Universidade Federal do ABC

Centro de Ciências Naturais e Humanas

Criptografia Quântica: Um Estudo do Código de Acesso Aleatório

Relatório Científico Final do projeto na modalidade Auxílio à Pesquisa Regular, fomentado pela Fundação de Amparo à Pesquisa do Estado de São Paulo.

Projeto FAPESP #2024/07740-4

Pesquisador Responsável: Mariana Gonzalez Veiga

Santo André, 5 de junho de 2025

Informações Gerais do Projeto

- Título do projeto:

  Criptografia Quântica: Um Estudo do Código de Acesso Aleatório

- Nome do pesquisador responsável:

  Mariana Gonzalez Veiga

- Instituição sede do projeto:

  Centro de Ciências Naturais e Humanas da Universidade Federal do ABC

- Equipe de pesquisa:

  Breno Marques Gonçalves Teixeira, Dr.

- Número do projeto de pesquisa:

  2024/07740-4

- Período de vigência:

  01/julho/2024 a 30/junho/2025

- Período coberto por este relatório científico:

  01/julho/2024 a 30/junho/2025

Resumo

O projeto aqui descrito explora os fundamentos da criptografia quântica, sobretudo nos protocolos BB84, o Código de Acesso Aleatório (Random Access Code - RAC) e sua alternativa quântica (QRAC). O intuito desta pesquisa é introduzir conceitos necessários para a compreensão do funcionamento desses protocolos, assim como abordar o desenvolvimento prático do QRAC. Esse estudo conta com uma revisão bibliográfica abrangente sobre o tema e com a elaboração de dois algoritmos em Python para o QRAC. O primeiro considera o cenário ideal de codificação de mensagens, enquanto o segundo algoritmo emprega a programação semidefinida para otimizar o processo de encriptação, inicialmente aleatório. Os resultados obtidos validaram a eficácia das abordagens, atingindo uma probabilidade de sucesso de $85,4\%$ na decodificação correta da mensagem, superando o limite clássico de 75%. Portanto, conclui-se que os resultados comprovam a vantagem da criptografia quântica em relação aos métodos tradicionais, destacando seu potencial para aplicações em comunicações seguras e desenvolvimento de novos protocolos de segurança cibernética. **Palavras-chave:** Criptografia quântica; BB84; Quantum Random Access Code; programação semidefinida.

Abstract

This project explores the fundamentals of quantum cryptography, focusing on the BB84 protocol, the Random Access Code (RAC), and its quantum counterpart (QRAC). The research aims to introduce essential concepts for understanding these protocols' operation while addressing the practical development of QRAC. This study combines a comprehensive literature review of the subject and the implementation of two Python algorithms for QRAC. The first algorithm considers the ideal scenario of message encoding, while the second algorithm employs semidefinite programming to optimize the initially random encryption process. The obtained results validated the approaches‘ effectiveness, achieving a success probability of 85.4% in correct message decoding, surpassing the classical limit of 75%. Therefore, it is concluded that the results prove the advantage of quantum cryptography over traditional methods, highlighting its potential for applications in secure communications and the development of new cybersecurity protocols. **Keywords:** Quantum cryptography; BB84; Quantum Random Access Code; semidefinite programming.

Sumário

1 Resumo do projeto proposto

O projeto aqui apresentado aborda a temática de algoritmos de criptografia quântica. A breve descrição da introdução ao tema destaca a relevância do estudo da tecnologia quântica enquanto uma nova ferramenta auxiliar que surge como uma resposta às ameaças que a computação quântica impõe aos sistemas criptográficos atuais. Dessa forma, o estudo de algoritmos como o Código de Acesso Aleatório, que é a principal área de interesse do projeto, fornece novas possibilidades para avanços na teoria da informação, impactando diretamente a comunicação e os protocolos de segurança cibernéticos.

1.1 Criptografia Clássica

Tipicamente, a criptografia clássica é embasada por aplicações matemáticas complexas e extensas cuja finalidade é dificultar ao máximo a quebra da chave criptográfica, a qual é responsável por encriptar o texto claro (texto original do emissor) para o texto cifrado, assim como a operação inversa de decriptação [1].

Esse ramo pode ser subdividido em duas categorias: criptografia simétrica, na qual a chave de encriptação e decriptação são iguais; e a criptografia assimétrica, na qual existem duas chaves que correspondem cada uma a uma etapa da comunicação, podendo ser uma chave pública (possível de ser acessada por qualquer pessoa) e uma privada (somente uma das partes da comunicação tem acesso). É válido ressaltar que, no último caso, quando a chave pública é usada para encriptar a mensagem, a chave privada deve ser usada para decriptar e vice-versa [2].

Nesse caso, a segurança do sistema criptográfico depende do alto grau de dificuldade de solucionar o problema matemático utilizado para a criação das chaves, o qual normalmente inclui a fatoração de um número grande em um produto de dois números primos igualmente grandes [2]. A complexidade da quebra da chave depende diretamente do poder de processamento dos computadores clássicos, os quais levariam muitos anos até conseguirem realizar a fatoração do número em questão. Entretanto, com a emergência do computador quântico, é imprescindível alertar-se para a sua alta capacidade de processamento, visto que eles são preparados para realizar essas tarefas em um tempo infinitamente menor que os computadores clássicos.

1.2 Criptografia Quântica

A criptografia quântica, por sua vez, emprega as leis da mecânica quântica a fim de manter a segurança de seus algoritmos apesar do avanço da capacidade de processamento computacional quântico. Desse modo, essa técnica não tem por objetivo substituir a criptografia clássica, mas sim fornecer um ambiente mais protegido para comunicação

para ambas as partes envolvidas, seja feita por meio de canais clássicos ou quânticos. Aprimorando, portanto, métodos pré-existentes de segurança, como: assinaturas digitais, protocolos de trocas de chaves e outros procedimentos criptográficos [1].

Os princípios da segurança da criptografia quântica residem em fundamentos básicos da física quântica. Dentre eles, destaca-se o Princípio da Superposição que infere que sistemas quânticos podem assumir múltiplos estados simultaneamente [3], como exemplifica o qubit com sua superposição entre o valor 0 e 1, cuja função de onda colapsa para um único valor apenas após a medição.

O Princípio da Incerteza de Heisenberg é outro ponto importante a ser destacado pois, segundo ele, não é possível medir simultaneamente com acurácia dois observáveis que não comutam entre si. Essa propriedade implica que, ao efetuar uma medida em uma base escolhida, as informações de sua base complementar serão perdidas. Por consequência, qualquer tentativa de um atacante interferir na comunicação perturbará inevitavelmente o sistema, tornando o ataque identificável para ambas as partes envolvidas [3]. Esse princípio será de grande importância na seção 2.1.1, onde será discutida a resistência do protocolo BB84 a ataques de intromissão.

Além disso, há também o Teorema da Não-Clonagem, o qual implica não ser possível efetuar uma cópia idêntica de um estado quântico arbitrário desconhecido [4]. Isso resulta na detecção de qualquer tentativa de intromissão: já que o atacante não é passível de clonar o estado da informação e nem de evitar a perturbação do sistema da mensagem interceptada, o estado de superposição colapsa, alertando à presença de um atacante.

Por fim, têm-se o emaranhamento que é um fenômeno observado em um sistema de duas partículas ou mais, com um alto grau de correlação, no qual seus estados se tornam interdependentes apesar das suas distâncias. Embora esse projeto não possua uma abordagem profunda a respeito do emaranhamento, esse princípio é de suma importância para o ramo da computação quântica e da criptografia quântica pois, para qualquer protocolo de comunicação segura, o uso do emaranhamento permite a identificação de possíveis ataques, já que qualquer alteração em um dos sistemas resultaria na perturbação dos demais [3].

2 Realizações do período

Este estudo aborda uma revisão teórica sobre os protocolos BB84, Código de Acesso Aleatório (RAC), assim como sua alternativa quântica (QRAC). Portanto, busca-se compreender os conceitos necessários para o desenvolvimento desses algoritmos de informação quântica.

Adicionalmente, projeto possui como alvo prático a reprodução do QRAC com a linguagem de programação Python. Essa linguagem foi escolhida por apresentar a biblioteca *Qiskit* que fornece ferramentas para montar circuitos quânticos desenvolvidos pela empresa IBM. Além disso, durante a segunda etapa do desenvolvimento do algoritmo do QRAC, a biblioteca *Picos* foi empregada para a realização dos códigos de otimização por meio da programação semidefinida.

É válido ressaltar que foi descartada qualquer forma de tratamento de ruídos ou possíveis códigos de correção de erro durante o desenvolvimento do projeto.

2.1 Distribuição de Chaves Quânticas

Os estudos do projeto deram início com um dos pilares do modelo criptográfico quântico que reside na Distribuição de Chaves Quânticas (do inglês, *Quantum Key Distribution - QKD*), a qual consiste na comunicação entre duas partes, comumente referidas como Alice (emissora) e Bob (receptor), a partir do compartilhamento de uma chave com garantia de segurança baseada no princípio da superposição [1]. Ademais, o QKD utiliza dois canais: canal quântico, que deve ser seguro para não apresentar ruídos; e um canal clássico que pode ser inseguro.

2.1.1 BB84

O protocolo BB84 foi criado em 1984 por Bennett e Brassard e utiliza a Distribuição de Chaves Quânticas por meio do uso de um canal quântico para enviar a chave e um canal clássico para conferir as respostas. A comunicação da chave é feita por meio de fótons polarizados que podem assumir quatro estados dependendo de sua base:

- Base linear X: $|0\rangle = (0, 1)$ ou $|1\rangle = (1, 0)$, que corresponde à polarização vertical e horizontal.
- Base diagonal Z: $|+\rangle = \frac{1}{\sqrt{2}}(1, 1)$ ou $|-\rangle = \frac{1}{\sqrt{2}}(1, -1)$, indica a polarização de $\pm 45°$ em relação à base X.

Para dar início à comunicação, Alice codifica uma sequência aleatória de bits com as bases descritas acima de maneira arbitrária e envia-a por meio de um canal quântico

seguro. No momento da decodificação, Bob escolhe aleatoriamente uma das duas bases para cada bit recebido e registra seu resultado, que será 0 ou 1.

Após essa primeira etapa, Alice divulga publicamente a sequência de bases usadas na codificação por meio de um canal clássico para que Bob consiga reservar os bits cujas bases são coincidentes e descartar os demais. Em seguida, Bob informa quais bits foram desprezados. Os bits remanescentes formam o que é conhecido no termo em inglês como *sifted key*, que se aproxima da ideia de uma combinação de bits após a retirada dos que estavam incorretos [3]. É apropriado evidenciar que Alice revela apenas as bases utilizadas e não os seus respectivos resultados.

Em seguida, para a verificação da chave obtida e da segurança do canal, Alice e Bob comparam a *sifted key* a fim de obter a taxa de acertos e efetuar eventuais códigos de correção de erro. Durante a comunicação, as bases podem sofrer desalinhamentos, ocasionando em possíveis rotações dos fótons polarizados e, por consequência, provocando erros de precisão em função da qualidade do canal [5]. Porém, uma alta taxa de imprecisão pode ser decorrente de um possível ataque de intromissão.

Há algumas maneiras de o atacante interferir no sistema, dentre elas Eva (a espiã) pode interceptar a mensagem enviada por Alice e depois reenviar uma nova sequência de bits para Bob. Para que o receptor não perceba que os bits foram interceptados, Eva deveria mandar a mesma sequência da mensagem original, porém, como já foi mencionado na seção 1.2, pelo teorema da não-clonagem, não é possível fazer uma cópia perfeita de um estado quântico desconhecido. Portanto, o reenvio dos bits será feito de maneira aleatória, assim como foi feito no caso inicial com Alice [5]. Ou ainda, Eva poderia fazer uma cópia imperfeita da sequência original, que aumentaria a probabilidade de ser o bit certo, mas mesmo assim não seria muito precisa.

Em suma, o protocolo BB84 possui uma taxa de acuracidade de 100% caso Alice e Bob meçam o bit na mesma base, enquanto com bases diferentes a taxa reduz para 50%. Dessa forma, o BB84 é uma técnica de comunicação quântica que evidencia a possibilidade de obter uma chave compartilhada secreta por meio do uso de um canal clássico inseguro com base em princípios da mecânica quântica.

2.1.2 Código de Acesso Aleatório

No código de acesso aleatório (do termo em inglês *Random Access Code - RAC*) Alice codifica uma palavra aleatória $x = x_1x_2 \dots x_n$ de tamanho n, composta por um alfabeto $X = \{1, 2, \dots, d\}$, cuja dimensão é equivalente à d. A mensagem binária codificada é enviada para Bob e deve ter um comprimento m, tal que $m < n$. O objetivo da comunicação é Bob conseguir acertar a *j-ésima letra* (x_j) com probabilidade p, a partir de um índice j aleatório, de modo que $j \in \{1, 2, \dots, n\}$.

De maneira arbitrária, o RAC pode assumir a seguinte notação: $n^d \to m$

2.1.2.1 Codificação Clássica

Classicamente esse modelo de comunicação pode ser ilustrado com um exemplo não-trivial: $2^2 \to 1$. Em um caso de uma palavra de dimensão 2, Alice envia sempre o valor do

dígito binário de uma das letras de sua mensagem, como por exemplo a primeira letra que corresponde ao x_0. Aleatoriamente será sorteado um dos índices j para Bob acertar a letra, caso $j = 0$ a probabilidade de sucesso é máxima, pois x_0 já é de conhecimento de Bob, logo $P_{x_0} = 1$; porém, se $j = 1$ for sorteado haverá duas possibilidades para a posição em questão, portanto Bob terá que chutar com probabilidade de $P_{x_1} = \frac{1}{2}$. Isto posto, no caso ideal a probabilidade máxima de Bob obter sucesso é $P = \frac{1}{2}\left(P_{x_0} + P_{x_1}\right) = \frac{1}{2}\left(1 + \frac{1}{2}\right) = \frac{3}{4}$.

De maneira geral, seguindo a mesma linha de raciocínio do exemplo anterior, porém, em um caso arbitrário $2^d \to 1$, a probabilidade de acerto do primeiro termo continua sendo máxima, enquanto o sucesso de qualquer letra com $j \neq 0$ é equivalente à $\frac{1}{d}$. Portanto, a probabilidade total será de $p = \frac{1}{2}\left(1 + \frac{1}{d}\right)$.

2.1.2.2 Codificação Quântica

Analogamente, o caso não trivial da codificação quântica seria $2^2 \to 1$ feito por meio do qubit:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{2.1}$$

Na esfera de Bloch ideal a otimização é máxima, $\theta = \frac{\pi}{2}$. Dessa forma, o estado $|\psi_{x_0x_1}\rangle$ pode ser representado da seguinte maneira:

$$|\psi_{00}\rangle = cos\left(\frac{\pi}{4}\right)|0\rangle + \left[cos\left(\frac{\pi}{4}\right) + i \cdot sin\left(\frac{\pi}{4}\right)\right]\left[sin\left(\frac{\pi}{4}\right)\right]|1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1+i}{\sqrt{2}}|1\rangle$$

$$|\psi_{00}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1+i}{\sqrt{2}}|1\rangle$$
$$|\psi_{01}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1-i}{\sqrt{2}}|1\rangle$$
$$|\psi_{10}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{-1+i}{\sqrt{2}}|1\rangle$$
$$|\psi_{11}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{-1-i}{\sqrt{2}}|1\rangle$$

Portanto, de maneira geral, o estado $|\psi_{x_0x_1}\rangle$ arbitrário pode ser demonstrado por:

$$|\psi_{x_0x_1}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{(-1)^{x_0} + i\,(-1)^{x_1}}{2}|1\rangle \tag{2.2}$$

Assim como no caso clássico, Alice sorteará um índice aleatório j para que Bob adivinhe sua respectiva letra, o qual indicará qual será a base que deverá ser utilizada para a decodificação:

- Se j = 0, a base de medição será $\sigma_x = \left\{\frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right)\right\} \equiv \{(|0_x\rangle\,;|1_x\rangle)\}$
- Se j = 1, Bob deverá medir na base $\sigma_y = \left\{\frac{1}{\sqrt{2}}\left(|0\rangle \pm i\,|1\rangle\right)\right\} \equiv \{(|0_y\rangle\,;|1_y\rangle)\}$

A título de compreensão da montagem do circuito computacional de decodificação quântica, a base σ_x corresponde ao uso da porta lógica Hadamard, enquanto a base σ_y tem a possibilidade de ser representada por meio de uma porta Hadamard juntamente com uma porta Pauli-Y.

De acordo com o Terceiro Postulado da Mecânica Quântica, o único possível resultado que uma quantidade física pode obter é um de seus autovalores que será correspondente ao seu observável [6]. Dessa forma, a medição na respectiva base resulta em um autovalor, o qual indicará o autoestado associado e que, por consequência, determinará qual é seu resultado final.

Essa associação é respaldada pelo Quinto Postulado, o colapso da função de onda, na qual o estado imediatamente após a medição equivale à projeção normalizada da função $|\psi\rangle$ no subespaço associado ao autovalor correspondente [6].

A aplicação dos postulados descritos acima se torna evidente na decodificação do *QRAC*. Caso Bob precise adivinhar a primeira letra ($j = 0$), por exemplo, ele deverá utilizar a base σ_x que poderá resultar no autovalor 1, cujo autoestado correlato é $|0_x\rangle$ revelando que $x_0 = 0$; ou então, caso o autovalor seja -1, ele obterá o autoestado $|1_x\rangle$ que equivale à $x_0 = 1$.

Assim sendo, a decodificação da segunda letra ($j = 1$) se dá da mesma maneira. Por meio da medição na base σ_y, Bob poderá obter o autovalor 1, cujo autoestado $|0_y\rangle$ retorna que $x_1 = 0$; ou seu autovalor poderá ser -1, indicando o autoestado $|1_y\rangle$ e seu resultado $x_1 = 1$.

Para obter as probabilidades de sucesso, de acordo com o Quarto Postulado da Mecânica Quântica [6] é preciso calcular $p = |\langle A_i|\psi_{x_0x_1}\rangle|^2$, onde A_i é cada um dos possíveis autoestados.

Afim de exemplo, retomamos a decodificação da primeira letra, na qual $j = 0$, cuja probabilidade ideal será:

$$
\begin{aligned}
p &= |\langle 0_x|\psi_{x_0x_1}\rangle|^2 \\
p &= \left|\left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1+i}{\sqrt{2}}|1\rangle\right)\right|^2 \\
p &= \left|\frac{2 + 2\sqrt{2} + 2i}{4\sqrt{2}}\right|^2 \\
p &= \frac{1}{2}\left(1 + \frac{\sqrt{2}}{2}\right) \approx 0,854
\end{aligned}
\tag{2.3}
$$

Ao aplicar esse procedimento para cada um dos autoestados de seus respectivos índices, a probabilidade de sucesso teórica deverá sempre ser igual ao que foi obtido na equação 2.3.

2.2 Parte inicial do desenvolvimento

O processo inicial do desenvolvimento do algoritmo QRAC se enraizou no procedimento básico descrito na Seção 2.1.2.2, baseando-se apenas na comunicação direta entre Alice e

Bob e suas porcentagens de acerto em cada experimento.

A codificação feita por Alice seguiu os cálculos das amplitudes de cada estado referenciados na equação 2.2, na qual a amplitude do ket $|0\rangle$ seria $\frac{1}{\sqrt{2}}$ e do ket $|1\rangle$ seria $\frac{(-1)^{x_0}+i(-1)^{x_1}}{2}$. Dessa maneira, obteve-se as amplitudes ideais para cada estado da função $|\psi\rangle$.

Dessa forma, o circuito quântico de decodificação da letra enviada por Alice era composto por uma porta lógica Hadamard, no caso de ser medido com a base σ_x; ou então, se a medição fosse feita na base σ_y, usou-se o conjunto das portas Pauli-Y e Hadamard, como já mencionado na Seção 2.1.2.2.

A decodificação do sistema passava por cada um dos 4 estados $\{00, 01, 10, 11\}$, aplicando o algoritmo em cada possibilidade de letra, ou seja, testando sempre x_0 e x_1 de cada estado, obtendo assim 8 possibilidades de combinações.

Como era esperado, a probabilidade média de acertos do Bob estava dentro da expectativa mencionada pela equação 2.3 de $85,4\%$. Isto posto, comprova-se que o caso base do algoritmo do Código de Acesso Aleatório Quântico foi desenvolvido corretamente, aplicando os conceitos de Mecânica Quântica de maneira adequada e provando a possibilidade de encontrar a probabilidade teórica.

Para a verificação do algoritmo descrito, confira o apêndice 5.

2.3 Aprimoramento do Algoritmo

Após alcançar o objetivo de reproduzir o algoritmo do QRAC, a segunda etapa do desenvolvimento focou em randomizar as amplitudes iniciais de codificação dos estados, priorizando, portanto, maximizar a função sucesso S_x que representa a probabilidade de acertos em cada estado. Essa abordagem permitiria que, após o envio das palavras criptografadas, as amplitudes fossem otimizadas progressivamente, aproximando-se o máximo possível dos valores ideais, conforme demonstrado na seção anterior.

Essa abordagem se torna muito relevante ao tratar um cenário mais próximo da realidade, o qual parte de um caso não ideal em que as amplitudes de cada estado não se encontram em seu cenário ótimo.

Para iniciar a execução do algoritmo, introduziu-se uma matriz de densidade aleatória ρ, responsável pela codificação dos estados quânticos $|\psi\rangle$. Conforme ilustrado abaixo, os elementos da diagonal principal de ρ representam as probabilidades de encontrar seus respectivos estados. Já os termos fora da diagonal, denominados termos de coerência, quando não nulos, indicam a presença de superposição entre os estados.

$$\rho_{x_0x_1} = |\psi_{x_0x_1}\rangle\langle\psi_{x_0x_1}| = \begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix} \tag{2.4}$$

O cálculo das amplitudes exige também a definição dos ângulos ϕ_a e ϕ_b. O primeiro é fixado em $\phi_a = 0$, representando o alinhamento dos estados com o eixo longitudinal da Esfera de Bloch, enquanto o segundo (ϕ_b) é inicializado aleatoriamente para, posteriormente, ser otimizado.

A partir da obtenção desses dados, a função $|\psi\rangle$ pode ser representada pela expressão:

$$|\psi\rangle = \sqrt{|a|^2} \cdot e^{i \cdot \phi_a} |0\rangle + \sqrt{|b|^2} \cdot e^{i \cdot \phi_a} |1\rangle \tag{2.5}$$

Analogamente, a decodificação também necessitou de adaptações. Introduziu-se, portanto, a matriz unitária U para representar a matriz de decriptação no circuito quântico, pois uma unitária possui a propriedade de conservar o produto escalar e, consequentemente, preservar também sua norma [6].

O requisito de uma matriz unitária U é satisfazer a relação $U^\dagger U = \mathbb{1}$. Isso implica que suas colunas são ortogonais, pois o produto interno entre duas colunas distintas é nulo, enquanto se forem iguais, deve ser igual a 1 [6]. Dessa forma, matriz unitária utilizada na aplicação do algoritmo foi:

$$U = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2}e^{i\phi} & \cos\frac{\theta}{2}e^{i\phi} \end{pmatrix} \tag{2.6}$$

Como ilustração do cálculo do processo de decodificação, suponha-se que Bob deverá adivinhar a primeira letra da palavra, sendo ela o 0. Essa letra será representada por $|\alpha\rangle$, que por estar na primeira posição, deverá ser aplicada ao $|0\rangle$, portanto, segue-se a lógica abaixo.

$$|\alpha\rangle = U|0\rangle = U\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2}e^{i\phi} \end{pmatrix} \tag{2.7}$$

Analogamente, esse raciocínio pode ser aplicado para qualquer um dos casos de decodificação dos estados de $|\psi\rangle$.

Desse modo, finaliza-se a lógica básica do algoritmo aleatório do Código de Acesso Aleatório. Entretanto, por não se tratar do cenário ideal, as probabilidades de acerto deixarão a desejar, tornando necessária a otimização desse algoritmo.

2.3.1 Otimização do código

A etapa final do desenvolvimento do algoritmo contava com o uso da programação semidefinida (SPD) para otimizar as amplitudes iniciais randomizadas. Esse modelo de otimização aborda um problema linear dentro de um domínio de um cone convexo [7], cujas restrições são positivas semidefinida e formam uma combinação afim de matrizes simétricas [8].

A programação semidefinida possui uma ampla área de atuação unificando diversos problemas base, dentre eles: programação quadrática e linear [8]. Ademais, problemas de correlação quântica que inicialmente não são solucionados com SPD, podem ter taxas de acurácia muito satisfatórias e, em alguns casos, podem apresentar exatidão se forem tratados por meio de sequências de aproximações usando SPD [7]. Com isso, a programação semidefinida é uma ferramenta de extrema utilidade e apresenta algoritmos acessíveis ao uso.

Uma matriz simétrica e positiva semidefinida (atribuída como $X \succeq 0$) deve atender ao seguinte requisito

$$v^T X v \geq 0, \ \forall v \in \mathbb{R}^n \tag{2.8}$$

isso implica que seus autovalores devem ser não-negativos.

A otimização é feita sob uma função linear em relação a um domínio convexo com a interseção de um cone positivo-semidefinido com hiperplanos e subespaços [7]. A representação matemática desse conceito pode assumir a seguinte forma

$$\begin{aligned} &\max \quad \langle C, X \rangle \\ &\text{tal que} \quad \langle A_i, X \rangle = b_i, \quad \forall i, \\ &\qquad\quad X \succeq 0 \end{aligned} \tag{2.9}$$

onde C, X e A_i são matrizes hermitianas e b é um vetor real, que representam os projetores das bases de medida, com componentes b_i e $\langle \cdot \ \cdot \rangle$ denota o produto interno.

Com isso, a correlação quântica pode ser obtida por meio da lei de Born apresentada abaixo, na qual os possíveis resultados são representados pelo x, e y indica as possíveis bases de medida.

$$p\left(b|x,y\right) = tr\left(\rho_x M_{b|y}\right) \tag{2.10}$$

No entanto, no caso de um cenário clássico, o modelo quântico deve ser adaptado, pois a mensagem clássica é representada por $\rho_x = \sum_m p(m|x) \left|m\right\rangle \left\langle m\right|$ e a ausência de superposição implica na medição em uma única base $M_{b|y} = \sum_m p(b|y,m) \left|m\right\rangle \left\langle m\right|$. Ademais, a adaptação da lei de Born para a correlação clássica é dada por:

$$p(b|x,y) = \sum_m p(m|x) \ p(b|y,m) \tag{2.11}$$

A expressão referenciada acima se torna relevante na determinação do modelo de comunicação pois, caso essa relação seja extrapolada, torna-se claro que trata-se de um cenário quântico e não de um caso clássico.

Em um contexto, como o do Código de Acesso aleatório, em que a mensagem enviada possui dimensão d, a probabilidade clássica de sucesso é definida por

$$S \equiv \sum_{b,x,y} c_{bxy} \ p(b|x,y) \geq 0 \tag{2.12}$$

onde c_{bxy} é a constante de normalização.

Dessa forma, como já foi citado na seção 2.1.2.2, o sucesso clássico máximo não pode ser maior que $0,75$, já que

$$p_{suc_{class}} \equiv \left(\frac{1}{8}\right) \sum_{x_0,x_1,y} p(b = x_0|x_0,x_1,y) \leq \frac{3}{4} \tag{2.13}$$

Enquanto isso, o cenário quântico supera essa probabilidade, alcançando o valor de $0,854$ como demonstrado pela equação 2.3.

Dessa forma, a otimização das amplitudes dos estados quânticos inicialmente randomizadas parte da matriz de densidade de cada estado ρ_x e da matriz de decodificação $M_{b|y}$ que tem seus valores fixados de tal modo que a expressão abaixo seja válida.

$$\begin{aligned} \max_{\{M_{b|y}\}} \quad & \sum_{b,x,y} c_{bxy} \operatorname{tr}(\rho_x M_{b|y}) \\ \text{tal que} \quad & \sum_{b} M_{b|y} = \mathbb{1} \quad \forall\, y, \\ & M_{b|y} \geq 0 \end{aligned} \tag{2.14}$$

Por sua vez, os valores da matriz de decodificação obtidos da otimização para cada estado x são substituídos na equação 2.15 para encontrar suas respectivas probabilidades individuais de acertos otimizadas S_x que, quando somadas, representam a probabilidade total do sistema: $S = \sum_x S_x$.

$$S_x = \sum_{b|y} c_{bxy}\ M_{b|y} \tag{2.15}$$

O processo, portanto, é iterativo de modo que a probabilidade deve convergir para o valor teórico calculado, aproximando-se ao máximo do que é esperado de sucesso no contexto quântico.

Para a verificação do algoritmo descrito, confira o apêndice 5.

2.4 Conclusão e perspectivas

A emergente área da criptografia quântica traz novas abordagens às ameaças que sua própria tecnologia impõe aos sistemas criptográficos atuais. Explorar os fundamentos da mecânica quântica permite uma nova perspectiva para aplicar conceitos nunca empregados antes em um cenário de segurança cibernética, como o princípio da superposição, o teorema da não-clonagem, o emaranhamento e o Princípio da Incerteza de Heisenberg.

Os estudos dos protocolos BB84, Código de Acesso Aleatório e sua versão quântica permitiram a melhor compreensão do uso prático desses conceitos, assim como esclareceram seu funcionamento. Além disso, o desenvolvimento do algoritmo do QRAC comprovou a probabilidade teórica de sucesso de decodificação da mensagem, legitimando o funcionamento correto dos códigos elaborados durante o período vigente desse projeto.

A otimização, por sua vez, obteve sucesso ao partir de um cenário não ideal de amplitudes aleatorizadas e atingir a taxa de sucesso esperada do contexto otimizado. Esse avanço permitiu aproximar o algoritmo de condições mais realistas de aplicação do QRAC, validando sua eficiência operacional em situações práticas.

Dessa forma, conclui-se a vantagem dos algoritmos de segurança quântica em relação aos métodos clássicos de criptografia, destacando-os como soluções promissoras para o desenvolvimento e aprimoramento de protocolos de informação. Como campo emergente, a criptografia quântica demanda contínuos esforços de pesquisa e desenvolvimento para consolidar seu potencial.

Esse projeto apresenta perspectivas futuras de aprofundamento, especialmente a respeito das aplicações do Código de Acesso Aleatório Quântico. Portanto, um dos possíveis caminhos que o estudo poderia seguir seria abordar a temática da construção de números aleatórios, ou até mesmo desenvolver funcionalidades práticas passíveis de serem utilizadas em experimentos laboratoriais como forma de tratamento dos dados coletados. Logo, manifesta-se um contínuo interesse em prosseguir com as pesquisas nesse assunto.

Ademais, destaca-se a possibilidade de colaboração acadêmica com os demais integrantes do grupo de Tecnologias Quânticas da Universidade Federal do ABC, o qual possui como um de seus mentores o Doutor Breno Marques Gonçalves Teixeira, orientador deste projeto. Essa colaboração visa, sobretudo, a aplicação dos algoritmos desenvolvidos durante o projeto no estudo de chips fotônicos.

3 Descrição e avaliação do Apoio Institucional recebido no período

O Apoio Institucional recebido durante o período da pesquisa foi um precursor para dar início aos estudos em uma área que sempre tive interesse. Isso contribuiu para que eu expandisse meus horizontes para além das disciplinas ofertadas pela minha grade curricular tradicional.

Por incentivo em aprofundar mais meus conhecimentos na área da criptografia quântica, fui motivada a cursar uma disciplina de Mecânica Quântica 1, que, se não fosse pela pesquisa, poderia não ter a possibilidade de participar. Com isso, foi uma ótima oportunidade de ingressar na área de pesquisa, sobretudo em um tema que possuo muito interesse em continuar estudando e aprimorando meus conhecimentos.

4 Participação em eventos científicos

Durante o período vigente do projeto, não foi feita nenhuma participação em eventos científicos. Em função de ser uma pesquisa introdutória no assunto, priorizou-se enraizar conceitos fundamentais para que o avanço de possíveis continuações de pesquisa possa partir de uma base sólida. Além disso, planeja-se apresentar o conteúdo desse estudo no XV Encontro de Iniciação Científica da Universidade Federal do ABC, que será realizado no terceiro quadrimestre de 2025, a fim de divulgar o que foi estudado para que mais estudantes possam se tornar familiarizados com o assunto da criptografia quântica e, possivelmente, demonstrar interesse em seguir nessa área de estudo.

5 Apêndice

Para a análise dos algoritmos descritos durante o desenvolvimento do projeto, por favor, verifique o repositório do projeto no GitHub, ou então acesse https://github.com/mariGveiga/Quantum_Random_Access_Code.

Referências Bibliográficas

[1] Tanmay Tripathi, Abhinav Awasthi, Shaurya Pratap Singh, and Atul Chaturvedi. Post quantum cryptography and its comparison with classical cryptography, 2024.

[2] W. Stallings. *Cryptography and Network Security: Principles and Practice, Global Edition*. Pearson Education, 2018.

[3] SujayKumar Reddy M and Chandra Mohan B. Comprehensive analysis of bb84, a quantum key distribution protocol, 2023.

[4] Partha Ghose. Quantum mechanics and quantum information science: The nature of ψ, 2014.

[5] A.L.P. Camargo, L.O. Pereira, W.F. Balthazar, and J.A.O. Huguenin. Simulação do protocolo bb84 de criptografia quântica utilizando um feixe laser intenso. *Revista Brasileira de Ensino de Física*, 39(2), 2017.

[6] Claude Cohen-Tannoudji, Bernard Diu, and Franck Laloë. *Quantum mechanics; 1st ed.* Wiley, New York, NY, 1977. Trans. of : Mécanique quantique. Paris : Hermann, 1973.

[7] Armin Tavakoli, Alejandro Pozas-Kerstjens, Peter Brown, and Mateus Araújo. Semidefinite programming relaxations for quantum correlations. *Reviews of Modern Physics*, 96(4), December 2024.

[8] Lieven Vandenberghe and Stephen Boyd. Semidefinite programming. *SIAM Review*, 38(1):49–95, 1996.