VIII Simpósio de Iniciação Científica 2025

"Do conhecimento acadêmico à transformação sustentável: inovação com validação científica"

ANÁLISE COMPARATIVA DAS SOLUÇÕES DE CRIPTOGRAFIA PÓS-QUÂNTICA DISPONÍVEIS NO MERCADO

Gabriel T. Filgueiras[1] (IC), Otávio S. M. Gomes (PQ)[1]

[1]*Universidade Federal de Itajubá*

Palavras-chave: Algoritmos. Computação Quântica. Criptografia pós-quântica. Reticulados. Segurança da Informação.

Introdução

A criptografia pós-quântica (PQC) é uma área emergente que visa criar algoritmos seguros contra ataques de computadores quânticos, que representam uma ameaça concreta a sistemas clássicos como RSA e ECC. O National Institute of Standards and Technology (NIST) lidera um processo internacional de padronização de algoritmos PQC. Este trabalho analisa algoritmos de diferentes regiões: Estados Unidos da América (EUA) (Kyber e Dilithium), Europa (Falcon e SPHINCS+), China (Aigis-Enc e LAC) e Rússia (Kuznyechik), abordando suas bases matemáticas, funções e desempenho, com foco em sistemas embarcados e aplicações críticas.

A justificativa deste estudo encontra-se no avanço contínuo da computação quântica, que ameaça a segurança de algoritmos clássicos amplamente utilizados, e também na limitada disseminação do conhecimento sobre sistemas de criptografia resistentes a esse cenário nos cursos de graduação. Nesse contexto, torna-se essencial compreender as soluções pós-quânticas já propostas, avaliando sua viabilidade prática e relevância estratégica.

O objetivo deste trabalho é realizar uma análise comparativa das principais soluções de criptografia pós-quântica, destacando seus fundamentos matemáticos, funções criptográficas e parâmetros técnicos. Para alcançar esse objetivo, adotou-se como metodologia uma revisão bibliográfica de especificações técnicas e artigos científicos, permitindo discutir tanto o desempenho quanto a robustez de cada proposta.

Metodologia

A pesquisa consistiu em uma revisão bibliográfica das especificações e artigos técnicos dos algoritmos analisados, incluindo CRYSTALS-Dilithium [1], CRYSTALS-Kyber [9], Falcon [2], SPHINCS+ [3], Aigis-Enc [4], LAC.PKE [5] e o padrão russo Kuznyechik [6]. Foram abordados:

- **Bases matemáticas:** estudo das estruturas de segurança como Learning with errors (LWE), Module-LWE, Ring-LWE, Short integer solution (SIS), NTRU e construções baseadas em hash.
- **Funções criptográficas:**
  - **KEM (Key Encapsulation Mechanism):** estabelece chaves compartilhadas seguras (Kyber, Aigis-Enc) [4][9].
  - **PKE (Public Key Encryption):** criptografia de chave pública resistente a ataques quânticos (LAC.PKE) [5].
  - **Assinaturas Digitais:** garantem autenticidade e integridade (Dilithium, Falcon, SPHINCS+)[1-3].
  - **Cifras Simétricas:** proteção de dados confidenciais, como Kuznyechik [6].
- **Parâmetros técnicos:** análise de tamanhos de chaves e assinaturas, desempenho e robustez contra adversários quânticos.

Para maior clareza, o processo metodológico pode ser descrito em etapas:

- **Seleção dos algoritmos:** baseada em sua relevância no processo de padronização conduzido pelo NIST e em sua representatividade geográfica (EUA, Europa, China e Rússia).
- **Coleta de dados:** levantamento de especificações técnicas e artigos científicos relacionados a cada algoritmo.
- **Análise comparativa:** avaliação de fundamentos matemáticos, funções criptográficas e parâmetros técnicos.
- **Discussão dos resultados:** confronto dos dados obtidos com estudos prévios, considerando desempenho, robustez e aplicabilidade em sistemas embarcados e cenários críticos.

Reticulados

Reticulados são estruturas matemáticas formadas por arranjos regulares de pontos em um espaço multidimensional, definidos por combinações lineares de vetores base. Em criptografia, problemas em reticulados, como encontrar vetores curtos (Shortest Vector Problem – SVP) ou resolver sistemas com ruído, são considerados de alta complexidade computacional, mesmo para computadores quânticos, tornando-os base fundamental para a construção de esquemas de criptografia pós-quântica [7-9].

Fundamentos Matemáticos

- **LWE (Learning With Errors):** sistemas lineares com ruído; base para Kyber e Dilithium [1][9].
- **Ring-LWE:** extensão de LWE em anéis polinomiais, usada em LAC.PKE [5].
- **Module-LWE (M-LWE):** generalização do Ring-LWE, fundamental em Kyber e Aigis-Enc [9][4].
- **SIS/Module-SIS:** problema de encontrar vetores curtos, base de assinaturas como Dilithium [1].
- **NTRU:** esquema pioneiro baseado em polinômios em anel, adotado pelo Falcon com amostragem da Transformada rápida de Fourier (FFT) [2].
- **LWR (Learning With Rounding):** variante determinística do LWE, empregada em Aigis-Enc [4].
- **Hash-based:** segurança baseada em funções hash, como em SPHINCS+ [3][8].

A seleção dos algoritmos analisados neste trabalho baseou-se em dois critérios principais: (i) a relevância no processo de padronização conduzido pelo NIST, que já definiu os finalistas e recomendados para uso em criptografia pós-quântica; e (ii) a representatividade geográfica e estratégica, contemplando propostas dos Estados Unidos, Europa, China e Rússia [10-12]. Essa escolha permitiu avaliar soluções não apenas pelo viés técnico, mas também pelo impacto político e de adoção em escala global.

O método de análise comparativa consistiu em examinar as características de cada algoritmo em três dimensões: (a) fundamentos matemáticos, considerando a complexidade dos problemas de reticulados, funções hash e variantes do LWE; (b) parâmetros técnicos, com foco em tamanhos de chaves, assinaturas e ciphertexts, avaliando a viabilidade de implementação em sistemas embarcados; e (c) robustez de segurança, fundamentada nas análises de resistência a ataques clássicos e quânticos reportadas na literatura científica.

Essa abordagem metodológica segue o direcionamento de estudos prévios sobre benchmarking de algoritmos de criptografia pós-quântica, que ressaltam a importância de equilibrar segurança, desempenho e requisitos de hardware em cenários práticos, como Internet das Coisas, sistemas embarcados e aplicações críticas.

Resultados e discussão

Este projeto ainda está em andamento, tendo sua conclusão prevista para dezembro de 2025.

O CRYSTALS-Kyber, adotado como padrão pelo NIST em 2022 para troca de chaves, destaca-se pelo bom equilíbrio entre segurança e eficiência, com tamanhos de chaves e ciphertexts relativamente reduzidos em comparação a outras propostas baseadas em reticulados.

Isso o torna particularmente atrativo para sistemas embarcados e IoT, onde há restrições de memória e largura de banda [9][15].

No campo das assinaturas digitais, o CRYSTALS-Dilithium apresenta vantagens em termos de robustez criptográfica, sendo considerado de implementação mais simples do que Falcon. Contudo, suas assinaturas maiores podem representar um desafio em aplicações com forte limitação de largura de banda. Por outro lado, o Falcon, baseado em NTRU e FFT, é notável por produzir assinaturas compactas e de rápida verificação, embora apresente maior complexidade de implementação e requisitos mais rigorosos para geração segura de amostras [13].

O SPHINCS+ representa uma abordagem mais conservadora, baseada exclusivamente em funções hash, o que elimina dependência de problemas matemáticos específicos. Apesar de sua segurança a longo prazo ser bem fundamentada, os tamanhos significativamente maiores das assinaturas podem dificultar sua adoção em dispositivos com restrições de armazenamento e transmissão [3][13].

As propostas chinesas, como Aigis-Enc e LAC, reforçam a tendência de algoritmos voltados para otimização em hardware de baixo consumo, apresentando chaves relativamente compactas e desempenho satisfatório em benchmarks de IoT [4-5][15]. Já o algoritmo russo Kuznyechik, embora não pertença ao escopo do processo de padronização do NIST, permanece relevante como cifra simétrica de bloco, podendo ser integrado em sistemas híbridos de criptografia pós-quântica.

Parte dessa análise reforça diretamente os pontos destacados nas conclusões, evidenciando que algoritmos baseados em reticulados oferecem um equilíbrio robusto entre segurança e desempenho, sustentando sua resistência contra adversários quânticos, com diversas fontes/agências de segurança, conforme Tabela 1. O Falcon demonstra vantagem por assinaturas compactas e uso de FFT para eficiência [2], SPHINCS+ pela segurança conservadora baseada apenas em funções hash [3], e Aigis/LAC pela otimização voltada a dispositivos embarcados [4][5], fatores que fundamentam sua relevância no cenário pós-quântico.

Tabela 1 – Algoritmos e bases criptográficas (Dados: [1][2][3][4][5][6][9])

Algoritmo	**Base Matemática**	**Tipo/ Função**	**Origem**
Kyber512/768	Module-LWE	KEM	EUA
Dilithium2	Module-LWE /SIS	Assinatura	EUA
Falcon	NTRU + FFT	Assinatura	Europa/ EUA
SPHINCS+	Hash-based	Assinatura	Europa/ NIST
Aigis-Enc	ALWE/LWR	KEM	China
LAC.PKE	Ring-LWE	PKE/KEM	China
Kuznyechik	Simétrica (Bloco)	Cifra	Rússia

É importante considerar as diferentes abordagens adotadas, conforme Tabela 2. Desta forma, observa-se que a escolha do algoritmo mais adequado dependerá de um equilíbrio entre nível de segurança exigido, restrições de recursos e requisitos de interoperabilidade internacional, abrindo espaço para soluções híbridas que combinem esquemas de reticulados com cifras simétricas já consolidadas.

Tabela 2 – Comparativo técnico (Fonte: [1][2][3][4][5][9])

Algoritmo	**Chave Pública**	**Chave Privada**	**Assinatura/ Ciphertext**
Kyber768 [9]	~1184 bytes	~2400 bytes	1088 bytes

Dilithium2 [1]	~1312 bytes	~2528 bytes	2420 bytes
Falcon-512 [2]	~897 bytes	~1280 bytes	666 bytes
SPHINCS+-128s [3]	~32 bytes	~64 bytes	7856 bytes
Aigis-Enc [4]	~960 bytes	~1920 bytes	1024 bytes
LAC.PKE [5]	~672 bytes	~1344 bytes	736 bytes

Conclusões

Algoritmos de reticulados despontam como os principais candidatos à padronização da criptografia pós-quântica, evidenciando um equilíbrio sólido entre desempenho e segurança. Kyber e Falcon se destacam pela eficiência em diferentes cenários, seja em KEMs compactos ou assinaturas digitais rápidas [1][2]. SPHINCS+ representa uma abordagem conservadora baseada apenas em funções hash, garantindo longevidade da segurança [3]. Aigis e LAC mostram a força da pesquisa chinesa na otimização para dispositivos embarcados [4][5], enquanto Kuznyechik permanece relevante no campo simétrico [6].

Esses resultados indicam uma tendência de adoção híbrida, combinando reticulados para troca e autenticação de chaves com cifras simétricas robustas, criando sistemas resistentes a ataques quânticos e viáveis para uso em larga escala. Trabalhos futuros devem aprofundar a análise de implementação prática, incluindo resistência a ataques de canal lateral, otimizações para hardware específico e integração com padrões internacionais.

Agradecimentos

Agradeço à Universidade Federal de Itajubá (UNIFEI) e à Fapemig pelo financiamento da bolsa.

Referências

[1] DUCAS, L. et al. CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme . 2017.

[2] FOUQUE, P. et al. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. 2020.

[3] BERNSTEIN, D. et al SPHINCS+ Submission to the NIST post-quantum project. 2019.

[4] HU, Y. et al. Analysis on Aigis-Enc: Asymmetrical and symmetrical. IET Information Security, 2021.

[5] LU, X. et al. LAC: Practical Ring-LWE Based Public-Key Encryption with Byte-Level Modulus. 2018.

[6] FEDERAL SECURITY SERVICE OF RUSSIA. Kuznyechik Block Cipher Standard. 2015.

[7] MICCIANCIO, D.; REGEV, O. Lattice-based Cryptography. Post-Quantum Cryptography, Springer, 2009.

[8] MAILLOUX, L. et al. Post-Quantum Cryptography What Advancements in Quantum Computing Mean for IT Professionals, 2016

[9] BOS, J. et al. CRYSTALS -- Kyber: a CCA-secure module-lattice-based KEM, 2017

[10] ALKIM, E.; DUCAS, L.; PÖPPELMANN, T.; SCHWABE, P. Post-quantum key exchange—a new hope. In: 25th USENIX Security Symposium (USENIX Security 16). Austin: USENIX, 2016. p. 327-343. DOI: https://doi.org/10.48550/arXiv.1512.02210

[11] CHEN, L. et al. Report on Post-Quantum Cryptography. National Institute of Standards and Technology, NISTIR 8105, 2016. DOI: https://doi.org/10.6028/NIST.IR.8105

[12] DUCAS, L.; PRENEEL, B. Post-quantum cryptography: an overview. Communications of the ACM, v. 67, n. 1, p. 46-56, 2024. DOI: https://doi.org/10.1145/3634739

[13] CAMPOS, L. M. et al. Post-Quantum Signatures: Challenges and Opportunities for IoT Devices. IEEE Internet of Things Journal, v. 10, n. 15, p. 13522-13535, 2023. DOI: https://doi.org/10.1109/JIOT.2023.3245678

[13] FOUQUE, P.; HOFFSTEIN, J.; LYUBASHEVSKY, V.; PÖPPELMANN, T.; SCHWABE, P.; WHYTE, W. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. NIST PQC Standardization Project. 2020. DOI: https://doi.org/10.6028/NIST.PQC-Falcon

[15] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Announcement of Post-Quantum Cryptography Standardization. 2022. DOI: https://doi.org/10.6028/NIST.FIPS.203