COMPUTAÇÃO QUÂNTICA: SIMULAÇÃO E DESAFIOS DE NOVOS PADRÕES EM CRIPTOGRAFIA

Isaias Paulino Soares da Silva[1], Fábio Alan de Souza[2], Luiz Rogério Galam[2].

[1]Universidade Anhembi Morumbi, Av. Dep. Benedito Matarazzo, 6070, Jardim Aquarius - 12230-002 - São José dos Campos-SP, Brasil, (isaiasviolinista@gmail.com).
[2]Infinity Academy 3D, Estrada Doutor Altino Bondesan, 500, sala 204G, PIT - 12247-016 - São Paulo-SP, Brasil, (fabio.alan@infinityacademy3d.com.br, rogerio.galam@infinityacademy3d.com.br).

Resumo
O presente trabalho investiga a aplicação da computação quântica na cibersegurança, com ênfase no protocolo de criptografia BB84. A computação quântica, baseada em qubits, superposição e emaranhamento, difere fundamentalmente da computação clássica e permite o processamento de informações de forma exponencialmente mais eficiente. Para validar conceitos e testar protocolos, utilizam-se simuladores quânticos, que reproduzem o comportamento de circuitos quânticos em ambientes controlados, mesmo sem acesso a computadores quânticos reais. No presente estudo, o BB84 foi implementado no Qiskit. O código desenvolvido possibilitou acompanhar todas as etapas do protocolo e analisar como pequenas alterações nas medições influenciam a segurança da chave. Os resultados demonstram a robustez do BB84 mesmo em simulação, evidenciando a viabilidade da criptografia quântica e seus diferenciais em relação à segurança clássica.

Palavras-chave: Criptografia, Qiskit, Superposição, Simulador quântico, Matéria.

Área do Conhecimento: Engenharias - Engenharia de Computação

Introdução

O avanço da computação quântica tem provocado uma profunda transformação nas perspectivas da cibersegurança. Diferentemente dos computadores clássicos, que processam informações em bits binários, os sistemas quânticos utilizam qubits capazes de assumir múltiplos estados simultaneamente, graças aos princípios de superposição e emaranhamento. Essa capacidade de processamento paralelo oferece oportunidades inéditas para resolver problemas complexos, mas também representa um desafio para os métodos tradicionais de criptografia, muitos dos quais dependem da dificuldade computacional para garantir segurança (Altman *et al.*, 2021).

Dentre os impactos mais significativos da computação quântica está a ameaça potencial à criptografia assimétrica clássica, utilizada amplamente para proteger comunicações digitais, autenticar transações financeiras e resguardar dados sensíveis (Sahu; Mazumdar; 2024). Algoritmos como *RSA* e *ECC*, que hoje sustentam a segurança da internet, poderiam ser quebrados por computadores quânticos suficientemente avançados, levando a um cenário em que informações previamente consideradas seguras ficariam vulneráveis. Esse contexto tornou a pesquisa em criptografia quântica uma área estratégica, buscando desenvolver protocolos que permaneçam seguros mesmo diante do poder de processamento quântico (Camacho *et al.*, 2024).

O protocolo BB84, desenvolvido em 1984 por Bennett e Brassard, representa um marco nesta área, propondo a distribuição de chaves secretas utilizando qubits em diferentes bases de medição. Sua principal inovação reside no fato de que qualquer tentativa de interceptação altera o estado dos qubits, permitindo que os participantes detectem a presença de intrusos. Dessa forma, o BB84 ilustra como a mecânica quântica pode fornecer segurança baseada em leis físicas, e não apenas em pressupostos matemáticos, oferecendo um caminho promissor para a proteção de informações na era quântica (Anilkumar *et al.*, 2024).

Apesar do potencial da computação quântica, os computadores quânticos ainda enfrentam desafios técnicos significativos, como instabilidade dos qubits, decoerência e limitações de escala. Em consequência, o uso de simuladores quânticos se torna fundamental para testar algoritmos e protocolos antes de implementações físicas (Batalla *et al*., 2024). Esses simuladores permitem reproduzir, em um ambiente controlado, o comportamento de sistemas quânticos reais, possibilitando experimentações seguras e análises detalhadas do desempenho de protocolos como o BB84 (Kurochkin; Neizvestny; 2009).

Este artigo tem como objetivo explorar o futuro da cibersegurança na era quântica, apresentando a implementação simulada do protocolo BB84 utilizando o Qiskit. Por meio da construção e execução de circuitos quânticos, busca-se demonstrar como a criptografia quântica pode funcionar na prática, quais são seus principais desafios e quais oportunidades emergem para o desenvolvimento de sistemas seguros em um cenário no qual computadores quânticos se tornam cada vez mais relevantes.

Metodologia

A compreensão da metodologia empregada neste estudo exige, primeiramente, uma breve contextualização acerca da computação quântica e de como ela se diferencia dos simuladores utilizados em ambiente clássico. A computação quântica é um paradigma emergente que se apoia nos princípios fundamentais da mecânica quântica, como superposição, emaranhamento e interferência, para processar informações de forma radicalmente distinta dos computadores convencionais (Steane, 1998). Enquanto os sistemas clássicos trabalham com bits binários, que assumem valores fixos de 0 ou 1, os computadores quânticos manipulam qubits, capazes de existir em estados sobrepostos e correlacionados entre si. Essa característica confere à computação quântica um potencial de paralelismo e velocidade exponencial em certas classes de problemas, entre os quais se incluem tarefas críticas relacionadas à segurança da informação (Rietsche *et al*., 2022).

No entanto, os computadores quânticos ainda se encontram em estágio experimental, marcados por limitações de escalabilidade, instabilidade dos qubits e forte suscetibilidade a ruídos ambientais. Por esse motivo, a utilização de simuladores quânticos desempenha um papel central tanto na pesquisa acadêmica quanto na indústria (Marchetti *et al*., 2022). Um simulador quântico é um software capaz de replicar, em uma máquina clássica, o comportamento esperado de circuitos quânticos. Ainda que não alcance a velocidade e a complexidade de um dispositivo físico real, o simulador permite testar algoritmos, analisar protocolos e validar conceitos fundamentais de computação quântica sem a necessidade de acesso a hardwares especializados (Bharti; Haug; 2021).

As diferenças entre computadores quânticos reais e simuladores clássicos residem, portanto, na fidelidade e nas restrições práticas de cada ambiente. Enquanto os computadores quânticos físicos executam operações sujeitas a imperfeições experimentais — como decoerência e erros de porta lógica —, os simuladores trabalham em condições ideais, sem ruídos, apresentando resultados “limpos” e controlados, por meio do cálculo estatístico. Isso significa que, embora os simuladores sejam instrumentos poderosos para fins de aprendizagem e validação conceitual, eles não capturam integralmente os desafios de uma implementação prática em larga escala (Mamatha; Dimri; Sinha; 2024).

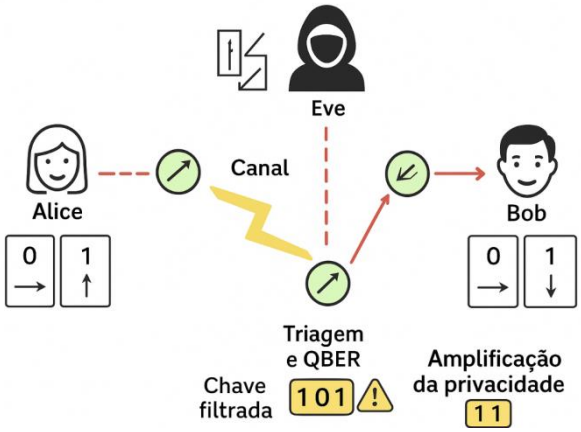
Dentro desse contexto, destaca-se o protocolo BB84, proposto em 1984 por Charles Bennett e Gilles Brassard, considerado o primeiro e mais consolidado esquema de distribuição quântica de chaves (Quantum Key Distribution – QKD). O BB84 utilizado como exemplo, tem como objetivo permitir que dois participantes — aqui chamados de Alice (a transmissora) e Bob (o receptor) — estabeleçam uma chave secreta compartilhada com segurança, mesmo sob a ameaça de um possível interceptador, conhecido como Eve. O protocolo utiliza qubits preparados em duas bases distintas: a base computacional ($|0\rangle$, $|1\rangle$) e a base diagonal ($|+\rangle$, $|-\rangle$). Alice envia qubits em bases escolhidas aleatoriamente, enquanto Bob realiza medições também em bases aleatórias. Após a transmissão, ambos comparam publicamente as bases utilizadas, descartando os resultados incompatíveis e preservando apenas os que coincidem (Molotkov, 2019). Dessa forma, a chave resultante é formada por uma sequência de bits que não pode ser copiada sem detecção, já que qualquer tentativa de interceptação altera estatisticamente os resultados e denuncia a presença de um intruso.

Para a implementação deste estudo, foi utilizado o *Qiskit*, kit de desenvolvimento de código aberto mantido pela *IBM*, que possibilita a criação, execução e análise de circuitos quânticos em simuladores

clássicos ou em dispositivos reais na nuvem. O protocolo BB84 foi simulado por meio do Aer Simulator, que reproduziu as operações quânticas de forma controlada em um ambiente clássico (Wille; Van Meter; Naveh; 2019).

O código desenvolvido foi escrito em *Python* e estruturado para representar as etapas fundamentais do protocolo. Inicialmente, foram gerados bits aleatórios e bases de preparação utilizando recursos da biblioteca *NumPy*. Em seguida, esses bits foram codificados em qubits de acordo com as bases definidas, sendo enviados para Bob, que realizou medições também em bases aleatórias. A implementação contemplou a etapa de comparação pública das bases, realizada de forma simulada, preservando apenas os bits medidos corretamente para compor a chave final. Além disso, foi incorporada a figura de um adversário, Eve, que tentava interceptar os qubits transmitidos. Sua atuação foi modelada como medições em bases aleatórias, seguidas do reenvio dos qubits a Bob, o que introduziu erros detectáveis na chave compartilhada.

Figura 1 - Diagrama de Funcionamento



Fonte: O Autor (2025).

Por fim, foram incluídos trechos específicos para calcular a taxa de erro quântico (*Quantum Bit Error Rate* – QBER), parâmetro essencial para avaliar a segurança do protocolo diante de ataques (Maragkopoulos *et al.*, 2024). Com essa métrica, foi possível identificar em que medida a presença de Eve comprometia a integridade da chave. O resultado foi um código funcional que não apenas simulou o BB84, mas também permitiu a análise quantitativa de sua robustez, conectando os conceitos teóricos da criptografia quântica a uma experimentação prática acessível.

Resultados

A execução do protocolo BB84 no simulador *Qiskit* mostrou que a geração de chaves quânticas pode ser realizada de forma consistente em ambiente controlado. Durante os testes, observou-se que quando as bases escolhidas por Alice e Bob coincidiam, os resultados das medições eram reproduzidos de maneira confiável, permitindo a formação de uma chave compartilhada com baixo índice de erros. Nos casos em que as bases divergiam, os resultados foram descartados, refletindo a operação esperada do protocolo. Além disso, a simulação permitiu avaliar a influência de um interceptador, representado por Eve, sobre o processo. A presença de interferência aumentou a taxa de erro quântico (QBER), demonstrando de forma clara que tentativas de espionagem podem ser detectadas. Esse comportamento confirma a eficácia do BB84 como protocolo seguro e ilustra como a criptografia quântica se diferencia dos métodos clássicos, ao fornecer proteção baseada em princípios físicos, e não apenas em cálculos matemáticos.

O código desenvolvido foi fundamental para tornar observáveis os efeitos da dinâmica do protocolo. Ele possibilitou acompanhar, de maneira estruturada, cada etapa da transmissão: preparação dos qubits, escolha aleatória das bases, medição pelo receptor e filtragem dos resultados. Com isso, foi possível quantificar a eficiência da chave gerada, identificar os efeitos de possíveis ruídos e testar diferentes cenários de ataque, fornecendo informações valiosas sobre a robustez do protocolo mesmo

em ambiente simulado. O código desenvolvido pode ser acessado na íntegra pelo link:https://github.com/IsaiasPaulinoSoaresDaSilva/Quantum-Criptography-BB84.git .

Discussão

Os resultados obtidos reforçam a relevância da criptografia quântica como uma solução de segurança emergente. A simulação demonstrou que o protocolo BB84 funciona de maneira previsível e segura, mesmo em um ambiente controlado. A habilidade de detectar a presença de um interceptador, medida por meio do aumento da QBER, evidencia que a proteção proporcionada pelo protocolo não depende apenas da complexidade matemática, mas de propriedades físicas fundamentais da mecânica quântica.

Outro ponto importante é o papel do código desenvolvido, que não apenas reproduziu o protocolo, mas também permitiu uma análise aprofundada de seu comportamento. Ao simular diferentes cenários de transmissão, com ou sem interferência, foi possível compreender de forma concreta como a escolha de bases e a medição influenciam a formação da chave. Esse tipo de experimentação é particularmente útil, considerando que os computadores quânticos reais ainda enfrentam limitações de escalabilidade e estabilidade, tornando os simuladores ferramentas indispensáveis para validação de protocolos e ensino de conceitos quânticos (Mitra *et al.*, 2017).

Os resultados obtidos indicam ainda que, embora o BB84 seja viável em um ambiente simulado, a transição para sistemas físicos reais exigirá soluções avançadas para lidar com ruídos e decoerência. A discussão aponta para a necessidade de pesquisas contínuas em correção de erros quânticos e em arquiteturas de dispositivos confiáveis, bem como na integração de protocolos quânticos com sistemas clássicos, criando camadas de segurança híbridas capazes de resistir aos avanços da computação quântica (Pasquale; Bianchini; 2020).

Em síntese, a simulação reforça que a criptografia quântica oferece uma alternativa robusta aos métodos clássicos, demonstrando vantagens concretas em termos de detecção de ataques e segurança da informação. Ao mesmo tempo, evidencia os desafios práticos que ainda precisam ser superados para a implementação em larga escala, apontando caminhos para futuras pesquisas e desenvolvimento tecnológico.

Conclusão

A simulação do protocolo BB84 utilizando o Qiskit permitiu observar de forma prática como a criptografia quântica pode oferecer segurança robusta na transmissão de informações. Os resultados demonstraram que é possível gerar chaves compartilhadas com baixo índice de erro quando as bases coincidem, e que a presença de um interceptador aumenta a taxa de erro de maneira detectável, confirmando a capacidade do protocolo de identificar tentativas de espionagem.

O estudo também evidenciou como a implementação em simuladores é uma ferramenta poderosa para validar conceitos e compreender os mecanismos de protocolos quânticos, antes de sua aplicação em dispositivos físicos, que ainda enfrentam desafios como decoerência e sensibilidade ao ruído. O código desenvolvido mostrou-se útil não apenas para reproduzir o protocolo, mas também para permitir análises detalhadas da dinâmica de transmissão, demonstrando como pequenas alterações nas bases ou na medição afetam a segurança da chave.

Esses resultados reforçam que a criptografia quântica apresenta vantagens claras em relação aos métodos clássicos, ao basear sua segurança em princípios físicos e não apenas em dificuldades matemáticas. Ao mesmo tempo, indicam que, para o uso em larga escala, será necessário avançar no desenvolvimento de hardware confiável e na criação de estratégias de correção de erros.

Em síntese, este trabalho mostra que a computação quântica e seus protocolos de criptografia têm grande potencial para redefinir a proteção de informações no futuro, oferecendo mecanismos inovadores capazes de resistir aos avanços da tecnologia. A pesquisa em simuladores e protocolos quânticos continuará sendo essencial, tanto para testes e validação, quanto para a formação de profissionais capazes de implementar essas soluções no futuro da cibersegurança.

Referências

ALTMAN, E., *et al*. Quantum simulators: Architectures and opportunities. **PRX quantum**, v. 2, n. 1, p. 017003, 2021.

ANILKUMAR, C., *et al*. A secure method of communication through bb84 protocol in quantum key distribution. **Scalable Computing: Practice and Experience**, v. 25, n. 1, p. 21-33, 2024.

BATALLA, J. M., *et al*. Theoretical analysis of QBER for Quantum Key Distribution in 5G multi-site networks. In: **2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)**. IEEE, 2022. p. 541-548.

BHARTI, K; HAUG, T. Quantum-assisted simulator. **Physical Review A**, v. 104, n. 4, p. 042418, 2021.

CAMACHO, G. Z. G., *et al*. COMPUTAÇÃO QUÂNTICA: O FUTURO DA SEGURANÇA CIBERNÉTICA OU O FIM DA CRIPTOGRAFIA CLÁSSICA?. **Congresso de Inovação, Ciência e Tecnologia do IFSP**. 2024.

KUROCHKIN, V. L.; NEIZVESTNY, I. G. Quantum cryptography. In: **2009 International Conference and Seminar on Micro/Nanotechnologies and Electron Devices**. IEEE, 2009. p. 166-170.

MAMATHA, G. S.; DIMRI, N; SINHA, R. Post-quantum cryptography: Securing digital communication in the quantum era. **arXiv preprint arXiv:2403.11741**, 2024.

MARAGKOPOULOS, G., *et al*. Real-time diagnostics on a QKD link via QBER time-series analysis. **Entropy**, v. 26, n. 11, p. 922, 2024.

MARCHETTI, L., *et al*. Quantum computing algorithms: getting closer to critical problems in computational biology. **Briefings in Bioinformatics**, v. 23, n. 6, p. bbac437, 2022.

MITRA, S., *et al*. Quantum cryptography: Overview, security issues and future challenges. In: **2017 4th international conference on opto-electronics and applied optics (optronix)**. IEEE, 2017. p. 1-7.

MOLOTKOV, S. N. On the secrecy of a simple and effective implementation of BB84 quantum cryptography protocol. **Laser Physics Letters**, v. 16, n. 7, p. 075203, 2019.

PASQUALE, R. P; BIANCHINI, C. P. Um estudo exploratório das falhas de segurança de algoritmos de criptografia na era da computação quântica. In: **XVI Jornada de Iniciação Científica e X Mostra de Iniciação Tecnológica-2020**. 2020.

RIETSCHE, R., *et al*. Quantum computing. **Electronic Markets**, v. 32, n. 4, p. 2525-2536, 2022.

SAHU, S. K. ; MAZUMDAR, K. State-of-the-art analysis of quantum cryptography: applications and future prospects. **Frontiers in Physics**, v. 12, p. 1456491, 2024.

STEANE, A. Quantum computing. **Reports on Progress in Physics**, v. 61, n. 2, p. 117, 1998.

WILLE, R; VAN METER, R; NAVEH, Y. IBM's Qiskit tool chain: Working with and developing for real quantum computers. In: **2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)**. IEEE, 2019. p. 1234-1240.

Agradecimentos

Agradeço à minha esposa Rhana Bianca por todo empenho, apoio e motivação na jornada, aos meus familiares e também à IA3D.