Análise de Viabilidade da Implantação de Algoritmos de Criptografia Pós-Quântica em *Blockchains* para IoT

Alison G. Schemitt [1], Roben C. Lunardi [1,2], Avelino F. Zorzo [1], Henrique F. da Silva [3], Diego Kreutz [3], Rodrigo B. Mansilha [3]

[1]PPGCC – Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)

[2]Instituto Federal do Rio Grande do Sul (IFRS)

[3]PPGES – Universidade Federal do Pampa (UNIPAMPA)

alison.schemitt@edu.pucrs.br, roben.lunardi@zonanorte.ifrs.edu.br, avelino.zorzo@pucrs.br, henriquefan.aluno@unipampa.edu.br, {diegokreutz,mansilha}@unipampa.edu.br

Abstract. *Quantum computing threatens current cryptography (RSA, ECC). NIST has standardized post-quantum cryptography (PQC) algorithms to mitigate this risk, but their evaluation in blockchain systems with IoT devices is still in its infancy. This work assesses the feasibility of deploying PQC algorithms in IoT blockchains using benchmarks and block-verification simulations. Results show that Falcon and Dilithium are the most suitable for resource-constrained devices, while MAYO presents unsatisfactory performance.*

Resumo. *A computação quântica ameaça a criptografia atual (RSA, ECC). O NIST padronizou algoritmos pós-quânticos (PQC) para mitigar esse risco, mas sua avaliação em blockchains com dispositivos IoT ainda é incipiente. Este trabalho avalia a viabilidade de implementar algoritmos PQC em blockchains IoT por meio de benchmarks e de simulações de verificação de blocos. Os resultados mostram que Falcon e Dilithium são os mais adequados para dispositivos restritos, enquanto MAYO apresenta desempenho insatisfatório.*

1. Introdução

A computação quântica tem avançado de forma a ameaçar a infraestrutura criptográfica atualmente utilizada [Upama et al. 2022]. Um computador quântico criptograficamente relevante pode executar o algoritmo de Shor [Shor 1994], capaz de recuperar chaves privadas de esquemas criptográficos baseados na fatoração de grandes números (e.g., RSA) e em logaritmos discretos (e.g., ECC). Esse cenário torna imperativa a migração para algoritmos de criptografia pós-quântica (PQC), projetados para resistir tanto a ataques de computadores quânticos quanto a de computadores clássicos, mantendo compatibilidade com a execução em plataformas computacionais clássicas.

De acordo com o National Institute of Standards and Technology (NIST), a transição para a infraestrutura criptográfica atualmente usada levou quase 20 anos [Chen et al. 2016]. Com isso, em 2016, o NIST iniciou um processo de padronização de algoritmos criptográficos pós-quânticos [NIST 2016]. Até o momento, foram selecionados dois algoritmos de encapsulamento de chaves (KEM) e três algoritmos de assinatura digital (DSA) [Alagic et al. 2022]. Paralelamente, o NIST conduz um processo adicional voltado a novos esquemas de assinatura digital baseados em diferentes paradigmas criptográficos [Alagic et al. 2024]. Apesar dos avanços, esses algoritmos foram projetados para uso geral e o impacto de sua adoção em sistemas *blockchain*, especialmente em arquiteturas IoT, ainda foi pouco explorado na literatura.

Portanto, este trabalho avalia o impacto da adoção de algoritmos PQC no desempenho de sistemas *blockchain* que utilizam dispositivos IoT para coleta de dados e criação/verificação de assinaturas digitais. Para isso, realizamos avaliação de algoritmos PQC considerando diferentes níveis de segurança em dispositivos físicos que podem atuar como *gateways* IoT, responsáveis por executar operações da *blockchain*. Os resultados focam no impacto do uso de PQC em ambientes de *blockchain* baseados em IoT.

2. Trabalhos Relacionados

Até onde sabemos, ainda há poucos estudos que investigam o uso e o impacto de algoritmos de criptografia pós-quântica (PQC) em sistemas de *blockchain* ou em dispositivos IoT. A Tabela 1 resume as principais características dos trabalhos similares desta área.

Tabela 1. Trabalhos Relacionados.

Trabalho	Algoritmos Padronizados	Algoritmos Extras	Múltiplos Níveis de Segurança	Desktop/ Laptop	IoT	Blockchain
[Commey et al. 2025]	✓	✓	✓	✓	✓	✗
[Lonc et al. 2023]	✓	✗	✓	✓	✓	✗
[Juaristi et al. 2025]	✓	✗	✓	✓	✗	✓
[Yokubov and Gan 2021]	✓	✓[a]	✓[b]	✓	✗	✓
[Schemitt et al. 2025]	✓	✓	✓	✓	✗	✓
Este Trabalho	✓	✓	✓	✓	✓	✓

[a] Foi utilizado o algoritmo Rainbow, que posteriormente foi considerado inseguro [Alagic et al. 2022].
[b] Testa os níveis de 1, 3 e 5 do algoritmo Rainbow e o nível 1 dos demais.

De forma geral, os trabalhos existentes concentram-se na avaliação do desempenho de algoritmos PQC padronizados ou candidatos à padronização pelo NIST, frequentemente em comparação com algoritmos criptográficos clássicos, como o ECDSA. Essas avaliações normalmente consideram métricas como o tempo de execução das operações criptográficas, o consumo de memória e o tamanho dos artefatos criptográficos.

Ainda, muitos estudos analisam apenas subconjuntos do problema, como o desempenho das operações criptográficas isoladas ou a análise dos custos de comunicação. Em alguns casos, as avaliações são realizadas em ambientes computacionais clássicos, como *desktops* ou servidores, enquanto outros trabalhos consideram cenários específicos de aplicação, como redes veiculares ou plataformas *blockchain* particulares.

Além disso, parte da literatura investiga o impacto da adoção de algoritmos PQC em sistemas *blockchain* por meio de *benchmarks* e análises de desempenho, avaliando operações críticas, como a geração de chaves, a criação e a verificação de assinaturas. Essas operações são particularmente relevantes em sistemas *blockchain*, nos quais a validação de blocos envolve a verificação de múltiplas transações assinadas digitalmente.

Apesar desses avanços, poucos trabalhos consideram simultaneamente diferentes níveis de segurança, múltiplas famílias de algoritmos PQC, ambientes com restrições computacionais e o impacto dessas operações no processamento de blocos em sistemas *blockchain*. Avaliações envolvendo dispositivos IoT permanecem pouco exploradas.

Neste contexto, este trabalho avalia o comportamento de algoritmos PQC previamente identificados como eficientes em ambientes *desktop* quando executados em dispositivos IoT, além de investigar seu impacto na verificação de blocos em sistemas *blockchain* baseados nos modelos do Bitcoin e do Ethereum.

3. Metodologia

A partir dos resultados obtidos em [Schemitt et al. 2025], selecionamos os algoritmos com melhor desempenho em ambientes *desktop*, potencialmente viáveis em dispositivos IoT, e os avaliamos nesses ambientes considerando todos os níveis de segurança disponíveis. A Tabela 2 apresenta os algoritmos e suas respectivas variantes analisadas.

Tabela 2. Algoritmos Avaliados. Apenas 2 algoritmos estão presentes no nível 2 de segurança e nenhum algoritmo existe para o nível 4.

			Variantes (16)				
PQC?	**#**	**Algoritmo (6)**	**Nível 1 (4)**	**Nível 2 (2)**	**Nível 3 (4)**	**Nível 4 (0)**	**Nível 5 (6)**
Não	1	ECDSA	P-256	—	P-384	—	P-521
Sim	2	ML-DSA*	—	ML-DSA-44	ML-DSA-65	—	ML-DSA-87
	3	Dilithium*	—	Dilithium2	Dilithium3	—	Dilithium5
	4	Falcon	Falcon-512	—	—	—	Falcon-1024
	5	Falcon-padded	Falcon-padded-512	—	—	—	Falcon-padded-1024
	6	Mayo	MAYO-2	—	MAYO-3	—	MAYO-5

* Inclui as versões pré- e pós-padronização pelo NIST.

Após a definição dos algoritmos avaliados, realizamos um *benchmark* para medir os tempos médios de execução das operações criptográficas. Para reduzir efeitos transitórios e aumentar a estabilidade das medições, executamos um conjunto de execuções de aquecimento, cujos resultados foram descartados antes da coleta efetiva de dados.

Com os tempos médios e desvios-padrão consolidados, utilizamos esses valores como entrada em um simulador (Blocksim [Alharby and van Moorsel 2020]), modificado para estimar o impacto dos algoritmos na verificação de blocos em sistemas de *blockchain*. A Tabela 3 apresenta os ambientes computacionais utilizados na coleta de dados. O ambiente Desktop Mid-end foi incluído como referência para comparação entre dispositivos IoT e plataformas com maior capacidade computacional. Foram realizadas 10.000 execuções no *benchmark*, precedidas por 1.000 de aquecimento. As simulações de verificação de blocos foram executadas com 1.000 repetições para as redes Bitcoin e Ethereum, considerando diferentes algoritmos e níveis de segurança apresentados na Tabela 2.

Tabela 3. Ambientes computacionais avaliados.

Máquina	CPU	Memória	Sistema Operacional
Raspberry PI3	Cortex-A53 (1.2 GHz)	1 GB	Raspberry Pi OS 12 (bookworm) Linux Kernel 6.12.47-v8+
Raspberry PI4	Cortex-A72 (1.8 GHz)	4 GB	Raspberry Pi OS 12 (bookworm) Linux Kernel 6.12.62-v8+
Desktop Mid-end	Intel i5-8500 (3.0 GHz)	16 GB	Ubuntu 25.10 Linux Kernel 6.14.0-37-generic

4. Resultados

A Tabela 4 apresenta os resultados do *benchmark* dos algoritmos avaliados. Conforme os níveis de segurança aumentam, há uma queda no desempenho de todas as operações criptográficas, comportamento esperado devido ao aumento da complexidade computacional e à mudança no conjunto de parâmetros dos algoritmos. Também há uma relação proporcional entre o aumento do desempenho dos dispositivos e o aumento de sua capacidade computacional, que também é um comportamento esperado.

Os dispositivos Raspberry Pi3 e Pi4 apresentam tendências semelhantes, com diferenças associadas principalmente à capacidade computacional. Com exceção do algoritmo MAYO, os demais algoritmos apresentam desempenho superior ao ECDSA na

Tabela 4. Resultados do desempenho dos algoritmos criptográficos (ms).

Algoritmo	Nível Inferior (1 ou 2)			Nível 3			Nível 5		
	keypair (mean ± std)	sign (mean ± std)	verify (mean ± std)	keypair (mean ± std)	sign (mean ± std)	verify (mean ± std)	keypair (mean ± std)	sign (mean ± std)	verify (mean ± std)
Raspberry Pi3									
ECDSA	0.279 ± 0.044	0.516 ± 0.067	0.861 ± 0.062	1.124 ± 0.054	1.914 ± 0.085	3.471 ± 0.085	1.693 ± 0.066	3.378 ± 0.097	5.921 ± 0.105
ML-DSA	0.644 ± 0.037	3.259 ± 2.175	0.723 ± 0.034	1.014 ± 0.043	5.281 ± 3.684	1.093 ± 0.040	1.576 ± 0.048	6.270 ± 3.893	1.700 ± 0.054
Dilithium	0.433 ± 0.034	1.167 ± 0.653	0.413 ± 0.028	0.714 ± 0.045	1.780 ± 0.996	0.652 ± 0.036	1.153 ± 0.057	2.302 ± 1.020	1.093 ± 0.046
Falcon	44.130 ± 12.828	1.484 ± 0.089	0.302 ± 0.040	-	-	-	122.437 ± 30.919	2.932 ± 0.100	0.543 ± 0.052
Falcon-padded	44.129 ± 12.724	1.482 ± 0.089	0.295 ± 0.029	-	-	-	122.146 ± 31.582	2.946 ± 0.123	0.533 ± 0.031
MAYO	4.961 ± 0.066	6.667 ± 0.118	2.085 ± 0.118	8.342 ± 0.075	18.122 ± 0.220	6.585 ± 0.244	21.569 ± 0.110	46.663 ± 0.366	16.550 ± 0.591
Raspberry Pi4									
ECDSA	0.093 ± 0.009	0.188 ± 0.046	0.373 ± 0.024	0.567 ± 0.015	0.943 ± 0.023	1.815 ± 0.022	0.886 ± 0.019	1.716 ± 0.028	3.169 ± 0.029
ML-DSA	0.227 ± 0.007	0.943 ± 0.592	0.238 ± 0.005	0.390 ± 0.009	1.508 ± 1.012	0.374 ± 0.007	0.579 ± 0.013	1.825 ± 1.063	0.598 ± 0.010
Dilithium	0.179 ± 0.007	0.498 ± 0.274	0.171 ± 0.005	0.318 ± 0.010	0.752 ± 0.415	0.274 ± 0.007	0.473 ± 0.013	0.973 ± 0.434	0.457 ± 0.009
Falcon	19.302 ± 5.902	0.673 ± 0.032	0.111 ± 0.013	-	-	-	53.748 ± 14.687	1.341 ± 0.047	0.200 ± 0.019
Falcon-padded	19.341 ± 5.960	0.672 ± 0.033	0.108 ± 0.005	-	-	-	53.635 ± 14.230	1.346 ± 0.058	0.196 ± 0.008
Mayo	2.137 ± 0.020	3.019 ± 0.027	0.842 ± 0.028	3.759 ± 0.024	8.284 ± 0.047	2.651 ± 0.046	10.001 ± 0.033	21.770 ± 0.075	6.582 ± 0.098
Desktop Mid-end									
ECDSA	0.023 ± 0.002	0.048 ± 0.318	0.079 ± 0.005	0.146 ± 0.007	0.236 ± 0.009	0.462 ± 0.018	0.149 ± 0.007	0.296 ± 0.017	0.519 ± 0.015
ML-DSA	0.028 ± 0.002	0.068 ± 0.036	0.027 ± 0.003	0.046 ± 0.007	0.108 ± 0.060	0.043 ± 0.007	0.069 ± 0.008	0.132 ± 0.057	0.066 ± 0.005
Dilithium	0.028 ± 0.002	0.068 ± 0.037	0.027 ± 0.002	0.045 ± 0.008	0.107 ± 0.059	0.043 ± 0.004	0.069 ± 0.004	0.132 ± 0.058	0.066 ± 0.005
Falcon	6.089 ± 1.506	0.229 ± 0.014	0.049 ± 0.004	-	-	-	18.032 ± 4.405	0.446 ± 0.018	0.091 ± 0.007
Falcon-padded	6.080 ± 1.514	0.230 ± 0.013	0.048 ± 0.004	-	-	-	18.066 ± 4.388	0.450 ± 0.020	0.090 ± 0.006
MAYO	0.039 ± 0.003	0.084 ± 0.005	0.024 ± 0.007	0.073 ± 0.008	0.236 ± 0.009	0.085 ± 0.008	0.160 ± 0.010	0.464 ± 0.017	0.170 ± 0.010

operação de verificação de assinaturas, independentemente do nível de segurança. No nível 1, o ECDSA apresenta os tempos mais baixos nas operações de geração de chaves e de assinatura. Nos níveis 3 e 5, entretanto, ML-DSA e Dilithium apresentam tempos de geração de chaves menores, enquanto Dilithium e Falcon apresentam melhor desempenho na criação de assinaturas. Observa-se também que o MAYO apresenta tempos significativamente maiores do que os dos demais algoritmos em praticamente todas as operações e níveis avaliados nos dispositivos IoT. Por outro lado, o Falcon apresenta os maiores tempos de geração de chaves em todos os níveis, comportamento associado ao uso de operações com ponto flutuante e consistente com os resultados de trabalhos anteriores.

No ambiente Desktop, o nível 1 apresenta tendências semelhantes às observadas nos dispositivos IoT. No nível 3, os algoritmos avaliados apresentam desempenho comparável ou superior ao do ECDSA em algumas operações. No nível 5, o ECDSA apresenta tempos mais elevados na operação de verificação, enquanto o ML-DSA e o Dilithium apresentam tempos menores nas operações de geração e de verificação de chaves. Os demais algoritmos apresentam tempos superiores ao do ECDSA em algumas operações, mas permanecem na mesma ordem de grandeza. Nesse ambiente, o MAYO apresenta desempenho mais próximo do dos demais algoritmos, enquanto o Falcon mantém o comportamento observado na geração de chaves.

4.1. Impacto em blockchain

A Tabela 5 apresenta os resultados das simulações de verificação de blocos nas *blockchains* analisadas, com base nos tempos obtidos na fase de *benchmark* das operações criptográficas. As diferenças observadas entre os modelos de *blockchain* estão associadas principalmente à quantidade média de transações por bloco. Em particular, a *blockchain* do Bitcoin apresenta, em média, um número maior de transações por bloco do que a da Ethereum, o que impacta diretamente o tempo total de verificação.

Os resultados indicam que, com exceção do algoritmo MAYO, o ECDSA apresenta tempos de verificação superiores aos observados para os algoritmos PQC avaliados nas redes *blockchain* consideradas. Esse comportamento está relacionado ao fato de que a operação de verificação de assinaturas do ECDSA apresenta tempos de execução maiores do que os dos demais algoritmos avaliados. Como a verificação de um bloco envolve a validação de múltiplas transações individuais, variações no custo dessa operação tendem

Tabela 5. Resultados das simulações nas blockchains (ms).

	Raspberry PI3 verify (mean ± std)			Raspberry PI4 verify (mean ± std)			Desktop Mid-end verify (mean ± std)		
Algoritmo	**Nível Inferior**	**Nível 3**	**Nível 5**	**Nível Inferior**	**Nível 3**	**Nível 5**	**Nível Inferior**	**Nível 3**	**Nível 5**
Bitcoin									
ECDSA	1489.98 ± 27.62	6000.51 ± 105.85	10249.58 ± 176.38	645.12 ± 11.60	3138.82 ± 60.90	5485.63 ± 93.01	137.46 ± 2.50	798.56 ± 14.10	898.06 ± 15.82
ML-DSA	1250.28 ± 22.19	1891.65 ± 31.75	2942.41 ± 51.80	411.80 ± 6.92	646.79 ± 11.48	1034.90 ± 17.97	46.77 ± 0.78	74.48 ± 1.29	113.51 ± 1.94
Dilithium	713.75 ± 12.35	1127.16 ± 20.98	1891.56 ± 32.56	294.96 ± 5.13	474.66 ± 8.70	790.06 ± 14.06	46.63 ± 0.81	74.18 ± 1.25	114.34 ± 1.99
Falcon	522.55 ± 9.35	-	940.36 ± 15.94	191.88 ± 3.44	-	345.63 ± 5.93	84.38 ± 1.48	-	156.76 ± 2.85
Falcon-padded	509.87 ± 8.79	-	921.02 ± 17.26	187.30 ± 3.45	-	339.16 ± 5.81	82.95 ± 1.47	-	155.35 ± 2.95
Mayo	3604.35 ± 68.39	11389.44 ± 197.23	28647.02 ± 457.71	1456.75 ± 25.82	4589.70 ± 80.81	11390.25 ± 192.11	42.17 ± 0.75	147.53 ± 2.67	294.32 ± 5.22
Ethereum									
ECDSA	113.61 ± 2.42	458.04 ± 9.15	780.30 ± 15.63	48.50 ± 1.02	236.31 ± 5.11	412.93 ± 9.07	10.27 ± 0.25	59.62 ± 1.49	67.04 ± 1.70
ML-DSA	95.51 ± 1.89	143.99 ± 2.85	224.10 ± 4.40	30.96 ± 0.65	48.65 ± 1.05	77.84 ± 1.68	3.49 ± 0.09	5.55 ± 0.14	8.46 ± 0.21
Dilithium	54.41 ± 1.09	85.98 ± 1.73	144.16 ± 2.87	22.23 ± 0.49	35.69 ± 0.80	59.51 ± 1.32	3.48 ± 0.09	5.54 ± 0.14	8.52 ± 0.22
Falcon	39.85 ± 0.79	-	71.64 ± 1.43	14.43 ± 0.34	-	26.00 ± 0.56	6.29 ± 0.16	-	11.69 ± 0.29
Falcon-padded	38.89 ± 0.75	-	70.26 ± 1.39	14.10 ± 0.30	-	25.55 ± 0.54	6.19 ± 0.16	-	11.60 ± 0.29
Mayo	275.04 ± 5.49	868.15 ± 17.48	2185.15 ± 41.36	109.73 ± 2.34	345.67 ± 7.46	856.19 ± 18.79	3.15 ± 0.08	11.01 ± 0.27	22.02 ± 0.51

a se refletir diretamente no tempo total de verificação do bloco.

4.2. Discussão e Limitações

Os resultados indicam que o desempenho dos algoritmos PQC depende da capacidade de cálculo do hardware. Em dispositivos IoT, os custos das operações criptográficas tornam-se mais relevantes do que em ambientes com maior capacidade de processamento.

Nos experimentos, algoritmos baseados em reticulados, como Falcon e Dilithium, apresentaram melhor desempenho na verificação de assinaturas, enquanto o MAYO apresentou desempenho significativamente inferior em dispositivos restritos. Observamos, ainda, que o ECDSA mantém vantagem na geração de chaves e assinaturas em níveis de segurança mais baixos, enquanto os algoritmos PQC tendem a apresentar melhor desempenho na verificação de assinaturas. As simulações indicam que, com exceção do MAYO, os algoritmos PQC avaliados podem superar o ECDSA nessa operação.

A avaliação foi realizada em um conjunto específico de dispositivos IoT *gateways*, excluindo dispositivos mais restritos, e o impacto na *blockchain* foi analisado por meio de simulações baseadas em *benchmarks* criptográficos, o que gera resultados aproximados; fatores como a latência, vazão, consumo energético e os custos de armazenamento estão fora do escopo deste trabalho, apesar de que o maior tempo necessário para a realização das operações criptográficas influencia diretamente algumas dessas métricas, pois a eficiência da verificação é um requisito central para garantir a alta vazão e a descentralização da blockchain. Ainda assim, os resultados indicam que a adoção de PQC em *blockchains* baseadas em dispositivos IoT é tecnicamente viável, desde que as características do hardware e dos algoritmos sejam consideradas no projeto do sistema.

5. Conclusão

Neste trabalho avaliamos o desempenho de algoritmos de criptografia pós-quântica (PQC) em comparação com o ECDSA em dispositivos IoT e Desktop, considerando operações criptográficas e a verificação de blocos em sistemas *blockchain*.

Os resultados mostram que o desempenho dos algoritmos PQC depende da capacidade de cálculo do hardware. Em dispositivos restritos, Falcon e Falcon-padded apresentam o melhor desempenho na verificação de assinaturas, seguidos por Dilithium e ML-DSA, enquanto o MAYO apresenta desempenho inferior. As simulações indicam que, com exceção do MAYO, os algoritmos PQC avaliados podem superar o ECDSA na verificação de assinaturas, sugerindo que a adoção de PQC em *blockchains* baseadas em dispositivos IoT é tecnicamente viável.

Como trabalhos futuros, investigaremos o impacto do aumento do tamanho dos artefatos criptográficos (com assinaturas que variam de 180B a 19KB, dependendo do algoritmo) nos custos de armazenamento e comunicação, além de avaliar implementações reais considerando escalabilidade, latência e consumo de recursos.

Agradecimentos: Este estudo foi parcialmente financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) – Brasil; pela Fundação de Amparo à Pesquisa do Estado do Rio Grande do Sul (FAPERGS) (25/2551-0002572-9); pela FAPESP (2020/05183-0) e 2023/00816-2); e pelo CNPq/MCTI/FNDCT Nº 22/2024, projeto #444727/2024-8. Roben Lunardi é apoiado pelo IFRS e é bolsista de pós-doutorado da CAPES (PIPD/CAPES).

Declaração de Uso de IA Generativa: Durante a preparação deste trabalho, os autores utilizaram a ferramenta NotebookLM para fins de revisão ortográfica e gramatical. Os autores revisaram e editaram o conteúdo conforme necessário e assumem total responsabilidade pelo conteúdo final da publicação.

Referências

Alagic, G. et al. (2022). Status report on the third round of the NIST Post-Quantum Cryptography Standardization process. Technical Report IR 8413-upd1, NIST (U.S.).

Alagic, G. et al. (2024). Status report on the first round of the additional digital signature schemes for the NIST post-quantum cryptography standardization process. Technical Report IR 8528, NIST (U.S.).

Alharby, M. and van Moorsel, A. (2020). BlockSim: An Extensible Simulation Tool for Blockchain Systems. *Frontiers in Blockchain*, 3.

Chen, L. et al. (2016). Report on Post-Quantum Cryptography. Technical Report IR 8105, NIST (U.S.).

Commey, D. et al. (2025). Performance analysis and deployment considerations of post-quantum cryptography for consumer electronics. Preprint arXiv:2505.02239 [cs.CR].

Juaristi, P. et al. (2025). Benchmarking post-quantum cryptography in ethereum-based blockchains. In *ESORICS*, pages 340–353.

Lonc, B. et al. (2023). Feasibility and Benchmarking of Post-Quantum Cryptography in the Cooperative ITS Ecosystem. In *2023 IEEE Vehicular Networking Conference (VNC)*, pages 215–222. IEEE.

NIST (2016). Call for proposals for public-key cryptographic algorithms. Federal Register Notice Vol. 81, No. 241, pp. 93915-93918, NIST.

Schemitt, A. G. et al. (2025). Assessing the Impact of Post-Quantum Digital Signature Algorithms on Blockchains. In *IEEE 24th (TrustCom)*, pages 2373–2380.

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th SFCS*, page 124–134, USA. IEEE Computer Society.

Upama, P. B. et al. (2022). Evolution of quantum computing: A systematic survey on the use of quantum computing tools. In *IEEE COMPSAC*.

Yokubov, B. and Gan, L. (2021). Comprehensive Comparison of Post-Quantum Digital Signature Schemes in Blockchain. In *ICEIB*, pages 158–161.