Assinatura Digital Pós-Quântica na Internet das Coisas: Uma Análise da Aplicabilidade do ML-DSA

Gabriel de Souza Rossetto[1], **Ana Cristina B. Kochem Vendramin**[1], **Daniel Fernando Pigatto**[1], **Juliana de Santi**[1]

[1]Departamento de Informática – Universidade Tecnológica Federal do Paraná (UTFPR)
CEP 80.230-901 – Curitiba – PR – Brasil

rossettog@alunos.utfpr.edu.br, {criskochem,pigatto,jsanti}@utfpr.edu.br

Abstract. *The advancement of quantum computing threatens classical cryptographic algorithms, such as RSA and ECDSA, which are widely used in IoT environments. In this context, this work investigates the application of the post-quantum digital signature algorithm ML-DSA, standardized by the NIST, in embedded systems and IoT devices. Experiments conducted on an ESP32 platform compared ML-DSA, RSA, and ECDSA at different security levels, considering execution time and memory consumption. The results show that ML-DSA achieves better temporal performance, although at the cost of higher memory consumption, highlighting the trade-off between computational efficiency and resource constraints in embedded systems.*

Resumo. *O avanço da computação quântica ameaça algoritmos criptográficos clássicos, como RSA e ECDSA, amplamente usados em ambientes IoT. Diante desse cenário, este trabalho investiga a aplicação do algoritmo pós-quântico de assinatura digital ML-DSA, padronizado pelo NIST, em sistemas embarcados e dispositivos IoT. Experimentos realizados em uma plataforma ESP32 compararam ML-DSA, RSA e ECDSA em diferentes níveis de segurança, considerando tempo de execução e consumo de memória. Os resultados mostram que o ML-DSA apresenta melhor desempenho temporal, porém com maior consumo de memória, evidenciando o compromisso entre eficiência computacional e restrições de recursos em sistemas embarcados.*

1. Introdução

A crescente integração de dispositivos da Internet das Coisas (IoT, do inglês *Internet of Things*) em infraestruturas críticas, indústrias e ambientes de consumo evidenciou a necessidade de garantir a segurança dos dados gerados e transmitidos por essas redes [Sharma and Rani 2025]. Estimativas apontam que o número de dispositivos IoT em operação superou 21 bilhões ao final de 2025, com projeções indicando que esse volume alcançará 40 bilhões até 2030 e ultrapassará 50 bilhões em 2035 [IOT Analytics 2025]. Esses dispositivos permeiam não apenas o cotidiano doméstico, mas também setores de elevado risco operacional, como saúde, automação industrial e infraestrutura críticas, incluindo redes de energia, sistemas de transporte, telecomunicações, e abastecimento de água. Nesse contexto, torna-se necessária a adoção de mecanismos criptográficos robustos capazes de assegurar a confidencialidade, a autenticidade, a verificabilidade e o não-repúdio dos dados gerados e transmitidos.

Chaves assimétricas permitem a implementação de mecanismos criptográficos que atendem a diferentes propriedades de segurança, dependendo de como são empregadas. Quando utilizadas em esquemas de cifragem, a chave pública do destinatário pode ser usada para codificar a mensagem, garantindo confidencialidade, uma vez que apenas o detentor da chave privada correspondente consegue realizar a decifragem [Stallings 2020]. Por outro lado, em esquemas de assinatura digital, foco deste artigo, a chave privada do emissor é utilizada para gerar uma assinatura sobre a mensagem ou seu resumo criptográfico (*hash*), a qual pode ser verificada por qualquer entidade com acesso à chave pública correspondente. Esse mecanismo fornece irretratabilidade (ou não-repúdio), pois o emissor não pode negar posteriormente a autoria da assinatura, já que apenas sua chave privada poderia tê-la gerado de forma válida. Adicionalmente, garante a integridade da mensagem, já que qualquer alteração no conteúdo resulta em uma discrepância entre o *hash* calculado e aquele utilizado na verificação da assinatura, invalidando-a [Kaur and Kaur 2012]. Atualmente, os algoritmos mais difundidos para assinatura digital são o RSA (*Rivest-Shamir-Adleman*), baseado na dificuldade de fatoração de grandes números inteiros, e o ECDSA (*Elliptic Curve Digital Signature Algorithm*), que utiliza a criptografia de curvas elípticas para oferecer níveis de segurança equivalentes ao RSA com chaves significativamente menores [Stallings 2020].

No cenário atual, sistemas IoT presentes em infraestruturas críticas, plantas energéticas, indústria automotiva, linhas de produção industrial, dispositivos de monitoramento de saúde e diversas outras aplicações, dependem de mecanismos de assinatura digital para validar a origem e a conformidade dos dados trafegados [Lin et al. 2017]. Entretanto, as restrições computacionais típicas desses dispositivos, como capacidade limitada de processamento, memória e energia, tornam desafiadora a adoção de algoritmos criptográficos robustos [NIST 2017].

Paralelamente, os avanços na computação quântica representam uma ameaça crítica aos algoritmos criptográficos convencionais amplamente utilizados atualmente [Chen et al. 2016]. Isso ocorre porque algoritmos quânticos, como o proposto por Shor [Shor 1994], permitem resolver problemas de fatoração de grandes números inteiros e logaritmos discretos em tempo polinomial, tornando vulneráveis os principais esquemas de chave pública vigentes. Diante desse cenário, torna-se imperativa a transição para métodos criptográficos resistentes a ataques quânticos. Assim, este trabalho investiga a viabilidade e a aplicabilidade do algoritmo *Module-Lattice-Based Digital Signature Algorithm* (ML-DSA), recentemente padronizado pelo NIST como um dos pilares da criptografia pós-quântica para assinaturas digitais [NIST 2024]. A análise foca no contexto de sistemas de recursos restritos, onde o equilíbrio entre segurança e desempenho é crítico.

As principais contribuições deste estudo são:

- Avaliação experimental comparativa entre o algoritmo pós-quântico ML-DSA e os algoritmos clássicos RSA e ECDSA em uma plataforma ESP32, considerando diferentes níveis de segurança equivalentes aos padrões do NIST;
- Análise do impacto da adoção de assinaturas pós-quânticas em dispositivos IoT com recursos restritos, considerando tempo de execução e consumo de memória;
- Investigação da viabilidade prática do ML-DSA em ambientes embarcados, evidenciando os compromissos entre desempenho, memória e resistência quântica;
- Disponibilização de uma implementação reprodutível utilizando ESP-IDF, *mbed-*

TLS e a biblioteca *mldsa-native* do projeto *Open Quantum Safe* (OQS), contribuindo para futuras pesquisas em assinatura digital pós-quântica aplicada à IoT.

Este artigo está organizado em cinco seções. A Seção 2 apresenta o referencial teórico sobre assinaturas digitais e os algoritmos RSA, ECDSA e ML-DSA. A Seção 3 discute os trabalhos relacionados. A Seção 4 descreve a metodologia e o ambiente experimental. A Seção 5 apresenta os resultados e a comparação entre os algoritmos. Por fim, a Seção 6 traz as conclusões e os trabalhos futuros.

2. Referencial teórico

Protocolos de segurança e mecanismos de autenticação tradicionais em ambientes IoT fundamentam-se em algoritmos de criptografia assimétrica, também denominada Criptografia de Chave Pública (PKC - *Public Key Cryptography*). A natureza assimétrica desses sistemas reside no uso de pares de chaves matematicamente relacionados, porém distintos: uma chave pública, destinada à distribuição ampla, e uma chave privada, mantida em sigilo absoluto pelo proprietário. No contexto de assinaturas digitais, essa estrutura permite garantir a autenticidade e a integridade de dados, uma vez que a assinatura é gerada de forma única através da chave privada e pode ser verificada universalmente pela chave pública correspondente [Stallings 2020].

A segurança dos sistemas assimétricos não reside no sigilo do algoritmo, mas na dificuldade computacional de resolver problemas matemáticos específicos para derivar a chave privada a partir da pública [Stallings 2020]. Tradicionalmente, a segurança dessas assinaturas tem sido sustentada por dois pilares matemáticos: a dificuldade de fatoração de grandes números inteiros compostos e na obtenção do logaritmo discreto em curvas elípticas. No entanto, o advento dos computadores quânticos e a crescente maturidade dessa tecnologia representam uma ameaça crítica a esses esquemas criptográficos, uma vez que algoritmos quânticos são capazes de solucionar tais problemas matemáticos em tempo polinomial, comprometendo a segurança dos mecanismos criptográficos clássicos atualmente empregados [Liu et al. 2024, Wang and Shahril Ismail 2025]. Diante desse desafio, faz-se necessário que a fundamentação desses algoritmos seja reavaliada sob a ótica da resistência a ataques quânticos.

Todavia, a aplicação prática de novas alternativas criptográficas deve considerar as especificidades do cenário de implantação. A proteção de redes IoT diante dessa ameaça enfrenta desafios adicionais decorrentes das limitações arquiteturais desses dispositivos. Nós sensores e dispositivos de borda frequentemente operam sob restrições de processamento, memória e consumo energético, especialmente em aplicações dependentes de baterias de longa duração [Mansoor et al. 2025]. Nesse contexto, a adoção de mecanismos criptográficos mais robustos deve ser equilibrada, de forma a não comprometer a autonomia operacional nem inviabilizar o propósito principal do dispositivo. Assim, a utilização de algoritmos criptográficos mais complexos ou a simples ampliação do tamanho das chaves assimétricas tradicionais tende a se tornar impraticável em ambientes IoT com recursos limitados [Sharma and Rani 2025].

Para compreender os impactos dessa transição e as barreiras impostas pela nova era da criptografia, as seções a seguir detalham as bases teóricas dos algoritmos analisados nesta pesquisa. Inicialmente, são apresentados os algoritmos de assinatura digital clássicos, mais especificamente o RSA e o ECDSA, cujas limitações diante de ameaças

quânticas motivaram o surgimento de novas abordagens. Na sequência, discute-se o paradigma da Criptografia Pós-Quântica (PQC - *Post-quantum cryptography*), com foco no algoritmo ML-DSA e nos desafios operacionais de sua integração em ecossistemas de recursos restritos.

2.1. Algoritmos de Assinatura Digital Clássicos

Os sistemas de assinatura digital clássicos baseiam-se em problemas matemáticos cuja resolução é considerada impraticável para computadores convencionais em tempo computacional viável. Neste artigo, os algoritmos RSA e ECDSA são utilizados como base de comparação por representarem o estado da arte na indústria atual de IoT.

O RSA é um dos primeiros e mais difundidos algoritmos de chave pública. Sua segurança fundamenta-se na dificuldade de fatoração de grandes números inteiros compostos por dois números primos [Stallings 2020]. Apesar de sua maturidade e facilidade de implementação, o RSA apresenta desafios para o ambiente IoT: as assinaturas e chaves são extensas, o que consome largura de banda, e a operação de geração de chaves é computacionalmente cara para dispositivos com processadores modestos.

O ECDSA é uma evolução do RSA, baseando sua segurança no problema do logaritmo discreto em curvas elípticas. A principal vantagem deste algoritmo é a eficiência: ele oferece o mesmo nível de segurança que o RSA, porém com chaves significativamente menores [Stallings 2020]. Devido ao menor tamanho de chave e ao menor consumo de memória, o ECDSA tornou-se o padrão de facto para dispositivos IoT. Contudo, assim como o RSA, sua segurança é estritamente dependente da incapacidade de resolver problemas de logaritmo discreto, uma tarefa que computadores quânticos podem realizar.

2.2. Criptografia Pós-Quântica e o Padrão ML-DSA

A Criptografia Pós-Quântica (*Post-quantum cryptography* (PQC)) tem se estabelecido como a principal via de mitigação contra a ameaça dos computadores quânticos, fundamentando-se em classes de problemas matemáticos que resistem tanto a ataques clássicos quanto a adversários quânticos [Kumar et al. 2025]. Para organizar essa transição, o NIST lidera um processo global de padronização voltado a algoritmos fundamentados em reticulados (*lattice-based*), códigos, *hashes* e equações multivariáveis [Wang and Shahril Ismail 2025].

Iniciado em 2024 com a validação do *Module-Lattice-based Key-Encapsulation Mechanism* (ML-KEM), destinado ao encapsulamento e à troca segura de chaves, o processo culminou, em 2025, na regulamentação do *Module-Lattice-Based Digital Signature Algorithm* (ML-DSA) e do *Stateless Hash-Based Digital Signature Algorithm* (SLH-DSA), ambos voltados para assinatura digital. Esses padrões representam um marco na consolidação de mecanismos criptográficos resistentes a ataques quânticos, cuja adoção em larga escala é prevista até 2035, período em que os algoritmos de criptografia assimétrica vulneráveis à computação quântica deverão ser descontinuados.

Além disso, o próprio NIST destaca que não existem impedimentos técnicos para o início imediato da migração, recomendando que sistemas críticos iniciem esse processo o quanto antes [IOT Analytics 2025]. Entre os padrões criptográficos recentemente aprovados para assinaturas digitais visando à resistência quântica, destaca-se o algoritmo ML-DSA, baseado no CRYSTALS-Dilithium, que vem sendo amplamente

reconhecido por sua forte garantia de segurança, aliada a sua eficiência temporal nas operações de verificação de assinaturas, sendo frequentemente apontado na literatura como o principal substituto prático das assinaturas digitais clássicas em relação ao SLH-DSA, que constitui uma alternativa baseada em uma hipótese criptográfica distinta (funções *hash*), podendo ser empregada caso vulnerabilidades significativas sejam descobertas em esquemas baseados em reticulados, como o ML-DSA [Mansoor et al. 2025, Wang and Shahril Ismail 2025, Salter et al. 2025]. Assim, o ML-DSA foi escolhido para o presente estudo.

A integração entre PQC e ambientes IoT, contudo, introduz novos desafios operacionais e limitações de projeto que impactam diretamente o desempenho e a viabilidade desses sistemas. Em particular, a adoção de algoritmos baseados em reticulados, como o ML-DSA, evidencia um compromisso importante: embora esses mecanismos apresentem baixa latência de execução em comparação com abordagens criptográficas tradicionais, eles demandam chaves públicas e assinaturas significativamente maiores, além de maior consumo de memória [Liu et al. 2024]. Em dispositivos IoT com recursos restritos, tais características podem comprometer aspectos críticos, como armazenamento, largura de banda e consumo energético. Dessa forma, garantir resistência a ataques quânticos sem degradar a estabilidade e a eficiência operacional dos nós IoT exige não apenas a adoção de novos algoritmos criptográficos, mas também otimizações arquiteturais e de *hardware* capazes de suportar os requisitos adicionais impostos pela PQC [Wang and Shahril Ismail 2025, Sharma and Rani 2025].

Diante desse cenário, este artigo propõe uma avaliação sistemática da aplicabilidade prática e da eficiência de algoritmos de assinatura digital em ambientes embarcados e dispositivos IoT com restrições de recursos. Embora estudos recentes já demonstrem a viabilidade da implementação de algoritmos pós-quânticos em plataformas com elevada capacidade computacional [Amorim and Henriques 2020], a análise de seu comportamento em dispositivos de baixa e média capacidade de processamento ainda permanece pouco explorada, especialmente em cenários que demandam migração urgente para esquemas criptográficos resistentes a ataques quânticos.

Nesse contexto, a abordagem adotada consiste na comparação do algoritmo pós-quântico ML-DSA com os padrões industriais clássicos RSA e ECDSA. Essa delimitação permite estabelecer uma linha de base representativa do desempenho de soluções criptográficas amplamente consolidadas, contrastando-as diretamente com uma das principais alternativas padronizadas pelo NIST para o cenário de migração pós-quântica. Dessa forma, busca-se analisar os impactos associados ao consumo de memória e às demandas de armazenamento impostas pelos diferentes algoritmos de assinatura digital em ambientes com recursos limitados.

3. Trabalhos Relacionados

A crescente preocupação com os impactos da computação quântica sobre os sistemas criptográficos tradicionais tem impulsionado pesquisas voltadas à avaliação de algoritmos de criptografia pós-quântica em ambientes embarcados e dispositivos IoT.

O trabalho de [Commey et al. 2025] analisa o desempenho de algoritmos pós-quânticos em dispositivos eletrônicos de consumo, considerando tempo de execução, custo de comunicação, uso de memória, custos de implantação e limitações operacionais

em ambientes restritos. De maneira semelhante, [Hanna et al. 2025] avalia a segurança pós-quântica em dispositivos IoT de consumo, analisando latência do *handshake* TLS (*Transport Layer Security*), consumo energético, *overhead* de comunicação, efeito do tamanho de certificados e assinaturas, desempenho em BLE (*Bluetooth Low Energy*) versus Wi-Fi, autenticação mútua e outros. O estudo destaca que a ameaça quântica também compromete a segurança das comunicações sem fio, frequentemente protegidas por mecanismos criptográficos leves devido às limitações computacionais desses dispositivos.

No trabalho de [Nielsen et al. 2025], é analisado o desempenho dos algoritmos de assinatura digital ML-DSA, Falcon e SPHINCS+ em um microcontrolador LoRa ESP32. A avaliação considera métricas como latência, uso de memória e parâmetros em diferentes níveis de segurança do NIST, os mesmos utilizados no presente estudo. Os resultados indicam que o ML-DSA apresenta melhor desempenho temporal, porém maior consumo de memória (*heap*), enquanto o SPHINCS+ mostrou-se inviável para aplicações IoT devido ao elevado custo computacional e ao grande tamanho das assinaturas.

Por sua vez, [Chhetri 2026] apresenta os primeiros testes isolados dos algoritmos ML-KEM (FIPS 203) e ML-DSA (FIPS 204) em um processador ARM Cortex-M0+ RP2040 operando a 133 MHz e com 264 KB de SRAM. O estudo avalia os três níveis de segurança padronizados pelo NIST, considerando operações de geração de chaves, assinatura e verificação.

Os trabalhos analisados demonstram que a criptografia pós-quântica já vem sendo amplamente investigada sob diferentes perspectivas em ambientes embarcados e IoT. Entretanto, observa-se que grande parte dessas pesquisas concentra-se em análises gerais de desempenho ou em plataformas com capacidades computacionais distintas, não explorando de maneira aprofundada a comparação direta entre algoritmos clássicos amplamente consolidados na indústria, como RSA e ECDSA, e algoritmos pós-quânticos como o ML-DSA em dispositivos IoT de recursos restritos.

Nesse contexto, este trabalho busca contribuir para a literatura ao realizar uma análise comparativa sistemática entre algoritmos criptográficos clássicos e pós-quânticos em uma plataforma ESP32. A proposta permite avaliar de forma mais concreta os desafios, limitações e vantagens da adoção do ML-DSA em ambientes IoT sujeitos às restrições típicas de processamento e memória.

A Tabela 1 apresenta um resumo dos principais trabalhos relacionados.

4. Metodologia

Os experimentos foram desenvolvidos utilizando o ESP-IDF versão 5.3.5, *framework* oficial da Espressif para dispositivos da família ESP32. Os algoritmos RSA e ECDSA foram implementados por meio da biblioteca *mbedTLS*, inclusa no *framework* por já ser bem estabelecida e validada. Para a implementação do algoritmo pós-quântico ML-DSA, foi utilizada a biblioteca *mldsa-native*, integrante do projeto *Open Quantum Safe* (OQS), iniciativa de código aberto voltada ao suporte da transição para mecanismos de criptografia pós-quântica [OQS 2025]. Ambas as bibliotecas foram utilizadas sem modificações, visando reproduzir um cenário real de adoção por desenvolvedores.

Os algoritmos foram organizados em três grupos (Tabela 2) conforme seus níveis de segurança equivalentes ao *Advanced Encryption Standard* (AES) [NIST 2020,

Tabela 1. Resumo dos trabalhos relacionados

Trabalho	**Plataforma**	**Algoritmos Avaliados**	**Principais Contribuições**
[Commey et al. 2025]	MacOS com Apple M4, Ubuntu x86, Raspberry Pi 4 CPU ARM.	ML-KEM, McEliece, BIKE, HQC, ML-DSA, Falcon, SPHINCS+	Análise de desempenho, eficiência computacional e desafios de implantação em ambientes restritos.
[Hanna et al. 2025]	Raspberry Pi 4 CPU ARM	ML-KEM, ML-DSA, Falcon, ECDHE, ECDSA	Avaliação da segurança pós-quântica em IoT com recursos limitados.
[Nielsen et al. 2025]	ESP32 + LoRa	ML-DSA, Falcon, SPHINCS+	Comparação de latência e memória de algoritmos pós quânticos em diferentes níveis de segurança da NIST.
[Chhetri 2026]	Raspberry PI Pico 2 CPU ARM	ML-KEM, ML-DSA	*Benchmarks* dos algoritmos FIPS 203 e FIPS 204 em plataforma embarcada de baixo custo.
Este artigo	ESP32 DevKit	RSA, ECDSA, ML-DSA	Comparação de CPU e memória entre algoritmos clássicos e pós quânticos em sistemas embarcados em diferentes níveis de segurança da NIST.

NIST 2024]: o nível N1 corresponde às implementações com segurança equivalente ao AES-128, isto é, 128 bits de segurança; o nível N3 corresponde ao AES-192, com 192 bits de segurança; e o nível N5 refere-se ao AES-256, equivalente a 256 bits de segurança.

Os testes foram realizados em uma placa ESP32 de 240MHz, com intervalo de confiança de 95% e 30 execuções por experimento para garantir representatividade estatística. Entretanto, devido ao elevado custo computacional do RSA 15360, equivalente ao nível de segurança N5 (Tabela 2), os resultados correspondentes não foram considerados na análise, uma vez que a execução prática do algoritmo tornou-se inviável na plataforma ESP32 utilizada. Todos os algoritmos foram avaliados sob as mesmas condições de *hardware*, assegurando imparcialidade e comparabilidade dos resultados.

As métricas analisadas foram o tempo de execução e o consumo de memória *stack*, amplamente utilizadas na avaliação de algoritmos criptográficos embarcados [Albarello et al. 2020]. Aspectos como consumo energético e desempenho em ambientes multitarefa não foram contemplados neste trabalho, constituindo perspectivas para pesquisas futuras. Para garantir a reprodutibilidade dos experimentos, todo o código usado no decorrer dos testes encontra-se disponível no repositório público no github: `https://github.com/R0SSETT0/MLDSA-on-ESP32`.

5. Resultados

Nesta seção são apresentados os resultados obtidos a partir dos experimentos realizados na plataforma ESP32. Inicialmente, é discutida a validação dos testes executados, verificando a corretude das operações criptográficas e a estabilidade dos algoritmos ava-

Tabela 2. Níveis de segurança dos algoritmos [NIST 2024, NIST 2020].

Nível N1 (128 bits)	**Nível N3 (192 bits)**	**Nível N5 (256 bits)**
RSA 3072	RSA 7680	RSA 15360
ECDSA 256	ECDSA 384	ECDSA 521
ML-DSA 44	ML-DSA 65	ML-DSA 87

liados. Em seguida, são analisadas as métricas de desempenho relacionadas ao tempo de execução e ao consumo de memória dos algoritmos RSA, ECDSA e ML-DSA, considerando diferentes níveis de segurança. Os resultados permitem avaliar a viabilidade da aplicação de esquemas criptográficos pós-quânticos em ambientes embarcados e dispositivos IoT com restrições de recursos.

Para validar as operações de assinatura e verificação na ESP32, foram utilizados mecanismos de *logging*. Durante os testes, o RSA apresentou inconsistência no nível de segurança N3 devido ao tamanho das chaves e às limitações de *hardware*. Em contrapartida, ECDSA e ML-DSA obtiveram taxa de sucesso de 100% em todos os níves de segurança, demonstrando estabilidade operacional mesmo em ambientes com recursos restritos.

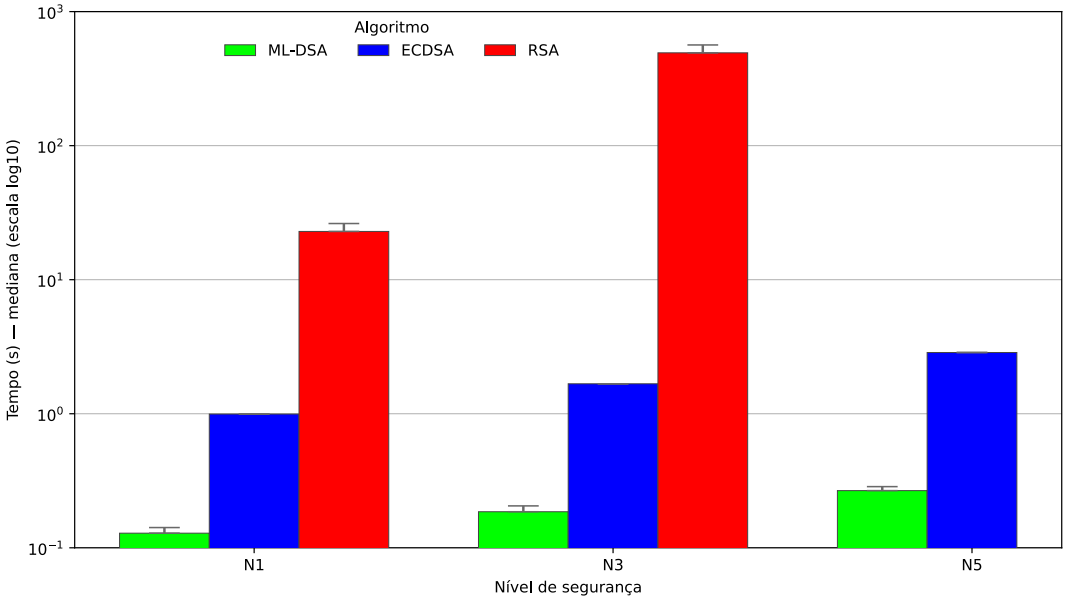

Figura 1. Tempo de execução.

A Figura 1 apresenta o tempo de execução das operações de assinatura. O algoritmo pós-quântico ML-DSA apresentou os menores tempos de execução em todos os níveis de segurança avaliados. Em comparação ao ECDSA, o ML-DSA demonstrou desempenho aproximadamente uma ordem de grandeza superior, enquanto em relação ao RSA a diferença tornou-se ainda mais expressiva, alcançando mais de duas ordens de magnitude nos níveis de segurança mais elevados. Observa-se também que o aumento do nível de segurança impacta significativamente o tempo de execução do RSA, cujo crescimento ocorre de forma acentuada devido ao aumento do tamanho das chaves criptográficas e da complexidade das operações matemáticas envolvidas. Em contrapartida,

os algoritmos ML-DSA e ECDSA apresentaram crescimento mais moderado, mantendo tempos de execução relativamente estáveis mesmo em configurações mais robustas. Esses resultados evidenciam as limitações de algoritmos criptográficos clássicos baseados em grandes tamanhos de chave em sistemas embarcados com restrições de processamento e reforçam a viabilidade do ML-DSA como alternativa para cenários IoT sensíveis à latência.

A Figura 2 apresenta o consumo de memória (*stack*) das operações de assinatura. Diferentemente do comportamento observado no tempo de execução, o algoritmo pós-quântico apresentou crescimento significativo no uso de memória à medida que o nível de segurança aumentou. No nível N5 de segurança, o ML-DSA demandou aproximadamente quatro vezes mais memória que o ECDSA e cerca de três vezes mais que o RSA, evidenciando o impacto do aumento do tamanho das chaves, assinaturas e estruturas matemáticas utilizadas pelo esquema baseado em reticulados. Em contraste, os algoritmos clássicos apresentaram variação relativamente pequena no consumo de memória entre os diferentes níveis de segurança, mantendo-se próximos de 3 KB de uso de *stack*. Esse comportamento sugere maior previsibilidade no gerenciamento de recursos, característica importante em dispositivos embarcados com restrições severas de memória.

Entretanto, é importante destacar que a implementação do ML-DSA utilizada neste trabalho, fornecida pela biblioteca *liboqs*, não foi especificamente otimizada para plataformas ESP32, ao contrário das implementações de RSA e ECDSA amplamente consolidadas em ambientes embarcados. Ainda assim, conforme discutido na literatura [Bos et al. 2022, Meneses et al. 2024, Shin et al. 2026], o maior consumo de memória é uma característica inerente de algoritmos criptográficos pós-quânticos baseados em reticulados modulares, principalmente em função do tamanho ampliado das chaves públicas, privadas e assinaturas digitais.

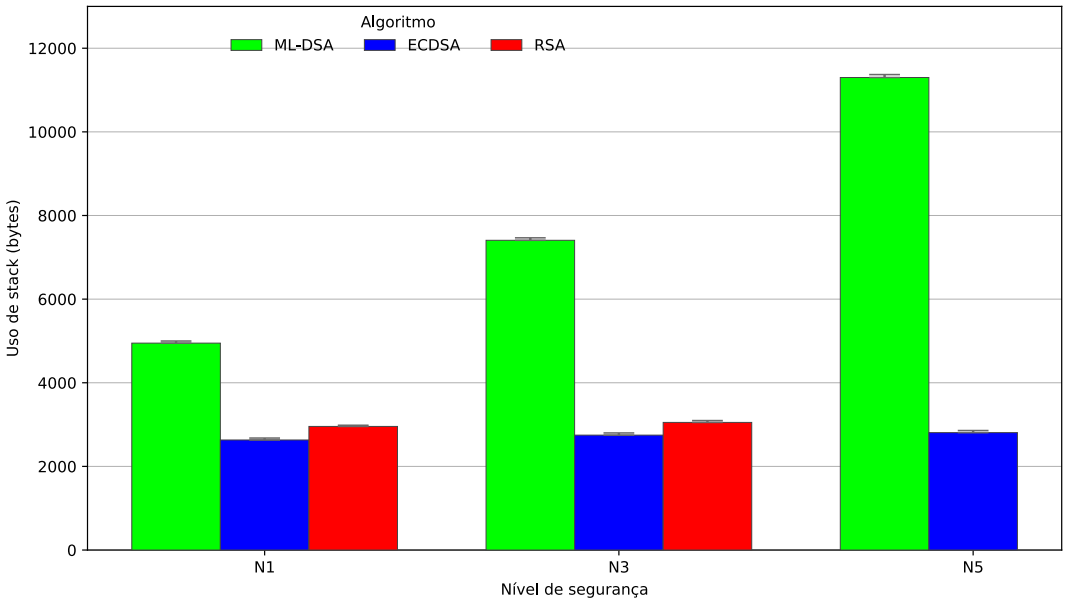

Figura 2. Consumo de memória.

Apesar dessas limitações, os resultados obtidos demonstram que o ML-DSA permanece viável para dispositivos embarcados que disponham de capacidade de memória

compatível com seus requisitos operacionais, oferecendo como contrapartida ganhos expressivos em desempenho computacional e resistência frente a ameaças oriundas da computação quântica.

Embora não tenham sido realizados testes específicos de consumo energético, os resultados sugerem que o ML-DSA pode ser mais eficiente energeticamente devido ao menor tempo de execução observado, já que tempo de processamento e consumo de energia apresentam forte correlação em sistemas embarcados [Rifà-Pous and Herrera-Joancomartí 2011, Jiang et al. 2013]. Além disso, estudos indicam que algoritmos pós-quânticos baseados em reticulados podem oferecer melhor eficiência energética em plataformas embarcadas [Sabani et al. 2023]. Dessa forma, os resultados deste trabalho reforçam o potencial do ML-DSA como alternativa promissora para aplicações IoT que demandam simultaneamente segurança pós-quântica, baixo tempo de resposta e eficiência energética.

6. Conclusões

Este trabalho avaliou a aplicabilidade do algoritmo de assinatura digital pós-quântico ML-DSA em dispositivos embarcados e ambientes IoT, comparando seu desempenho com RSA e ECDSA em diferentes níveis de segurança, em uma plataforma ESP32. Os resultados demonstraram que o ML-DSA apresenta melhor desempenho temporal e maior estabilidade operacional, alcançando taxa de sucesso de 100% em todas as execuções, ao contrário do RSA nos níveis de segurança mais elevados, o que evidencia limitações práticas do RSA em dispositivos com recursos restritos. Além disso, sua resistência a ataques quânticos posiciona o ML-DSA como uma alternativa promissora aos algoritmos clássicos em sistemas embarcados e cenários IoT.

Por outro lado, o principal desafio observado foi o maior consumo de memória, inerente aos algoritmos baseados em reticulados devido ao maior tamanho de chaves, assinaturas e estruturas matemáticas utilizadas. Ainda assim, futuras otimizações, especialmente para a plataforma ESP32, podem reduzir esse impacto em sistemas embarcados.

Diante da necessidade de migração para criptografia pós-quântica, os resultados indicam que o ML-DSA é uma alternativa viável para dispositivos IoT com capacidade de memória adequada para suportar seus requisitos operacionais, evidenciando o compromisso entre desempenho computacional e consumo de recursos.

Como trabalhos futuros, propõe-se avaliar o consumo energético do ML-DSA, analisar cenários multitarefa em IoT e investigar otimizações para reduzir memória e melhorar desempenho em plataformas embarcadas. Também se sugere ampliar os experimentos para outras arquiteturas e algoritmos pós-quânticos do NIST, como o SLH-DSA.

Agradecimentos

Os autores agradecem à Fundação Araucária pelo apoio financeiro, por meio de bolsa PIBIC concedida no âmbito do Edital PROPPG/UTFPR nº 02/2025.

Declaração sobre uso de Inteligência Artificial

Os autores declaram que não utilizaram ferramentas de inteligência artificial na elaboração deste artigo.

Referências

Albarello, R., Oyamada, M., and de Camargo, E. (2020). Avaliação de algoritmos de criptografia e implementação de um protocolo leve para comunicação entre dispositivos iot. In *Anais Estendidos do X Simpósio Brasileiro de Engenharia de Sistemas Computacionais*, pages 65–72, Porto Alegre, RS, Brasil. SBC.

Amorim, P. and Henriques, M. (2020). Uma comparação de desempenho de algoritmos para criptografia pós-quântica. In *Anais Estendidos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 256–269. SBC.

Bos, J. W., Renes, J., and Sprenkels, A. (2022). Dilithium for memory constrained devices. https://eprint.iacr.org/2022/323. Cryptology ePrint Archive.

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., and Smith-Tone, D. (2016). Report on post-quantum cryptography. Technical Report NISTIR 8105, National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.IR.8105.

Chhetri, R. (2026). Pqc benchmarks on arm cortex-m0+ (rp2040). https://zenodo.org/doi/10.5281/zenodo.19393777. Acessado em: 16 de Maio de 2026.

Commey, D., Appiah, B., Klogo, G. S., Bagyl-Bac, W., Gadze, J. D., Alsenani, Y., and Crosby, G. V. (2025). Performance analysis and deployment considerations of post-quantum cryptography for consumer electronics. https://arxiv.org/abs/2505.02239.

Hanna, Y., Bozhko, J., Tonyali, S., Harrilal-Parchment, R., Cebe, M., and Akkaya, K. (2025). A comprehensive and realistic performance evaluation of post-quantum security for consumer iot devices. *Internet of Things*, 33:101650.

IOT Analytics (2025). State of iot 2025: Number of connected iot devices growing 14% to 21.1 billion globally. https://iot-analytics.com/number-connected-iot-devices/. Acessado em: 13 de abril de 2026.

Jiang, W., Guo, Z., Ma, Y., and Sang, N. (2013). Measurement-based research on cryptographic algorithms for embedded real-time systems. *Journal of Systems Architecture*, 59(10, Part D):1394–1404.

Kaur, R. and Kaur, A. (2012). Digital signature. In *2012 International Conference on Computing Sciences*, pages 295–301.

Kumar, K. B. A., Mohith, L. S., Jain, K., Krishnan, P., Venkatachalam, N., and Buyya, R. (2025). Post-Quantum Cryptography-Based Multimedia Encryption Communication Scheme in IoT Consumer Electronics. *IEEE Transactions on Consumer Electronics*, 71(2):4995–5006.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., and Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4(5):1125–1142.

Liu, T., Ramachandran, G., and Jurdak, R. (2024). Post-quantum cryptography for internet of things: A survey on performance and optimization. https://arxiv.org/abs/2401.17538.

Mansoor, K., Afzal, M., Iqbal, W., and Abbas, Y. (2025). Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices. *Cluster Computing*, 28(2):93.

Meneses, R., Teixeira, C., and Henriques, M. (2024). Compact memory implementations of the ml-dsa post-quantum digital signature algorithm. In *Anais Estendidos do XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 233–243. SBC.

Nielsen, M., Kjeldsen, M., Turnip, T., and Andersen, B. (2025). Post-quantum digital signature algorithms on iot: Evaluating performance on lora esp32 microcontroller. In *Proc. International Conference on Security and Cryptography - Volume 1: SECRYPT*, pages 592–600. INSTICC, SciTePress.

NIST (2017). Report on lightweight cryptography. Technical Report NISTIR 8114, U.S. Department of Commerce. `https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf`.

NIST (2020). Recommendation for Key Management: Part 1 – General. Technical Report SP 800-57 Part 1 Rev. 5, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-57pt1r5.

NIST (2024). Fips 204 module-lattice-based digital signature standard. https://csrc.nist.gov/pubs/fips/204/final. Acessado em: 11 de Maio de 2026.

OQS (2025). software for the transition to quantum-resistant cryptography. `https://openquantumsafe.org/`. Acessado em: 19 de Abril de 2026.

Rifà-Pous, H. and Herrera-Joancomartí, J. (2011). Computational and energy costs of cryptographic algorithms on handheld devices. *Future Internet*, 3(1):31–48.

Sabani, M. E., Savvas, I. K., Poulakis, D., Garani, G., and Makris, G. C. (2023). Evaluation and comparison of lattice-based cryptosystems for a secure quantum computing era. *Electronics*, 12(12).

Salter, B., Raine, A., and Geest, D. V. (2025). Use of the ML-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS). RFC 9882. `https://doi.org/10.17487/RFC9882`.

Sharma, A. and Rani, S. (2025). Post-Quantum Cryptography (PQC) for IoT-Consumer Electronics Devices Integrated With Deep Learning. *IEEE Transactions on Consumer Electronics*, 71(2):4925–4933.

Shin, D., Kim, Y., Khalid, A., O'Neill, M., and Seo, S. C. (2026). Optimized implementations of keccak, kyber, and dilithium on the msp430 microcontroller. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2026(2):409–440.

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

Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice*. Pearson, 8 edition.

Wang, Y. and Shahril Ismail, E. (2025). A Review on the Advances, Applications, and Future Prospects of Post-Quantum Cryptography in Blockchain and IoT. *IEEE Access*, 13:112962–112977.