ML-KEM-768 em Rede 4G: Desempenho e Qualidade de Implementação em Aplicação Web de Proteção à Mulher

Rayane Pimentel[1], **Julio Pedro Siqueira Junior**[2], **Claudia Bianchi Progetti**[2]

[1]Serviço Nacional de Aprendizagem do Comércio (Senac) – São Carlos, SP, Brasil

[2]Serviço Nacional de Aprendizagem do Comércio (Senac) – São Paulo, SP, Brasil

rayanepimentel101@gmail.com, {julio.psjunior, claudia.bprogetti}@sp.senac.br

Abstract. *The quantum threat to asymmetric cryptography motivates this evaluation of ML-KEM-768 via liboqs in a web application simulating a police reporting system, tested on 4G across two locations in the state of São Paulo. The hybrid X25519+ML-KEM-768 mode showed 2.8% overhead in localhost and below 5% in the field; field differences were not statistically significant (Mann-Whitney U). Static and dynamic analysis detected no memory errors, vulnerabilities or CWEs, with test coverage of at least 93%. Results indicate technical viability for adoption in sensitive public web services.*

Resumo. *A ameaça quântica à criptografia assimétrica motiva a avaliação do ML-KEM-768 via liboqs em aplicação web simulando a Delegacia Eletrônica, testada em rede 4G em duas localidades paulistas. O modo híbrido X25519+ML-KEM-768 apresentou overhead de 2,8% em localhost e abaixo de 5% em campo; as diferenças em campo não foram estatisticamente significativas (Mann-Whitney U). A análise estática e dinâmica não detectou erros de memória, vulnerabilidades ou CWEs, com cobertura de ao menos 93%. Os resultados indicam viabilidade técnica para adoção em serviços públicos sensíveis.*

1. Introdução

O avanço da computação quântica ameaça tornar obsoletos os principais algoritmos de criptografia assimétrica em uso hoje, como RSA e ECC — responsáveis pelo estabelecimento seguro de chaves e pela autenticação em protocolos web. Algoritmos quânticos como o de Shor poderão, em um futuro próximo, quebrar esses esquemas em questão de horas, comprometendo a confidencialidade de dados sensíveis, inclusive por meio da estratégia "*harvest now, decrypt later*" — coleta agora, decifra depois —, tornando a ameaça retroativa: dados capturados hoje podem ser decifrados quando o hardware quântico estiver disponível [Le et al. 2025, Shor 1997].

Diante desse cenário, o National Institute of Standards and Technology (NIST) finalizou em 2024 a padronização dos primeiros algoritmos de criptografia pós-quântica (PQC), entre eles o Kyber, denominado ML-KEM no padrão FIPS 203 [NIST 2024], um mecanismo de encapsulamento de chave (KEM) utilizado no TLS. Optou-se pelo ML-KEM-768 por representar o balanço ideal recomendado pelo NIST entre segurança robusta (nível 3) e desempenho web interativo. O ML-KEM baseia sua segurança no problema de aprendizado com erros sobre módulos (Module-LWE), considerado resistente a ataques de computadores quânticos.

A Delegacia Eletrônica da Polícia Civil do Estado de São Paulo (PCSP) é tomada como referência contextual neste estudo por representar um serviço digital crítico que lida com informações de extrema sensibilidade. Durante o registro de ocorrências de violência doméstica, as vítimas submetem dados sigilosos, incluindo o envio de mídias como fotos de ferimentos e capturas de tela de ameaças [Polícia Civil do Estado de São Paulo 2024]. A exposição futura desses dados sob a estratégia *harvest now, decrypt later* representa um risco direto à integridade física e moral das vítimas, justificando a adoção de PQC. Além da sensibilidade, o acesso a esse sistema ocorre em diferentes condições de conectividade. Segundo dados da Anatel, 61,1% dos acessos de telefonia móvel no estado de São Paulo ocorrem via rede 4G [Agência Nacional de Telecomunicações 2026]. Cabe ressaltar que este trabalho não realiza qualquer interação com o sistema oficial, adotando apenas um fluxo funcional inspirado em suas características gerais para fins de simulação e análise.

Embora a viabilidade técnica de integrar PQC em servidores web já tenha sido demonstrada [Silva 2024, Tadepalli 2024], persiste uma lacuna metodológica relevante: não foram identificados estudos que combinassem análise de qualidade de engenharia de software das implementações disponíveis (liboqs) com testes funcionais em rede 4G real no estado de São Paulo, em contexto de sistemas de proteção social.

Este trabalho busca responder: a implementação do ML-KEM-768 via liboqs apresenta qualidade de engenharia e desempenho compatíveis com adoção em aplicações web públicas sensíveis, em ambiente controlado e em rede 4G real no estado de São Paulo?

O objetivo é avaliar qualidade e desempenho do ML-KEM-768 via liboqs, produzindo critérios orientados por dados para adoção segura em serviços públicos. Especificamente: (1) configurar ambiente reproduzível com suporte a X25519, ML-KEM-768 e modo híbrido; (2) desenvolver aplicação simulando o fluxo da Delegacia Eletrônica; (3) realizar testes em ambiente controlado e em rede 4G real em duas localidades paulistas; e (4) analisar estaticamente e dinamicamente os módulos ML-KEM da liboqs.

Os materiais sobre a Delegacia Eletrônica utilizados neste estudo são exclusivamente públicos (guias e páginas informativas). Não são coletados dados de usuárias reais e nenhum acesso é realizado ao sistema oficial [Polícia Civil do Estado de São Paulo 2024]. O protótipo tem fins exclusivamente acadêmicos.

2. Referencial Teórico

Esta seção apresenta os fundamentos teóricos que sustentam as três dimensões de avaliação do estudo: a transição criptográfica para ambientes TLS resistentes a ataques quânticos, os riscos associados à qualidade de implementação de bibliotecas criptográficas, e os critérios de viabilidade operacional de PQC em aplicações web móveis sensíveis.

2.1. Criptografia pós-quântica e transição para ambientes TLS

No handshake TLS 1.3, o ECDH estabelece um segredo compartilhado por meio de operações em curvas elípticas: ambos os lados contribuem com parâmetros públicos e derivam independentemente o mesmo segredo, sem transmiti-lo. O ML-KEM substitui essa operação por um mecanismo de encapsulamento: o servidor publica uma chave pública,

o cliente encapsula um segredo aleatório sob essa chave e envia o texto cifrado resultante, e o servidor decapsula o segredo com sua chave privada. Ambos chegam ao mesmo valor sem que um interceptador possa reproduzi-lo, mesmo com acesso a hardware quântico, pois a segurança repousa no problema Module-LWE e não em estruturas vulneráveis ao algoritmo de Shor [NIST 2024]. A configuração híbrida X25519+ML-KEM-768 combina os dois mecanismos em paralelo: o segredo final é derivado da combinação de ambos, garantindo segurança mesmo que um deles seja individualmente comprometido [Henriques and Mendes 2023, NIST 2024]. A viabilidade dessa integração em servidores web já foi demonstrada em estudos recentes [Silva 2024, Tadepalli 2024].

2.2. Segurança de implementação e qualidade de software em bibliotecas criptográficas

O ataque KyberSlash demonstrou que vulnerabilidades em implementações criptográficas decorrem não de falhas no algoritmo, mas de propriedades indesejadas do código — no caso, uma divisão cujo tempo de execução variava conforme os dados, permitindo inferir a chave privada por análise de temporização [Bernstein et al. 2025]. Essa classe de falha não é detectável por testes funcionais, exigindo ferramentas de análise estática e dinâmica. A complexidade ciclomática quantifica o número de caminhos independentes em um módulo — valores elevados aumentam a probabilidade de caminhos não testados, onde vulnerabilidades residem. A detecção de CWEs críticos por ferramentas como CodeQL identifica padrões conhecidamente inseguros antes da implantação, enquanto ASan e UBSan detectam em tempo de execução falhas de memória e comportamento indefinido que não emergem estaticamente. Baseri et al. (2025) destacam que a transição para PQC exige avaliação de vulnerabilidades em múltiplas camadas — algorítmica, de protocolo e de infraestrutura —, o que motiva a análise de implementação conduzida neste trabalho [Baseri et al. 2025].

2.3. Desempenho e viabilidade operacional de PQC em aplicações web móveis sensíveis

Tadepelli (2024), Rigon (2025) e Silva (2024) avaliaram o desempenho de PQC em ambientes controlados [Tadepalli 2024, Rigon 2025, Silva 2024]. Rigon (2025), especificamente, demonstrou que ML-KEM apresenta desempenho equilibrado com baixa latência entre os algoritmos PQC avaliados no protocolo QUIC, mantendo resiliência comparável aos algoritmos clássicos mesmo sob perda de pacotes [Rigon 2025]. Contudo, no contexto de aplicações web via TLS, persiste a necessidade de avaliar o impacto em condições reais de rede móvel, caracterizadas por alta variabilidade de sinal e perda de pacotes, fenômenos inerentes a redes 4G, conforme analisado por Polak et al. (2024) em ambiente industrial pesado — cenário mais adverso que redes urbanas, o que reforça a validade externa dos resultados aqui obtidos [Polak et al. 2024].

Esse ponto é relevante porque o overhead criptográfico representa apenas uma fração do tempo total percebido pelo usuário — a maior parte é composta pela latência de rede de ida e volta. Arapakis et al. (2021) identificam que atrasos superiores a 7–10 segundos têm impacto significativo na experiência do usuário em buscas web móveis, adotando-se 8 segundos como referência operacional de viabilidade neste trabalho [Arapakis et al. 2021].

Além disso, Kampanakis e Childs-Klein (2024) propõem o *Time-To-Last-Byte* (TTLB) como uma métrica de desempenho mais realista que o *Time-To-First-Byte* (TTFB) para algoritmos *data-heavy*, pois o impacto do overhead criptográfico dilui-se no tempo total da transação [Kampanakis and Childs-Klein 2024]. Dados de latência em redes 4G apresentam distribuição assimétrica com cauda longa, tornando o teste de Mann-Whitney U — não-paramétrico e robusto a outliers — a alternativa estatística adequada. A potência do sinal (RSRP) e a qualidade (RSRQ) são registradas para correlacionar condições de cobertura 4G com o overhead observado.

3. Método de pesquisa

Este trabalho adota abordagem empírica, quantitativa e comparativa, estruturada em três fases complementares. A metodologia distingue explicitamente três dimensões de avaliação: (a) desempenho criptográfico em ambiente controlado; (b) desempenho percebido em condições reais de rede móvel 4G; e (c) qualidade da implementação dos módulos ML-KEM na biblioteca *liboqs*.

3.1. Fase 1: Ambiente experimental e avaliação de desempenho

A primeira fase compreende a configuração de um ambiente reproduzível (Figura 1) com Docker, Nginx, OpenSSL 3.3.2 e *oqs-provider* na AWS EC2 (servindo 3 portas TLS distintas), suportando três configurações: (a) X25519 (baseline clássico); (b) ML-KEM-768; e (c) híbrida X25519+ML-KEM-768 [NIST 2024].

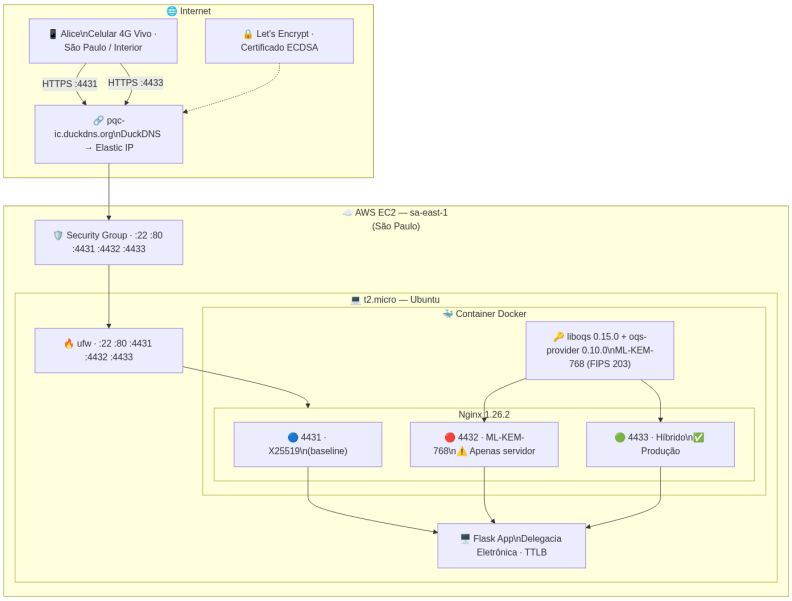

Figura 1. Arquitetura experimental: cliente móvel 4G conectando-se ao Nginx (AWS EC2) via oqs-provider e três portas para isolar as suítes TLS (ambiente de campo; ambiente controlado utiliza a mesma stack Docker em localhost).

Paralelamente, é desenvolvida uma aplicação web conforme a Figura 2, que simula um fluxo funcional inspirado na Delegacia Eletrônica, composta por três etapas: (i) formulário de dados pessoais da vítima; (ii) descrição dos fatos e upload de imagem sintética de até 2MB [Polícia Civil do Estado de São Paulo 2024]; e (iii) geração e

exibição de protocolo. Esse fluxo representa uma aproximação mínima do sistema oficial, suficiente para mensurar os componentes de maior peso no TTLB: upload de arquivo e processamento no servidor, sem interagir com o sistema real.

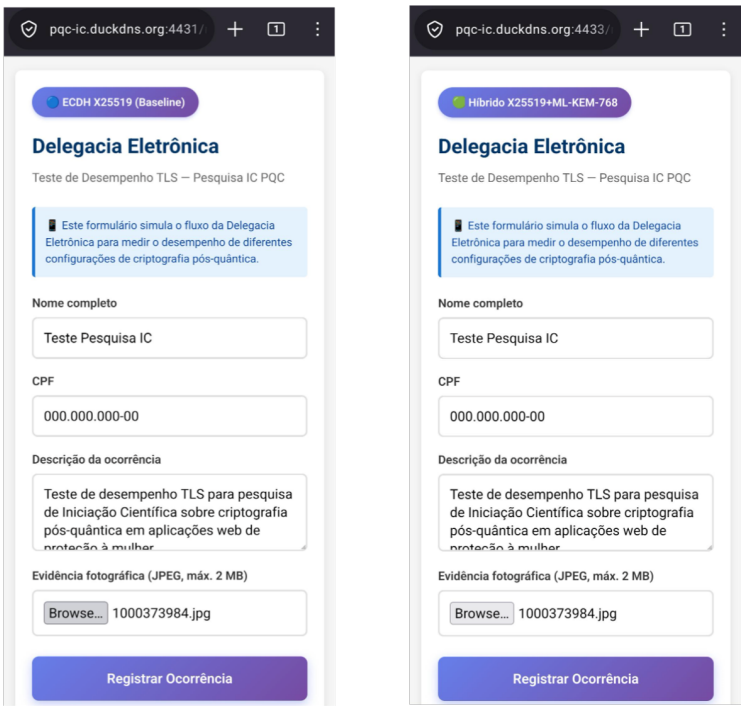

Figura 2. Tela da aplicação simulando o fluxo da Delegacia Eletrônica.

As medições em campo são realizadas em duas localidades do estado de São Paulo (Tabela 1), em dois períodos: fora de pico (10h–11h) e pico (18h–20h).

Tabela 1. Localidades de coleta de campo (dados ANATEL, fev. 2026)

Localidade	Perfil	Banda larga fixa/100 hab
São Paulo	Centro urbano	39,71
São Carlos	Cidade média	42,90

Os resultados dos testes controlados são reportados como mediana, desvio padrão e P95. A métrica central nos testes de campo é o TTLB — do carregamento da primeira página até a exibição do protocolo —, em detrimento do TTFB, que superestima o overhead criptográfico em transações com transferência de dados [Kampanakis and Childs-Klein 2024]. A comparação entre configurações adota o teste de Mann-Whitney U, não-paramétrico e robusto à distribuição assimétrica de latências em 4G, descartando o teste t de Student, que assume normalidade. A potência do sinal 4G (RSRP) e a qualidade (RSRQ) foram registradas manualmente por meio do aplicativo *Network Cell Info Lite* (Android), que exibe em tempo real as métricas da célula servidora.

3.2. Fase 2: Análise estática e dinâmica da liboqs

A segunda fase realiza uma análise de qualidade focada exclusivamente nos módulos ML-KEM da biblioteca *liboqs* (diretório `src/kem/ml_kem`), sem abranger a totalidade da biblioteca. O objetivo é avaliar se a implementação apresenta características mínimas de auditabilidade, robustez e segurança de execução compatíveis com uso em ambientes sensíveis.

A análise é conduzida sobre a versão 0.15.0 da *liboqs*, com *oqs-provider* 0.10.0 e OpenSSL 3.3.2. Para a análise dinâmica com sanitizers, os módulos são compilados com `-fsanitize=address,undefined -g -O1`, que ativam o AddressSanitizer e o UndefinedBehaviorSanitizer sem otimizações que possam ocultar comportamentos indefinidos. Para a medição de cobertura, uma compilação separada utiliza `--coverage -g -O0`.

São empregadas ferramentas estáticas e dinâmicas complementares:

- **Análise estática:** o SonarQube é utilizado para inspecionar atributos estruturais do código, como complexidade ciclomática, duplicações, débito técnico e cobertura dos testes já existentes nos módulos analisados. O CodeQL é empregado para identificar padrões potencialmente inseguros, com ênfase em CWEs críticos relevantes para implementações criptográficas, incluindo construções que possam favorecer vazamentos por temporização.
- **Análise dinâmica:** o AddressSanitizer (ASan) e o UndefinedBehaviorSanitizer (UBSan) são ativados em tempo de compilação para detectar vazamentos de memória, acessos inválidos e comportamentos indefinidos. O Valgrind Massif complementa essa etapa medindo o consumo de *heap* durante as operações KEM. A cobertura de testes é medida com `gcov` e `lcov`.

3.3. Fase 3: Consolidação e checklist de qualidade

Os dados das fases anteriores são consolidados em um checklist para adoção segura de PQC (Tabela 8), com limiares fundamentados na literatura [Tadepalli 2024, Arapakis et al. 2021] e em padrões consolidados de engenharia de software (como a métrica de complexidade de McCabe e diretrizes NIST FIPS 203).

4. Resultados e Discussão

Em ambiente controlado, foram realizadas duas sessões independentes de medição (26/03/2026 e 23/04/2026), cada uma com 50 repetições por configuração TLS, totalizando 100 medições por configuração (300 no total). Os resultados estão sumarizados na Tabela 2.

Tabela 2. Resultados dos testes automatizados controlados (n=100 por configuração)

Configuração	Mediana (s)	DP (s)	P95 (s)	Overhead
X25519 (baseline)	0,0435	0,0103	0,0531	—
Híbrido X25519+ML-KEM-768	0,0447	0,0063	0,0563	+2,8%
ML-KEM-768 puro	0,0469	0,0077	0,0581	+7,8%

DP = Desvio Padrão; P95 = Percentil 95

Os testes de significância estatística (Mann-Whitney U, α=0,05, teste bilateral) revelaram: X25519 vs. híbrido (p=0,018); X25519 vs. ML-KEM-768 (p=0,008); híbrido vs. ML-KEM-768 (p=0,778, não significativo). A indistinguibilidade estatística entre o modo híbrido e o ML-KEM puro indica que adotar a configuração híbrida não impõe overhead adicional perceptível.

Ambos os overheads observados (2,8% e 7,8%) estão significativamente abaixo do limiar de 10% definido no checklist de viabilidade, adaptado de [Tadepalli 2024] para TTLB — métrica que dilui o overhead do handshake no tempo total da transação, tornando o critério mais conservador que o original.

Em rede 4G real, as medições foram realizadas com 10 repetições manuais por configuração TLS em cada localidade (5 no horário de pico e 5 fora de pico), alternando entre X25519 e Híbrido a cada requisição para mitigar vieses de flutuação de rede. A Tabela 3 apresenta os tempos totais de transação (TTLB) medianos e as condições de sinal.

Tabela 3. Resultados dos testes em rede 4G real (TTLB mediano e sinal)

Localidade	Configuração	Med. Pico	Med. Fora	RSRP	RSRQ
São Carlos	X25519	0,340s	0,364s	-82 dBm	-11 dB
São Carlos	Híbrido	0,350s	0,329s	-82 dBm	-11 dB
São Paulo	X25519	0,295s	0,273s	-94 dBm	-12 dB
São Paulo	Híbrido	0,327s	0,278s	-94 dBm	-12 dB

RSRP = Reference Signal Received Power (dBm); RSRQ = Reference Signal Received Quality (dB). Timestamps em UTC; medições no horário de Brasília (UTC-3).

Para a análise de significância estatística, as amostras de pico e fora de pico foram agrupadas ($n = 10$ por configuração), uma vez que o interesse primário é o efeito do algoritmo, não do horário. Embora o tamanho amostral de campo constitua uma limitação de amostragem, o uso da estatística não-paramétrica (Mann-Whitney U) pareada ao controle em localhost ($n = 100$) sustenta a validade interna dos resultados.

Tabela 4. Overhead e significância estatística por ambiente

Ambiente	Tempo base	Overhead abs.	Overhead %	Valor-p
Localhost (n=100)	43,5ms	+1,2ms	+2,8%	0,018
São Carlos (n=10)	340ms	+7ms	+2,2%	0,60
São Paulo (n=10)	279ms	+12ms	+4,3%	0,47

Tempo base = Mediana X25519. Overhead abs. = Mediana Híbrido $-$ Mediana X25519. Overhead % = (Overhead abs. / Tempo base) $\times$ 100. Mann-Whitney U bilateral.

A Tabela 4 evidencia o fenômeno de diluição do overhead: o impacto percentual do ML-KEM cai em campo porque o TTLB base é muito maior que em localhost. Em todas as localidades coletadas, o teste Mann-Whitney U não indicou diferença significativa. O TTLB máximo observado foi 0,364s (São Carlos, X25519 fora de pico), duas ordens de grandeza abaixo do limiar de 8s. O intervalo de RSRP entre as localidades coletadas (-82 dBm em São Carlos e -94 dBm em São Paulo) não alterou esse padrão: o overhead

permaneceu não significativo mesmo com qualidade de sinal distinta, sugerindo robustez do ML-KEM a diferentes condições de cobertura 4G.

A terceira dimensão avaliada é a qualidade da implementação. A análise dos módulos `src/kem/ml_kem` da liboqs 0.15.0 foi conduzida com cinco ferramentas complementares, cujos resultados estão sintetizados na Tabela 5.

Tabela 5. Síntese da análise dos módulos ML-KEM (liboqs 0.15.0)

Ferramenta	Escopo	Resultado
ASan + UBSan	Memória e comportamento indefinido	0 erros
Valgrind Massif	Heap dinâmico	4 KB (apenas I/O)
gcov + lcov	Cobertura de testes	93,0% / 98,1%
SonarQube	Vulnerabilidades e bugs	0 vulns, 0 bugs
CodeQL	CWEs em `ml_kem`	0 alertas

Na análise dinâmica, os testes `test_kem`, `test_kem_mem` e `speed_kem` foram executados com ASan e UBSan ativos. Nenhum erro de memória ou comportamento indefinido foi detectado. O Valgrind Massif reportou pico de heap de 4.104 bytes, integralmente atribuído ao buffer de I/O do `printf` — as operações de KeyGen, Encaps e Decaps operam exclusivamente sobre stack. A Tabela 6 apresenta os tempos médios das operações ML-KEM-768.

Tabela 6. Tempo médio das operações ML-KEM-768

Operação	Tempo (μs)
KeyGen	30,8
Encaps	40,9
Decaps	41,0

Na análise estática, o SonarQube (Community Build 26.4.0.121862) atribuiu Rating A em segurança, confiabilidade e manutenibilidade, com 0 vulnerabilidades, 0 bugs e 0% de duplicação. Os 8 code smells reportados — tabs em assembly x86_64 e justificativas de skip em testes Python — são externos ao escopo dos módulos ML-KEM. O CodeQL (CLI 2.25.3, suite `cpp-security-extended`) não detectou nenhum CWE em `src/kem/ml_kem`; os 442 alertas do relatório completo concentram-se em `src/sig` (assinaturas digitais).

Os resultados das cinco ferramentas são convergentes: a implementação do ML-KEM-768 não apresenta vazamentos de memória, comportamento indefinido, vulnerabilidades estáticas ou CWEs detectáveis. A cobertura de testes atingiu 93,0% de linhas e 98,1% de funções. A Tabela 7 consolida a avaliação.

Tabela 7. Avaliação dos módulos ML-KEM frente aos critérios de qualidade

Critério	Resultado	Status
Complexidade ciclomática < 15	Quality Gate aprovado	Aprovado
Cobertura $> 90\%$ (gcov+lcov)	93,0% linhas / 98,1% funções	Aprovado
Zero CWEs críticos (CodeQL)	0 alertas em `ml_kem`	Aprovado
Zero memory leaks (ASan/UBSan)	0 erros	Aprovado
Pico de heap viável (Valgrind)	4 KB (apenas I/O)	Aprovado

A Tabela 8 apresenta o checklist preenchido com os resultados das três fases.

Tabela 8. Checklist de qualidade para adoção segura de PQC

Dimensão	Critério	Status
(a) Desempenho funcional	Overhead $< 10\%$ vs. ECDH (2,8% / 7,8%)	Aprovado
	TTLB $<$ 8s em 4G real (2/2 locais atenderam)	Aprovado
(b) Qualidade da implementação	Compl. ciclomática < 15	Aprovado
	Cobertura $> 90\%$ (93,0% / 98,1%)	Aprovado
	Zero CWEs críticos (CodeQL)	Aprovado
	Zero memory leaks (ASan/UBSan)	Aprovado
(c) Configuração segura	Modo híbrido X25519+ML-KEM-768	Aprovado
	Sanitizers em compilação	Aprovado
	oqs-provider configurado	Aprovado
(d) Reprodutibilidade	Dockerfile, scripts e dados no GitHub	Aprovado
(e) Eficiência de memória	Heap via Valgrind Massif (4 KB)	Aprovado

A dimensão (a) é validada pelos resultados dos testes controlados e de campo (Tabelas 2 e 4). As dimensões (b), (c) e (e) foram verificadas pela análise estática e dinâmica da liboqs (Tabelas 5 e 7). A dimensão (d) é atendida pelo versionamento completo no GitHub (`https://github.com/rayanepimentel/2026-ic`), com Dockerfile, scripts de medição e resultados brutos publicamente disponíveis. O checklist está integralmente aprovado, indicando que a implementação do ML-KEM-768 na liboqs 0.15.0 atende aos critérios de qualidade estabelecidos para adoção segura em aplicações web públicas sensíveis.

5. Considerações finais

Este trabalho avaliou qualidade de engenharia e desempenho do ML-KEM-768 via liboqs 0.15.0, em ambiente controlado e em rede 4G real no estado de São Paulo. Os resultados das três fases permitem responder afirmativamente à questão de pesquisa.

Em ambiente controlado, o modo híbrido X25519+ML-KEM-768 apresentou overhead de 2,8% sobre o baseline clássico — operacionalmente irrelevante frente ao limiar de 10% adotado. A indistinguibilidade estatística entre o modo híbrido e o ML-KEM puro (p=0,778) indica que a transição para a configuração mais segura não impõe custo adicional perceptível.

Em rede 4G real, o fenômeno de diluição do overhead foi confirmado: São Carlos (+2,2%; p=0,60) e São Paulo (+4,3%; p=0,47) não apresentaram diferença estatisti-

camente significativa entre configurações, e os tempos permaneceram muito abaixo do limiar de 8 segundos.

A análise estática e dinâmica revelou ausência de vazamentos de memória, comportamento indefinido, vulnerabilidades e CWEs detectáveis, com cobertura de 93,0% de linhas e 98,1% de funções. O checklist de qualidade foi aprovado em todas as dimensões verificadas.

Os resultados indicam que o ML-KEM-768 via liboqs 0.15.0 apresenta qualidade de engenharia adequada e overhead negligenciável em uso móvel real, constituindo opção viável para adoção segura em aplicações web públicas sensíveis.

Como trabalhos futuros, destaca-se a incorporação de assinaturas digitais pós-quânticas — como Dilithium ou Falcon — nos certificados TLS, permitindo avaliar o impacto de uma migração PQC integral, não apenas no estabelecimento de chaves, mas também na autenticação. A replicação dos experimentos em redes 5G e sob carga concorrente no servidor constituem extensões naturais para validar a escalabilidade da solução em cenários de produção.

Referências

Agência Nacional de Telecomunicações (2026). Painel de acessos — telefonia móvel. período: dez. 2025. uf: Sp. Disponível em: `https://informacoes.anatel.gov.br/paineis/acessos`. Acesso em: 27 fev. 2026.

Arapakis, I., Park, S., and Pielot, M. (2021). Impact of response latency on user behaviour in mobile web search. In *Proceedings of the 2021 ACM SIGIR Conference on Human Information Interaction and Retrieval (CHIIR)*, New York. ACM. Disponível em: `https://doi.org/10.1145/3406522.3446038`. Acesso em: 5 mar. 2026.

Baseri, Y. et al. (2025). Evaluation framework for quantum security risk assessment: a comprehensive strategy for quantum-safe transition. *Computers & Security*, 150:104272. Disponível em: `https://doi.org/10.1016/j.cose.2024.104272`. Acesso em: 20 out. 2025.

Bernstein, D. J. et al. (2025). KyberSlash: Exploiting secret-dependent division timings in Kyber implementations. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2025(2):209–234. Disponível em: `https://tches.iacr.org/index.php/TCHES/article/view/12046`. Acesso em: 20 mar. 2026.

Henriques, M. A. A. and Mendes, J. P. P. V. (2023). Estudo sobre a implementação híbrida de algoritmos criptográficos pré e pós-quânticos em dispositivos restritos. In *Congresso de Iniciação Científica da Unicamp*, Campinas. Unicamp. Disponível em: `https://sistemas-prp.unicamp.br/inscricao-congresso/resumos/2023P22261A3900903517.pdf`. Acesso em: 20 mar. 2026.

Kampanakis, P. and Childs-Klein, W. (2024). The impact of data-heavy, post-quantum TLS 1.3 on the time-to-last-byte of real-world connections. Cryptology ePrint Archive, Paper 2024/176. Disponível em: `https://eprint.iacr.org/2024/176`. Acesso em: 20 mar. 2025.

Le, T. D. et al. (2025). Are enterprises ready for quantum-safe cybersecurity? a gap analysis framework. arXiv:2509.01731. Disponível em: https://arxiv.org/abs/2509.01731. Acesso em: 20 out. 2025.

NIST (2024). Fips 203: Module-lattice-based key-encapsulation mechanism standard. Technical report, NIST, Gaithersburg. Disponível em: https://doi.org/10.6028/NIST.FIPS.203. Acesso em: 13 out. 2025.

Polak, L. et al. (2024). Measurement and analysis of 4g/5g mobile signal coverage in a heavy industry environment. *Sensors*, 24(8):2538. Disponível em: https://doi.org/10.3390/s24082538. Acesso em: 15 fev. 2026.

Polícia Civil do Estado de São Paulo (2024). *Guia de utilização da Delegacia Eletrônica: passo a passo para registrar ocorrência de violência doméstica e familiar contra a mulher*. PCSP, São Paulo, 2 edition. Disponível em: https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home. Acesso em: 20 out. 2025.

Rigon, P. H. C. (2025). Avaliação abrangente do desempenho da criptografia pós-quântica no protocolo quic. Dissertação (mestrado em ciência da computação), Universidade Federal do Rio Grande do Sul, Porto Alegre. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/301497/001301308.pdf. Acesso em: 20 mar. 2026.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509. Disponível em: https://doi.org/10.1137/s0097539795293172. Acesso em: 19 maio 2026.

Silva, I. d. O. (2024). Criptografia pós-quântica: comunicação segura usando openssl. Trabalho de conclusão de curso (tecnologia em análise e desenvolvimento de sistemas), FATEC Americana, Americana. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/21598. Acesso em: 10 out. 2025.

Tadepalli, A. (2024). The impact of quantum-safe cryptography (qsc) on website response. Disponível em: https://arxiv.org/abs/2411.05024. Acesso em: 20 out. 2025.