UNIVERSIDADE DA INTEGRAÇÃO INTERNACIONAL DA LUSOFONIA AFRO-BRASILEIRA

INSTITUTO DE ENGENHARIAS E DESENVOLVIMENTO SUSTENTÁVEL

CURSO DE GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

ELÊNCIO CALADO CUSTUME ZIVANE

ANÁLISE DE VIABILIDADE DE ALGORITMOS HÍBRIDOS DE CRIPTOGRAFIA PÓS-QUÂNTICA BASEADOS EM RETICULADOS PARA DISPOSITIVOS IOT COM RECURSOS LIMITADOS

REDENÇÃO

2025

ELÊNCIO CALADO CUSTUME ZIVANE

ANÁLISE DE VIABILIDADE DE ALGORITMOS HÍBRIDOS DE CRIPTOGRAFIA PÓS-QUÂNTICA BASEADOS EM RETICULADOS PARA DISPOSITIVOS IOT COM RECURSOS LIMITADOS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Computação do Instituto de Engenharias e Desenvolvimento Sustentável da Universidade da Integração Internacional da Lusofonia Afro-Brasileira, como requisito parcial à obtenção do grau de bacharel em Engenharia de Computação.

Orientador: Prof. Dr. André Luís da Costa Mendonça

REDENÇÃO

2025

Universidade da Integração Internacional da Lusofonia Afro-Brasileira
Sistema de Bibliotecas da UNILAB
Catalogação de Publicação na Fonte.

Zivane, Elêncio Calado Custume.

Z82a

Análise de viabilidade de algoritmos híbridos de criptografia pós-quântica baseados em reticulados para dispositivos iot com recursos limitados / Elêncio Calado Custume Zivane. - Redenção, 2025.
58f: il.

Monografia - Curso de Engenharia de Computação, Instituto De Engenharias e Desenvolvimento Sustentável, Universidade da Integração Internacional da Lusofonia Afro-Brasileira, Redenção, 2025.

Orientador: Prof. Dr. André Luís da Costa Mendonça.

1. Criptografia pós-quântica. 2. Algoritmos híbridos. 3. Kyber. 4. Dilithium. 5. Internet das Coisas (IoT). I. Título

CE/UF/BSCA CDD 005.82

ELÊNCIO CALADO CUSTUME ZIVANE

ANÁLISE DE VIABILIDADE DE ALGORITMOS HÍBRIDOS DE CRIPTOGRAFIA PÓS-QUÂNTICA BASEADOS EM RETICULADOS PARA DISPOSITIVOS IOT COM RECURSOS LIMITADOS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Computação do Instituto de Engenharias e Desenvolvimento Sustentável da Universidade da Integração Internacional da Lusofonia Afro-Brasileira, como requisito parcial à obtenção do grau de bacharel em Engenharia de Computação.

Aprovada em:

BANCA EXAMINADORA

Prof. Dr. André Luís da Costa Mendonça (Orientador)
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

Prof. Dr. Antônio Manoel Ribeiro de Almeida
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

Dr. Iago Castro Chaves
Laboratório de Sistemas e Bancos de Dados
(LSBD/UFC)

Dedico este trabalho aos meus pais, Calado Custume Rulane e Aneia Marcos Tembe, por acreditarem na minha educação e na dos meus irmãos.

AGRADECIMENTOS

Primeiramente, agradeço a Deus por me conceder força, sabedoria e perseverança ao longo desta jornada.

Ao meu orientador, Prof. Dr. André Luís da Costa Mendonça, pela confiança depositada em meu tema, pela orientação dedicada desde o desenvolvimento do projeto até a escrita final, e pelos conselhos e pela presença em todas as etapas deste processo.

Aos meus irmãos, Valério Calado Zivane, pelos conselhos e apoio incondicional, e Rucay Calado Zivane e Dilen Calado Zivane, por serem fontes constantes de inspiração e motivação para meu crescimento pessoal e como irmão mais velho.

Ao meu tio, Hélder Zivane, pelos ensinamentos, motivação e conselhos que sempre orientaram a minha caminhada estudantil.

Ao meu amigo de longa data, Edilson Rogerio Cuambe, pela parceria, pelas ideias e aprendizados compartilhados, e por dividirmos o sonho de crescer juntos. Que Deus nos abençoe!

Ao Pastor Hermenegildo Guilande e à sua esposa Celeste Guilande, pela orientação espiritual, conselhos e constante motivação que fortaleceram minha fé e determinação durante esta jornada.

Ao Sr. Joaquim Constantino, pelo apoio durante o processo até chegar ao Brasil.

Aos meninos António Paulo Uamba e Daniel da Conceição Agostinho.

Às meninas Helena Mahumane, Shelby Virgílio Macuvele, Michela Virgílio Macuvele, Djenny Leonardo Sambo, Shania Orlando Zibia, Tamires da Conceição Semedo e Chonil Ximene.

Ao Instituto de Bolsas de Estudos de Moçambique (IBE), pela oportunidade e pelo apoio que tornaram este sonho possível.

Por fim, agradeço a todos que, de forma indireta, contribuíram na minha caminhada estudantil.

“Coloque Deus em primeiro lugar em tudo o que você faz.”

(Denzel Washington)

RESUMO

A computação quântica representa uma ameaça direta aos algoritmos criptográficos clássicos, especialmente aos baseados em fatoração e logaritmos discretos, como RSA, ECDH e ECDSA, que podem ser quebrados de forma eficiente pelo algoritmo de Shor. Diante desse cenário, a Criptografia Pós-Quântica (PQC) surge como uma alternativa essencial para garantir a segurança a longo prazo, com destaque para os algoritmos Kyber e Dilithium, padronizados pelo NIST e baseados em problemas difíceis de reticulados. Entretanto, a adoção dessas soluções em dispositivos de Internet das Coisas (IoT) apresenta desafios devido às suas restrições de recursos, como processamento e memória. Dessa forma, este trabalho investiga a viabilidade prática de esquemas criptográficos híbridos, os quais combinam algoritmos clássicos e pós-quânticos, aplicados a dispositivos IoT com recursos limitados. Foram implementados dois cenários híbridos: o primeiro para o encapsulamento de chaves e o segundo para assinaturas digitais. Os resultados demonstraram que, embora os algoritmos pós-quânticos aumentem o custo computacional e o volume de dados transmitidos, as combinações híbridas mostram-se viáveis para uma parcela de dispositivos IoT com recursos limitados, mantendo níveis adequados de desempenho. Assim, o trabalho contribui para a compreensão do processo de transição para a criptografia pós-quântica, evidenciando que soluções híbridas representam uma estratégia segura e pragmática para mitigar riscos enquanto sistemas legados continuam operacionalmente necessários.

Palavras-chave: Criptografia Pós-Quântica. Algoritmos Híbridos. Kyber. Dilithium. Internet das Coisas (IoT)

ABSTRACT

Quantum computing represents a direct threat to classical cryptographic algorithms, especially those based on factorization and discrete logarithms, such as RSA, ECDH, and ECDSA, which can be efficiently broken by Shor's algorithm. Given this scenario, Post-Quantum Cryptography (PQC) emerges as an essential alternative to ensure long-term security, highlighting the Kyber and Dilithium algorithms, which have been standardized by NIST and are based on hard lattice problems. However, the adoption of these solutions in Internet of Things (IoT) devices presents challenges due to their resource constraints, such as processing power and memory. Thus, this work investigates the practical viability of hybrid cryptographic schemes, which combine classical and post-quantum algorithms, applied to resource-constrained IoT devices. Two hybrid scenarios were implemented: the first for key encapsulation and the second for digital signatures. The results demonstrated that, although post-quantum algorithms increase computational costs and the volume of transmitted data, the hybrid combinations prove to be viable for a portion of resource-constrained IoT devices, maintaining adequate performance levels. Therefore, the work contributes to the understanding of the transition process to post-quantum cryptography, showing that hybrid solutions represent a safe and pragmatic strategy to mitigate risks while legacy systems remain operationally necessary.

Keywords: Post-Quantum Cryptography. Hybrid Algorithms. Kyber. Dilithium. Internet of Things (IoT).

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AES	*Advanced Encryption Standard*/Padrão Criptografia Avançada
AES-GCM	*Advanced Encryption Standard in Galois/Counter Mode*/Padrão de Criptografia Avançada em Modo Galois/Contador
BLE	*Bluetooth Low Energy*/Bluetooth de Baixa Energia
CIA	*Confidentiality, Integrity and Availability*/Confidencialidade, Integridade e Disponibilidade
CPU	*Central Processing Unit*/Unidade Central de Processamento
CRYSTALS-Dilithium	*Cryptographic Suite for Algebraic Lattices - Dilithium*
CRYSTALS-Kyber	Cryptographic Suite for Algebraic Lattices - Kyber
CVP	*Closest Vector Problem*/Problema do Vetor Mais Próximo
DH	Diffie-Hellman
DRBG	*Deterministic Random Bit Generators*/Geradores Determinísticos de Bits Aleatórios
DSA	*Digital Signature Algorithm*/Algoritmo de Assinatura Digital
ECC	*Elliptic Curve Cryptography*/Criptografia de Curva Elíptica
ECDH	*Elliptic Curve Diffie-Hellman*/Diffie-Hellman de Curva Elíptica
ECDLP	*Elliptic Curve Discrete Logarithm Problem*/Problema do Logaritmo Discreto em Curvas Elípticas
ECDSA	*Elliptic Curve Digital Signature Algorithm*/Algoritmo de Assinatura Digital em Curvas Elípticas
GCM	*Galois/Counter Mode*/Modo Galois/Contador
HKDF	*HMAC-based Key Derivation Function*/Função de Derivação de Chaves baseada em HMAC
HQC	*Hamming Quasi-Cyclic*
HTTPS	*Hypertext Transfer Protocol Secure*/Protocolo de Transferência de Hipertexto Seguro
IETF	*Internet Engineering Task Force*
IoT	*Internet of Things*/Internet das Coisas
KEM	*Key Encapsulation Mechanism*/Mecanismo de Encapsulamento de Chaves
LoRA	*Low-rank Adaptation*/Adaptação de Baixo Nível

LWE	*Learning With Errors*/Aprendizado com Erros
ML-DSA	*Module Lattice-Based Digital Signature Algorithm*/Algoritmo de Assinatura Digital Baseado em Módulo de Reticulados
ML-KEM	*Module Lattice-Based Key Encapsulation Mechanism*/Mecanismo de Encapsulamento de Chaves Baseado em Módulo de Reticulados
MLWE	*Module Learning With Errors*/Aprendizado em Módulo com Erros
MQ	*Multivariate Quadratic*/Quadrático Multivariado
MQTT	*Message Queuing Telemetry Transport*
MSIS	*Module Short Integer Solution*/Solução de Inteiros Curtos em Módulos
NIST	*National Institute of Standards and Technology*
NTRU	*Nth-degree Truncated polynomial Ring Unit*/Unidade de Anel Polinomial Truncado de Grau *n*
PKI	*Public Key Infrastructure*/Infraestrutura de Chave Pública
PQC	*Post-Quantum Cryptography*/Criptografia Pós-Quântica
RLWE	*Ring Learning With Errors*/Aprendizado em Anél com Erros
RSA	Rivest, Shamir e Adleman
SBC	*Single Board Computers*/Computadores de Placa Única
SDP	*Syndrome Decoding Problem*/Problema da Decodificação por Síndrome
SIS	*Short Integer Solution*/Solução de Inteiros Curtos
SPHINCS+	*Stateless Practical Hash-Based Incredibly Nice Cryptographic Signature*
SSH	*Secure Shell*/Shell Seguro
SSL	*Secure Sockets Layer*/Camada de Soquetes Segura
SVP	*Shortest Vector Problem*/Problema do Vetor Mais Curto
TLS	*Transport Layer Security*/Segurança da Camada de Transporte
VPNs	*Virtual Private Networks*/Redes Privadas Virtuais

SUMÁRIO

1 INTRODUÇÃO

A evolução tecnológica e o crescimento exponencial da conectividade digital têm impulsionado o desenvolvimento de sistemas cada vez mais integrados, inteligentes e interconectados. Nesse contexto, a *Internet of Things*/Internet das Coisas (IoT) destaca-se como um dos pilares da transformação digital, possibilitando a comunicação entre dispositivos, sensores e plataformas de processamento em larga escala, com o objetivo de coletar, transmitir e analisar dados em tempo real (ATZORI *et al.*, 2010; GREENGARD, 2021).

De acordo com (AL-FUQAHA *et al.*, 2015), a IoT representa uma arquitetura composta por múltiplas camadas: percepção, rede e aplicação, permitindo a interação entre o mundo físico e o digital. Essa capacidade de integração favorece a automação de processos, o monitoramento remoto e a criação de serviços inteligentes, impulsionando inovações em setores como saúde, agricultura, transporte e indústria.

Entretanto, o aumento da conectividade também amplia a superfície de ataque dos sistemas, tornando a segurança da informação um dos principais desafios na adoção de soluções IoT (ROMAN *et al.*, 2013). Devido à heterogeneidade e às restrições de hardware, energia e comunicação, muitos dispositivos IoT não conseguem empregar algoritmos criptográficos convencionais, o que os torna vulneráveis a ameaças como interceptação, falsificação de dados e controle remoto indevido (GEBAUER *et al.*, 2022).

Dessa forma, torna-se imprescindível o desenvolvimento de mecanismos de segurança eficientes e leves, capazes de equilibrar proteção e desempenho em ambientes com recursos limitados. É nesse cenário que a criptografia assume um papel central, sendo responsável por assegurar a confidencialidade, integridade e autenticidade das comunicações digitais (STALLINGS, 2013).

A criptografia constitui um dos pilares fundamentais da segurança da informação, sendo essencial para a proteção de dados em sistemas computacionais e redes de comunicação. Protocolos amplamente utilizados, como *Hypertext Transfer Protocol Secure*/Protocolo de Transferência de Hipertexto Seguro (HTTPS), *Secure Sockets Layer*/Camada de Soquetes Segura (SSL) e *Transport Layer Security*/Segurança da Camada de Transporte (TLS), dependem de mecanismos criptográficos para garantir comunicações seguras. O advento da criptografia de chave pública, introduzida por (DIFFIE; HELLMAN, 1976), marcou uma revolução nesse campo, permitindo a troca segura de informações em canais não confiáveis. Desde então, algoritmos clássicos, como Rivest, Shamir e Adleman (RSA), *Elliptic Curve Diffie-Hellman*/Diffie-Hellman

de Curva Elíptica (ECDH) e *Elliptic Curve Digital Signature Algorithm*/Algoritmo de Assinatura Digital em Curvas Elípticas (ECDSA), tornaram-se a base dos sistemas modernos de segurança digital, sustentados em problemas matemáticos de difícil resolução, como a fatoração de grandes números primos e o cálculo do logaritmo discreto em curvas elípticas.

Contudo, o avanço das pesquisas em computação quântica ameaça os fundamentos dessa segurança. Computadores quânticos suficientemente poderosos poderão executar o algoritmo de Shor (SHOR, 1994), capaz de resolver problemas de fatoração e logaritmo discreto em tempo polinomial, comprometendo diretamente os esquemas assimétricos clássicos. Essa possibilidade representa uma ameaça existencial à infraestrutura criptográfica global, incluindo sistemas bancários, protocolos de internet e mecanismos de autenticação digital. Diante desse cenário, emerge a *Post-Quantum Cryptography*/Criptografia Pós-Quântica (PQC), um novo campo de estudo que busca desenvolver algoritmos capazes de resistir a ataques tanto clássicos quanto quânticos. Segundo o *National Institute of Standards and Technology* (NIST), o objetivo central da PQC é desenvolver sistemas criptográficos que sejam seguros contra computadores quânticos e clássicos (STANDARDS; TECHNOLOGY, 2016).

Em resposta a essa ameaça, o NIST iniciou, em 2016, um processo de padronização da criptografia pós-quântica, envolvendo a avaliação pública e colaborativa de dezenas de propostas de algoritmos. Esse processo resultou na seleção de novas primitivas criptográficas, dentre as quais se destacam o Cryptographic Suite for Algebraic Lattices - Kyber (CRYSTALS-Kyber), para encapsulamento de chaves (*Key Encapsulation Mechanism*/Mecanismo de Encapsulamento de Chaves (KEM)), e o *Cryptographic Suite for Algebraic Lattices - Dilithium* (CRYSTALS-Dilithium), para assinaturas digitais (*Digital Signature Algorithm*/Algoritmo de Assinatura Digital (DSA)). Ambas as soluções pertencem à família de algoritmos baseados em módulos de reticulados (*module lattices*), reconhecida pela alta segurança e eficiência, mesmo diante de adversários com poder de computação quântica.

A migração completa para algoritmos pós-quânticos, contudo, apresenta desafios significativos. Além das questões de desempenho e compatibilidade com sistemas legados, há limitações práticas relacionadas ao tamanho das chaves e assinaturas, que tendem a ser substancialmente maiores do que as dos algoritmos clássicos. Nesse contexto, uma abordagem híbrida, combinando algoritmos clássicos e pós-quânticos, surge como uma estratégia de transição segura e gradual (STANDARDS; TECHNOLOGY, 2021). Essa abordagem promove uma defesa em profundidade, na qual a camada clássica garante interoperabilidade e compatibilidade retroativa,

enquanto a camada quântica assegura resistência a ataques futuros, oferecendo proteção a longo prazo durante o período de adaptação tecnológica.

Assim, a necessidade de estratégias híbridas torna-se especialmente relevante no domínio da Internet das Coisas (IoT). Dispositivos IoT caracterizam-se por recursos computacionais restritos, capacidade limitada de processamento, memória reduzida, baixo consumo de energia e largura de banda estreita. Implementar algoritmos pós-quânticos em tais dispositivos representa, portanto, um desafio técnico substancial.

1.1 Problema de Pesquisa

Como os esquemas PQC, como Kyber e Dilithium, demandam chaves públicas e assinaturas significativamente maiores do que os equivalentes clássicos (ECDH e ECDSA), surge uma questão central de pesquisa: "*Qual é a viabilidade prática e o impacto no desempenho ao implementar esquemas criptográficos híbridos (clássicos + quânticos) em ambientes IoT, considerando as restrições de hardware e comunicação desses dispositivos?*".

Responder a essa pergunta é essencial para orientar a transição segura de sistemas embarcados e dispositivos conectados para a era pós-quântica, garantindo a continuidade da segurança digital sem comprometer a eficiência operacional.

1.2 Objetivos

Os objetivos geral e específicos são descritos a seguir.

1.2.1 Objetivo Geral

Analisar a viabilidade e o desempenho de algoritmos criptográficos híbridos (clássicos + quânticos) em ambientes de Internet das Coisas (IoT), avaliando o impacto computacional e de comunicação em esquemas de encapsulamento de chaves (KEM) e de assinatura digital (DSA).

1.2.2 Objetivos Específicos

- Implementar dois cenários de criptografia híbrida: (i) ECDH + CRYSTALS-Kyber para encapsulamento de chaves; e (ii) ECDSA + CRYSTALS-Dilithium para assinatura digital.
- Configurar ambientes de simulação em contêineres Docker para representar dispositivos

IoT com diferentes perfis de hardware.

- Avaliar o desempenho computacional dos dispositivos durante a execução dos algoritmos.
- Analisar o impacto na comunicação dos dispositivos durante a execução dos algoritmos.
- Determinar a viabilidade prática da adoção dessas soluções híbridas em dispositivos IoT com recursos limitados.

1.3 Estrutura do Trabalho

O restante deste trabalho está estruturado da seguinte forma:

- O Capítulo 2 apresenta a fundamentação teórica, abordando os conceitos de criptografia clássica, a ameaça da computação quântica, os princípios da criptografia pós-quântica (PQC) e os algoritmos baseados em reticulados, além de mencionar o processo de padronização conduzido pelo NIST.
- O Capítulo 3 revisa os trabalhos relacionados, destacando as principais pesquisas anteriores sobre o desempenho e a viabilidade de algoritmos PQC em sistemas embarcados e em ambientes IoT.
- O Capítulo 4 descreve a metodologia adotada, detalhando os cenários híbridos implementados.
- O Capítulo 5 apresenta e discute os resultados obtidos, comparando o desempenho computacional e o impacto na comunicação entre os esquemas clássicos, pós-quânticos e híbridos.
- O Capítulo 6 apresenta as conclusões, propondo direções para a continuidade da pesquisa na aplicação de criptografia híbrida em ambientes IoT.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, exploraremos os conceitos e teorias fundamentais que são essenciais para a compreensão do tema em estudo. Aqui, abordaremos as principais definições relevantes que formam a base deste trabalho.

2.1 Fundamentos de Criptografia

A criptografia constitui um dos pilares fundamentais da segurança da informação, exercendo papel essencial na proteção de dados armazenados e transmitidos em sistemas computacionais e redes de comunicação. De acordo com (STALLINGS, 2013), trata-se do conjunto de princípios e técnicas destinados a converter informações legíveis em formatos ininteligíveis, assegurando que apenas destinatários autorizados possam compreender o conteúdo transmitido. O termo "criptografia" origina-se do grego *kryptós* (oculto) e *gráphein* (escrever), refletindo seu propósito histórico de ocultar mensagens e resguardar informações contra acessos indevidos.

Segundo (MENEZES *et al.*, 1996), a criptografia é o estudo de técnicas matemáticas relacionadas a aspectos da segurança da informação, como confidencialidade, integridade de dados, autenticação de entidades e autenticação da origem dos dados. Essa definição destaca o caráter multidimensional da criptografia moderna, relacionando-a diretamente ao modelo da tríade *Confidentiality, Integrity and Availability*/Confidencialidade, Integridade e Disponibilidade (CIA), que representa os princípios fundamentais da segurança da informação. Nesse modelo, a confidencialidade impede o acesso não autorizado a dados, a integridade assegura que as informações não sejam alteradas sem permissão e a disponibilidade garante que os sistemas permaneçam acessíveis a usuários legítimos (STALLINGS, 2013).

Além de preservar a confidencialidade, a criptografia atua como um elemento essencial em mecanismos de autenticação e controle de acesso, sustentando tecnologias como a *Public Key Infrastructure*/Infraestrutura de Chave Pública (PKI) e os certificados digitais. Esses mecanismos viabilizam protocolos amplamente utilizados, como HTTPS, SSL e TLS, assegurando a proteção de comunicações corporativas, financeiras e governamentais.

O avanço decisivo da criptografia moderna ocorreu em 1976, com a introdução do conceito de criptografia de chave pública (DIFFIE; HELLMAN, 1976). Essa abordagem revolucionou o campo ao eliminar a necessidade de compartilhamento prévio de uma chave secreta entre as partes, superando uma limitação fundamental dos sistemas simétricos. Nesse

novo paradigma, cada usuário possui um par de chaves: uma pública, que pode ser livremente divulgada, e uma privada, mantida em sigilo. A segurança desse modelo baseia-se na dificuldade computacional de derivar a chave privada a partir da chave pública.

Posteriormente, (MENEZES *et al.*, 1996) aprofundaram esses conceitos ao introduzir as funções unidirecionais e as funções de alçapão unidirecionais (*trapdoor one-way functions*). Tais funções são de fácil cálculo em uma direção, mas praticamente impossíveis de inverter sem um dado adicional. Essa propriedade possibilitou o desenvolvimento de algoritmos assimétricos amplamente utilizados, como o RSA e o ElGamal, baseados, respectivamente, na dificuldade de fatoração de grandes números primos e na complexidade do problema do logaritmo discreto.

Com base nesses avanços, a criptografia moderna passou a ser tradicionalmente classificada em dois grandes grupos:

- **Criptografia Simétrica:** Utiliza uma única chave para cifrar e decifrar os dados.
  Exemplos: Algoritmos *Advanced Encryption Standard*/Padrão Criptografia Avançada (AES) e ChaCha20.
- **Criptografia Assimétrica:** Utiliza um par de chaves distintas (pública e privada).
  Exemplos: Algoritmos RSA, ECDH e ECDSA.

Essa evolução consolidou a criptografia como ferramenta essencial na segurança digital contemporânea, servindo de base para o desenvolvimento de sistemas mais robustos, escaláveis e adaptados a novos contextos computacionais, como a Internet das Coisas (IoT) e a computação pós-quântica (PQC). Tais fundamentos são indispensáveis para compreender os desafios atuais e as estratégias híbridas que combinam algoritmos clássicos e pós-quânticos na proteção de comunicações digitais, conforme abordado nas seções seguintes deste trabalho.

2.2 Criptogradia Clássica

A criptografia clássica, também conhecida como criptografia convencional, compreende o conjunto de técnicas utilizadas para garantir a segurança da informação antes da introdução dos sistemas de chave pública. Essa vertente é caracterizada pelo uso de chaves secretas compartilhadas, sendo que o emissor e o receptor de uma mensagem utilizam a mesma chave tanto para cifrar quanto para decifrar os dados (STALLINGS, 2013).

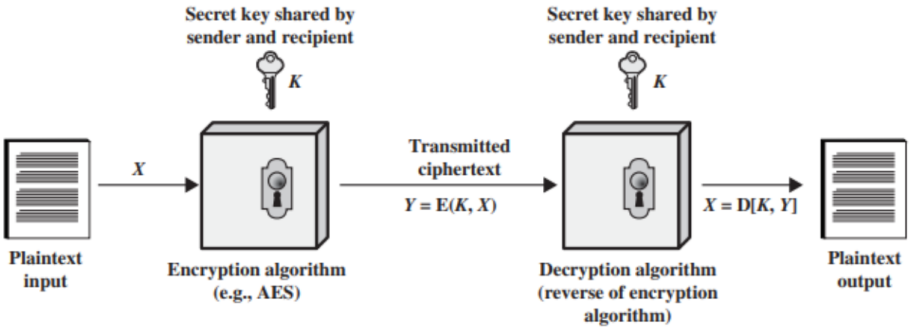
Segundo (SCHNEIER, 2007), a principal limitação desses sistemas reside no processo de distribuição de chaves, uma vez que, para que a comunicação seja segura, é necessário que as partes envolvidas compartilhem previamente a chave secreta por um canal igualmente

seguro, o que nem sempre é viável em ambientes distribuídos ou abertos, como a internet.

2.2.1 Criptogradia Simétrica

Na criptografia simétrica, a segurança depende da confidencialidade da chave compartilhada. Se essa chave for comprometida, todo o sistema torna-se vulnerável. Por outro lado, os algoritmos simétricos são notoriamente eficientes do ponto de vista computacional, o que os torna ideais para aplicações que demandam alto desempenho e baixo consumo de recursos, como comunicações em tempo real e dispositivos IoT (STALLINGS, 2013). A Figura 1 apresenta um diagrama de um sistema de criptografia simétrica, ilustrando o processo de cifragem e decifragem com uma chave secreta compartilhada.

Figura 1 – Diagrama de um sistema de criptografia simétrica, ilustrando o processo de cifragem e decifragem com uma chave secreta compartilhada.



Fonte: (STALLINGS, 2013).

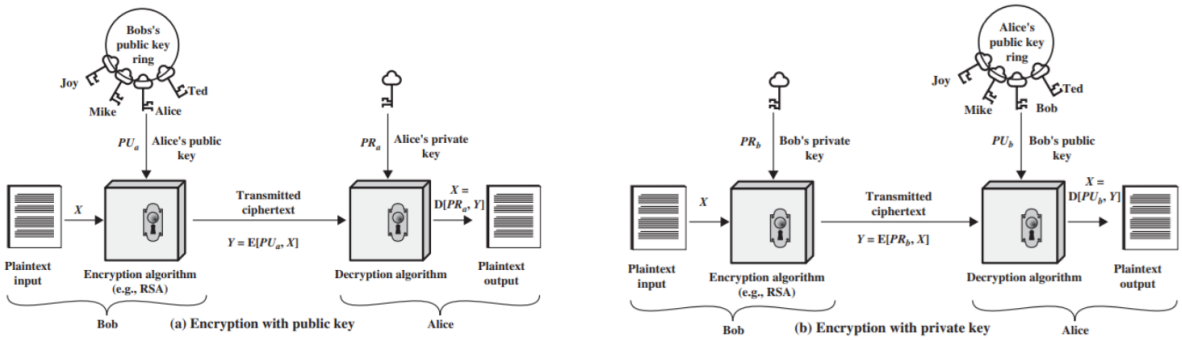
Entre os principais algoritmos simétricos modernos, destacam-se o AES, padronizado pelo NIST em 2001, e o ChaCha20, amplamente utilizado em aplicações móveis e protocolos de segurança como o TLS. O AES opera sobre blocos de 128 bits e permite chaves de 128, 192 ou 256 bits, proporcionando um equilíbrio eficiente entre segurança e desempenho (DAEMEN; RIJMEN, 2002). Já o ChaCha20, projetado por (BERNSTEIN *et al.*, 2008), utiliza operações aritméticas simples em palavras de 32 bits, o que o torna altamente otimizado para processadores embarcados e de baixo consumo energético.

O modo de operação *Galois/Counter Mode*/Modo Galois/Contador (GCM), frequentemente aplicado em conjunto com o AES, é outro avanço relevante, pois, além de cifrar os dados, garante autenticidade e integridade, evitando ataques de falsificação de mensagens. Essa capacidade de autenticação embutida é particularmente importante em sistemas distribuídos e dispositivos conectados, onde o tráfego pode ser interceptado ou modificado.

2.2.2 Criptografia Assimétrica

A criptografia assimétrica, ou de chave pública, surgiu como resposta ao desafio da distribuição segura de chaves, introduzido por (DIFFIE; HELLMAN, 1976). Diferentemente dos sistemas simétricos, esse modelo utiliza dois pares de chaves distintas: uma pública, utilizada para cifrar os dados ou verificar assinaturas, e uma privada, utilizada para decifrar ou assinar. Essa estrutura elimina a necessidade de um canal seguro prévio para o compartilhamento de segredos. A Figura 2 apresenta um diagrama de um sistema de criptografia assimétrica (chave pública), apresentando a cifragem com chave pública e a cifragem com chave privada (assinatura digital).

Figura 2 – Diagrama de um sistema de criptografia assimétrica (chave pública), apresentando a cifragem com chave pública e a cifragem com chave privada (assinatura digital).



Fonte: (STALLINGS, 2013).

Os algoritmos assimétricos mais amplamente utilizados baseiam-se em problemas matemáticos de difícil inversão, como:

- O problema da fatoração de números primos, que fundamenta o algoritmo RSA (RIVEST *et al.*, 1978).
- O problema do *Elliptic Curve Discrete Logarithm Problem*/Problema do Logaritmo Discreto em Curvas Elípticas (ECDLP), que forma a base da segurança de muitos sistemas criptográficos de *Elliptic Curve Cryptography*/Criptografia de Curva Elíptica (ECC), como os protocolos ECDH e o ECDSA (MENEZES *et al.*, 1996).

Segundo (KOBLITZ, 1987), as curvas elípticas proporcionam níveis equivalentes de segurança com tamanhos de chave menores quando comparadas ao RSA, o que reduz significativamente o consumo de recursos computacionais, sendo uma característica crucial em dispositivos IoT e em ambientes restritos de hardware. Essa vantagem fez com que os algoritmos baseados em ECC se tornassem padrão em protocolos modernos de segurança, como o TLS, o

Secure Shell/Shell Seguro (SSH) e as assinaturas digitais em *blockchain*.

Contudo, apesar de sua robustez e eficiência, os sistemas de chave pública clássicos compartilham uma vulnerabilidade comum: a dependência de problemas matemáticos que podem ser resolvidos com o advento da computação quântica. De acordo com (SHOR, 1994), um computador quântico suficientemente poderoso seria capaz de fatorar números grandes e resolver logaritmos discretos de forma exponencialmente mais rápida que os computadores clássicos, comprometendo a segurança de algoritmos como RSA, DSA e ECC.

2.2.2.1 Elliptic Curve Diffie-Hellman (ECDH)

A troca de chaves é um elemento essencial na criptografia moderna, permitindo que duas partes estabeleçam um segredo compartilhado sobre um canal inseguro. O protocolo Diffie-Hellman (DH), proposto em 1976, foi o primeiro método prático a resolver esse problema por meio de operações de exponenciação modular sobre números inteiros (STALLINGS, 2013). Posteriormente, o método foi aprimorado com a introdução das curvas elípticas, resultando no ECDH.

As curvas elípticas são estruturas matemáticas definidas sobre corpos finitos, cuja aplicação à criptografia foi proposta de forma independente por (KOBLITZ, 1987; MILLER, 1985). O ECDH baseia-se na dificuldade computacional do Problema do Logaritmo Discreto em Curvas Elípticas (ECDLP), considerado intratável para os recursos computacionais clássicos atuais (STALLINGS, 2013).

Na prática, o protocolo ECDH funciona da seguinte forma:

- Cada participante (por exemplo, Alice e Bob) gera uma chave privada e as respectivas chaves públicas.
- As chaves públicas são trocadas entre as partes.
- Ambos calculam o mesmo segredo compartilhado, que pode ser usado como chave simétrica para a comunicação segura.

Os parâmetros da curva são padronizados por órgãos como o NIST e o *Internet Engineering Task Force* (IETF). Entre as curvas mais utilizadas, destacam-se a Curve25519 e a Curve448, ambas baseadas em curvas de Montgomery, que otimizam a aritmética e o desempenho em sistemas embarcados e dispositivos de baixa potência (GEBAUER *et al.*, 2022).

2.2.2.2 Elliptic Curve Digital Signature Algorithm (ECDSA)

O ECDSA é um algoritmo criptográfico assimétrico amplamente utilizado para a geração e verificação de assinaturas digitais. Ele foi especificado pelo NIST, no documento FIPS 186-5 - *Digital Signature Standard* (DSS), em 2023 (STANDARDS; TECHNOLOGY, 2023), que define os requisitos e procedimentos para a criação de assinaturas digitais seguras com base em chaves públicas.

O ECDSA é considerado a versão baseada em curvas elípticas do tradicional algoritmo DSA. A principal diferença entre ambos está na substituição do grupo multiplicativo utilizado no DSA pelo grupo de pontos de uma curva elíptica definida sobre um corpo finito (JOHNSON *et al.*, 2001).

A segurança do ECDSA baseia-se na dificuldade computacional do Problema do Logaritmo Discreto em Curvas Elípticas ECDLP, para o qual não existem algoritmos subexponenciais conhecidos. Essa característica confere ao ECDSA uma maior força criptográfica por bit de chave quando comparado a sistemas baseados em fatoração de inteiros ou logaritmos discretos clássicos (JOHNSON *et al.*, 2001).

Em sua estrutura, o ECDSA é composto por três processos fundamentais: geração de chaves, assinatura e verificação. Na geração de chaves, o usuário cria um par assimétrico composto por uma chave privada e uma chave pública. Durante o processo de assinatura, o emissor calcula o valor de *hash* da mensagem e gera um número aleatório k por mensagem. Para a verificação da assinatura, o receptor utiliza a chave pública do emissor para verificar a autenticidade, integridade e o não repúdio das informações assinadas (STANDARDS; TECHNOLOGY, 2023).

De acordo com o FIPS 186-5, o ECDSA deve ser utilizado em conjunto com funções de hash aprovadas, como as especificadas nos padrões FIPS 180-4 (SHA-2) e FIPS 202 (SHA-3), além das curvas recomendadas no NIST SP 800-186, como P-256, P-384 e P-521.

Entre as principais vantagens do ECDSA estão a redução do tamanho das chaves e assinaturas, o desempenho superior em ambientes com restrição de processamento e a robustez criptográfica, mesmo com parâmetros menores (JOHNSON *et al.*, 2001). Por essas razões, o ECDSA é amplamente empregado em protocolos e aplicações como TLS, SSH, certificados digitais e sistemas de *blockchain*.

Entretanto, a segurança do ECDSA depende fortemente da correta geração do número aleatório k em cada assinatura. A reutilização ou previsibilidade desse valor pode

comprometer a chave privada. Por esse motivo, o FIPS 186-5 recomenda o uso de *Deterministic Random Bit Generators*/Geradores Determinísticos de Bits Aleatórios (DRBG) e a adoção de variantes determinísticas, como a definida pela RFC 6979 (PORNIN, 2013), que gera k de forma determinística a partir da chave privada e do hash da mensagem, mitigando vulnerabilidades associadas a falhas de aleatoriedade.

2.3 Computação Quântica

A computação quântica representa uma nova fronteira no processamento de informações, ao empregar os princípios da mecânica quântica para realizar cálculos que são inatingíveis pelos computadores clássicos. Enquanto os bits tradicionais assumem apenas um de dois estados possíveis (0 ou 1), os computadores quânticos utilizam bits quânticos, ou *qubits*, que podem existir em uma superposição de ambos os estados simultaneamente. Essa característica, aliada ao entrelaçamento quântico, permite que sistemas quânticos explorem um espaço de estados exponencialmente maior, abrindo possibilidades inéditas para resolver problemas complexos em áreas como criptografia, otimização, inteligência artificial e simulação de sistemas físicos.

2.3.1 Qubits e Superposição

O *qubit* é a unidade fundamental da computação quântica. De acordo com (NIELSEN; CHUANG, 2010), ele pode ser definido como um sistema quântico de dois níveis, representado como um vetor em um espaço de Hilbert bidimensional. A propriedade de superposição permite que um *qubit* exista em uma combinação linear dos dois estados base, $|0\rangle$ e $|1\rangle$. Isso implica que um único *qubit* pode codificar uma quantidade de informação exponencialmente maior do que um bit clássico, sendo essa a base da vantagem computacional dos sistemas quânticos.

2.3.1.1 Entrelaçamento Quântico

Outro conceito essencial da computação quântica é o entrelaçamento quântico, descrito por (GRIFFITHS; SCHROETER, 2018) como uma correlação não local entre dois ou mais sistemas quânticos. Quando dois *qubits* estão entrelaçados, o estado de um deles depende instantaneamente do estado do outro, independentemente da distância física que os separa. Essa interdependência é uma das manifestações mais profundas da natureza quântica da matéria.

Esse fenômeno evidencia que o entrelaçamento é um efeito inerente à estrutura matemática dos estados compostos da mecânica quântica e não apenas uma curiosidade experimental. Ele é, portanto, um recurso físico fundamental explorado em algoritmos e protocolos quânticos, como a teleportação quântica e a criptografia quântica.

2.4 Criptografia Pós-Quantica (PQC)

O avanço da computação quântica representa uma ameaça concreta aos sistemas criptográficos clássicos, cujas bases matemáticas, antes consideradas intratáveis, podem ser resolvidas de forma eficiente por algoritmos quânticos.

De acordo com o NIST, o objetivo da criptografia pós-quântica é desenvolver sistemas criptográficos que sejam seguros tanto contra computadores quânticos quanto contra computadores clássicos (STANDARDS; TECHNOLOGY, 2016). Essa definição evidencia o propósito central da PQC, o qual consiste em desenvolver algoritmos que permaneçam seguros frente a ataques realizados tanto por computadores clássicos quanto por computadores quânticos, sem depender dos princípios da mecânica quântica para sua implementação.

2.4.1 Impactos dos Computadores Quânticos na Criptografia Clássica

A motivação para o desenvolvimento da PQC decorre diretamente da vulnerabilidade dos algoritmos de chave pública atuais. O NIST alerta que muitos sistemas criptográficos de chave pública amplamente utilizados serão quebrados por computadores quânticos suficientemente grandes (STANDARDS; TECHNOLOGY, 2016). O algoritmo de Shor (SHOR, 1994) permite fatorar números inteiros e calcular logaritmos discretos em tempo polinomial, comprometendo a segurança de sistemas amplamente utilizados, como RSA, DSA, ECDH e ECDSA.

Além disso, o algoritmo de Grover (GROVER, 1996) oferece uma aceleração quadrática em buscas não estruturadas, o que reduz parcialmente a segurança de sistemas simétricos e funções hash. Assim, enquanto mecanismos de criptografia simétrica podem ser reforçados com o aumento do tamanho das chaves (por exemplo, de 128 para 256 bits), os esquemas de chave pública exigem substituições completas.

O NIST (2022) destaca que o processo de migração dos algoritmos de criptografia exigirá um esforço significativo e coordenado, pois envolve não apenas a substituição de algo-

ritmos, mas também a adaptação de protocolos e infraestruturas, como TLS, *Virtual Private Networks*/Redes Privadas Virtuais (VPNs) e certificados digitais.

Por fim, enfatiza-se o conceito de *crypto-agility*, ou seja, a capacidade de alterar algoritmos criptográficos sem comprometer a integridade ou a disponibilidade de sistemas. Essa característica será essencial para garantir resiliência e interoperabilidade durante o processo de transição para algoritmos pós-quânticos.

2.4.2 Famílias de Algoritmos Pós-Quânticos

Diversas famílias de algoritmos têm sido estudadas com o objetivo de oferecer resistência a ataques quânticos. As principais são:

- Baseadas em reticulados (*lattice-based*)
- Baseadas em código (*code-based)*.
- Baseadas em funções hash (*hash-based*).
- Baseadas em polinômios multivariados (*multivariate-based*).

2.4.2.1 Criptografia Baseada em Reticulados

A criptografia baseada em reticulados (*lattice-based cryptography*) constitui uma das áreas mais promissoras da criptografia pós-quântica, reconhecida por sua eficiência, robustez matemática e resistência comprovada a ataques quânticos. Diferentemente de esquemas de criptografia clássicos, como o RSA e ECC, que se apoiam em problemas de fatoração e logaritmo discreto vulneráveis ao algoritmo de Shor, a segurança dos sistemas de reticulados deriva de problemas geométricos de difícil solução, como o *Shortest Vector Problem*/Problema do Vetor Mais Curto (SVP) e o *Closest Vector Problem*/Problema do Vetor Mais Próximo (CVP) (REGEV, 2009).

Um reticulado é definido como o conjunto de todas as combinações lineares inteiras de um conjunto de vetores linearmente independentes em um espaço vetorial $\Re^n$. A dificuldade computacional central consiste em, dado um ponto no espaço, encontrar o vetor do reticulado mais próximoCVP ou o vetor não nulo mais curto SVP. Esses problemas permanecem NP-difíceis mesmo em versões aproximadas, o que garante uma base teórica sólida de segurança, inclusive contra ataques de computadores quânticos (AJTAI, 1996).

Diversas famílias de esquemas criptográficos baseados em reticulados foram desenvolvidas nas últimas décadas, entre as quais se destacam: o *Learning With Errors*/Aprendizado

com Erros (LWE) (REGEV, 2009) e suas variantes *Ring Learning With Errors*/Aprendizado em Anél com Erros (RLWE) *Module Learning With Errors*/Aprendizado em Módulo com Erros (MLWE) (LYUBASHEVSKY *et al.*, 2010), o *Nth-degree Truncated polynomial Ring Unit*/Unidade de Anel Polinomial Truncado de Grau *n* (NTRU) (HOFFSTEIN *et al.*, 1998), o Kyber (BOS *et al.*, 2018) e o Dilithium (DUCAS *et al.*, 2018). Todas essas famílias compartilham o mesmo princípio, que consiste em utilizar a dificuldade de encontrar vetores curtos em reticulados de alta dimensão como base de segurança.

2.4.2.1.1 CRYSTALS-Kyber

O CRYSTALS-Kyber é um dos algoritmos de encapsulamento de chaves (KEM) desenvolvidos no contexto da criptografia pós-quântica (PQC), sendo um dos primeiros a ser selecionado pelo NIST para o processo de padronização. Trata-se de um esquema de criptografia pública baseado em módulos de reticulados (*module lattices*), projetado para oferecer resistência a ataques quânticos e, simultaneamente, alta eficiência computacional em comparação com os métodos clássicos, como o RSA e o ECC.

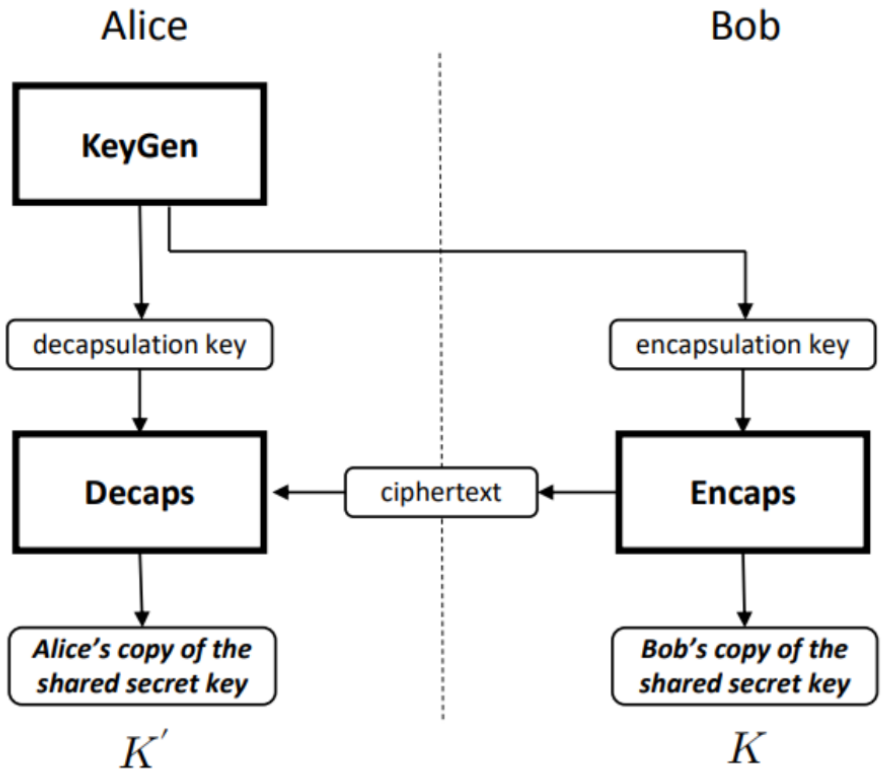
Segundo (BOS *et al.*, 2018), o Kyber é um mecanismo de encapsulamento de chaves seguro contra ataques adaptativos escolhidos por cifra, baseado no problema MLWE, projetado para alta eficiência e simplicidade de implementação. O algoritmo opera com três funções principais: geração de chaves, encapsulamento e desencapsulamento. A Figura 3 apresenta o processo de troca de chaves utilizando o algoritmo Kyber. Essa estrutura garante que apenas o destinatário legítimo possa derivar a chave secreta compartilhada, mesmo que o conteúdo da mensagem cifrada seja interceptado.

Uma das principais vantagens do Kyber é o equilíbrio entre segurança e desempenho. Em experimentos recentes, (KOKARE *et al.*, 2025) relatam que o algoritmo Kyber512, uma variante do Kyber, completou a operação de cifragem três vezes mais rápido do que o RSA-2048, levando apenas 5 *ms* contra 15 *ms*, e a decifragem foi quase três vezes mais eficiente (7 *ms* contra 20 *ms*).

2.4.2.1.2 CRYSTALS-Dilithium

O CRYSTALS-Dilithium é um dos algoritmos de assinatura digital pós-quântica mais promissores e eficientes desenvolvidos no âmbito do processo de padronização conduzido pelo NIST. Baseado em módulos de reticulados (*module lattices*), o Dilithium combina um alto

Figura 3 – Processo de troca de chaves utilizando o algoritmo Kyber.



Fonte: (STANDARDS; TECHNOLOGY, 2025a).

nível de segurança, simplicidade de implementação e excelente desempenho computacional. De acordo com (DUCAS *et al.*, 2018), o Dilithium fornece assinaturas digitais seguras baseadas em reticulados, com forte fundamentação teórica e eficiência prática comparável aos esquemas clássicos, mas com resistência comprovada a ataques quânticos.

O algoritmo fundamenta-se em dois problemas matemáticos considerados difíceis, mesmo para computadores quânticos: o MLWE e o *Module Short Integer Solution*/Solução de Inteiros Curtos em Módulos (MSIS). Esses problemas derivam das versões vetoriais do LWE *Short Integer Solution*/Solução de Inteiros Curtos (SIS), amplamente estudadas na criptografia pós-quântica. A estrutura do algoritmo Dilithium é composta por três fases principais: geração de chaves, assinatura e verificação.

Uma das principais vantagens do Dilithium é sua simplicidade e eficiência, o que o diferencia de outros esquemas de assinatura baseados em reticulados, como o Falcon. Embora o Falcon produza assinaturas menores, ele exige operações matemáticas mais complexas e de difícil implementação segura. Em contraste, o Dilithium prioriza um design simples e facilmente auditável, sem comprometer a segurança. Em experimentos recentes, (KOKARE *et al.*, 2025) relatam que a verificação de assinaturas com o algoritmo Dilithium foi até três vezes mais rápida

do que com o algoritmo DSA, levando apenas 10 *ms* contra 30 *ms* em testes experimentais.

2.4.2.2 Criptografia Baseada em Código

A criptografia baseada em código (*code-based cryptography*) é uma das abordagens mais antigas e consolidadas da criptografia pós-quântica, cuja segurança fundamenta-se na dificuldade de decodificar códigos lineares aleatórios. O problema central sobre o qual essa classe de algoritmos se apoia é o *Syndrome Decoding Problem*/Problema da Decodificação por Síndrome (SDP), considerado NP-difícil, mesmo para computadores quânticos.

O primeiro e mais influente esquema dessa categoria foi o McEliece, proposto por (MCELIECE, 1978), utilizando códigos de Goppa como base matemática. Nesse sistema, a chave pública é uma matriz geradora de código linear disfarçada por transformações aleatórias, enquanto a chave privada contém a estrutura necessária para decodificar eficientemente as mensagens. Conforme descrito no relatório do NIST IR 8545 (STANDARDS; TECHNOLOGY, 2025b), o esquema de McEliece, embora proposto há mais de quatro décadas, continua sendo uma construção muito segura, pois sua base matemática tem resistido a décadas de tentativas de ataques. Portanto, a criptografia baseada em código oferece, assim, um dos pilares mais sólidos da segurança pós-quântica.

2.4.2.3 Criptografia Baseada em Hash

A criptografia baseada em hash (*hash-based cryptography*) é uma das vertentes mais antigas e promissoras da criptografia pós-quântica. Os esquemas baseados em hash utilizam apenas funções hash unidirecionais, as quais permanecem seguras mesmo diante de capacidades quânticas (SRIVASTAVA *et al.*, 2023).

Os algoritmos dessa categoria baseiam-se na propriedade de unidirecionalidade e resistência a colisões das funções hash, ou seja, é computacionalmente inviável reverter o hash para obter o dado original ou encontrar duas entradas diferentes que produzem o mesmo valor. Essa robustez faz dos algoritmos baseados em hash uma alternativa segura e eficiente para autenticação e integridade de dados, mesmo em um cenário pós-quântico.

Uma das grandes vantagens da criptografia baseada em hash é que, caso uma função hash venha a ser considerada insegura, ela pode ser substituída por outra sem comprometer a estrutura geral do sistema. Além disso, ela apresenta eficiência computacional elevada, baixo custo de implementação e tamanho de chave moderado, tornando-a adequada para aplicações em

dispositivos com restrições de recursos, como IoT (SRIVASTAVA *et al.*, 2023).

2.4.2.4 Criptografia Multivariada

A criptografia multivariada (*multivariate public key cryptography*) é uma das abordagens mais consolidadas dentro da criptografia pós-quântica, sendo considerada uma das alternativas mais promissoras aos sistemas baseados em fatoração (RSA) e curvas elípticas (ECC). Ela fundamenta sua segurança na dificuldade de resolver sistemas de equações polinomiais não lineares sobre corpos finitos, um problema conhecido como *Multivariate Quadratic*/Quadrático Multivariado (MQ), considerado NP-difícil (DING; YANG, 2009).

De forma geral, em um esquema multivariado, a chave pública é composta por um conjunto de polinômios quadráticos sobre um corpo finito, enquanto a chave privada contém um "*trapdoor*", uma estrutura secreta que permite resolver o sistema de equações de maneira eficiente. A ideia central desse tipo de criptografia é construir um mapa público a partir de uma composição de transformações afins secretas, aplicadas sobre um mapa central que é fácil de inverter.

A vantagem dos esquemas multivariados é que suas operações são baseadas em aritmética simples em corpos finitos, o que os torna rápidos e adequados para dispositivos com recursos limitados, como os dispositivos IoT. Contudo, um ponto negativo a ser destacar é o grande tamanho das suas chaves públicas, que podem chegar a dezenas de kilobytes (DING; YANG, 2009). Ainda assim, devido à resistência comprovada contra ataques quânticos baseados no algoritmo de Shor, a criptografia multivariada é considerada uma das abordagens mais promissoras para o futuro da segurança digital.

2.4.3 O Processo de Padronização do NIST

O avanço das pesquisas em computação quântica tem colocado em risco a segurança dos sistemas criptográficos clássicos. Diante desse cenário, o NIST iniciou, em 2016, um processo formal de padronização da criptografia pós-quântica (PQC), com o objetivo de identificar e selecionar algoritmos seguros e eficientes contra ataques quânticos.

De acordo com o relatório NIST IR 8545 (STANDARDS; TECHNOLOGY, 2025b), o objetivo da iniciativa é desenvolver e padronizar algoritmos criptográficos públicos que sejam resistentes tanto a ataques clássicos quanto a ataques de computadores quânticos, garantindo a segurança a longo prazo das comunicações digitais. Esse projeto foi estruturado em múltiplas

rodadas públicas de avaliação, nas quais pesquisadores do mundo todo submeteram propostas de algoritmos para serem analisadas sob critérios de segurança, desempenho e viabilidade prática.

Na primeira rodada, iniciada em 2017, o NIST recebeu 82 propostas de algoritmos de diferentes instituições acadêmicas e empresas. Após extensas análises teóricas e experimentais, 26 candidatos foram selecionados para a segunda rodada, realizada entre 2019 e 2020, conforme descrito no relatório. Durante essa fase, o foco esteve na avaliação da robustez matemática, resistência a ataques conhecidos e eficiência de implementação. Em seguida, a terceira rodada, ocorrida no período entre 2020 e 2022, reduziu o conjunto a sete finalistas, dentre os quais foram escolhidos os primeiros algoritmos a serem padronizados: CRYSTALS-Kyber, CRYSTALS-Dilithium, *Stateless Practical Hash-Based Incredibly Nice Cryptographic Signature* (SPHINCS+) e Falcon.

O processo de padronização, contudo, não se encerrou com essas publicações. Em 2022, o NIST iniciou a quarta rodada de avaliação, focada na análise de algoritmos adicionais para diversificar a base matemática dos padrões já existentes. Segundo o NIST IR 8545 (STANDARDS; TECHNOLOGY, 2025b), o algoritmo *Hamming Quasi-Cyclic* (HQC) foi selecionado como o próximo a ser padronizado, ampliando a diversidade dos mecanismos de encapsulamento de chaves (KEM) e fortalecendo a segurança global das comunicações pós-quânticas.

Conforme documentado pelo FIPS 203 (STANDARDS; TECHNOLOGY, 2024b), o NIST selecionou o CRYSTALS-Kyber, renomeado oficialmente como *Module Lattice-Based Key Encapsulation Mechanism*/Mecanismo de Encapsulamento de Chaves Baseado em Módulo de Reticulados (ML-KEM), como o algoritmo padrão de encapsulamento de chaves (KEM). O ML-KEM. Por sua vez, o mesmo documento estabeleceu o CRYSTALS-Dilithium, denominado *Module Lattice-Based Digital Signature Algorithm*/Algoritmo de Assinatura Digital Baseado em Módulo de Reticulados (ML-DSA), como o padrão oficial de assinaturas digitais pós-quânticas. Ambos os algoritmos foram selecionados por oferecerem um equilíbrio superior entre segurança, desempenho e facilidade de implementação, adequados à ampla adoção em sistemas comerciais e governamentais. Além deles, o FIPS 205 (STANDARDS; TECHNOLOGY, 2024c) padronizou o SPHINCS+, um esquema baseado em funções hash com o objetivo de complementar o portfólio de assinaturas digitais resistentes a computadores quânticos.

A importância desse processo é reconhecida mundialmente, pois estabelece padrões globais interoperáveis para a transição da criptografia clássica à pós-quântica. A padronização da criptografia pós-quântica representa um marco histórico na segurança digital, assegurando a confi-

dencialidade e a integridade das comunicações na era quântica (STANDARDS; TECHNOLOGY, 2025b).

2.5 Criptografia Pós-Quântica Híbrida

A criptografia pós-quântica híbrida consiste na utilização simultânea de algoritmos clássicos amplamente consolidados, como RSA, ECDH e ECDSA, com algoritmos pós-quânticos recentemente padronizados pelo NIST, como o Kyber (ML-KEM) e o Dilithium (ML-DSA). A adoção desse modelo decorre da necessidade de garantir segurança durante o período de transição para a era pós-quântica, uma vez que os algoritmos clássicos permanecem altamente confiáveis frente a ataques convencionais, enquanto os algoritmos pós-quânticos, embora resistentes a ataques baseados em computadores quânticos, ainda possuem maturidade limitada e podem revelar vulnerabilidades com o tempo.

Existem quatro formas de realizar combinações híbridas em criptografia, sendo: i) o modelo por camadas; ii) o modelo híbrido composto; iii) o modelo de assinaturas híbridas; e iv) o modelo interoperável, cada um oferecendo um equilíbrio distinto entre compatibilidade, segurança e flexibilidade durante a transição para algoritmos pós-quânticos.

No modelo por camadas, a criptografia pós-quântica é adicionada como uma camada externa que envolve a criptografia clássica sem modificar sua estrutura interna, reforçando o sistema contra ataques quânticos e mantendo a operação original intacta. Por sua vez, no modelo híbrido composto, a troca de chaves clássica e a pós-quântica são executadas simultaneamente, e seus resultados são combinados por uma função de derivação de chaves, formando um único segredo cuja segurança depende dos dois algoritmos. Nos modelos de assinaturas híbridas, o documento recebe duas assinaturas: uma clássica e outra pós-quântica, e a validação ocorre apenas quando ambas são verificadas, garantindo proteção simultânea contra adversários tradicionais e quânticos. Por fim, no modelo interoperável, o sistema negocia dinamicamente entre os algoritmos clássicos e pós-quânticos, permitindo a compatibilidade entre dispositivos de gerações distintas e facilitando a migração gradual. (GUAN, 2024; SAARELA, 2022)

2.6 Internet das Coisas (IoT)

A Internet das Coisas (IoT) representa um dos pilares da transformação digital contemporânea, integrando o mundo físico e o digital por meio da conexão de objetos inteligentes

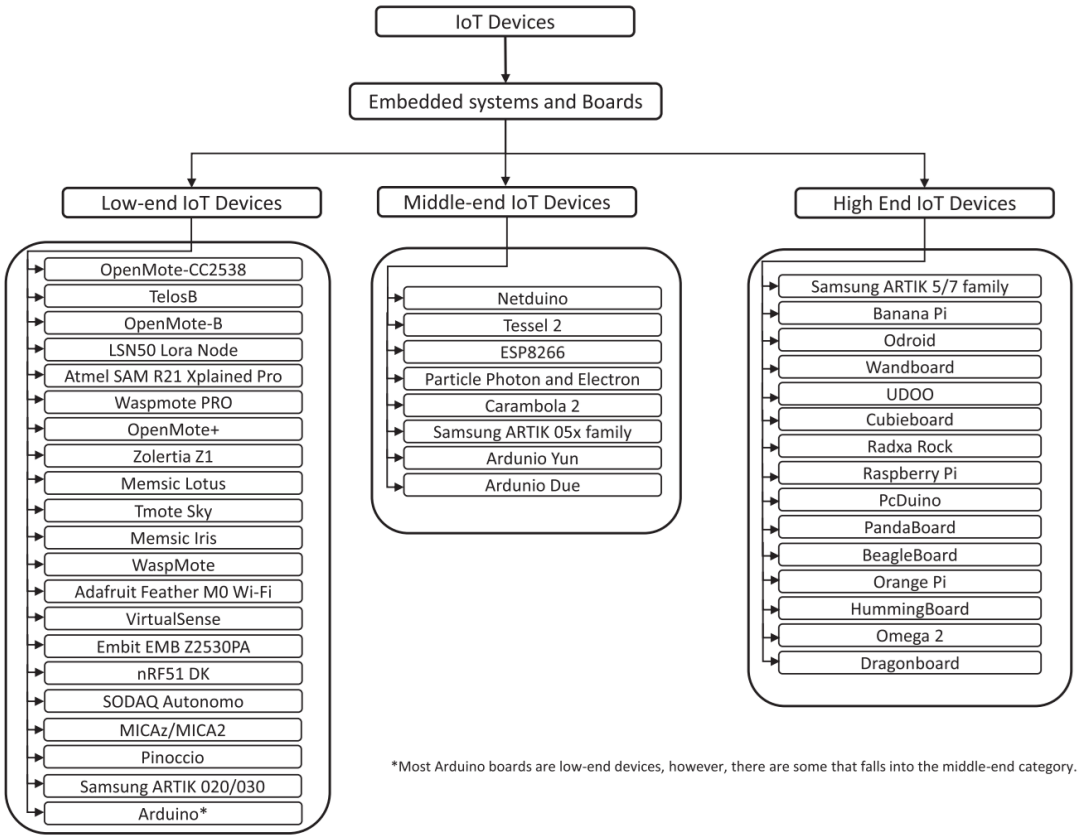
capazes de coletar, processar e compartilhar informações (GREENGARD, 2021). Em sua essência, a IoT consiste em uma rede de dispositivos físicos: sensores, atuadores, controladores e sistemas embarcados que interagem entre si e com aplicações na nuvem, permitindo automação, monitoramento e análise de dados em tempo real (ATZORI *et al.*, 2010). Essa interconexão impulsiona inovações em diversos setores, como saúde, agricultura, transporte e manufatura, mas também introduz novos riscos à segurança da informação.

A arquitetura típica de um sistema IoT é composta por três camadas principais: a camada de percepção, responsável pela coleta de dados através de sensores e atuadores; a camada de rede, que realiza a transmissão dos dados utilizando protocolos de comunicação como Wi-Fi, ZigBee, *Bluetooth Low Energy*/Bluetooth de Baixa Energia (BLE) e *Message Queuing Telemetry Transport* (MQTT); e a camada de aplicação, onde os dados são processados e transformados em informações úteis (AL-FUQAHA *et al.*, 2015). Essas camadas interagem continuamente, formando um ecossistema distribuído e dinâmico que demanda mecanismos de segurança e criptografia adaptados às suas limitações.

De acordo com (OJO *et al.*, 2018), os dispositivos IoT podem ser classificados em três categorias conforme sua capacidade de hardware: baixo custo (*low-end*), médio custo (*middle-end*) e alto custo (*high-end*). Os dispositivos de baixo custo, como sensores simples e microcontroladores, possuem recursos restritos de processamento e memória, o que dificulta a adoção de algoritmos criptográficos complexos. Já os dispositivos de médio custo equilibram desempenho e consumo energético, sendo adequados para aplicações mais elaboradas e testes experimentais. Por sua vez, os dispositivos de alto custo, como os *Single Board Computers*/Computadores de Placa Única (SBC) (por exemplo, o Raspberry Pi), permitem o uso de sistemas operacionais completos e a implementação de algoritmos mais robustos. A Figura 4 apresenta uma classificação de dispositivos IoT, conforme as suas capacidades: *low-end*, *middle-end* e *high-end*.

Essas diferenças de capacidade impactam diretamente o nível de segurança possível em cada cenário. Segundo (ROMAN *et al.*, 2013), a heterogeneidade e a limitação de recursos tornam a IoT um dos ambientes mais vulneráveis a ataques cibernéticos, incluindo interceptação de dados, falsificação de identidade e manipulação de informações. Para mitigar essas ameaças, é essencial o uso de protocolos criptográficos eficientes, que garantam confidencialidade, integridade e autenticidade sem comprometer o desempenho do sistema.

Figura 4 – Classificação de dispositivos IoT.



Fonte: (OJO *et al.*, 2018).

3 TRABALHOS RELACIONADOS

A crescente ameaça da computação quântica à segurança dos sistemas criptográficos atuais impulsionou a pesquisa e o desenvolvimento de algoritmos pós-quânticos (PQC) e soluções híbridas que combinam criptografia clássica e quântica. Este capítulo apresenta uma análise de trabalhos relacionados que abordam a implementação e avaliação de algoritmos criptográficos em contextos vulneráveis a ataques quânticos.

3.1 Cibersegurança na Computação Quântica (AUGUSTO, 2022)

Este trabalho oferece um entendimento do impacto da computação quântica na segurança da informação. O estudo realiza uma investigação sobre as implicações dos algoritmos quânticos nos sistemas de criptografia clássicos, evidenciando as fragilidades de métodos amplamente utilizados, como RSA e ECC, diante do avanço de técnicas quânticas, como os algoritmos de Shor, Grover e Simon. A autora destaca, também, que os algoritmos quânticos de fatoração e busca comprometem diretamente a segurança dos sistemas assimétricos e simétricos tradicionais, ao reduzirem drasticamente o tempo necessário para a quebra de chaves e funções hash.

Diante dessa vulnerabilidade, a autora analisa soluções de criptografia pós-quântica, agrupadas em três grandes eixos: distribuição de chaves, criação de chaves seguras e assinaturas digitais resistentes a ataques quânticos. Entre as técnicas discutidas, sobressaem-se os protocolos de distribuição quântica de chaves, como o BB84 e o E91, bem como as famílias de algoritmos baseados em reticulados e sistemas multivariados quadráticos. Apesar de o trabalho contribuir para o estudo sobre a ameaça quântica à criptografia clássica e apresentar as principais abordagens para mitigar esses riscos, seu caráter acaba sendo mais teórico e de revisão, não apresentando implementações práticas ou avaliações de desempenho dos algoritmos mencionados.

3.2 Desempenho de Algoritmos Pós-Quânticos Candidatos à Padronização no KEMTLS Híbrido (NASCIMENTO *et al.*, 2024)

Os autores investigam a viabilidade e o desempenho de algoritmos PQC candidatos à padronização pelo NIST no contexto do protocolo KEMTLS híbrido. O objetivo principal foi integrar algoritmos da quarta rodada de padronização no KEMTLS híbrido e avaliar seu desempenho em um ambiente realista, comparando-o com o TLS híbrido. A metodologia empregada envolveu a implementação e avaliação de algoritmos como o BIKE, que se destacou

pelo desempenho em diferentes níveis de segurança. As contribuições do estudo incluem a demonstração de que o KEMTLS híbrido pode apresentar melhor desempenho em níveis de segurança mais altos (3 e 5) em comparação com o TLS híbrido, especialmente sem cache de certificados. Apesar de o trabalho ter se concentrado em ambientes realistas, ele acabou não verificando sua aplicabilidade em cenários de IoT com maiores restrições de recursos.

3.3 Análise da Viabilidade de Aplicação de Métodos de Criptografia Pós-Quântica Aplicados ao Sistema de Pagamentos Instantâneos Brasileiro (Pix) (FERREIRA *et al.*, 2022)

Este trabalho investiga a aplicabilidade de algoritmos pós-quânticos no contexto de um sistema financeiro de alta demanda. O objetivo foi analisar a viabilidade da implementação de PQC no Pix, focando em segurança, performance e cripto-agilidade. A metodologia envolveu a análise do estado atual da PQC e da criptografia do Pix, com testes de implementação do esquema de assinatura digital Picnic. As contribuições incluem a avaliação experimental da integração de PQC em um sistema crítico e a análise do impacto na performance das assinaturas digitais, evidenciando que, nas condições atuais, o Picnic ainda não atende às exigências de latência do Pix. Uma limitação do estudo é que ele se concentrou especificamente no ambiente do Pix e no algoritmo Picnic, não explorando a gama de algoritmos PQC.

3.4 Estudos de Otimização do Algoritmo de Criptografia Pós-Quântica CRYSTALS-KYBER (FERRO *et al.*, 2021)

Os autores focam na otimização do algoritmo CRYSTALS-Kyber para reduzir o consumo de memória e o tempo de processamento, visando a sua aplicação em dispositivos de diversos portes. A metodologia empregada consistiu na aplicação de diversas técnicas de otimização, incluindo a remoção de dependências, como a biblioteca OpenSSL e o acesso a arquivos, e a avaliação do desempenho em diferentes cenários, até mesmo em ambientes restritos. As contribuições incluem a demonstração de reduções significativas nos ciclos de *Central Processing Unit*/Unidade Central de Processamento (CPU) e no consumo de memória, tornando o Kyber mais viável para ambientes restritos. No entanto, o estudo limita-se ao algoritmo CRYSTALS-Kyber.

3.5 Estudo Comparativo de Desempenho em Assinaturas Digitais Pós-Quânticas para Plataformas de IoT (NAGATA; HENRIQUES, 2020)

O trabalho apresenta uma contribuição significativa para o entendimento das viabilidades práticas dos algoritmos candidatos à padronização do NIST. O foco do trabalho foi examinar os *trade-offs* entre segurança e desempenho a partir do tamanho das chaves e assinaturas, visando identificar quais algoritmos pós-quânticos são mais adequados à realidade de dispositivos IoT. O estudo baseou-se na comparação empírica de desempenho dos algoritmos candidatos à padronização do NIST para assinaturas digitais. Os testes foram conduzidos em duas plataformas: um ambiente robusto e um ambiente mais restrito, simulando condições típicas de sistemas IoT. Foram avaliadas métricas como o tempo de geração de chaves, assinatura e verificação, bem como os tamanhos de chaves e assinaturas, com foco nos requisitos de desempenho de nós sensores que precisam assinar e transmitir dados frequentemente. No entanto, o estudo não realiza uma análise considerando algoritmos híbridos de criptografia pós-quântica, além de não considerar ambientes *IoT* com recursos mais limitados.

3.6 Análise de Desempenho de Algoritmos Criptográficos Pós-Quânticos em Sistemas Operacionais Embarcados (YAMAMOTO *et al.*, 2023)

Os autores apresentam uma avaliação experimental aprofundada do comportamento de alguns dos principais algoritmos de criptografia pós-quântica em dispositivos de baixo poder computacional, tendo como foco o Raspberry Pi. O objetivo central do estudo foi analisar o consumo de memória e o tempo de execução das operações criptográficas fundamentais desses algoritmos, verificando sua viabilidade prática em sistemas embarcados, um cenário crítico para a adoção de soluções de segurança pós-quântica. O estudo envolveu a execução de testes de desempenho e de uso de memória nos quatro algoritmos candidatos à terceira rodada do processo de padronização do NIST (CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon e SPHINCS+), além do algoritmo clássico RSA, utilizado como referência comparativa. Apesar de analisar vários algoritmos, o trabalho também não considera algoritmos híbridos de criptografia pós-quântica, além de não considerar ambientes com recursos mais limitados.

3.7 Resumo

Os trabalhos apresentados evidenciam a evolução das pesquisas na área da criptografia pós-quântica e sua aplicação em contextos de segurança digital, desde abordagens teóricas até estudos experimentais e de otimização. Em conjunto, esses trabalhos apontam para uma necessidade de soluções criptográficas híbridas que conciliem a robustez dos esquemas pós-quânticos com a compatibilidade e a eficiência dos algoritmos clássicos. Entretanto, observa-se uma lacuna significativa quanto à avaliação prática de algoritmos híbridos, especialmente em dispositivos IoT de baixo poder computacional.

4 METODOLOGIA

Neste capítulo, descreveremos os procedimentos adotados para desenvolver os algoritmos híbridos de criptografia pós-quântica.

A metodologia de esquemas híbridos, que combina algoritmos clássicos e pós-quânticos, constitui uma estratégia recomendada pelo NIST (STANDARDS; TECHNOLOGY, 2016). Nessa abordagem, duas camadas de criptografia (clássica e pós-quântica) são aplicadas em conjunto, exigindo que um invasor comprometa ambos os sistemas, um potencialmente vulnerável a ataques quânticos e outro, em tese, resistente. Essa configuração de defesa em profundidade eleva o custo computacional do ataque e garante resiliência mesmo em caso de falhas de design nos novos algoritmos pós-quânticos.

4.1 Definição dos Cenários

Dois cenários foram definidos para representar as operações criptográficas: **Encapsulamento de Chaves** e **Assinatura Digital**. Essa combinação permite a construção de um sistema híbrido completo, cobrindo tanto os aspectos de confidencialidade quanto os de autenticação.

4.1.1 Cenário A - Encapsulamento de Chaves

A motivação desse cenário consiste em proteger a confidencialidade dos dados em trânsito. Os algoritmos adotados foram o ECDH (clássico) e o CRYSTALS-Kyber (pós-quântico).

A escolha do ECDH fundamenta-se em sua relevância histórica e técnica como protocolo clássico de troca de chaves assimétricas, amplamente utilizado em sistemas de segurança modernos. Os sistemas de curvas elípticas proporcionam uma força criptográfica superior por bit de chave, o que permite alcançar níveis equivalentes de segurança com parâmetros menores em comparação com esquemas baseados em fatoração ou logaritmos discretos convencionais. Essa característica torna o ECDH altamente eficiente para aplicações que demandam baixo consumo de recursos e alta segurança (MENEZES *et al.*, 1996).

Por sua vez, o Kyber foi escolhido por sua segurança comprovada, eficiência e padronização oficial (STANDARDS; TECHNOLOGY, 2024b). Baseado no problema de MLWE, ele oferece resistência a ataques quânticos e desempenho superior em ambientes com recursos limitados, tornando-o ideal para esquemas híbridos e aplicações em IoT (BOS *et al.*, 2018).

O cenário foi dividido em duas fases:

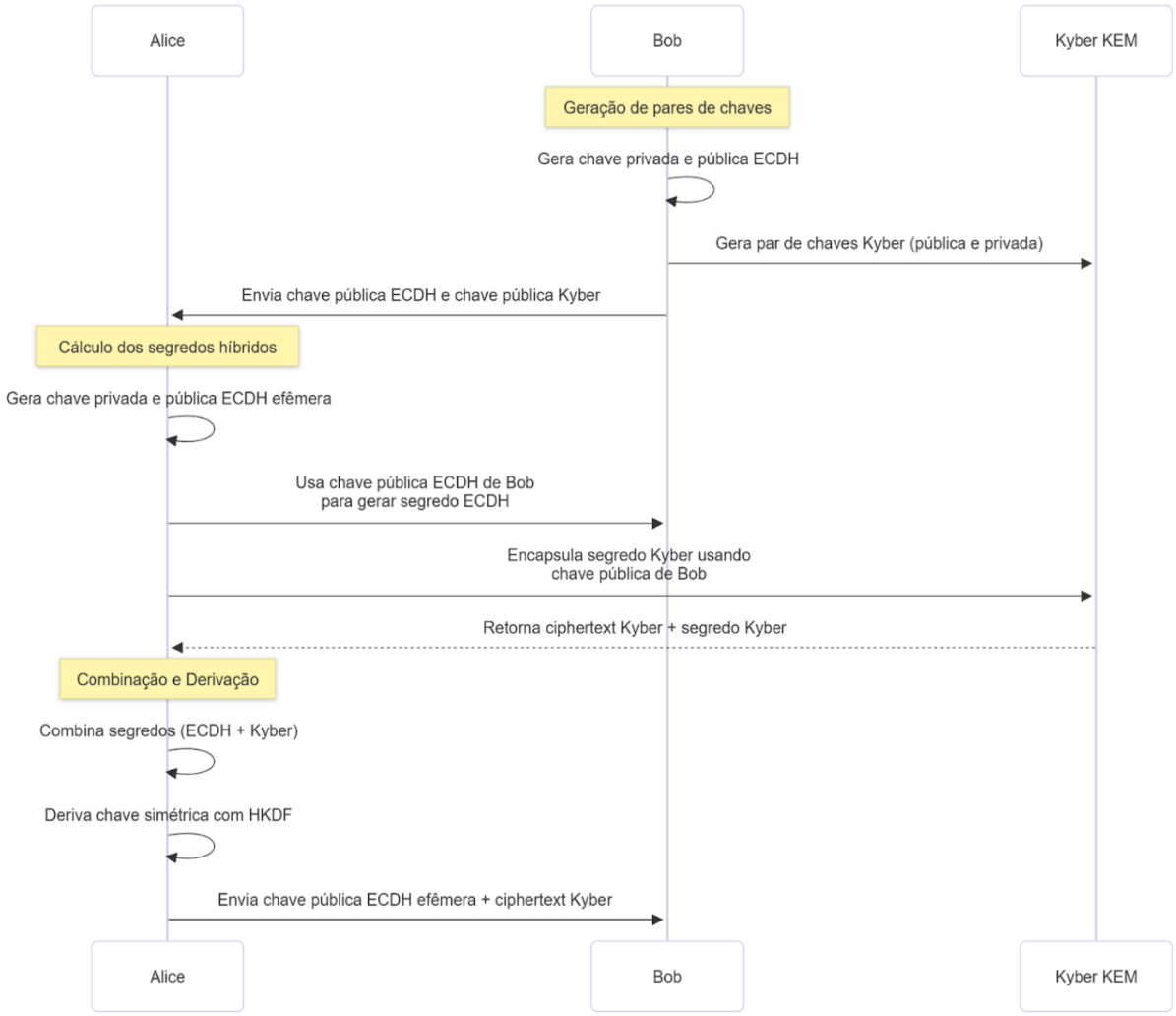
- **Fase 1: Geração de Chaves e Compartilhamento dos Segredos.**
- **Fase 2: Criptografia e Descriptografia.**

Para facilitar o entendimento dos fluxos, iremos considerar a existência de dois usuários hipotéticos durante o processo de troca de mensagens, chamados de Alice e Bob.

Na *Fase 1 - Geração de Chaves e Compartilhamento dos Segredos*, o processo começa com Bob, que gera dois pares de chaves: um par clássico, utilizando o algoritmo ECDH, e um par pós-quântico, utilizando o algoritmo Kyber. Bob mantém suas chaves privadas em sigilo e envia a Alice apenas as chaves públicas correspondentes. Ao receber essas chaves, Alice gera um par de chaves efêmeras para o ECDH e, combinando sua chave privada com a chave pública de Bob, obtém o segredo ECDH. Em paralelo, ela utiliza a chave pública Kyber de Bob para encapsular um segredo Kyber, resultando em dois elementos: o *ciphertext* Kyber, que será enviado a Bob, e o segredo Kyber, que permanece com Alice. Em seguida, Alice combina os dois segredos, o ECDH e o Kyber, e aplica o *HMAC-based Key Derivation Function*/Função de Derivação de Chaves baseada em HMAC (HKDF), utilizando o algoritmo de hash, para derivar uma chave simétrica final. Essa chave será usada posteriormente para a criptografia da mensagem. Após derivar a chave, Alice envia a Bob sua chave pública ECDH efêmera e o *ciphertext* Kyber. Bob, por sua vez, utiliza sua chave privada ECDH e a chave pública efêmera de Alice para calcular o mesmo segredo ECDH e, com sua chave privada Kyber, desencapsula o *ciphertext* Kyber para recuperar o segredo Kyber. Ele então combina ambos os segredos e aplica o mesmo HKDF, obtendo a mesma chave simétrica final derivada por Alice. Essa fase estabelece um segredo híbrido compartilhado, que combina segurança clássica e pós-quântica, garantindo que, mesmo diante de um futuro computador quântico capaz de quebrar o ECDH, o componente Kyber continue a proteger o canal de comunicação. A Figura 5 apresenta o fluxo da Fase 1.

Na *Fase 2 - Criptografia e Descriptografia*, com a chave simétrica derivada na fase anterior, inicia-se o processo de troca de mensagens seguras entre Alice e Bob. Alice prepara a mensagem original e a cifra utilizando algum algoritmo de criptografia, como o *Advanced Encryption Standard in Galois/Counter Mode*/Padrão de Criptografia Avançada em Modo Galois/Contador (AES-GCM), que fornece tanto confidencialidade quanto autenticação. Um *nonce* aleatório é gerado para garantir que cada criptografia seja única, evitando a reutilização de chaves e fortalecendo a segurança. O resultado dessa operação é o *ciphertext* AES, que Alice envia a Bob juntamente com o *nonce* e as informações necessárias para a decifragem. Ao receber os dados, Bob utiliza a mesma chave simétrica e o *nonce* para executar o processo inverso de

Figura 5 – Fluxo de geração de chaves e compartilhamento dos segredos (ECDH + Kyber).



Fonte: Autor.

descriptografia. A Figura 6 apresenta o fluxo da Fase 2.

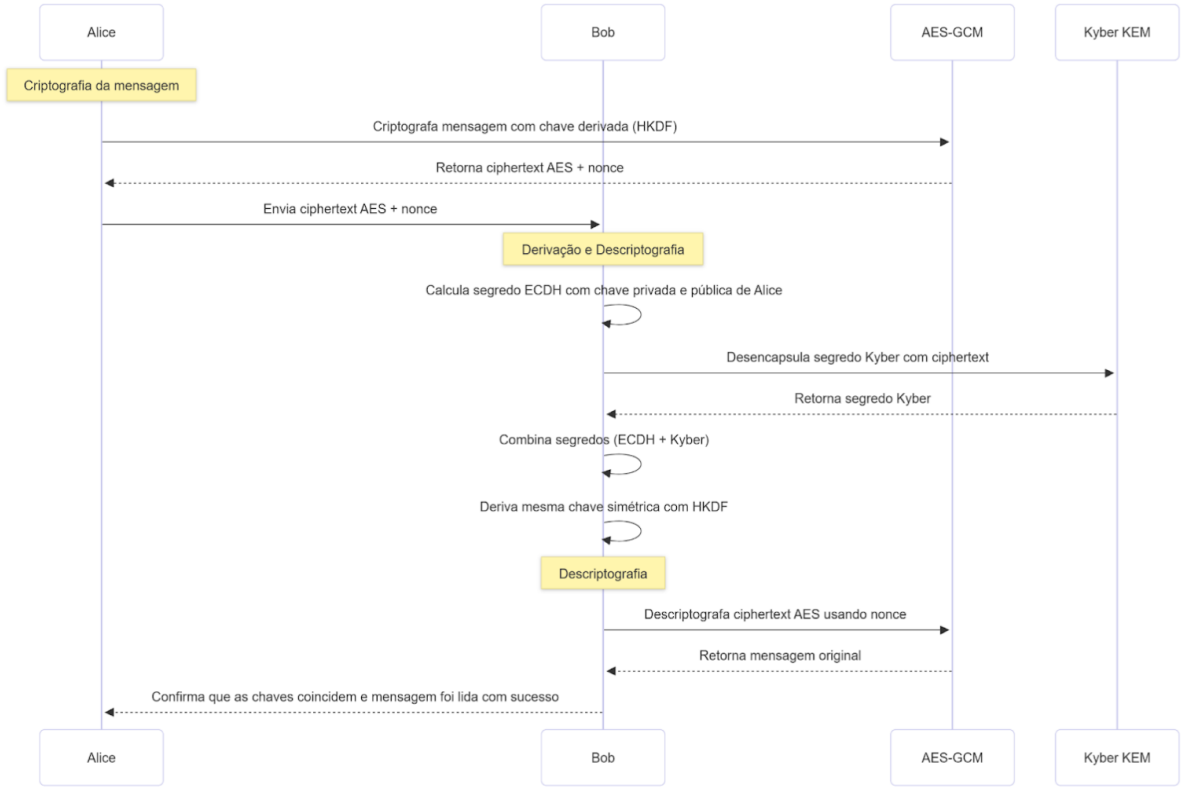
Assim, a combinação das duas fases garante um canal de comunicação seguro, eficiente e resistente tanto a ataques clássicos quanto a futuros ataques quânticos.

4.1.2 Cenário B - Assinaturas Digitais

A motivação desse cenário consiste em assegurar a autenticidade e a integridade em comunicações e documentos digitais. Os algoritmos adotados foram o ECDSA (clássico) e o CRYSTALS-Dilithium (pós-quântico).

A escolha do ECDH fundamenta-se na dificuldade do problema do logaritmo discreto em curvas elípticas, o qual permite alcançar o mesmo grau de segurança com parâmetros menores, resultando em assinaturas mais rápidas, chaves mais curtas e menor consumo de recursos. Essa

Figura 6 – Fluxo de criptografia e descriptografia.



Fonte: Autor.

característica torna o ECDSA particularmente adequado para ambientes com restrições de processamento e armazenamento, como dispositivos IoT e aplicações embarcadas.

Por sua vez, o Dilithium justifica-se por representar uma das soluções mais maduras e seguras da criptografia pós-quântica, recentemente padronizada pelo NIST. Além de oferecer resistência comprovada a ataques quânticos, o Dilithium mantem um desempenho competitivo e facilidade de implementação (DUCAS *et al.*, 2018).

O cenário foi dividido em duas fases:

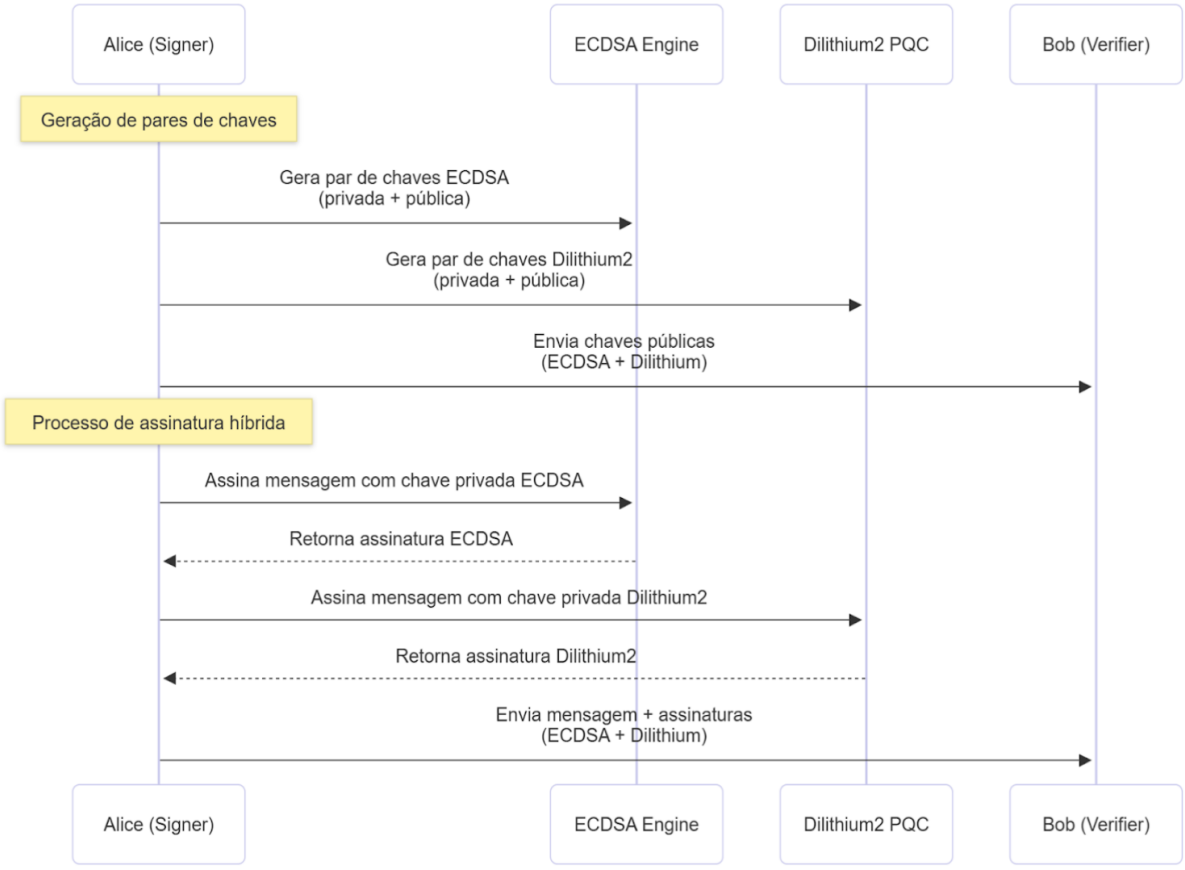
- **Fase 1: Geração de Chaves e Assinatura.**
- **Fase 2: Verificação das Assinaturas.**

Para facilitar o entendimento dos fluxos, iremos manter a existência dos dois usuários hipotéticos (Alice e Bob) durante o processo de troca de mensagens.

Na *Fase 1 - Geração de Chaves e Assinatura*, Alice é responsável por gerar os pares de chaves que serão utilizados para assinar as mensagens. Ela cria uma chave pública e privada utilizando o algoritmo ECDSA. Em seguida, gera um segundo par de chaves utilizando o algoritmo Dilithium. Ao final dessa etapa, Alice possui um conjunto híbrido de chaves, um par clássico (ECDSA) e outro pós-quântico (Dilithium), e compartilha apenas as chaves públicas com

Bob, garantindo que apenas ela possa assinar mensagens autênticas. A seguir, Alice utiliza suas chaves privadas para assinar a mesma mensagem em dois níveis. Primeiramente, Alice assina com a chave privada ECDSA, gerando uma assinatura digital clássica. Em seguida, assina com a chave privada Dilithium, gerando uma segunda assinatura. Por fim, ambas as assinaturas são enviadas a Bob, juntamente com a mensagem e as chaves públicas correspondentes. Dessa forma, a mensagem fica protegida simultaneamente por dois mecanismos criptográficos complementares. A Figura 7 apresenta o fluxo da Fase 1.

Figura 7 – Fluxo de geração de chaves e assinaturas.

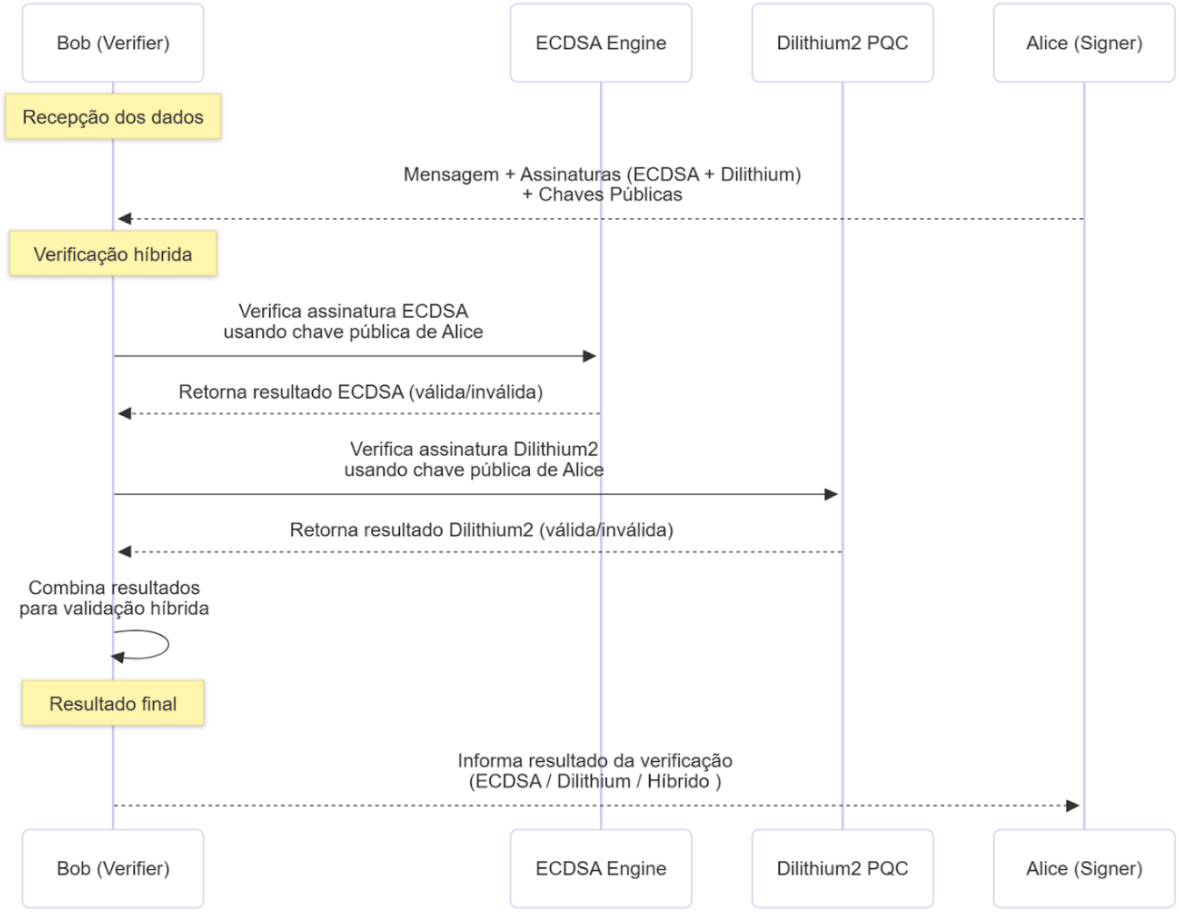


Fonte: Autor.

Na *Fase 2 - Verificação das Assinaturas*, Bob recebe a mensagem, as assinaturas e as chaves públicas de Alice. Primeiramente, Bob realiza a verificação da assinatura ECDSA utilizando a chave pública. Se a assinatura for válida, Bob confirma que a mensagem não foi alterada e que veio de Alice. Depois disso, Bob verifica a assinatura pós-quântica com o esquema Dilithium, utilizando a chave pública correspondente. Somente se ambas as verificações forem bem-sucedidas é que a assinatura híbrida é considerada válida, garantindo assim um nível duplo de segurança: resistência a ataques clássicos e proteção frente a possíveis ataques quânticos. A

Figura 8 apresenta o fluxo da Fase 2.

Figura 8 – Fluxo de verificação das assinaturas.



Fonte: Autor.

5 RESULTADOS EXPERIMENTAIS

Neste capítulo, apresentamos os resultados obtidos a partir da execução dos algoritmos híbridos de criptografia pós-quântica em dispositivos IoT com recursos limitados. A análise permite verificar a viabilidade prática da adoção desses algoritmos em dispositivos IoT.

5.1 Ambiente de Experimentação

Os experimentos foram executados em um notebook Acer Aspire V15, com as seguintes especificações:

- **Processador:** Intel® Core™ i7-13620H (13ª Geração, 2.40 GHz).
- **Memória RAM:** 16 GB.
- **Armazenamento:** SSD de 480 GB.
- **Sistema Operacional:** Ubuntu 22.04 LTS.

Utilizamos o Docker para criar contêineres que representam os dispositivos IoT com diferentes especificações de recursos. Para cada contêiner, foram aplicadas restrições de CPU e memória, de modo a simular as limitações reais dos dispositivos IoT.

5.2 Dispositivos Simulados

Três perfis de dispositivos IoT foram simulados, conforme a Tabela 1. O dispositivo *high-end* possui o maior poder computacional, enquanto o *low-end* o menor. Intuitivamente, o dispositivo *middle-end* possui um nível intermediário de poder computacional.

Tabela 1 – Especificação dos dispositivos IoT simulados no Docker.

Categoria	Modelo Simulado	Processador	Memória
High-end	Raspberry Pi 4 Model B	Broadcom BCM2711, Quad-core Cortex-A72 @ 1.8 GHz	2 GB
Middle-end	ESP32-S3R16V	Xtensa LX7 Dual-core @ 240 MHz	16 MB
Low-end	ATmega1284	AVR 8 bits @ 20 MHz	16 KB

5.3 Algoritmos, Parâmetros e Bibliotecas

Conforme já mencionado no Capítulo 4, foram analisados dois algoritmos clássicos (ECDH e ECDSA) e dois algoritmos pós-quânticos (Kyber e Dilithium), combinados de maneira híbrida em seus respectivos cenários de aplicação.

- **Encapsulamento de Chaves:** ECDH + Kyber.
- **Assinatura Digitail:** ECDSA + Dilithium.

Cada algoritmo de criptografia foi configurado com parâmetros particulares. Os algoritmos ECDH e ECDSA foram configurados com a curva elíptica SECP256R1. Essa variante oferece nível de segurança equivalente a 128 bits, desempenho eficiente e ampla compatibilidade com dispositivos IoT. Para o algoritmo Kyber, foi adotada a sua versão intermediária padronizada pelo NIST, o Kyber768 (ML-KEM-768). Essa variante pertence à categoria de segurança 3, com aproximadamente 192 bits de força criptográfica, sendo indicada pelo NIST como o parâmetro padrão recomendado por garantir uma ampla margem de segurança com um custo computacional moderado (STANDARDS; TECHNOLOGY, 2024b). Para o algoritmo Dilithium, foi adotada a sua versão intermediária padronizada pelo NIST, o Dilithium3. Semelhante ao Kyber768, essa variante também pertence à categoria de segurança 3, oferecendo um bom equilíbrio entre desempenho e robustez (STANDARDS; TECHNOLOGY, 2024a). Por fim, foi adotado o algoritmo AES-GCM no *Cenário A - Encapsulamento de Chaves* para a cifragem de mensagens.

Os algoritmos foram implementados na linguagem Python 3.14, utilizando bibliotecas auxiliares contendo as implementações de métodos de criptografia. Para os algoritmos criptográficos clássicos, utilizamos a biblioteca `cryptography`. Por sua vez, para os algoritmos criptográficos pós-quânticos, utilizamos a biblioteca `liboqs` (STEBILA; MOSCA, 2017).

5.4 Métricas de Avaliação

As métricas foram divididas em duas categorias principais:

1. Métricas de Desempenho Computacional
    - Tempo de geração de chaves (*ms*).
    - Tempo de geração de assinatura (*ms*).
    - Tempo de verificação de assinatura (*ms*).
2. Métricas de Comunicação
    - Tamanho das chaves públicas e *ciphertext* (*bytes*).
    - Tamanho das assinaturas (*bytes*).

Cada experimento foi executado 1.000 vezes para cada combinação de algoritmo e dispositivo. A escolha desse número de execuções deve-se ao fato de ser um número suficientemente grande para reduzir eventuais ruídos causados por variações momentâneas no ambiente virtualizado. É importante ressaltar que essas variações também poderiam ocorrer em

um ambiente de IoT real.

5.5 Resultados

Esta seção apresenta e discute os resultados obtidos nos experimentos utilizando os algoritmos criptográficos híbridos. A análise foi conduzida em duas dimensões principais: desempenho computacional e impacto na comunicação. Para cada um desses eixos de análise, avaliaremos os dois cenários híbridos propostos: encapsulamento de chaves e assinatura digital.

Antes de iniciar as análises, é importante mencionar que o dispositivo de especificação *low-end* não conseguiu executar os algoritmos devido à sua limitação extrema de recursos. Portanto, os resultados irão trazer os comparativos apenas entre os dispositivos com especificações *middle-end* e *high-end*.

5.5.1 Análise do Desempenho Computacional

A avaliação do desempenho computacional concentrou-se nas operações criptográficas fundamentais: geração de chaves, assinatura e verificação.

5.5.1.1 Encapsulamento de Chaves

Conforme pode ser evidenciado na Tabela 2, o algoritmo Kyber apresentou um tempo médio de geração de chaves 171% superior ao ECDH no dispositivo *middle-end* (1,901 *ms* contra 0,701 ms). Essa diferença reduziu-se significativamente no *high-end* (0,155 *ms* contra 0,069 *ms*), revelando que o desempenho do Kyber é fortemente sensível à capacidade de processamento.

Tabela 2 – Tempo médio de execução para a geração de chaves nos algoritmos ECDH e Kyber. (DP = desvio padrão).

	High-end		***Middle-end***	
Operação	**Média (*ms*)**	**DP (*ms*)**	**Média (*ms*)**	**DP (*ms*)**
ECDH	0.069	0.260	0.701	8.853
Kyber	0.155	1.305	1.901	13.858
ECDH + Kyber	0.226	1.415	2.607	19.040

Essa variação é explicada pela natureza matemática do Kyber, que realiza operações intensivas de multiplicação e transformação de polinômios, exigindo mais ciclos de CPU. Já o ECDH, baseado no cálculo de multiplicações escalares em curvas elípticas, depende menos dos recursos e é mais estável em arquiteturas mais simples.

5.5.1.2 Assinatura Digitais

Conforme pode ser evidenciado na Tabela 3, as tendências do tempo gasto para a geração de chaves nos algoritmos clássicos e pós-quânticos mantiveram-se semelhantes à análise anterior. No entanto, as análises das operações associadas às assinaturas digitais revelaram diferenças importantes, conforme pode ser evidenciado na Tabela 3. O algoritmo Dilithium apresentou um tempo de assinatura 40% maior que o ECDSA no dispositivo *middle-end* (3,002 *ms* contra 2,136 *ms*), mas, em contrapartida, obteve 33,5% melhor desempenho na verificação (2,113 *ms* contra 3,180 *ms*). Essa assimetria é relevante, pois a verificação é a operação mais frequente em servidores e dispositivos receptores, como, por exemplo, na autenticação TLS e na validação de mensagens.

É possível observar que houve uma inversão entre os algoritmos ECDSA e Dilithium nas operações de assinatura e verificação. O ECDSA foi mais rápido na etapa de assinatura, enquanto o Dilithium foi mais rápido na verificação. O esperado era que o Dilithium fosse mais custoso em ambas as situações, dada a sua natureza mais complexa. Uma possível explicação pode estar relacionada às implementações das bibliotecas utilizadas, o que sugere uma implementação mais otimizada dos algoritmos presentes na biblioteca `liboqs` em comparação à biblioteca `cryptography`.

Tabela 3 – Tempo médio de execução para a geração de chaves, assinatura e verificação nos algoritmos ECDSA e Dilithium. (DP = desvio padrão).

	High-end		***Middle-end***	
Operação	**Média *(ms)***	**DP (ms)**	**Média (*ms*)**	**DP (*ms*)**
ECDSA (chaves)	0.112	1.206	0.998	10.403
Dilithium (chaves)	0.226	1.832	2.074	13.889
ECDSA + Dilithium (chaves)	0.340	2.202	3.076	19.497
ECDSA (assinatura)	0.264	2.102	2.136	13.346
Dilithium (assinatura)	0.362	2.251	3.002	15.603
ECDSA + Dilithium (assinatura)	0.629	3.085	5.200	20.931
ECDSA (verificação)	0.363	2.639	3.180	16.175
Dilithium (verificação)	0.156	1.209	2.113	13.286
ECDH + Dilithium (verificação)	0.647	3.156	6.872	23.413

5.5.2 Análise do Custo de Comunicação

A avaliação do custo de comunicação concentrou-se no impacto dos tamanhos de chaves, *ciphertexts* e assinaturas sobre o volume total de dados transmitidos entre os dois usuários

(cliente e servidor). Apesar de não termos avaliado o tempo decorrido durante as trocas de informações entre entidades distintas, o conhecimento do tamanho das informações trocadas pela rede funciona como um grande indicativo acerca desses custos envolvendo o envio de informações.

5.5.2.1 Encaplusmento de Chaves

Conforme a Tabela 4, o algoritmo Kyber requer uma chave pública de 1.184 bytes, um aumento de 1.721% em relação ao ECDH (65 bytes). O *ciphertext* Kyber adiciona mais 1.088 bytes, elevando o tráfego total de dados para cerca de, pelo menos, 1.249 bytes (65 + 1184 bytes na direção servidor $\rightarrow$ servidor) e 1.153 bytes (65 + 1088 bytes na direção cliente $\rightarrow$ servidor). Esse aumento é um dos principais *trade-offs* da segurança quântica. Em redes IoT baseadas em *Low-rank Adaptation*/Adaptação de Baixo Nível (LoRA) ou Zigbee, a transmissão de $\approx$1,2 KB pode representar mais de $\approx$10 pacotes fragmentados (devido ao tamanho de seus *payloads*), impactando diretamente a latência e o consumo energético. Assim, ainda que o tempo de execução seja aceitável, o custo de comunicação continua sendo um fator limitante para a adoção em ambientes de baixa largura de banda.

Tabela 4 – Tamanho das chaves e *ciphertexts* nos algoritmos ECDH e Kyber.

Operação	**Tamanho (*bytes*)**
ECDH (chave pública)	65
Kyber (chave pública)	1184
Ciphertext	1088

5.5.2.2 Assinaturas Digitais

Conforme a Tabela 5, o algoritmo Dilithium possui uma chave pública de 1.952 bytes e uma assinatura de 3.293 bytes, totalizando 5.245 bytes. Por sua vez, o ECDSA possui um custo total de 137 bytes (65 bytes da chave pública e 72 bytes da assinatura). Tais valores representam um aumento de quase 3.728% quando comparamos o custo total do Dilithium sobre o ECDSA.

Em aplicações IoT típicas, nas quais sensores enviam mensagens assinadas com frequência (por exemplo, telemetria a cada segundo), esse volume é insustentável. Por exemplo, em uma rede de 250 kbps, cada assinatura híbrida adicionaria aproximadamente 100 *ms* de transmissão extra, multiplicando o consumo energético em dispositivos a bateria. Esses resultados

Tabela 5 – Tamanho das chaves e assinaturas nos algoritmos ECDSA e Dilithium.

Operação	**Tamanho (*bytes*)**
ECDSA (chave pública)	65
Dilithium (chave pública)	1952
ECDSA (assinatura)	72
Dilithium (assinatura)	3293

evidenciam que, para dispositivos IoT com recursos restritos, o impacto das assinaturas pós-quânticas não está no tempo de processamento, mas no tamanho das mensagens transmitidas, um desafio que requer novas variantes otimizadas dos esquemas PQC direcionadas a esses dispositivos.

6 CONCLUSÃO

Este capítulo busca consolidar os resultados alcançados ao longo do trabalho, a partir da análise de viabilidade dos esquemas criptográficos híbridos, que combinam algoritmos clássicos (ECDH e ECDSA) e pós-quânticos (Kyber e Dilithium), em dispositivos IoT restritos. A pesquisa partiu da necessidade de investigar alternativas seguras e compatíveis para o período de transição que antecede a plena adoção da criptografia pós-quântica, frente à ameaça imposta pelo advento da computação quântica.

O estudo permitiu analisar o comportamento dos algoritmos sob restrições típicas de dispositivos IoT, com diferentes níveis de capacidade de processamento. A utilização de contêineres Docker possibilitou reproduzir diferentes cenários realistas, assegurando reprodutibilidade e controle sobre os recursos computacionais alocados.

Os resultados demonstraram que a abordagem híbrida é tecnicamente viável e eficiente para dispositivos com especificações *high-end* e *mid-end* (como o Raspberry Pi 4 Model B e o ESP32-S3R16V, respectivamente), apresentando um impacto computacional moderado e ganhos expressivos em segurança. Essa evidência corrobora as recomendações do NIST quanto à adoção progressiva de mecanismos híbridos como uma etapa de transição segura. Entretanto, é preciso destacar a impossibilidade de execução dos esquemas PQC em dispositivos *low-end*, como no ATmega1284, devido aos seus recursos de hardware extremamente restritos.

Por outro lado, o estudo evidenciou limitações práticas significativas relacionadas ao tamanho das chaves e das assinaturas dos algoritmos pós-quânticos. O aumento superior a 3.500% no tráfego de comunicação, em comparação com os algoritmos clássicos, torna a implementação direta dos algoritmos pós-quânticos inviável para dispositivos que operam em redes de baixa largura de banda.

Tais resultados sustentam que a criptografia híbrida representa um caminho intermediário estratégico, conciliando a compatibilidade com o ecossistema clássico e a resistência às futuras ameaças quânticas. No entanto, embora os algoritmos pós-quânticos tenham alcançado maturidade teórica e padronização formal, seu uso em IoT ainda demanda avanços significativos em estratégias de otimização.

REFERÊNCIAS

AJTAI, M. Generating hard instances of lattice problems. In: **Proceedings of the twenty-eighth annual ACM symposium on Theory of computing**. [S.l.: s.n.], 1996. p. 99–108.

AL-FUQAHA, A.; GUIZANI, M.; MOHAMMADI, M.; ALEDHARI, M.; AYYASH, M. Internet of things: A survey on enabling technologies, protocols, and applications. **IEEE communications surveys & tutorials**, Ieee, v. 17, n. 4, p. 2347–2376, 2015.

ATZORI, L.; IERA, A.; MORABITO, G. The internet of things: A survey. **Computer networks**, Elsevier, v. 54, n. 15, p. 2787–2805, 2010.

AUGUSTO, A. L. A. Cibersegurança na computação quântica. Universidade Federal do Rio Grande do Norte, 2022.

BERNSTEIN, D. J. *et al.* Chacha, a variant of salsa20. In: LAUSANNE, SWITZERLAND. **Workshop record of SASC**. [S.l.], 2008. v. 8, n. 1, p. 3–5.

BOS, J.; DUCAS, L.; KILTZ, E.; LEPOINT, T.; LYUBASHEVSKY, V.; SCHANCK, J. M.; SCHWABE, P.; SEILER, G.; STEHLÉ, D. Crystals-kyber: a cca-secure module-lattice-based kem. In: IEEE. **2018 IEEE European symposium on security and privacy (EuroS&P)**. [S.l.], 2018. p. 353–367.

DAEMEN, J.; RIJMEN, V. **The design of Rijndael**. [S.l.]: Springer, 2002. v. 2.

DIFFIE, W.; HELLMAN, M. E. New directions in cryptography. **IEEE Transactions on Information Theory**, v. 22, n. 6, p. 644–654, November 1976.

DING, J.; YANG, B.-Y. Multivariate public key cryptography. In: **Post-quantum cryptography**. [S.l.]: Springer, 2009. p. 193–241.

DUCAS, L.; LEPOINT, T.; LYUBASHEVSKY, V.; SCHWABE, P.; SEILER, G.; STEHLÉ, D. Crystals–dilithium: Digital signatures from module lattices. 2018.

FERREIRA, R.; RIPPER, P.; VERíSSIMO, R.; NETO, A. **Análise da Viabilidade de Aplicação de Métodos de Criptografia Pós-Quântica Aplicados ao Sistema de Pagamentos Instantâneos Brasileiro (Pix)**. [S.l.]: Banco Central do Brasil, 2022.

FERRO, L. F.; RAMPAZZO, F. J.; HENRIQUES, M. A. Estudos de otimização do algoritmo de criptografia pós-quântica crystals-kyber. In: SBC. **Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)**. [S.l.], 2021. p. 205–218.

GEBAUER, L.; TRSEK, H.; HEISS, S. Secure communication in factories-benchmarking elliptic curve diffie-hellman key exchange implementations on an embedded system. In: IEEE. **2022 IEEE 18th International Conference on Factory Communication Systems (WFCS)**. [S.l.], 2022. p. 1–4.

GREENGARD, S. **The internet of things**. [S.l.]: MIT press, 2021.

GRIFFITHS, D. J.; SCHROETER, D. F. **Introduction to quantum mechanics**. Third edition. Cambridge ; New York, NY: Cambridge University Press, 2018. ISBN 978-1-107-18963-8.

GROVER, L. K. A fast quantum mechanical algorithm for database search. **Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC)**, ACM, p. 212–219, 1996. Also available as quant-ph/9605043 on arXiv.

GUAN, T. T. **What is hybrid post-quantum encryption?** 2024. Acessado em: 25-11-2025. Disponível em: <https://qcve.org/blog/what-is-hybrid-post-quantum-encryption>.

HOFFSTEIN, J.; PIPHER, J.; SILVERMAN, J. H. Ntru: A ring-based public key cryptosystem. In: SPRINGER. **International algorithmic number theory symposium**. [S.l.], 1998. p. 267–288.

JOHNSON, D.; MENEZES, A.; VANSTONE, S. The elliptic curve digital signature algorithm (ecdsa). **International journal of information security**, Springer, v. 1, n. 1, p. 36–63, 2001.

KOBLITZ, N. Elliptic curve cryptosystems. **Mathematics of computation**, v. 48, n. 177, p. 203–209, 1987.

KOKARE, P.; VORA, D.; DESHMUKH, G.; SHELAR, A.; CHOUDHARI, P. Enhancing mass mailing with post-quantum cryptography: Implementation of crystal kyber and crystal dilithium. In: IEEE. **2025 International Conference on Intelligent and Cloud Computing (ICoICC)**. [S.l.], 2025. p. 1–6.

LYUBASHEVSKY, V.; PEIKERT, C.; REGEV, O. On ideal lattices and learning with errors over rings. In: SPRINGER. **Annual international conference on the theory and applications of cryptographic techniques**. [S.l.], 2010. p. 1–23.

MCELIECE, R. J. A public-key cryptosystem based on algebraic. **Coding Thv**, v. 4244, n. 1978, p. 114–116, 1978.

MENEZES, A. J.; VANSTONE, S. A.; OORSCHOT, P. C. V. **Handbook of Applied Cryptography**. 1st. ed. USA: CRC Press, Inc., 1996. ISBN 0849385237.

MILLER, V. S. Use of elliptic curves in cryptography. In: SPRINGER. **Conference on the theory and application of cryptographic techniques**. [S.l.], 1985. p. 417–426.

NAGATA, V.; HENRIQUES, M. A. Estudo comparativo de desempenho em assinaturas digitais pós-quânticas para plataformas de iot. In: SBC. **Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)**. [S.l.], 2020. p. 284–297.

NASCIMENTO, J. P. A. d. *et al.* Desempenho de algoritmos pós-quânticos candidatos à padronização no kemtls híbrido. Florianópolis, SC., 2024.

NIELSEN, M. A.; CHUANG, I. L. **Quantum computation and quantum information**. [S.l.]: Cambridge university press, 2010.

OJO, M. O.; GIORDANO, S.; PROCISSI, G.; SEITANIDIS, I. N. A review of low-end, middle-end, and high-end iot devices. **IEEE Access**, IEEE, v. 6, p. 70528–70554, 2018.

PORNIN, T. **RFC 6979: Deterministic usage of the digital signature algorithm (DSA) and elliptic curve digital signature algorithm (ECDSA)**. [S.l.]: RFC Editor, 2013.

REGEV, O. On lattices, learning with errors, random linear codes, and cryptography. **Journal of the ACM (JACM)**, ACM New York, NY, USA, v. 56, n. 6, p. 1–40, 2009.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. **Communications of the ACM**, ACM New York, NY, USA, v. 21, n. 2, p. 120–126, 1978.

ROMAN, R.; ZHOU, J.; LOPEZ, J. On the features and challenges of security and privacy in distributed internet of things. **Computer networks**, Elsevier, v. 57, n. 10, p. 2266–2279, 2013.

SAARELA, P. **Hybrid models connect the post-quantum with the classical security**. 2022. Acessado em: 25-11-2025. Disponível em: <https://xiphera.com/hybrid-models-connect-the-post-quantum-with-the-classical-security/>.

SCHNEIER, B. **Applied cryptography: protocols, algorithms, and source code in C**. [S.l.]: john wiley & sons, 2007.

SHOR, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In: IEEE. **Proceedings 35th annual symposium on foundations of computer science**. [S.l.], 1994. p. 124–134.

SRIVASTAVA, V.; BAKSI, A.; DEBNATH, S. K. An overview of hash based signatures. **Cryptology ePrint Archive**, 2023.

STALLINGS, W. **Cryptography and Network Security: Principles and Practice**. 6th. ed. USA: Prentice Hall Press, 2013. ISBN 0133354695.

STANDARDS, N. I. of; TECHNOLOGY. **Report on Post-Quantum Cryptography**. Washington, D.C., 2016.

STANDARDS, N. I. of; TECHNOLOGY. **Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms**. Washington, D.C., 2021.

STANDARDS, N. I. of; TECHNOLOGY. **Digital Signature Standard (DSS)**. Washington, D.C., 2023.

STANDARDS, N. I. of; TECHNOLOGY. **Module-Lattice-Based Digital Signature Standard**. Washington, D.C., 2024.

STANDARDS, N. I. of; TECHNOLOGY. **Module-Lattice-Based Key-Encapsulation Mechanism Standard**. Washington, D.C., 2024.

STANDARDS, N. I. of; TECHNOLOGY. **Stateless Hash-Based Digital Signature Standard**. Washington, D.C., 2024.

STANDARDS, N. I. of; TECHNOLOGY. **Recommendations for Key-Encapsulation Mechanisms**. Washington, D.C., 2025.

STANDARDS, N. I. of; TECHNOLOGY. **Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process**. Washington, D.C., 2025.

STEBILA, D.; MOSCA, M. Post-quantum key exchange for the Internet and the Open Quantum Safe project. In: AVANZI, R.; HEYS, H. (Ed.). **Selected Areas in Cryptography (SAC) 2016**. Springer, 2017. (LNCS, v. 10532), p. 1–24. Disponível em: <https://openquantumsafe.org>.

YAMAMOTO, F. K. A.; DANTAS, L. P.; SILVA, M. C. B. da; CANNO, L. C.; SOUSA, F. S. de. Análise de desempenho de algoritmos criptográficos pós quânticos em sistemas operacionais embarcados. **Revista Científica SENAI-SP-Educação, Tecnologia e Inovação| SENAI-SP Scientific Journal-Education, Technology and Innovation**, v. 1, n. 4, p. 49–63, 2023.