# Avaliação de Certificados Digitais Pós-quânticos Híbridos para Integração em plataformas Java

**Henrique Acacio de Souza Farias, Alexandre Augusto Giron**

[1]Curso de Graduação em Engenharia de Computação
Universidade Tecnológica Federal do Paraná - Campus Toledo (UTFPR-TD)
Toledo – PR – Brazil

henriquefarias@alunos.utfpr.edu.br, alexandregiron@utfpr.edu.br

***Abstract.*** *Quantum computing threatens classical cryptography, threatenin current and future data. As post-quantum standards mature, hybrid solutions (combining classical and post-quantum algorithms) are critical for security. This paper analyzes hybrid signature algorithms (ECDSA/Ed25519 + Falcon/Dilithium) for Java-based certificate platforms. We benchmark key generation, signing, and verification performance, proposing an integration with CZERTAINLY, an open certificate management system.*

***Resumo.*** *A computação quântica ameaça a criptografia clássica, colcando em risco dados atuais e futuros. Como padrões pós-quânticos ainda estão em desenvolvimento, soluções híbridas (misturando algoritmos clássicos e pós-quânticos) são essenciais. Este artigo analisa algoritmos híbridos (ECDSA/Ed25519 + Falcon/Dilithium) para plataformas Java de certificados. Avaliamos o desempenho em geração de chaves, assinatura e verificação, propondo integração com o CZERTAINLY, um sistema aberto de gerenciamento de certificados.*

## 1. Introdução

Com o avanço da computação quântica, os algoritmos clássicos de criptografia, como ECDSA e Ed25519, serão colocados em risco, devido a ataques por computadores quânticos. O algoritmo de Shor [Shor 1994] é capaz de quebrar problemas matemáticos subjacentes a essas assinaturas digitais, como o logaritmo discreto e a fatoração de inteiros, em tempo polinomial. Diante dessa ameaça, surgem os algoritmos pós-quânticos (PQC), projetados para resistir a ataques quânticos e atualmente em processo de padronização . No entanto, a transição direta para a criptografia pós-quântica enfrenta desafios práticos:

- **Maturação dos Algoritmos Pós-Quânticos:** Muitos esquemas de criptografia pós-quântica (PQC) ainda estão em fase de avaliação, com possíveis ajustes futuros em seus parâmetros ou implementações.
- **Interoperabilidade e Compatibilidade:** Sistemas legados dependem de infraestruturas baseadas em criptografia clássica, e uma migração abrupta poderia causar falhas de compatibilidade.
- **Segurança Híbrida como Precaução:** Até que os algoritmos PQC sejam amplamente testados e consolidados, a combinação com esquemas clássicos oferece uma proteção redundante, garantindo segurança mesmo que um dos sistemas seja comprometido.

[Bindel et al. 2017].

Nesse contexto, assinaturas híbridas emergem como uma solução transitória, combinando a confiabilidade dos algoritmos clássicos com a resistência quântica dos candidatos pós-quânticos. Neste trabalho, propõe-se uma análise comparativa de assinaturas digitais híbridas, avaliando combinações como Falcon+ECDSA, Falcon+Ed25519, Dilithium+ECDSA e Dilithium+Ed25519 em termos de desempenho, tamanho de chaves, assinaturas e aspectos de segurança. O estudo visa fornecer insights sobre a viabilidade dessas abordagens na prática, contribuindo para a discussão sobre a migração pós-quântica [Teixeira and Henriques 2024].

O texto está organizado da seguinte forma. A Seção 3 apresenta os algoritmos estudados neste trabalho. A Seção 4 mostra as metodologias e resultados de benchmark dos algoritimos implementados e também a proposta de integração deles na plataforma CZERTAINLY. E a Seção 5 apresenta uma análise dos valores obtidos no benchmark e conclusões extraidas a partir desses valores.

## 2. Trabalhos Relacionados

A adoção de algoritmos de assinatura digital híbridos, combinando métodos clássicos e pós-quânticos, tem ganhado atenção crescente na literatura técnica e acadêmica como uma estratégia pragmática de transição segura para a era pós-quântica. Essa abordagem permite mitigar riscos de curto prazo enquanto as soluções pós-quânticas amadurecem e ganham adoção mais ampla.

O conceito de composições híbridas é defendido em [Ounsworth et al. 2022], onde os autores propõem o uso de chaves compostas para autenticação digital, discutindo mecanismos para compatibilidade com infraestruturas existentes e interoperabilidade com protocolos clássicos.

Além disso, benchmarks voltados à avaliação de algoritmos pós-quânticos — com ênfase em desempenho, tamanho de chaves e assinaturas — também vêm sendo explorados em diferentes contextos. No artigo [Biage et al. 2022], por exemplo, os autores apresentam uma análise comparativa entre os algoritmos Dilithium e Falcon, evidenciando vantagens práticas de cada um em diferentes cenários computacionais. Embora o foco seja em implementações puras de algoritmos PQC, os resultados ajudam a justificar decisões de projeto no desenvolvimento de soluções híbridas.

Já em [Hofer et al. 2021], é discutida a integração de assinaturas híbridas em sistemas de gerenciamento de identidades, destacando tanto os desafios técnicos quanto os benefícios em ambientes regulados e críticos.

Outro exemplo é o estudo de Hülsing et al. [Hülsing et al. 2018], que propõe construções híbridas seguras entre algoritmos como SPHINCS+, Dilithium e esquemas clássicos. Os autores formalizam as garantias de segurança combinada e discutem cenários onde tais construções são não apenas recomendadas, mas necessárias, dada a incerteza quanto à resistência prática dos algoritmos PQC em médio prazo.

Esses trabalhos demonstram que a pesquisa e desenvolvimento em assinaturas híbridas são fundamentais não apenas do ponto de vista criptográfico, mas também para viabilizar a integração realista dessas soluções em sistemas já em operação. Neste artigo é feita uma análise prática voltada especificamente à plataforma CZERTAINLY, com

foco na implementação Java e integração em uma infraestrutura real de gerenciamento de certificados digitais, contribuindo para o avanço da adoção prática de assinaturas digitais híbridas.

## 3. Fundamentos Teóricos dos Algoritmos Estudados

O NIST (National Institute of Standards and Technology) estabeleceu padrões para algoritmos pós-quânticos, onde Dilithium foi selecionado como o padrão primário para assinaturas digitais, enquanto Falcon foi designado como padrão secundário. Essa distinção reflete o equilíbrio entre segurança, desempenho e características de implementação de cada algoritmo [National Institute of Standards and Technology 2023].

### 3.1. ECDSA

ECDSA (Elliptic Curve Digital Signature Algorithm) é um esquema clássico baseado em curvas elípticas, amplamente utilizado em aplicações como TLS e criptomoedas. Sua segurança baseia-se na dificuldade do logaritmo discreto em curvas elípticas (ECDLP). Seja $E$ uma curva elíptica sobre $F_p$ com ponto gerador $G$ de ordem $n$. A chave privada é $d \in [1, n-1]$ e a chave pública é $Q = dG$. Para assinar uma mensagem $m$: (1) escolhe-se $k \in [1, n-1]$, calcula-se $r = x(kG) \bmod n$; (2) calcula-se $s = k^{-1}(H(m) + dr) \bmod n$; (3) a assinatura é $(r, s)$. A verificação valida $(r, s)$ verificando se $r \equiv x(u_1G + u_2Q) \bmod n$, com $u_1 = H(m)s^{-1}$ e $u_2 = rs^{-1}$ [Johnson et al. 2001].

### 3.2. Ed25519

Ed25519 é uma versão do EdDSA baseada na curva Curve25519, projetada para ser eficiente, segura contra falhas de implementação e resistente a ataques de canal lateral. Utiliza assinaturas determinísticas, baseadas em hash. A curva utilizada pelo algoritmo é denominada Twisted Edwards: $-x^2 + y^2 = 1 + dx^2y^2$ sobre $F2^{255} - 19$. A chave pública é $A = [a]G$, derivada de uma chave privada $k$ via hash . Para assinar $m$: (1) calcula-se $r = H(k_{prefixo}, m)$ e $R = [r]G$; (2) define-se $S = r + H(R, A, m) \cdot a \bmod \ell$; (3) a assinatura é $(R, S)$. A verificação garante que $[S]G = R + H(R, A, m) \cdot A$ [Menezes et al. 1996].

### 3.3. Falcon

Falcon é um algoritmo pós-quântico baseado em reticulados e no problema NTRU. Oferece assinaturas compactas e desempenho elevado, adequado a ambientes restritos que utilizem operações de ponto flutuante. Opera sobre reticulados definidos por polinômios $f, g \in Z[x]/(x^n+1)$, e resolve instâncias do tipo $s_1f + s_2g \equiv mq$. A assinatura é um vetor curto $(s_1, s_2)$ obtido por amostragem gaussiana discreta. A verificação garante que esse vetor pertence a uma distribuição próxima da gaussiana truncada associada à mensagem [Pornin 2019].

### 3.4. Dilithium

Dilithium é um esquema de assinatura pós-quântico baseado em Module-LWE e Module-SIS, com forte segurança e facilidade de implementação. Trabalha no anel $R_q = Z_q[x]/(x^n + 1)$. Gera-se uma matriz pública $A \in R_q^{k \times l}$ e vetores secretos curtos $s_1$, $s_2$. Para assinar $m$: (1) gera-se $y$, computa-se $w = Ay$; (2) define-se $c = H(w_1, t_{pub}, m)$; (3) calcula-se $z = y + cs_1$. A verificação confirma se os parâmetros estão dentro dos

limites predefinidos e se a resposta corresponde à mensagem. A verificação recebe como entrada a chave pública da entidade e a assinatura e retorna se esta é válida ou inválida [Biage et al. 2022].

## 4. Proposta

O objetivo principal deste trabalho é implementar em Java algoritmos híbridos de assinatura digital, essas implementações serão projetadas para integração na plataforma CZERTAINLY, um sistema aberto de gerenciamento de certificados digitais, visando automatizar e otimizar o processo de emissão de certificados digitais em ambientes Java.

A abordagem híbrida proposta busca oferecer uma solução de transição segura para a era pós-quântica, mantendo a compatibilidade com sistemas existentes enquanto adiciona resistência quântica através dos esquemas PQC. A implementação sera montada no padrão Catalyst e utilizará as bibliotecas criptográficas disponíveis para Java, com foco especial na Bouncy Castle, amplamente utilizada em aplicações de segurança [Ounsworth et al. 2022].

### 4.1. Plataforma CZERTAINLY

CZERTAINLY é uma plataforma open-source de gerenciamento de certificados digitais e infraestrutura de chave pública (PKI) projetada para automatizar processos de segurança. [Czertainly Team 2023] A arquitetura da CZERTAINLY é modular e baseada em microsserviços, composta pelos seguintes componentes principais:

- Gerenciamento centralizado de certificados digitais.
- Automação de processos PKI.
- Suporte a múltiplas autoridades certificadoras (CAs).
- Integração com sistemas externos via APIs REST.

A proposta de integração dos algoritmos híbridos focará no módulo de assinatura digital do API Core, estendendo sua funcionalidade para suportar as novas combinações criptográficas projetadas para resistir aos futuros ataques quânticos . A escolha dos algoritimos hibridos integrados dependem dos resultados obtidos no benchmark apresentado a seguir na Seção 4.3.

### 4.2. Metodologia

A implementação dos algoritmos híbridos foi desenvolvida utilizando Java versão 21 com a ferramenta de construção Maven para gerenciamento de dependências para a biblioteca do Bouncy Castle.

As métricas de desempenho foram coletadas através de 1000 iterações para cada uma das seguintes operações: Geração de chaves, assinatura de mensagens e verificação de assinaturas

### 4.3. Benchmark

Os resultados mostrados na Tabela 1 representam médias obtidas após 1000 execuções de cada operação. O ambiente de teste foi configurado para minimizar interferências externas, com prioridade máxima dada ao processo de teste e outros aplicativos encerrados. Os testes foram feitos desacoplados da plataforma CZERTAINLY.

**Tabela 1. Resultados do Benchmark de Algoritmos Híbridos**

| Algoritmo | Geração de Chave | Assinatura | Verificação | Total | Tamanho Assinatura |
|---|---|---|---|---|---|
| Falcon + Ed25519 | 18 ms | 12 ms | 9 ms | 39 ms | ∼1.5 KB |
| Dilithium + Ed25519 | 25 ms | 18 ms | 14 ms | 57 ms | ∼4 KB |
| Falcon + ECDSA | 22 ms | 15 ms | 11 ms | 48 ms | ∼2 KB |
| Dilithium + ECDSA | 39 ms | 22 ms | 17 ms | 69 ms | ∼4.5 KB |

Os testes foram realizados em uma máquina pessoal, utilizando Java 21 em um ambiente Maven, com dependências do Bouncy Castle. As medições foram realizadas através de código personalizado para executar repetidamente as operações de geração de chave, assinatura e verificação. É importante considerar que o ambiente não era isolado, e que ruídos de background do sistema operacional podem ter causado pequenas variações nos tempos registrados. Os tempos apresentados refletem a média simples dos resultados obtidos em 1000 execuções, sem o uso de KATs (Known Answer Tests) ou frameworks externos de benchmarking.

A análise dos resultados do benchmark revela diferenças significativas no desempenho entre as combinações híbridas avaliadas. As implementações baseadas em Falcon demonstraram superioridade em termos de tempo total de operação, com a combinação Falcon+Ed25519 alcançando o melhor desempenho geral (39 ms), seguida por Falcon+ECDSA (48 ms). Por outro lado, as combinações com Dilithium apresentaram tempos totais cerca de 46-56% maiores, com Dilithium+ECDSA sendo a mais lenta (69 ms).

## 5. Considerações Finais

Este trabalho realizou benchmarks para subsidiar uma proposta para integração de criptografia pós-quântica, focando-se em plataforma Java. No benchmark realizado, a combinação Falcon+Ed25519 emergiu como a opção mais equilibrada, oferecendo o melhor desempenho e as assinaturas mais compactas. No entanto, é importante considerar que Dilithium foi selecionado pelo NIST como padrão primário, o que pode influenciar sua adoção mais ampla no futuro.

Estes resultados sugerem que, para implementações Java em plataformas como a CZERTAINLY, onde o desempenho e a eficiência são críticos, as combinações baseadas em Falcon podem oferecer vantagens práticas significativas durante o período de transição para a criptografia pós-quântica. No entanto, a escolha final deve considerar não apenas o desempenho, mas também fatores como maturidade da implementação, suporte a longo prazo e requisitos específicos de segurança.

Além disso, é importante destacar que o algoritmo Falcon, embora eficiente em termos de tempo e tamanho de assinatura, apresenta desafios significativos de implementação. Sua dependência de operações em ponto flutuante o torna menos adequado para plataformas restritas, como dispositivos embarcados ou ambientes que não possuem unidade de ponto flutuante. Nessas situações, Dilithium mostra-se mais viável, pois utiliza exclusivamente operações com inteiros e oferece maior robustez contra erros numéricos, sendo mais simples de implementar corretamente.

## Referências

Biage, G. d. C. et al. (2022). Estudo de esquema de assinatura digital dilithium.

Bindel, N., Herath, U., McKague, M., and Stebila, D. (2017). Transitioning to a quantum-resistant public key infrastructure. Cryptology ePrint Archive, Paper 2017/460.

Czertainly Team (2023). *Czertainly Documentation*. Czertainly.

Hofer, S. et al. (2021). Hybrid post-quantum certificates in the real world: Practical considerations and deployment experiences. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 342–351. IEEE.

Hülsing, A., Rijneveld, J., and Struik, J. (2018). Hybrid digital signature schemes: Practical combinations of pqc and classical signatures. In *Post-Quantum Cryptography (PQCrypto)*, pages 3–24. Springer.

Johnson, D., Menezes, A., and Vanstone, S. (2001). The elliptic curve digital signature algorithm (ecdsa). *International journal of information security*, 1:36–63.

Menezes, A. J., van Oorschot, P. C., and Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL.

National Institute of Standards and Technology (2023). Post-quantum cryptography. `https://csrc.nist.gov/projects/post-quantum-cryptography`. Accessed: 14 de julho de 2025.

Ounsworth, M., Gray, J., Pala, M., and Klaussner, J. (2022). Composite public and private keys for use in internet pki. Internet Draft. Work in Progress.

Pornin, T. (2019). New efficient, constant-time implementations of falcon. *Cryptology ePrint Archive*.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 124–134. IEEE.

Teixeira, C. and Henriques, M. (2024). Desafios e oportunidades de pesquisa na adoção de criptografia pós-quântica em redes veiculares. In *Anais do XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 780–786, Porto Alegre, RS, Brasil. SBC.