQKD, então, se caracteriza por utilizar equipamentos não confiáveis para distribuir chaves secretas em uma rede insegura, resolvendo, em teoria, eventuais lacunas

de implementação associadas a fontes suscetíveis a falhas (SCHWONNEK et al., 2021).

> By removing all assumptions about the quantum devices from the security analysis, a higher level of safety is achieved, as the security proof applies to all possible implementations of the states and measurements involved in the protocol (RENNER, 2022).

No DIQKD, *Alice* e *Bob* recebem equipamentos de medição que eles utilizam para performar medidas randômicas em uma sequência de pares emaranhados provisionados por uma fonte externa não confiável (SCHWONNEK et al., 2021). *Alice* e *Bob*, então, verificam as estatísticas dos dados de entrada e saída dos equipamentos validando se a desigualdade de Bell é violada (PIRANDOLA, 2019). A ideia fundamental para que seja possível utilizar equipamentos não confiáveis é que eles próprios estão sendo testados ao longo da execução do protocolo, utilizando, o supracitado teste de desigualdade de Bell, que fornece a segurança associada ao DIQKD (RENNER, 2022).

O contexto é que, ao verificar o emaranhamento entre os pares recebidos por *Alice* e *Bob*, pode-se certificar da quantidade de informação eventualmente adquirida pela entidade bisbilhoteira, *Eve*, simplesmente checando a estatística dos dados de entrada e saída (RENNER, 2022). Nesse sentido, caso algum teste não resulte conforme o esperado, a execução do protocolo é abortada.

Outra vantagem associada ao DIQKD em relação ao QKD seria, portanto, não ter a necessidade de constantemente testar a funcionalidade dos equipamentos visando garantir que o comportamento está dentro do previsto: nenhum teste sofisticado é necessário no DIQKD para detectar dispositivos que não estão funcionando suficientemente bem (PIRANDOLA, 2019).

Apesar do DIQKD ser considerado mais seguro que o QKD, contudo, ele é mais difícil de ser implementado, tendo uma demonstração prática dos protocolos fora do alcance da tecnologia atual, apesar dos progressos teóricos associados (NADLINGER et al., 2022). A dificuldade está muito alinhada ao fato de não ser realizada qualquer suposição sobre os equipamentos, fazendo ser necessário considerar o pior cenário possível no qual *Eve* tem total controle sobre os equipamentos. A consequência é que são obtidas taxas menores no DIQKD, resultando em maiores requisitos em implementações experimentais (RENNER, 2022).

> The practical implementation of DIQKD, however, remains a major scientific challenge. This is mainly due to the need to have extremely good channel parameters (i.e., high Bell violation and low bit error rate), which in practice requires ultra-low-noise setups with very high detection efficiencies (SCHWONNEK et al., 2021).

Dado a dificuldade prática de implementar o DIQKD e a sua limitação em relação às taxas de chaves obtidas, surge a ideia de formular um meio termo entre o QKD e

o DIQKD, visando adotar uma estratégia mais confiável, mas que não necessite que todos os dispositivos quânticos sejam tratados como caixas-pretas. Nesse sentido, surgem os protocolos de semi-independência de dispositivos, ou semi-device-independent, no qual apenas algumas suposições são feitas sobre os dispositivos (PORTMANN, 2021). Dentro dessa classe genérica de protocolos, destaca-se a Distribuição Quântica de Chave Independente de Dispositivo de Medição, citada na subseção a seguir.

5.7.1 Distribuição Quântica de Chave Independente de Dispositivo de Medição

A Distribuição Quântica de Chave Independente de Dispositivo de Medição, do inglês measurement device independent, MDI-QKD, é uma estratégia de QKD no qual nenhuma suposição é feita a respeito dos dispositivos de medição, mas adota-se suposições a respeito dos equipamentos de geração de sinal e sobre a transmissão.

Em uma estratégia típica do MDI-QKD, *Alice* e *Bob* terão perfeito controle sobre estados quânticos que serão preparados e enviados para um recebedor central, diferentemente do que ocorre no DIQKD. Por outro lado, a diferença principal entre o MDIQKD e os protocolos do QKD dependentes de dispositivos, é que nenhuma suposição é feita em relação ao dispositivo medidor, sendo este, no MDIQKD um equipamento de detecção centralizado que pode, inclusive, estar sob o controle de *Eve* (PIRANDOLA, 2019).

> MDIQKD cannot provide the same level of security as DIQKD because the quantum state preparation has to be trusted. On the other hand, the characterization of the state preparation results in fewer requirements on experimental implementations and easier security proofs (RENNER, 2022).

6 Conclusão

A importância da comunicação é inquestionável ao longo da história da humanidade, desde os primórdios até os dias atuais. Na contemporaneidade, contudo, se torna cada vez mais necessário também a utilização de criptografia na troca de dados, visando não somente proteger informações sigilosas, mas também a proteção de informações e bens pessoais, como as técnicas de autenticação utilizadas em transações financeiras. Dentro do contexto atual, uma das grandes ferramentas clássicas utilizadas para garantir tal segurança está atrelada a problemas matemáticos difíceis para o computador, como a fatoração de números grandes em números primos, através do RSA, por exemplo. Os avanços na computação quântica, contudo, ameaçam tais procedimentos, dado a iminência da implementação de algoritmos como o algoritmo de Shor.

As limitações da criptografia clássica, contudo, não impedem uma comunicação teoricamente segura e resiliente a avanços de hardware e software, dado a existência de protocolos como o one-time-pad, que utiliza uma chave clássica simétrica. A dificuldade de implementá-lo, contudo, reside no desafio logístico de seguramente armazenar chaves simétricas grandes e numerosas que seriam detidas por ambas as partes comunicantes e utilizadas, cada uma, uma única vez.

O trabalho em tela explorou não só os desafios supracitados, mas o outro lado dos avanços da computação quântica, mais especificamente as oportunidades por ela geradas no que tange a distribuição quântica de chaves (QKD). O que é tirado com uma mão (Shor e a quebra do RSA), portanto, seria fornecido pela outra (QKD) pela mecânica quântica, com a defesa de que a correta implementação de algoritmos de Distribuição Quântica de Chaves levariam à potencial geração de chaves simétricas tão grandes quanto se queira de forma segura, permitindo a correta e facilitada implementação do algoritmo one-time-pad nos casos de sucesso da geração de chave.

A pesquisa, então, explorou as possibilidades de gerar chaves a partir da implementação do protocolo de QKD de seis estados. Através de uma implementação prática utilizando o IBM Quantum Experience platform, destacou-se a eficácia da implementação em casos ideais (sem ruído) e em casos com ruído (distorções geradas pelo meio-ambiente), com um QBER dentro do limiar tolerado. Adentrando em casos mais interessantes e mais profundos, verificou-se ainda o que ocorria quando havia interferência de entidades maliciosas, rotuladas de *Eve*, realizando medições indevidas em todos os qubits. Corroborando aquilo que fora proposto pela teoria, portanto, evidenciou-se que o trabalho da entidade maliciosa é realmente muito complexo. Para as partes comunicantes, *Alice* e *Bob*, asseguradas corretas condições de implementação do protocolo e comportamento esperado

dos dispositivos, a presença de um bisbilhoteiro que realiza medições em todos os qubits trafegados fica evidente, com um QBER extremamente elevado. Não é, portanto, uma tarefa trivial para *Eve* camuflar seus vestígios, neste caso de estudo específico. Reforça-se a ideia fundamental defendida pelo QKD de que não necessariamente a execução do protocolo irá gerar e distribuir chaves de maneira segura, mas de que, caso a distribuição não seja segura, ou seja, caso ocorra interferência externa, essa ação indevida será percebida e o protocolo poderá ser abortado, levando a uma nova tentativa de geração de chave até que o sucesso seja obtido de maneira satisfatória e segura.

Os resultados obtidos na implementação do protocolo de seis estados, sob diversas condições, revelam as complexidades envolvidas e o quão distante poderia-se ficar da idealidade devido a erros de geração e medição mesmo nos casos onde não há presença de adversários, apenas pelos ruídos de meio-ambiente. Em processos de pós-comunicação, contudo, os erros poderiam ser mitigados através da reconciliação da informação. Nos casos mais preocupantes, onde há de fato a presença de uma entidade maliciosa, procedimentos como a amplificação privada garantiriam uma segurança extra ao procedimento, levando, por fim, à geração de chaves clássicas teoricamente seguras. A compreensão desses desafios e o assertivo conhecimento dos dispositivos e do canal quântico envolvidos na implementação do protocolo são essenciais para uma execução segura do procedimento, adotando contramedidas que promovam maior segurança para os comunicantes. Destaca-se, contudo, o fato de sempre existir a possibilidade de algum ataque de canal lateral acontecer, o que é reforçado pela impossibilidade atual de implementar o protocolo utilizando equipamentos ideais. Indica-se, nesse contexto, o DIQKD como uma possível solução ao problema de dispositivos imperfeitos.

Conclui-se, assim, que, apesar dos desafios, os estudos na computação quântica oferecem uma perspectiva viável para avanços na segurança da informação. Não existe, portanto, apenas o lado ruim da potencial quebra de protocolos como o RSA, mas sim uma vasta gama de possibilidades ainda a serem exploradas para que, cada vez mais, seja possível obter uma comunicação segura com a utilização da computação quântica.

O estudo em tela visa contribuir para a base de conhecimento a respeito da Distribuição Quântica de Chaves com a certeza de que, ao continuar explorando as fronteiras do que tange a QKD, incríveis novos avanços serão atingidos no que diz respeito à segurança da comunicação, essencial para o mundo contemporâneo. Entende-se como um campo fértil para estudos futuros os modelos de QKD baseados na comunicação via satélites, dado a capacidade teórica desses modelos transcenderem as limitações impostas pelas infraestruturas terrestres, estabelecendo, assim, a possibilidade de comunicação segura também a longas distâncias.

> Although remarkable progress in QKD has been performed, one of the most important problems is photon loss in the channel, so that

the distance of peer-to-peer QKD with reasonable key rates is about thousand of kilometers. This seems to be a limitation to applying the QKD technology at the global scale. Overcoming this challenge of the distance is possible with the use of satellite-to-ground QKD (FANG et al., 2023).

Satellite-based quantum communications including quantum key distribution (QKD) represent one of the most promising approaches toward global-scale quantum communications (BEHERA; SINHA, 2024).

Referências

BEHERA, S. R.; SINHA, U. *Estimating the link budget of satellite-based Quantum Key Distribution (QKD) for uplink transmission through the atmosphere*. 2024. Citado na página 101.

BENNETT, C. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, v. 68, 1992. Citado na página 50.

BENNETT, C. H.; BRASSARD, G. Quantum cryptography: Public key distribution and coin tossing. Bangalore, India, 1984. Citado na página 47.

BENNETT, C. H. et al. Generalized privacy amplification. *IEEE Transactions on Information Theory*, v. 41, n. 6, p. 1915–1923, 1995. Citado na página 87.

BERNSTEIN, D.; DAHMEN, E.; BUCH. *Introduction to Post-Quantum Cryptography*. [S.l.]: Springer-Verlag Berlin Heidelberg, 2010. Citado na página 33.

BONE, S.; CASTRO, M. A brief history of quantum computing. *Surveys and Presentations in Information Systems Engineering (SURPRISE)*, v. 4, n. 3, p. 20–45, 1997. Disponível em: <http://www.doc.ic.ac.uk/~nd/surprise97/journal/vol4/spb3/>. Citado na página 32.

BRASSARD, G. et al. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, v. 85, p. 1330, 2000. Disponível em: <https://doi.org/10.1103/PhysRevLett.85.1330>. Citado na página 92.

BROWN, P. Algorithmic advances in cryptanalysis. *Proceedings of the International Cryptology Conference*, 2021. Citado 2 vezes nas páginas 25 e 28.

COMPUTING, T. N. M. of. The enigma machine. Acesso em: 2023. 2023. Disponível em: <https://www.tnmoc.org/bh-2-the-enigma-machine>. Citado na página 20.

EKERT, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, v. 67, p. 661, 1991. Citado na página 53.

ELKOUSS, D. Information reconciliation for quantum key distribution. *arXiv:1007.1616 [quant-ph]*, 2010. Citado na página 87.

FANG, K. et al. Quantum network: from theory to practice. *Science China Information Sciences*, Springer Science and Business Media LLC, v. 66, n. 8, jul. 2023. ISSN 1869-1919. Disponível em: <http://dx.doi.org/10.1007/s11432-023-3773-4>. Citado na página 101.

GIDNEY, C.; EKERA, M. How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits. *Quantum*, Verein zur Forderung des Open Access Publizierens in den Quantenwissenschaften, v. 5, p. 433, abr. 2021. ISSN 2521-327X. Disponível em: <http://dx.doi.org/10.22331/q-2021-04-15-433>. Citado na página 32.

GOUZIEN, ; SANGOUARD, N. Factoring 2048-bit rsa integers in 177 days with 13 436 qubits and a multimode memory. *Phys. Rev. Lett.*, v. 127, n. 14, p. 140503, Sep. 2021. Citado na página 32.

GREYDANUS, S. Learning the enigma with recurrent neural networks. *arXiv:1708.07576v2 [quant-ph]*, 2017. Citado na página 19.

GROVER, L. K. *A fast quantum mechanical algorithm for database search*. 1996. Citado na página 32.

H., A. S.; PATHAK, A. Quantum cryptography: key distribution and beyond. *arXiv:1802.05517 [quant-ph]*, 2018. Citado 6 vezes nas páginas 33, 42, 68, 79, 85 e 95.

HARARI, Y. N. *Sapiens: A brief history of humankind*. [S.l.]: Random House, 2014. Citado na página 16.

HERRERO-COLLANTES, M.; GARCIA-ESCARTIN, J. C. Quantum random number generators. *Reviews of Modern Physics*, American Physical Society (APS), v. 89, n. 1, fev. 2017. ISSN 1539-0756. Disponível em: <http://dx.doi.org/10.1103/RevModPhys.89.015004>. Citado na página 78.

HIDARY, J. *Quantum Computing: An Applied Approach*. [S.l.]: Springer, 2019. Citado na página 31.

JONES, A. Post-quantum cryptography: A comprehensive review. *International Journal of Information Security*, v. 18, n. 3, 2019. Citado 2 vezes nas páginas 25 e 28.

KAM, J. F. et al. *Generation and Preservation of Large Entangled States on Physical Quantum Devices*. 2023. Citado na página 32.

KAYE, P.; LAFLAMME, R.; MOSCA, M. *An Introduction to Quantum Computing*. [S.l.]: Oxford University Press, 2007. Citado na página 31.

KERN, O.; RENES, J. Improved one-way rates for BB84 and 6-state protocols. *Quantum Information and Computation*, Rinton Press, v. 8, n. 8&9, p. 756–772, sep 2008. Disponível em: <https://doi.org/10.26421%2Fqic8.8-9-6>. Citado na página 52.

MAVROEIDIS, V. et al. The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications*, The Science and Information Organization, v. 9, n. 3, 2018. ISSN 2158-107X. Disponível em: <http://dx.doi.org/10.14569/IJACSA.2018.090354>. Citado 2 vezes nas páginas 32 e 33.

MAYERS, D.; YAO, A. *Quantum Cryptography with Imperfect Apparatus*. 1998. Citado na página 96.

MENG, C. et al. *Generation of True Quantum Random Numbers with On-Demand Probability Distributions via Single-Photon Quantum Walks*. 2024. Citado na página 78.

MERMIN, N. D. *Quantum Computer Science: An Introduction*. [S.l.]: Cambridge University Press, 2007. Citado na página 31.

MUSKAN; MEENA, R.; BANERJEE, S. *Analysing QBER and secure key rate under various losses for satellite based free space QKD*. 2024. Citado 4 vezes nas páginas 64, 80, 81 e 84.

NADLINGER, D. P. et al. Experimental quantum key distribution certified by bell's theorem. *Nature*, Springer Science and Business Media LLC, v. 607, n. 7920, p. 682–686, jul. 2022. ISSN 1476-4687. Disponível em: <http://dx.doi.org/10.1038/s41586-022-04941-5>. Citado na página 97.

NAKAHARA, M.; OHMI, T. *Quantum Computing: From Linear Algebra to Physical Realizations*. [S.l.]: CRC Press, 2008. Citado na página 31.

NIELSEN, M. A.; CHUANG, I. L. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2011. ISBN 9781107002173. Disponível em: <https://www.amazon.com/Quantum-Computation-Information-10th-Anniversary/dp/1107002176?SubscriptionId=AKIAIOBINVZYXZQZ2U3A&tag=chimbori05-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=1107002176>. Citado 15 vezes nas páginas 6, 32, 41, 42, 44, 46, 47, 50, 51, 53, 68, 87, 88, 89 e 91.

PIRANDOLA, S. Advances in quantum cryptography. *arXiv:1906.01645 [quant-ph]*, 2019. Citado 9 vezes nas páginas 38, 42, 51, 53, 92, 93, 94, 97 e 98.

PORTMANN, C. Security in quantum cryptography. *arXiv:2102.00021 [quant-ph]*, 2021. Citado 10 vezes nas páginas 57, 82, 89, 90, 92, 93, 94, 95, 96 e 98.

PORTUGAL, R. *Basic Quantum Algorithms*. [S.l.: s.n.], 2022. Citado na página 31.

Qiskit. Noise models. Acessado em 20 de novembro de 2023. 2023. Disponível em: <https://qiskit.org/documentation/stable/0.19/apidoc/aer_noise.html>. Citado 2 vezes nas páginas 61 e 63.

REJEWSKI, M. How polish mathematicians broke the enigma cipher. *IEEE Annals of the History of Computing*, v. 3, n. 3, p. 213–234, 1981. Citado 3 vezes nas páginas 19, 20 e 21.

RENNER, R. Quantum advantage in cryptography. *arXiv:2206.04078 [quant-ph]*, 2022. Citado 14 vezes nas páginas 17, 22, 24, 25, 28, 29, 30, 32, 33, 34, 42, 96, 97 e 98.

RIEFFEL, E.; POLAK, W. *Quantum Computing, a Gentle Introduction*. [S.l.]: MIT Press, 2011. Citado na página 31.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, v. 21, n. 2, p. 120–126, 1978. Citado na página 23.

SANDFUCHS, M.; WOLF, R. *Coherent attacks are stronger than collective attacks on DIQKD with random postselection*. 2023. Citado na página 95.

SCHERER, W. *Mathematics of Quantum Computing: An Introduction*. [S.l.]: Springer, 2019. Citado na página 31.

SCHWONNEK, R. et al. Device-independent quantum key distribution with random key basis. *Nature Communications*, Springer Science and Business Media LLC, v. 12, n. 1, maio 2021. ISSN 2041-1723. Disponível em: <http://dx.doi.org/10.1038/s41467-021-23147-3>. Citado na página 97.

SHOR, P. W. Algorithms for quantum computation: discrete logarithms and factoring. p. 124–134, 1994. Citado 3 vezes nas páginas 29, 30 e 31.

SHOR, P. W.; PRESKILL, J. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, American Physical Society (APS), v. 85, n. 2, p. 441–444, jul. 2000. ISSN 1079-7114. Disponível em: <http://dx.doi.org/10.1103/PhysRevLett.85.441>. Citado na página 51.

SHU, H. Asymptotically optimal prepare-measure quantum key distribution protocol. *International Journal of Theoretical Physics*, Springer Science and Business Media LLC, v. 62, n. 8, ago. 2023. ISSN 1572-9575. Disponível em: <http://dx.doi.org/10.1007/s10773-023-05447-0>. Citado 6 vezes nas páginas 51, 52, 65, 67, 69 e 72.

SINGH, S. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. [S.l.]: Doubleday, 2000. Citado 2 vezes nas páginas 17 e 18.

SMITH, J. Quantum computing and its impact on cybersecurity. *Journal of Cybersecurity*, v. 1, n. 2, 2020. Citado 2 vezes nas páginas 25 e 28.

SOUSA, D. P. d.; PIRES, J. D. Criptoanálise como proposta didática para o ensino de estatística. *Revista de Ensino de Ciências e Matemática*, v. 9, n. 2, p. 1–11, 2018. Disponível em: <https://revistapos.cruzeirodosul.edu.br/index.php/rencima/article/view/1639>. Citado na página 19.

STALLINGS, W. *Cryptography and Network Security: Principles and Practice*. 8th. ed. [S.l.]: Pearson, 2021. Citado 3 vezes nas páginas 22, 24 e 29.

STOLZE, J.; SUTER, D. *Quantum Computing, Revised and Enlarged: A Short Course from Theory to Experiment*. [S.l.]: Wiley-VCH, 2008. Citado na página 31.

TAMAKI, K.; KOASHI, M.; IMOTO, N. Unconditionally secure key distribution based on two nonorthogonal states. *Physical Review Letters*, American Physical Society (APS), v. 90, n. 16, abr. 2003. ISSN 1079-7114. Disponível em: <http://dx.doi.org/10.1103/PhysRevLett.90.167904>. Citado na página 51.

WARKE, A.; BEHERA, B.; PANIGRAHI, P. Experimental realization of three quantum key distribution protocols. *DOI: 10.13140/RG.2.2.15812.78725*, 2019. Citado na página 52.

YANOFSKY, N. S.; MANNUCCI, M. *Quantum Computing for Computer Scientists*. [S.l.]: Cambridge University Press, 2008. Citado na página 31.

Apêndices

APÊNDICE A – Códigos associado às implementações do BB84 com 6 estados

A.1 QASM QKD ideal

```
OPENQASM 2.0;
include "qelib1.inc";
qreg q[5];
creg c[5];
x q[0];
x q[1];
x q[2];
h q[0];
h q[3];
s q[0];
h q[2];
s q[3];
sdg q[0];
h q[2];
sdg q[3];
h q[0];
h q[3];
measure q[0] -> c[0];
measure q[1] -> c[1];
measure q[2] -> c[2];
measure q[3] -> c[3];
measure q[4] -> c[4];
```

A.2 QASM QKD com ruído genérico p = 0.9 flipagem de bits

```
qreg q[5];
creg c[5];

x q[0];
x q[1];
```

```
x q[2];
h q[0];
h q[2];
h q[3];
s q[0];
s q[3];
u(0.64350, 0, 0) q[0];
u(0.64350, 0, 0) q[1];
u(0.64350, 0, 0) q[2];
u(0.64350, 0, 0) q[3];
u(0.64350, 0, 0) q[4];
sdg q[0];
h q[2];
sdg q[3];
h q[0];
h q[3];
sdg q[3];
```

A.3 QASM QKD com a presença de Eve

```
OPENQASM 2.0;
include "qelib1.inc";
qreg q[5];
creg c[5];

x q[0];
x q[1];
x q[2];
h q[0];
h q[2];
h q[3];
s q[0];
s q[3];
h q[0];
sdg q[2];
h q[4];
h q[2];
measure q[0] -> c[0];
h q[0];
```

```
measure q[1] -> c[1];
measure q[2] -> c[2];
h q[2];
measure q[3] -> c[3];
s q[2];
measure q[4] -> c[4];
h q[4];
sdg q[0];
h q[2];
sdg q[3];
h q[0];
h q[3];
measure q[0] -> c[0];
measure q[1] -> c[1];
measure q[2] -> c[2];
measure q[3] -> c[3];
measure q[4] -> c[4];
```

A.4 QASM QKD com a presença de Eve - apenas medições

```
OPENQASM 2.0;
include "qelib1.inc";
qreg q[5];
creg c[5];
x q[0];
x q[1];
x q[2];
h q[0];
h q[3];
s q[0];
h q[2];
s q[3];
measure q[0] -> c[0];
measure q[1] -> c[1];
measure q[2] -> c[2];
measure q[3] -> c[3];
measure q[4] -> c[4];
sdg q[0];
h q[2];
```

```
sdg q[3];
h q[0];
h q[3];
measure q[0] -> c[0];
measure q[1] -> c[1];
measure q[2] -> c[2];
measure q[3] -> c[3];
measure q[4] -> c[4];
```

A.5 QASM QKD Ideal com Bob errando uma decodificação

```
OPENQASM 2.0;
include "qelib1.inc";

qreg q[5];
creg c[5];

x q[0];
x q[1];
x q[2];
h q[0];
h q[2];
h q[3];
s q[0];
s q[3];
sdg q[0];
h q[1];
h q[2];
sdg q[3];
h q[0];
h q[3];
measure q[0] -> c[0];
measure q[1] -> c[1];
measure q[2] -> c[2];
measure q[3] -> c[3];
measure q[4] -> c[4];
```

A.6 Comandos úteis e importantes menções para correto funcionamento do código

A.6.1 Provider IBM utilizado

```
provider = IBMProvider()
```

A.6.2 Backends disponíveis

```
print(provider.backends())
```

Disponíveis em 11 de agosto de 2023:

- ibmq_qasm_simulator
- ibmq_quito
- simulator_mps
- simulator_stabilizer
- ibmq_manila
- ibm_lagos
- ibm_perth
- ibmq_lima
- ibmq_belem
- simulator_extended_stabilizer
- simulator_statevector
- ibm_nairobi
- ibmq_jakarta

A.6.3 Criação do circuito a partir do QASM

```
quantum_circuit_QKD_ideal = QuantumCircuit.from_qasm_str(QKD_ideal)
```

A.6.4 Execução do código

```
job_QKD_ideal = execute(quantum_circuit_QKD_ideal,
backend = ibmq_simulator_backend)
```

A.6.5 Obtenção dos resultados e plotagem em histograma

```
result = job_QKD_ideal.result()
```

A.6.6 Plotagem em histograma

```
plot_histogram(result.get_counts(quantum_circuit_QKD_ideal))
```

A.6.7 Criação de erros utilizando a biblioteca de noise do Qiskit

Definindo probabilidades ocorrência

```
prob_1 = 0.2
prob_2 = 0.25
param_amp = 0.2
param_phase = 0.2
```

Criando erros

```
error_1 = noise.depolarizing_error(prob_1, 1)
error_2 = noise.depolarizing_error(prob_2, 2)
error_3 = noise.phase_amplitude_damping_error(param_amp,param_phase)
```

Adicionando erros ao modelo

```
noise_model.add_all_qubit_quantum_error(error_1, ['u1', 'u2', 'u3'])
noise_model.add_all_qubit_quantum_error(error_2, ['cx'])
noise_model.add_all_qubit_quantum_error(error_3, 'x1')
```

A.6.8 Adicionando erros de backend utilizando a biblioteca de noise do Qiskit

```
quantum_computer = provider.get_backend('ibm_lagos')
simulator_backend = 'qasm_simulator'
simulator = Aer.get_backend(simulator_backend)
noise_model_backend = noise.NoiseModel.from_backend(backend=quantum_computer)
```

A.6.9 Criação manual e plotagem de erros duplicados

```
counts_duplicated = {'00001': 20, '00010': 36, '00011': 364,
'00100': 60, '00101': 366, '00110': 518, '00111': 2546,
'01111': 42, '10011': 4, '10100': 2, '10101': 16,
'10110': 2, '10111': 24}
plot_histogram(counts_duplicated,title="QKD Belem Erro duplicado")
```

APÊNDICE B – Tabelas completares associadas à criação de Figuras do Capitulo 2 e aos resultados do Capítulo 4

x	$f1(x)$	$f2(x)$
0	0	0
1	10	5
2	10	5
3	10	14
4	20	14
5	20	14
6	20	24
7	25	24
8	30	24
9	30	34
10	40	34
11	40	34

Tabela 12 – Valores para $f1(x)$ e $f2(x)$ utilizados na criação da Figura 2

x	$f1(x)$	$f2(x)$
0	0	0
1	10	5
2	10	5
3	10	14
4	20	14
5	20	14
6	20	24
7	25	24
8	30	24
9	30	34
10	70	34
11	70	34
12	70	40
13	70	40
14	70	40

Tabela 13 – Valores para $f1(x)$ e $f2(x)$ utilizados na criação da Figura 3

x	$f1(x)$	$f2(x)$
0	0	0
1	10	5
2	10	5
3	10	14
4	20	14
5	20	14
6	20	24
7	25	24
8	30	24
9	30	34
10	70	34
11	70	34
12	70	34
13	70	34
14	70	120
15	70	120
16	70	120
17	70	120
18	70	120

Tabela 14 – Valores para $f1(x)$ e $f2(x)$ utilizados na criação da Figura 4

Chave	Contagem
10000	29
10001	29
10010	40
10011	30
10100	38
10101	34
10110	36
10111	31
11000	31
11001	20
11010	35
11011	24
11100	29
11101	25
11110	36
11111	25
00000	38
00001	36
00010	30
00011	32
00100	35
00101	25
00110	36
00111	25
01000	30
01001	32
01010	33
01011	28
01100	34
01101	25
01110	35
01111	34

Tabela 15 – Resultados associados à Figura 18

Chave	Contagem
10000	129
10001	115
10010	111
10011	118
10100	109
10101	141
10110	123
10111	118
11000	138
11001	138
11010	145
11011	107
11100	115
11101	122
11110	133
11111	138
00000	109
00001	95
00010	123
00011	125
00100	120
00101	104
00110	145
00111	122
01000	124
01001	134
01010	107
01011	145
01100	137
01101	113
01110	154
01111	143

Tabela 16 – Resultados associados à Figura 19

Chave	Contagem
00000	31
00001	37
00010	24
00011	36
00100	40
00101	35
00110	28
00111	38
01000	33
01001	23
01010	26
01011	30
01100	31
01101	36
01110	35
01111	37
10000	26
10001	26
10010	33
10011	29
10100	35
10101	40
10110	31
10111	26
11000	38
11001	21
11010	29
11011	36
11100	35
11101	36
11110	30
11111	33

Tabela 17 – Resultados associados à Figura 20

Chave	Contagem
10000	116
10001	116
10010	160
10011	120
10100	152
10101	136
10110	144
10111	124
11000	124
11001	80
11010	140
11011	96
11100	116
11101	100
11110	144
11111	100
00000	152
00001	144
00010	120
00011	128
00100	140
00101	100
00110	144
00111	100
01000	120
01001	128
01010	132
01011	112
01100	136
01101	100
01110	140
01111	136

Tabela 18 – Resultados associados à Figura 18 com valores multiplicados por 4

Chave	Contagem
00001	10
00010	18
00011	182
00100	30
00101	183
00110	259
00111	3273
01111	21
10011	2
10100	1
10101	8
10110	1
10111	12

Tabela 19 – Resultados associados à Figura 13

Valor	Frequência	Nº bits errados	Nº total bits errados
00000	38	3	114
00001	36	2	72
00010	30	2	60
00011	32	1	32
00100	35	2	70
00101	25	1	25
00110	36	1	36
00111	25	0	0
01000	30	4	120
01001	32	3	96
01010	33	3	99
01011	28	2	56
01100	34	3	102
01101	25	2	50
01110	35	2	70
01111	34	1	34
10000	29	4	116
10001	29	3	87
10010	40	3	120
10011	30	2	60
10100	38	3	114
10101	34	2	68
10110	36	2	72
10111	31	1	31
11000	31	5	155
11001	20	4	80
11010	35	4	140
11011	24	3	72
11100	29	4	116
11101	25	3	75
11110	36	3	108
11111	25	2	50

Tabela 20 – Resultados de cálculos de QBER associados à Figura 18

Valor	Frequência	Nº bits errados	Nº total bits errados
00000	109	3	327
00001	95	2	190
00010	123	2	246
00011	125	1	125
00100	120	2	240
00101	104	1	104
00110	145	1	145
00111	122	0	0
01000	124	4	496
01001	134	3	402
01010	107	3	321
01011	145	2	290
01100	137	3	411
01101	113	2	226
01110	154	2	308
01111	143	1	143
10000	129	4	516
10001	115	3	345
10010	111	3	333
10011	118	2	236
10100	109	3	327
10101	141	2	282
10110	123	2	246
10111	118	1	118
11000	138	5	690
11001	138	4	552
11010	145	4	580
11011	107	3	321
11100	115	4	460
11101	122	3	366
11110	133	3	399
11111	138	2	276

Tabela 21 – Resultados de cálculos de QBER associados à Figura 19

Valor	Frequência	Nº bits errados	Nº total bits errados
00000	31	3	93
00001	37	2	74
00010	24	2	48
00011	36	1	36
00100	40	2	80
00101	35	1	35
00110	28	1	28
00111	38	0	0
01000	33	4	132
01001	23	3	69
01010	26	3	78
01011	30	2	60
01100	31	3	93
01101	36	2	72
01110	35	2	70
01111	37	1	37
10000	26	4	104
10001	26	3	78
10010	33	3	99
10011	29	2	58
10100	35	3	105
10101	40	2	80
10110	31	2	62
10111	26	1	26
11000	38	5	190
11001	21	4	84
11010	29	4	116
11011	36	3	108
11100	35	4	140
11101	36	3	108
11110	30	3	90
11111	33	2	66

Tabela 22 – Resultados de cálculos de QBER associados à Figura 20