Desafios e Perspectivas da Criptografia Pós-Quântica na Segurança Computacional Moderna

Victor Reis

[1]Centro de Desenvolvimento Técnologico – Universidade Federal de Pelotas (UFPel)
Caixa Postal 354. 96010-900 – Pelotas – RS – Brazil

Abstract. *This paper explores the challenges and prospects of post-quantum cryptography (PQC) in light of the advancements in quantum computing and its implications for information security. With the development of quantum algorithms capable of breaking classical cryptographic schemes such as RSA and ECC, there is an urgent need for new solutions that are resistant to this emerging paradigm. The study presents the fundamentals of classical and post-quantum cryptography, the main algorithms currently undergoing standardization by NIST, and the technical and strategic obstacles to their practical adoption. Finally, a case study comparing the performance of the RSA-2048 and Kyber512 algorithms highlights the practical advantages of Post-Quantum Cryptography in terms of execution time, reinforcing its relevance for the future of computational security.*

Resumo. *Este trabalho explora os desafios e as perspectivas da criptografia pós-quântica (PQC) frente ao avanço da computação quântica e suas implicações na segurança da informação. Com o desenvolvimento de algoritmos quânticos capazes de quebrar esquemas criptográficos clássicos como algoritmos RSA e ECC, surge a necessidade urgente de novas soluções resistentes a esse paradigma emergente. O estudo apresenta os fundamentos da criptografia clássica e pós-quântica, os principais algoritmos em processo de padronização pelo NIST, e os obstáculos técnicos e estratégicos para sua adoção prática. Por fim, um estudo de caso comparando o desempenho dos algoritmos RSA-2048 e Kyber512 evidencia as vantagens práticas da PQC em termos de tempo de execução, reforçando sua relevância para o futuro da segurança computacional.*

1. INTRODUÇÃO

Nas últimas décadas, os avanços na tecnologia da informação e na comunicação impulsionaram uma crescente dependência de sistemas digitais para a troca e o armazenamento de dados sensíveis. A segurança desses sistemas tem sido historicamente garantida por técnicas criptográficas baseadas em problemas matemáticos considerados intratáveis para os computadores clássicos, como a fatoração de grandes números inteiros (RSA) e o logaritmo discreto (ECC). No entanto, o desenvolvimento da computação quântica representa uma ameaça significativa a essas abordagens tradicionais [Mailloux et al. 2016]. Algoritmos quânticos como o de Shor e o de Grover demonstram que, uma vez viáveis em larga escala, os computadores quânticos poderão quebrar muitos dos esquemas criptográficos amplamente utilizados hoje [Shor 1994] [Grover 1996].

Este trabalho tem como objetivo analisar os principais desafios e perspectivas da criptografia pós-quântica no contexto da segurança computacional moderna. Serão discutidos os fundamentos da criptografia clássica e quântica, os tipos de algoritmos pós-quânticos em desenvolvimento, os entraves para sua adoção prática e as possíveis estratégias de transição. Além disso, examinar-se-á o impacto da PQC (Post-Quantum Cryptography) em diferentes áreas tecnológicas e sua importância estratégica diante da iminente realidade da computação quântica.

2. Fundamento da Criptografia

A criptografia é uma área da ciência da computação e da matemática aplicada que se ocupa da proteção da informação por meio da transformação de dados em formas ininteligíveis a terceiros não autorizados. Seu principal objetivo é garantir os pilares da segurança da informação: confidencialidade, integridade, autenticidade e disponibilidade. Nesse contexto, a criptografia pode ser classificada em dois tipos principais: simétrica e assimétrica [Gabriel et al. 2013].

2.1. Criptografia Simétrica

Na criptografia simétrica, o mesmo segredo (chave) é utilizado tanto para cifrar quanto para decifrar a informação. Algoritmos como o AES (Advanced Encryption Standard) e o DES (Data Encryption Standard) são exemplos amplamente utilizados. Sua principal vantagem é o alto desempenho computacional, mesmo em dispositivos com recursos limitados. No entanto, o gerenciamento e o compartilhamento seguro das chaves entre as partes envolvidas representam um grande desafio, especialmente em redes amplas e dinâmicas [Maziero 2020].

2.2. Criptografia Assimétrica

A criptografia assimétrica, ou de chave pública, utiliza um par de chaves matematicamente relacionadas: uma pública (para cifrar) e uma privada (para decifrar). Esse paradigma elimina o problema do compartilhamento prévio de segredos, possibilitando a criação de sistemas de comunicação seguros mesmo entre partes que nunca se comunicaram antes. Um algoritmo que pertence a essa categoria é o RSA (Rivest–Shamir–Adleman) [Maziero 2020].

3. A Ameaça da Computação Quântica

A computação quântica representa uma nova fronteira tecnológica que promete revolucionar diversas áreas do conhecimento, incluindo a inteligência artificial, a simulação de sistemas físicos e, especialmente, a criptografia. Diferentemente dos computadores clássicos, que operam com bits binários (0 ou 1), os computadores quânticos utilizam qubits, que exploram fenômenos da mecânica quântica como superposição e entrelaçamento. Essas propriedades permitem aos computadores quânticos realizar certos cálculos de forma exponencialmente mais eficiente do que seus equivalentes clássicos [Putu Agus Eka Pratama and Gusti Ngu
Embora os computadores quânticos ainda estejam em estágios iniciais de desenvolvimento, os avanços recentes sugerem que, em um futuro não tão distante, dispositivos quânticos com capacidade de quebrar algoritmos criptográficos amplamente utilizados atualmente se tornarão viáveis. Essa perspectiva tem gerado grande preocupação na comunidade de segurança da informação, pois ameaça comprometer a confidencialidade e a integridade de dados sensíveis em escala global [Thakur et al. 2024].

4. Criptografia Pós-Quântica (PQC)

Diante da ameaça representada pela computação quântica aos sistemas criptográficos clássicos, a criptografia pós-quântica surgiu como uma resposta estratégica. Seu principal objetivo é desenvolver algoritmos criptográficos que sejam seguros contra ataques de computadores quânticos, mas que ainda possam ser implementados eficientemente em computadores clássicos [Ishaque and Al-Anesi 2025].

4.1. Características da Criptografia Pós-Quântica

Os algoritmos pós-quânticos são desenvolvidos com base em problemas matemáticos que permanecem difíceis mesmo para computadores quânticos, como o problema do reticulado (lattice), códigos corretores de erro, sistemas de equações multivariadas e funções hash [Mailloux et al. 2016]. Entre suas principais características, destacam-se:

- Resistência a ataques quânticos, incluindo os algoritmos de Shor e Grover;
- Implementação clássica, sem necessidade de hardware quântico;
- Desempenho variável, com algoritmos que exigem maior uso de memória, largura de banda ou tempo de processamento em comparação com criptografia clássica;
- Flexibilidade para aplicação em múltiplos contextos: autenticação, troca de chaves, assinaturas digitais, entre outros [Bobrysheva and Zapechnikov 2019].

A seguir, são apresentadas as abordagens mais promissoras da PQC:

4.2. Processo de Padronização pelo NIST

Em 2017, o National Institute of Standards and Technology (NIST) iniciou um processo internacional para a padronização de algoritmos pós-quânticos, com a colaboração de pesquisadores, universidades e empresas de todo o mundo. Após várias rodadas de avaliação, o NIST anunciou, em 2022, os primeiros algoritmos selecionados para padronização:

- Kyber para criptografia e troca de chaves;
- Dilithium, SPHINCS+ e Falcon para assinaturas digitais.

A padronização está sendo realizada com base em critérios de segurança, desempenho, simplicidade e resistência a ataques colaterais (side-channel attacks). Essa iniciativa é fundamental para orientar governos e indústrias na transição para um ambiente criptográfico seguro frente à computação quântica [National Institute of Standards and Technology 2017].

5. Desafios da Criptografia Pós-Quântica

Apesar do progresso significativo na pesquisa e desenvolvimento de algoritmos pós-quânticos, sua adoção em escala global ainda enfrenta diversos desafios técnicos, operacionais e estratégicos. Esses obstáculos envolvem desde questões de desempenho até barreiras de compatibilidade e segurança prática. Compreender esses desafios é essencial para planejar uma transição segura e eficiente para um novo paradigma criptográfico.

5.1. Desempenho e Eficiência

Muitos algoritmos pós-quânticos, embora seguros contra ataques quânticos, apresentam sobrecarga computacional em relação às soluções clássicas. Isso pode se manifestar em:

- Tamanhos maiores de chaves e assinaturas: por exemplo, o algoritmo Classic McEliece possui chaves públicas que podem ultrapassar 1 MB, dificultando seu uso em dispositivos com recursos limitados ou conexões de baixa largura de banda.

- Tempo de execução: algumas operações são mais lentas em comparação com RSA ou ECC, impactando sistemas em tempo real.
- Uso intensivo de memória e armazenamento: o custo computacional pode ser proibitivo para aplicações em dispositivos embarcados, como sensores IoT, smartphones ou cartões inteligentes.

[Bobrysheva and Zapechnikov 2019]

5.2. Compatibilidade com Sistemas Legados

Grande parte da infraestrutura digital atual — como protocolos TLS (Transport Layer Security), certificados digitais, VPNs, hardware criptográfico e bibliotecas de software — foi construída com base em algoritmos clássicos. A introdução de algoritmos pós-quânticos requer:

- Atualização de protocolos e padrões existentes;
- Adaptação de APIs, sistemas operacionais e bibliotecas de criptografia;
- Revisão de hardware embarcado e chips de segurança;
- Cuidado com a interoperabilidade entre sistemas clássicos e pós-quânticos, especialmente durante o período de transição. [Hasan et al. 2024]

5.3. Processo de Transição e Hibridização

A migração da criptografia clássica para a pós-quântica não pode ser feita de forma abrupta. Como muitos sistemas dependem de infraestrutura crítica e serviços contínuos, o NIST e outras instituições recomendam uma transição gradual, utilizando esquemas híbridos, que combinam algoritmos clássicos e pós-quânticos. No entanto, isso também introduz desafios:

- Complexidade adicional nos protocolos;
- Aumento no uso de recursos computacionais;
- Necessidade de auditoria dupla de segurança.

[Hasan et al. 2024]

6. Estudo de Caso: Comparação Prática entre RSA e Kyber512

6.1. Objetivo e metodologia

O objetivo deste experimento é comparar, de forma prática, o desempenho dos algoritmos RSA (clássico) e Kyber512 (pós-quântico) em operações criptográficas fundamentais: geração de chaves, cifragem e decifragem. Essa comparação visa ilustrar, com base em tempos de execução reais, como a criptografia pós-quântica se comporta frente a um algoritmo amplamente utilizado na segurança computacional moderna.

Sendo assim, o teste foi realizado utilizando um código em Python (disponivel em: `https://github.com/VictorReis18/Compara-o-Criptografia-Kyber512-RSA2048.git`) que mede o tempo de execução (em segundos) das seguintes operações:

- Geração de chave pública/privada
- Cifragem da mensagem (ou encapsulamento, no caso do Kyber)
- Decifragem da mensagem (ou decapsulamento)
- Verificação de integridade da chave secreta compartilhada (Kyber)

A biblioteca cryptography foi utilizada para a implementação do RSA-2048, enquanto a biblioteca liboqs-python, que fornece acesso a algoritmos pós-quânticos padronizados pelo NIST, foi usada para o Kyber512. A mensagem usada no teste foi:

"Desafios e perspectivas da Criptografia Pós-Quântica na Segurança Computacional Moderna".

6.2. Resultados e discussão

Foi calculada a média dos valores de tempo obtidos para a análise, onde foi compilado 20 vezes. A Tabela 1 apresenta a comparação entre os algoritmos RSA e Kyber, acompanhada dos resultados experimentais referentes à geração de chaves, à cifragem e à decifragem.

Algoritmo	**Geração da chave (s)**	**Cifragem (s)**	**Decifragem (s)**
RSA (2048 bits)	0,126978	0,001785	0,003265
Kyber (512 bits)	0,001300	0,001153	0,000972

Tabela 1. Comparação de desempenho entre RSA e Kyber

- O algoritmo Kyber512 demonstrou ser significativamente mais rápido que o RSA em todas as etapas do processo.
- A diferença de desempenho é especialmente notável na geração de chaves, onde o Kyber é cerca de 100 vezes mais rápido.
- O encapsulamento e decapsulamento de Kyber também são mais eficientes que a cifragem e decifragem com RSA.
- A verificação da chave compartilhada confirma a segurança funcional do Kyber512 no processo de troca segura de informações.

Dessa forma, esses resultados evidenciam que algoritmos pós-quânticos não apenas oferecem resistência a ataques quânticos, mas também podem ser mais eficientes que algoritmos tradicionais em termos de tempo de execução, especialmente em dispositivos com recursos limitados.

7. Conclusão

A computação quântica impõe sérios desafios à segurança baseada em criptografia clássica. Diante dessa ameaça, a criptografia pós-quântica surge como uma solução promissora e estratégica. Este trabalho apresentou os fundamentos da PQC, seus principais algoritmos e os obstáculos para sua adoção. O estudo prático mostrou que o Kyber512, além de seguro contra ataques quânticos, também é mais eficiente que o RSA em termos de tempo de execução. Portanto, é essencial que a transição para algoritmos pós-quânticos seja iniciada com planejamento, visando garantir a segurança digital na era quântica.

Referências

[Bobrysheva and Zapechnikov 2019] Bobrysheva, J. and Zapechnikov, S. (2019). Post-quantum security of communication and messaging protocols: Achievements, challenges and new perspectives. In *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pages 1803–1806.

[Gabriel et al. 2013] Gabriel, A., Alese, B., Adetunmbi, A., and Adewale, O. (2013). Post-quantum crystography: A combination of post-quantum cryptography and steganography. In *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, pages 449–452.

[Grover 1996] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 212–219, New York, NY, USA. Association for Computing Machinery.

[Hasan et al. 2024] Hasan, K. F., Simpson, L., Baee, M. A. R., Islam, C., Rahman, Z., Armstrong, W., Gauravaram, P., and McKague, M. (2024). A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies. *IEEE Access*, 12:23427–23450.

[Ishaque and Al-Anesi 2025] Ishaque, M. and Al-Anesi, B. (2025). Quantum cryptography and post-quantum security: Safeguarding cryptographic protocols against quantum threats. In *2025 2nd International Conference on Advanced Innovations in Smart Cities (ICAISC)*, pages 1–7.

[Mailloux et al. 2016] Mailloux, L. O., Lewis II, C. D., Riggs, C., and Grimaila, M. R. (2016). Post-quantum cryptography: What advancements in quantum computing mean for it professionals. *IT Professional*, 18(5):42–47.

[Maziero 2020] Maziero, C. (2020). *Sistemas Operacionais: Conceitos e Mecanismos*.

[National Institute of Standards and Technology 2017] National Institute of Standards and Technology (2017). Post-quantum cryptography standardization. Accessed: 2025-08-06.

[Putu Agus Eka Pratama and Gusti Ngurah Agung Krisna Adhitya 2022] Putu Agus Eka Pratama, I. and Gusti Ngurah Agung Krisna Adhitya, I. (2022). Post quantum cryptography: Comparison between rsa and mceliece. In *2022 International Conference on ICT for Smart Society (ICISS)*, pages 01–05.

[Shor 1994] Shor, P. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134.

[Thakur et al. 2024] Thakur, M. S. D., Vidhani, K., Syed, H. B., and M.A., R. (2024). Enterprise post quantum cryptography migration tools. In *2024 16th International Conference on COMmunication Systems NETworkS (COMSNETS)*, pages 327–329.