Uma plataforma de testes para estratégias de expansão de chaves quânticas

João Bessa, Sabrina Rufo, Vítor Andrezo e Rosiane de Freitas

***Resumo*— A expansão de chaves quântica (Quantum Key Expansion – QKE) é uma etapa fundamental para aumentar a eficiência e a viabilidade prática dos protocolos de distribuição de chaves quânticas (QKD), permitindo que pequenas chaves previamente compartilhadas sejam estendidas para gerar segredos criptográficos de maior comprimento. Neste trabalho é apresentada uma ferramenta de análise comparativa de diferentes técnicas de QKE, com foco na implementação em Python e em sua integração a protocolos de comunicação quântica, como BB84 e variantes autenticadas. Através de um testbed em Python e Jupyter foram avaliadas estratégias baseadas em códigos corretores de erros, amplificação de privacidade e autenticação clássica, considerando cenários com canais ruidosos e adversários ativos. O testbed inclui módulos (funções delimitadas para inserção dos códigos teste) de geração de qubits, inserção controlada de ruído, aplicação de estratégias de reconciliação e procedimentos de compressão de chave. Ao aplicar uma estratégia de expansão de chaves baseado em Wegman-Carter MAC, foi possível realizar diversos cenários de teste e aferir o seu desempenho em taxa de erro de qubits.**

***Palavras-Chave*— comunicação quântica, criptografia quântica, distribuição de chaves quânticas, expansão de chaves quânticas, plataforma de testes.**

***Abstract*— Quantum key expansion (QKE) is a fundamental step in increasing the efficiency and practical feasibility of quantum key distribution (QKD) protocols, allowing small, previously shared keys to be extended to generate longer cryptographic secrets. This work presents a tool for comparative analysis of different QKE techniques, focusing on implementation in Python and its integration with protocols such as BB84 and authenticated variants. Through a testbed in Python and Jupyter, strategies based on error-correcting codes, privacy amplification, and classical authentication were evaluated, considering scenarios with noisy channels and active adversaries. The testbed includes modules (functions delimited for inserting test codes) for generating qubits, controlled noise insertion, applying reconciliation algorithms, and key compression procedures. By applying a Wegman-Carter MAC based key expansion strategy, it was possible to perform several test scenarios and assess their performance in terms of qubit error rate.**

***Keywords*— quantum communication, quantum criptography, quantum key distribution, quantum key expansion, testbed.**

I. Introdução

A criptografia quântica representa um avanço significativo na segurança da informação, permitindo a troca de chaves secretas com segurança garantida pelos princípios da mecânica quântica. O protocolo BB84 [1], proposto por Bennett e Brassard em 1984, é um dos pilares dessa área, demonstrando que duas partes podem estabelecer uma chave secreta segura mesmo diante da presença de um adversário com capacidade computacional ilimitada.

Entretanto, apesar da promessa teórica de segurança incondicional, a aplicação prática da distribuição de chaves quânticas (Quantum Key Distribution, QKD) [2] enfrenta obstáculos substanciais, especialmente relacionados ao ruído nos canais quânticos. Interferências ambientais, imperfeições em dispositivos de medição e limitações na fidelidade dos estados quânticos geram erros que comprometem a integridade das chaves geradas. Para contornar esses desafios, diversas técnicas de mitigação de erros têm sido propostas, envolvendo protocolos de correção de erros e amplificação de privacidade.

Diferente do QKD tradicional, a técnica de expansão de chaves quânticas (Quantum Key Expansion, QKE) [3] parte de uma chave curta previamente compartilhada e a expande de forma segura utilizando canais quânticos e comunicação clássica autenticada. A vantagem dessa abordagem está na redução dos requisitos de recursos quânticos, pois permite que uma chave curta sirva de base para gerar grandes quantidades de chave segura, mesmo na presença de ruído moderado. Contudo, a confiabilidade desses protocolos depende diretamente de sua capacidade de operar de forma eficaz mesmo sob condições de ruído e imperfeições experimentais.

A motivação central deste trabalho reside na investigação e avaliação de técnicas de mitigação de erros na expansão de chaves quânticas, com ênfase na análise de protocolos de correção de erros e amplificação de privacidade aplicáveis em cenários realistas. Embora a QKE ofereça vantagens práticas consideráveis, como a reutilização de uma chave curta para gerar chaves maiores, sua aplicação ainda demanda mecanismos robustos para tratar discrepâncias introduzidas durante a transmissão quântica e comunicações auxiliares.

Dessa forma, esta pesquisa busca contribuir com a caracterização e simulação de técnicas clássicas e quânticas que permitam o funcionamento seguro de protocolos de QKE em ambientes ruidosos, considerando cenários com diferentes níveis de perda e taxas de erro de bit (Quantum Bit Error Rate QBER). A plataforma de testes (Testbed) apresentado neste trabalho visa simular cenários de Expansão no protocolo BB84 e possui módulos para inserção de implementação de técnicas de expansão de chaves e correção de erro, bem como uma interface de simulação de cenários com variação de ruído, quantidade de bits, blocos, vazamento e ataque.

II. Distribuição Quântica de chaves

A distribuição quântica de chaves (QKD) [2] é um método de comunicação segura que permite a geração de chaves secretas entre duas partes com base nos princípios funda-

[1]João Bessa, [1,2]Sabrina Rufo, [2]Vítor Andrezo, [1]Rosiane de Freitas. [1]Instituto de Computação, Universidade Federal do Amazonas, Manaus- AM, e-mails: {joao.bessa, sabrinarufo, rosiane}@icomp.ufam.edu.br. [2]Instituto Militar de Engenharia-IME, Rio de Janeiro-RJ, e-mail: andrezo@ime.eb.br.

mentais da mecânica quântica. Diferentemente da criptografia tradicional, que depende da complexidade computacional de certos problemas matemáticos, a segurança do QKD é garantida por propriedades físicas, como a impossibilidade de medir um estado quântico sem perturbá-lo. Essa característica permite detectar qualquer tentativa de interceptação, assegurando a integridade da chave compartilhada. Apesar de sua segurança comprovada, uma rede QKD exige um canal clássico autenticado, o que pode limitar sua aplicabilidade prática frente a sistemas criptográficos convencionais, que já oferecem segurança eficaz com menor custo.

As abordagens da QKD são classificadas, principalmente, em protocolos do tipo *prepare-and-measure* e baseados em emaranhamento. O primeiro explora a alteração inevitável dos estados quânticos provocada pela medição para detectar espionagem, enquanto o segundo se baseia na correlação entre partículas entrelaçadas, onde qualquer interferência externa modifica o sistema como um todo. Ambas as abordagens podem ser implementadas por meio de codificações por variáveis discretas, variáveis contínuas ou referência de fase distribuída, sendo a codificação por variáveis discretas a mais difundida devido à simplicidade e maturidade experimental. O QKD, portanto, atua exclusivamente na distribuição de chaves, que podem ser utilizadas em algoritmos simétricos convencionais, como one-time pad, quando se busca segurança absoluta.

III. Expansão Quântica de Chaves

Quantum Key Expansion (QKE) [3] é o processo de gerar uma chave secreta maior a partir de uma chave inicial curta já compartilhada, utilizando um protocolo de distribuição quântica de chaves (como o BB84 [1]), aliado a técnicas de autenticação clássica e pós-processamento, como correção de erros e amplificação de privacidade.

Alice e Bob possuem uma chave curta comum, usada para autenticar mensagens no canal clássico (por esquemas como Wegman-Carter Message Authentication Code - MAC [4]). Eles rodam um protocolo, como o BB84, usando um canal quântico e um canal clássico autenticado. Após a distribuição, eles aplicam: Sifting (filtragem das bases corretas), Estimativa de erro (para detectar possíveis ataques), Correção de erros (ex: Cascade ou Winnow), Amplificação de privacidade (para eliminar possíveis informações do espião). A chave final é maior que a chave inicial e segura contra qualquer adversário.

IV. Testbed para experimentação de estratégias de Expansão de chaves

O Testbed tem o objetivo de simular cenários de expansão de chaves geradas por protocolos QKD, como o BB84. O ambiente foi construído em *Python* em ambiente *Jupyter* notebook, a interface interativa foi gerada através da biblioteca *ipywidgets* e a geração de ruído e interações através da biblioteca *Qiskit*. A Fig. 1 apresenta as funções modificáveis do testbed, vale ressaltar que as funções para expansão baseada em MAC pode ser substituída por outros métodos desde que retorne as variáveis de entrada no restante do Testbed.

O ambiente de experimentação possui cinco variáveis de variação de cenário: Quantidade de Bits, Quantidade de Ruído,

```
def parity(bits):
def correct_errors(alice, bob, block_size):
def create_mac(message: bytes, key: bytes):
def verify_mac(message: bytes, mac: str, key: bytes):
def privacy_amplification(key_bits, leakage_fraction):
def run_simulation(bits, noise, eve_attack, leakage, block_size):
```

Fig. 1. Mapa das funções e variáveis de entrada do Testbed.

Ataque, Vazamento e Blocos de correção. A simulação retorna o resultado do sifting, QBER antes e depois da correção, Tamanho da chave segura e paridade da chave. A Fig. 2 mostra o resultado de uma simulação de uma expansão via MAC.

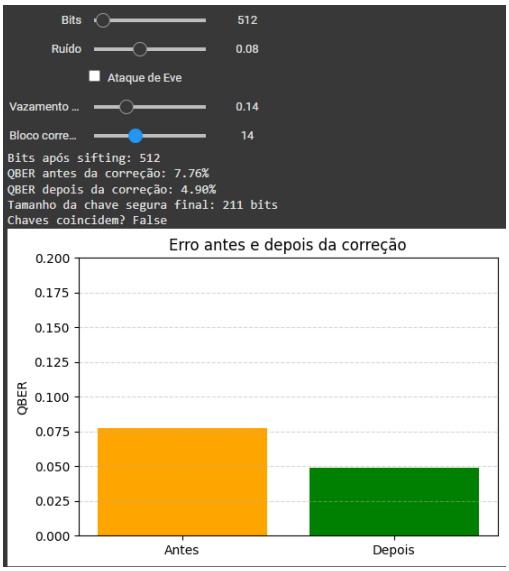

Fig. 2. Interface de simulação das estratégias de Expansão de chaves, gerada em Jupyter através da biblioteca *ipywidgets*.

Agradecimentos

Os autores gostariam de agradecer à agência federal FINEP pelo apoio financeiro através do projeto 3310/2024. Este trabalho também é parcialmente apoiado pelas agências CAPES PROEX - Financiamento Código 001, CNPq e FAPEAM.

Referências

[1] Bennett, C. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*. **560** pp. 7-11 (2014), https://www.sciencedirect.com/science/article/pii/S0304397514004241, Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84

[2] Lo, H. & Lütkenhaus, N. Quantum Cryptography: from Theory to Practice. (2007), https://arxiv.org/abs/quant-ph/0702202

[3] Luo, Z. & Devetak, I. Efficiently implementable codes for quantum key expansion. *Phys. Rev. A*. **75**, 010303 (2007,1), https://link.aps.org/doi/10.1103/PhysRevA.75.010303

[4] Kon, W., Chu, J., Loh, K., Alia, O., Amer, O., Pistoia, M., Chakraborty, K. & Lim, C. Quantum Authenticated Key Expansion with Key Recycling. (2024), https://arxiv.org/abs/2409.16540