Algoritmos de Assinatura Digital Baseada em Reticulados Candidatos a Padrão Pós-Quântico

Guilherme Dias Belarmino[1], **Denise Hideko Goya**[1]

[1]Centro de Matemática, Computação e Cognição – Universidade Federal do ABC
Avenida dos Estados, 5001, Santo André, SP, CEP 09210-580

{g.dias, denise.goya}@ufabc.edu.br

Abstract. *Advances in development of quantum computers and the fact that several of cryptographic algorithms are insecure in the presence of a large quantum computer led NIST to promote a procces to standardize post quantum cryptographic algorithms. In this paper lattice-based digital signature schemes selected to the second round of the contest are compared, based on properties, security and performance of the algorithms.*

Resumo. *Avanços na construção de computadores quânticos e o fato de vários dos atuais padrões criptográficos serem inseguros na presença de um eventual computador quântico de maior porte levaram o NIST a promover um concurso de padronização de algoritmos pós-quânticos, caracterizados pela segurança em computadores convencionais e quânticos. Neste trabalho são comparados esquemas de assinatura digital baseada em reticulados que participam da segunda fase do concurso, com base nas propriedades, segurança e desempenho dos algoritmos.*

1. Introdução

Os chamados algoritmos criptográficos pós-quânticos são aqueles seguros em computadores clássicos e resistentes a ataques quânticos [Barreto et al. 2013], como os de Shor, que fatora inteiros e calcula logaritmos discretos em tempo polinomial sob modelo computacional quântico [Shor 1997]. Desde 2016, encontra-se em andamento o concurso *Post-Quantum Cryptography Standardization* (PQCS), que visa avaliar e padronizar um ou mais algoritmos de criptografia de chave pública pós-quânticos [NIST 2018]. Entre os algoritmos de assinatura digital em análise, destacam-se os baseados em reticulados, que podem apresentar demonstrações formais de segurança e/ou implementações eficientes e relativamente simples [Chen et al. 2016]. Esses algoritmos possuem vantagens e desvantagens, considerando-se os diversos critérios adotados pelo NIST para avaliação, como a aplicação do algoritmo (em protocolos), segurança (resistência a ataques conhecidos) e eficiência [NIST 2016], apenas para citar alguns exemplos.

Este trabalho compila propriedades dos algoritmos de assinatura digital baseada em reticulados que foram selecionados para a segunda rodada do PQCS e apresenta comparações relacionadas a segurança, custo e eficiência, levando em conta parâmetros como modelo de segurança, tamanhos de chave e de assinatura, tempo de execução dos algoritmos para gerar chaves, assinar e verificar.

2. Reticulados e Assinatura Digital

Um reticulado é um conjunto de pontos em um espaço n-dimensional com estrutura periódica [Regev 2006]. De uma maneira mais formal, dados n vetores linearmente independentes, chamados base do reticulado, $v_1, v_2, \ldots, v_n \in \mathbb{R}^n$, o reticulado gerado por eles é o conjunto de vetores $L(v_1, \ldots, v_n) := \{\sum_{i=1}^{n} \alpha_i v_i | \alpha_i \in \mathbb{Z}\}$.

O estudo sobre reticulados no contexto da criptografia ganhou relevância a partir de resultados obtidos por Ajtai, que descobriu que poderiam ser usados não somente como ferramenta para criptanálise, mas também para se construir primitivas criptográficas [Ajtai 1996]. A segurança de algoritmos baseados em reticulados está associada a problemas computacionais difíceis, como o chamado *Shortest Vector Problem (SVP)*, em que dada uma base de um reticulado, busca-se o menor vetor não-nulo no reticulado [Regev 2006]. Existem outros problemas de interesse, dentre os quais destacam-se:

1. Learning With Errors (LWE): versátil para construções de esquemas criptográficos, por possibilitar alto nível teórico de segurança e ser flexível [Regev 2009, Regev 2010]. O problema está baseado em encontrar um segredo $\mathbf{s} \in \mathbb{Z}_q^n$ dada uma sequência aleatória de equações lineares aproximadas em s. Variantes do LWE podem ser criadas quando o reticulado e o problema de interesse são definidos sobre um anel (RLWE) ou um grupo modular (MLWE).
2. Short Integer Problem (SIS): um problema "dual" com o LWE [Regev 2010], definido da seguinte maneira: dada uma sequência de vetores $\boldsymbol{a_1}, \boldsymbol{a_2}, \ldots$ escolhidos uniformemente de $\mathbb{Z}_n^q$, busca-se encontrar um subconjunto (ou uma combinação linear com coeficientes pequenos) dentre eles cuja soma seja igual a 0 [Barreto et al. 2013]. Analogamente, MSIS é uma variante modular do SIS.

2.1. Segurança Clássica para Assinatura Digital

Um esquema de assinatura digital é composto por três algoritmos: de geração de chaves, geração de assinatura e de verificação. Nesse tipo de esquema, o objetivo de um atacante basicamente é forjar assinaturas que serão aceitas como válidas [Menezes et al. 1996] e é classificado conforme o poder que o adversário tem sobre o sistema:

1. Quebra total: o adversário pode gerar informações da chave privada do signatário ou encontrar algoritmos eficientes de assinar.
2. Forja seletiva: o adversário está apto para criar assinaturas válidas para mensagens particulares ou classes de mensagens escolhidas.
3. Forja existencial: o adversário é capaz de forjar a assinatura de pelo menos uma mensagem. Adversário com essa capacidade é o mais fraco que os anteriores e, portanto, os esquemas minimamente seguros são existencialmente não-falsificáveis (*existential unforgeability*, ou EUF).
4. Forja forte: o adversário pode forjar nova assinatura válida sobre uma mensagem da qual ele já tinha informações sobre assinatura [Blazy et al. 2014]; esquemas seguros contra esse tipo de adversário são *strong unforgeability*, ou SUF.

Há dois tipos de ataques contra esquemas de assinatura digital:

1. Ataque de chave (*key-only attacks*): o adversário conhece somente a chave pública do signatário.
2. Ataque de mensagens (*message attacks*): o adversário pode examinar assinaturas correspondentes a mensagens conhecidas ou mensagens escolhidas:

(a) Ataque de mensagem conhecida: o adversário conhece a chave pública e um conjunto de pares mensagens-assinaturas [Canetti 2008].
(b) Ataque de mensagem escolhida (*chosen-message attack*, ou CMA): o adversário conhece apenas a chave pública; pode gerar mensagens e receber suas respectivas assinaturas válidas. No contexto do concurso do NIST, os ataques CMA são realizados de forma adaptativa [NIST 2016].

Um esquema de assinatura é dito seguro quando se pode demonstrar (ou apresentar evidências heurísticas) que um adversário não atinge um dos objetivos citados sob um dos tipos de ataque. Assim, diz-se por exemplo que um esquema de assinatura é EUF-CMA se é existencialmente não-falsificável sob ataque de mensagem escolhida.

2.2. Níveis de Segurança para Assinatura Digital Pós-quântica

O NIST propõe ainda uma abordagem de segurança em níveis, em que a força não está baseadas em bits de segurança. Isto acontece, pois existem incertezas em estimar a segurança de criptossistemas pós-quânticos. Os níveis são os seguintes:

1. Qualquer ataque que quebre a definição de segurança relevante deve requerer recursos computacionais comparáveis ou superiores aos necessários para uma busca de chave de uma cifra de bloco com chave de 128-bits (e.g. AES128);
2. Qualquer ataque que quebre a definição de segurança relevante deve requerer recursos computacionais comparáveis ou superiores aos necessários para uma busca de colisão de uma função hash de 256 bits (e.g. SHA256/SHA3-256);
3. Qualquer ataque que quebre a definição de segurança relevante deve requerer recursos computacionais comparáveis ou superiores aos necessários para uma busca de chave de uma cifra de bloco com chave de 192 bits (e.g. AES192);
4. Qualquer ataque que quebre a definição de segurança relevante deve requerer recursos computacionais comparáveis ou superiores aos necessários para uma busca de colisão de uma função hash de 384 bits (e.g. SHA384/SHA3-384);
5. Qualquer ataque que quebre a definição de segurança relevante deve requerer recursos computacionais comparáveis ou superiores aos necessários para uma busca de chave de uma cifra de bloco com chave de 256 bits (e.g. AES256).

2.3. Algoritmos de Assinatura Digital Candidatos do PQCS

Os algoritmos escolhidos para análise neste trabalho são os que foram classificados para a segunda rodada do Post-Quantum Cryptography Standardization [NIST 2019], no início de 2019. Para a primeira rodada, foram selecionados cinco algoritmos, dos quais três foram qualificados: Crystals-Dilithium [Ducas et al. 2019], Falcon [Fouque et al. 2018] e qTESLA [Bindel et al. 2019]. A seguir, é apresentada uma breve descrição de cada um.

2.3.1. Crystals-Dilithium

O algoritmo CRYSTALS-DILITHIUM (*Cryptographic Suite for Algebraic Lattices Dilithium)* foi proposto por Ducas et al. e apresenta uma proposta de assinatura digital [Ducas et al. 2019]. O esquema possui tanto a opção determinística quanto a aleatória para implementação. Porém, os autores sugerem a versão determinística como padrão com exceção do caso em que o adversário pode explorar o determinismo via ataques de canal lateral.

O Dilithium está baseado nos problemas computacionais LWE e SIS, mais precisamente, nas variações *MLWE – Module Learning with Errors* e *MSIS – Module Short Integer Solution*. É possível mostrar que o esquema é seguro contra ataques de mensagem escolhida SUF-CMA, a noção mais forte de segurança formal.

2.3.2. FALCON

FALCON (*Fast-Fourier Lattice-bases Compact Signatures over NTRU*) é um algoritmo de assinatura digital pós-quântico proposto por Fouque et al. [Fouque et al. 2018]. O problema computacional associado ao algoritmo é o SIS sobre reticulados NTRU.

O esquema de assinatura digital está baseado no framework GPV [Gentry et al. 2007], que possui demonstrações de segurança contra oráculos clássicos e também quânticos. Trata-se de um algoritmo com design modular, ou seja, através de uma instância do framework GPV é utilizada a classe de reticulados NTRU. Porém, é possível utilizar outras classes de reticulados.

2.3.3. qTESLA

O qTESLA é uma família baseada no problema RLWE [Bindel et al. 2019] e no framework de [Lyubashevsky 2009]. Em duas versões com diferentes abordagens de projeto, há o *qTESLA heurístico*, em que a geração de parâmetros segue uma heurística de segurança aliada a maior eficiência, e o *qTESLA demonstravelmente seguro (provably-secure qTESLA)*, com maior segurança teórica, via demonstração por redução de problemas computacionais, sob modelo do oráculo aleatório.

O esquema possui um design que busca facilitar a segurança prática, isto é, na implementação. Em particular, são suportadas implementações *constant-time*, que são seguras contra ataques de canais laterais temporais e baseados em cache.

3. Comparações

Nesta seção, são apresentadas comparações entre os algoritmos selecionados, com base nas documentações submetidas ao PQCS, no início do concurso. Os critérios para comparação estão baseados em suas operações básicas (geração de chave, assinatura e verificação) bem como seus aspectos técnicos (implementação) e de segurança. Os gráficos apresentados estão relacionados com as implementações referência do algoritmo (sem otimizações, caso haja). Um resumo sobre os esquemas de assinatura analisados pode ser encontrado na Tabela 1, onde o caractere "−" representa que não há informações sobre o item associado na documentação.

3.1. Segurança

Dois esquemas de assinatura digitais estão baseados no mesmo problema computacional, o *LWE*. Entretanto, de fato, são utilizadas variações deste problema. O Dilithium se baseia na versão modular (tanto do LWE quanto do SIS) e o qTESLA se baseia na versão anelar. O FALCON está baseado no problema SIS sobre reticulados NTRU [Fouque et al. 2018].

Tabela 1. Características dos esquemas de assinatura digital

	Crystals-Dilithium	**FALCON**	**qTESLA**
Níveis de segurança atendidos (NIST)	1, 2 e 3	1, 4 e 5	1, 2, 3 e 5
Demonstração de segurança	Direta via reduções de problemas	Indireta baseada no framework	Direta via reduções de problemas
Segurança EUF-CMA	Sim	–	Sim
Segurança SUF-CMA	Sim	–	–
Problema computacional associado	MLWE e MSIS	SIS sobre reticulados NTRU	RLWE
Quantidade de conjuntos de parâmetros oferecido	3	3	12
Trabalhos relacionados estudados	3	3	2

Os esquemas atendem diferentes níveis de segurança do NIST de acordo com os conjuntos de parâmetros utilizados. Apenas para os esquemas Dilithium e qTESLA são apresentadas reduções de seguranças que corroboram a segurança do algoritmo, de maneira mais explícita.

3.2. Custo

Um dos critérios para comparação dos esquemas está relacionado ao custo, visto que é também é um dos critérios adotados pelo NIST. São apresentados gráficos referentes ao tamanho da chave pública e da assinatura (Figura 1) e ao desempenho para execução das operações de assinatura, verificação e geração de chave (Figura 2). As comparações estão divididas de acordo com o nível de segurança do NIST. Valores muito distantes da média aparecem como "etiquetas" junto às respectivas barras, para facilitar as comparações. Os dados foram extraídos da documentação oficial de cada esquema de assinatura digital.

Note que as versões do FALCON não aparecem nos gráficos de desempenho, pois em sua documentação são apresentados dados em operações/segundo e não em ciclos de CPU. Apenas o FALCON-1024 possui um conjunto de parâmetros que atende o nível 4 de segurança do NIST e, por esse motivo, não apresentamos gráficos para este nível.

Vale ressaltar que, como os dados foram retirados das respectivas documentações dos esquemas de assinatura digital, os autores realizaram testes em diferentes máquinas (com diferentes especificações), entretanto a unidade é dada em ciclos de CPU, permitindo uma comparação.

3.3. Discussão

Observe que nenhum esquema de assinatura digital abrange todos os níveis de segurança proposto pelo NIST. O qTESLA se aproxima mais atendendo 4 diferentes níveis (1, 2, 3 e 5). Por outro lado, a flexibilidade do algoritmo (diferentes parâmetros, adaptabilidade do código, etc) é importante devido às possíveis aplicações dos algoritmos (sejam eles em sistemas mais sofisticados ou não, por exemplo). Logo, dos algoritmos estudados, existem aqueles que são mais eficientes, outros com tamanho de parâmetros menores e, também, aqueles com demonstrações de segurança, ou seja, a escolha do algoritmo depende de como o mesmo será empregado e qual a maior necessidade (segurança, eficiência, etc).

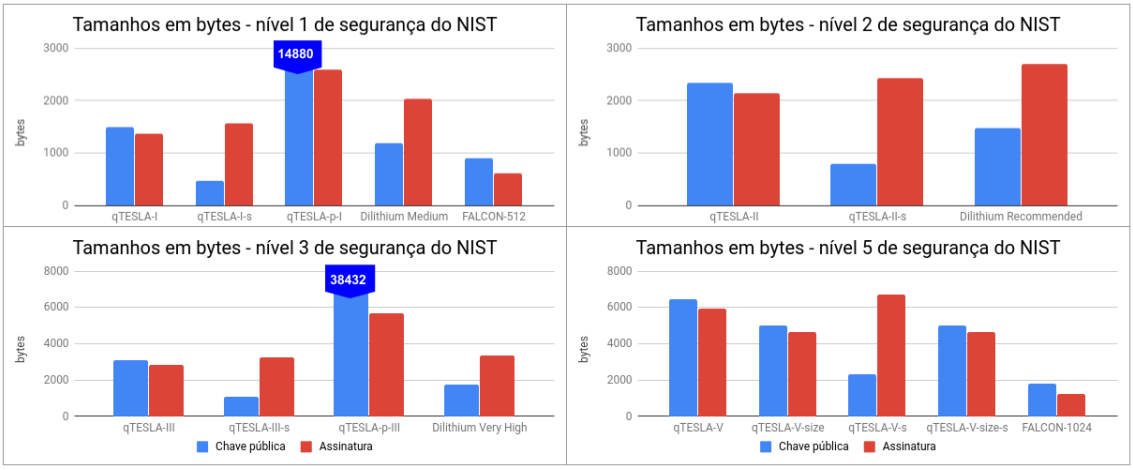

Figura 1. Comparação de tamanhos: chave pública e assinatura gerada.

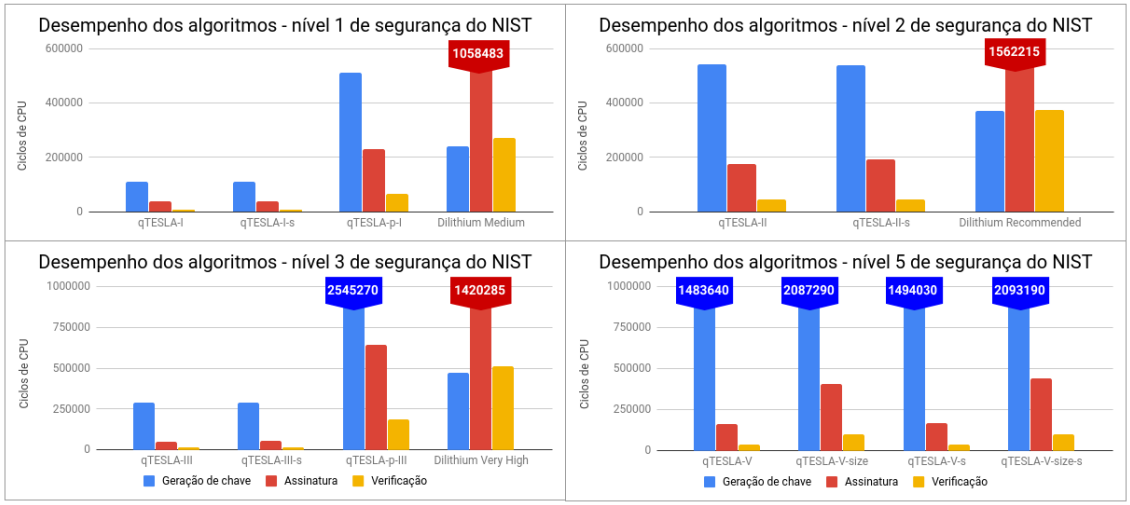

Figura 2. Comparação do desempenho dos algoritmos, em ciclos de CPU.

Assim, é possível verificar que o FALCON apresenta, para os níveis de segurança 1, 4 e 5 do NIST, o menor **tamanho dos parâmetros** (soma da chave pública e da assinatura gerada) que os demais esquemas. Para os demais níveis, o qTESLA se sobressai em relação ao Dilithium.

Observando o quesito **desempenho**, analisando o menor tempo consumido em ciclos de CPU tem-se que, para as três operações básicas de assinatura digital, o qTESLA, em sua maioria, supera o Dilithium em todos os níveis de segurança do NIST. Ao se comparar as versões demonstravelmente seguras do qTESLA com o Dilithium (comparação mais justa), o qTESLA em geral é mais lento para gerar as chaves, porém mais veloz para assinar e verificar (o que é desejável para a maioria das aplicações). Vale lembrar que o FALCON não aparece na comparação devido à discrepância das unidades de medida (o FALCON apresenta a eficiência em operações por segundo e não em ciclos de CPU).

Analisando, agora, as **demonstrações de segurança**, tanto os algoritmos qTESLA e Dilithium apresentam demonstrações de seguranças diretas baseada em reduções de problemas, enquanto que o FALCON apresenta demonstrações indiretas baseadas nos

frameworks utilizados e nos reticulados NTRU.

Finalmente, na Tabela 2, há uma síntese com os aspectos positivos e negativos dos esquemas de assinatura digital baseados em reticulados analisados.

Tabela 2. Resumo de aspectos positivos e negativos dos esquemas analisados de assinatura digital baseados em reticulados.

	Aspectos Positivos	Aspectos Negativos
Crystals-Dilithium	• Possui demonstração de segurança com base em redução de problemas, para todas suas versões. • Seguro contra ataques no modelo SUF-CMA, mais forte que EUF-CMA. • Segurança no modelo do oráculo aleatório clássico e quântico. • Há uma versão otimizada que suporta conjunto de instruções AVX2.	• Mais lento para assinar e verificar, quando comparado com o qTESLA. • Vulnerabilidades conhecidas relacionadas a ataques de uso de *nonces* e de canal lateral, embora haja estudo que mostra como contornar este último.
FALCON	• Parâmetros com menor tamanho (somados chave pública e assinatura). • Segurança no modelo do oráculo aleatório clássico e quântico. • Design modular.	• Demonstração de segurança indireta, baseada no framework utilizado.
qTESLA	• Versatilidade em se adequar a diferentes cenários, balanceando maior velocidade ou maior segurança. • Abrange mais níveis do NIST. • Compressão de chave parametrizável. • Possui versões demonstravelmente seguras. • Melhor desempenho geral. • Há uma versão otimizada que suporta conjunto de instruções AVX2, a partir da segunda rodada.	• Geração de chave mais lenta principalmente nas versões demonstravelmente seguras.

4. Trabalhos Relacionados

Como o concurso encontra-se em andamento, ainda há poucos trabalhos publicados sobre os algoritmos selecionados para a segunda fase. Foi realizado um mapeamento no repositório *Cryptology ePrint Archive*[1] utilizando como palavras-chave o nome dos algoritmos. A seguir, são resumidos alguns trabalhos encontrados.

Para o Crystals-Dilithium foram encontrados três artigos, onde o primeiro relata um ataque de injeção de falhas contra o esquema [Ravi et al. 2018]. Já o segundo retrata sobre uma vulnerabilidade do algoritmo propondo um ataque de canal lateral [Prasanna Ravi and Bhasin 2018]. Por fim, o último aponta uma proposta de correção com o objetivo de reduzir ataques de canal lateral [Migliore et al. 2019].

No caso do FALCON, foram encontrados três artigos. O primeiro apresenta uma variante para assinatura em anel [Lu et al. 2018]. O segundo apresenta novos algoritmos para solução da equação NTRU (parte custosa) [Lu et al. 2018]. Por último, o trabalho de [Karmakar et al. 2019] otimiza a amostragem gaussiana discreta em tempo constante e reporta um estudo de caso sobre o FALCON.

[1] `https://eprint.iacr.org/`

Para o qTESLA, foram encontrados dois artigos relacionados. O primeiro relata sobre uma vulnerabilidade no esquema qTESLA e Dilithium contra ataques de injeção de falha [Ravi et al. 2019]. O segundo apresenta uma correção para o problema com a aplicação de máscaras [Gérard and Rossi 2019].

5. Conclusão

Neste trabalho, foram realizadas comparações sobre os candidatos a padrão pós-quântico para assinatura digital, que são baseados em reticulados e que foram aprovados para a segunda fase do concurso PQCS. As propriedades dos algoritmos foram compiladas, com base nas documentações oficiais submetidas ao NIST.

Os critérios de comparação foram baseados na categoria custo do NIST, em que foram considerados os tamanhos de chave e de assinatura, desempenho nominal dos algoritmos e aspectos de segurança formal, como segurança teórica demonstrável e problema computacional associado.

Com base no levantamento realizado, é possível observar que cada algoritmo tem seus pontos fortes e fracos se comparados nos diferentes níveis de segurança propostos pelo NIST. Sobre o tamanho dos parâmetros o FALCON possui vantagem em relação aos demais, enquanto no quesito eficiência (análise de desempenho) e demonstrações de segurança o qTESLA apresenta melhores resultados. Vale lembrar que para o quesito eficiência, foi comparado apenas os esquemas qTESLA e Crystals-Dilithium.

Portanto, a escolha dos algoritmos depende da aplicação, isto é, para determinados casos um esquema pode ser mais vantajoso enquanto que em outros casos, outro algoritmo pode apresentar resultados melhores. Por exemplo, para aplicações de software embarcado com baixa capacidade de armazenamento, o esquema mais interessante seria o FALCON, por apresentar menor tamanho de parâmetros. Em aplicações onde a prioridade é máxima velocidade, o qTESLA (na versão heurística) se mostra mais aplicável. Por outro lado, se o principal requisito for um alto nível de segurança, o *provably-secure qTESLA* é mais indicado. Assim, a flexibilidade do esquema tem uma grande importância nas análises.

Diante disso, por apresentar maiores conjuntos de parâmetros e bons resultados sobre desempenho, o esquema de assinatura digital qTESLA possui vantagem sobre os demais participantes do concurso.

Para trabalhos futuros, diferentes abordagens podem ser seguidas. Uma vertente mais teórica visa análises mais aprofundadas dos esquemas para a realização de comparações mais detalhadas, assim como o levantamento de novos estudos relacionados (em criptanálise ou otimizações, por exemplo). Por uma abordagem mais prática, é possível realizar implementações e testes em diferentes cenários de aplicações específicas, como por exemplo sistemas embarcados para internet das coisas. Assim, futuramente, pretende-se avaliar, de maneira minuciosa, outros aspectos dos esquemas de assinatura digital bem como a performance e a viabilidade dos algoritmos em diferentes situações.

Referências

Ajtai, M. (1996). Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 99–108. ACM.

Barreto, P., Biasi, F. P., Dahab, R., César, J., Pereira, G., and Ricardini, J. E. (2013). Introdução à criptografia pós-quântica. *Minicursos do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais-SBSeg*.

Bindel, N., Alkim, E., Barreto, P. S. L. M., Akleylek, S., Buchmann, J., , Eaton, E., Gutoski, G., Kramer, J., Longa, P., Polat, H., Ricardini, J. E., and Zanon, G. (2019). Submission to nist's post-quantum project (2nd round): lattice-based digital signature scheme qtesla. Disponível em: `https://qtesla.org/wp-content/uploads/2019/04/qTESLA_round2_04.2019.pdf`.

Blazy, O., Kakvi, S. A., Kiltz, E., and Pan, J. (2014). Tightly-secure signatures from chameleon hash functions. Cryptology ePrint Archive, Report 2014/1021. Disponível em: `https://eprint.iacr.org/2014/1021`.

Canetti, R. (2008). Lecture 8: Digital signatures. Último acesso em 22 ago 2018. Disponível em: `https://www.cs.tau.ac.il/~canetti/f08-materials/scribe8.pdf`.

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., and Smith-Tone, D. (2016). Report on post-quantum cryptography. *National Institute of Standards and Technology Internal Report 8105*. Disponível em: `https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf`.

Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., and Stehlé, D. (2019). Crystals-dilithium algorithm specifications and supporting documentation. Disponível em: `https://pq-crystals.org/dilithium/data/dilithium-specification-round2.pdf`.

Fouque, P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., and Zhang, Z. (2018). Falcon: Fast-fourier lattice-based compact signatures over ntru. Specifications v1.1.

Gentry, C., Peikert, C., and Vaikuntanathan, V. (2007). Trapdoors for hard lattices and new cryptographic constructions. Cryptology ePrint Archive, Report 2007/432. Disponível em: `https://eprint.iacr.org/2007/432`.

Gérard, F. and Rossi, M. (2019). An efficient and provable masked implementation of qtesla. Cryptology ePrint Archive, Report 2019/606. `https://eprint.iacr.org/2019/606`.

Karmakar, A., Roy, S. S., Vercauteren, F., and Verbauwhede, I. (2019). Pushing the speed limit of constant-time discrete gaussian sampling. a case study on falcon. Cryptology ePrint Archive, Report 2019/267. Disponível em: `https://eprint.iacr.org/2019/267`.

Lu, X., Au, M. H., and Zhang, Z. (2018). Raptor: A practical lattice-based (linkable) ring signature. Cryptology ePrint Archive, Report 2018/857. Disponível em: `https://eprint.iacr.org/2018/857`.

Lyubashevsky, V. (2009). Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In Matsui, M., editor, *Advances in Cryptology – ASIACRYPT 2009*, pages 598–616, Berlin, Heidelberg. Springer Berlin Heidelberg.

Menezes, A. J., Vanstone, S. A., and Oorschot, P. C. V. (1996). *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1st edition.

Migliore, V., Gérard, B., Tibouchi, M., and Fouque, P.-A. (2019). Masking dilithium: Efficient implementation and side-channel evaluation. Cryptology ePrint Archive, Report 2019/394. Disponível em: https://eprint.iacr.org/2019/394.

NIST (2016). Submission requirements and evaluation criteria for the post-quantum cryptography standardization process. Último acesso em em 02 jun 2019. Disponível em: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

NIST (2019). Pqc standardization process: Second round candidate announcement. Último acesso em em 11 mar 2019. Disponível em: https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates.

NIST, C. S. R. C. (2018). Post-quantum cryptography. Último acesso em 08 jul 2018. Disponível em https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

Prasanna Ravi, Mahabir Prasad Jhanwar, J. H. A. C. and Bhasin, S. (2018). Side-channel assisted existential forgery attack on dilithium - a nist pqc candidate. Cryptology ePrint Archive, Report 2018/821. Disponível em: https://eprint.iacr.org/2018/821.

Ravi, P., Jhanwar, M. P., Howe, J., Chattopadhyay, A., and Bhasin, S. (2019). Exploiting determinism in lattice-based signatures - practical fault attacks on pqm4 implementations of nist candidates. Cryptology ePrint Archive, Report 2019/769. https://eprint.iacr.org/2019/769.

Ravi, P., Roy, D. B., Bhasin, S., Chattopadhyay, A., and Mukhopadhyay, D. (2018). Number "not used"once - practical fault attack on pqm4 implementations of nist candidates. Cryptology ePrint Archive, Report 2018/211. Disponível em: https://eprint.iacr.org/2018/211.

Regev, O. (2006). Lattice-based cryptography. In *Annual International Cryptology Conference*, pages 131–141. Springer.

Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):34. Preliminary version in STOC'05.

Regev, O. (2010). The learning with errors problem. In *Proc. of 25th IEEE Annual Conference on Computational Complexity (CCC)*, pages 191–204.

Shor, P. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.