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

Guilherme Dias Belarmino, Denise Hideko Goya
Centro de Matemática, Computação e Cognição, CMCC – UFABC
{g.dias, denise.goya}@ufabc.edu.br

Abstract: Evoluções na construção de computadores quânticos e o fato de que vários dos atuais padrões em algoritmos criptográficos são 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. O concurso encontra-se em andamento e sua primeira fase deve se encerrar em 2019. Paralelamente às análises oficiais, este trabalho visa comparar os algoritmos de assinatura digital baseada em reticulados que participam desse concurso. Apresenta-se uma análise preliminar com base na descrição técnica e nos parâmetros dos competidores.

1. Introdução

Os algoritmos de criptografia pós-quânticos surgiram da necessidade de se proteger contra ataques a criptossistemas clássicos através de computadores quânticos, visto que, em 1997, Shor descobriu um algoritmo quântico capaz de quebrar a segurança de técnicas utilizadas atualmente. O algoritmo de Shor resolve os problemas de fatoração de inteiros grandes e do cálculo de logaritmos discretos em tempo hábil, ou seja, padrões atuais como o RSA e DSA tornam-se inseguros caso computadores quânticos de grande porte sejam construídos [Shor 1997]. Assim, uma informação criptografada nos dias atuais não está, necessariamente, segura em um momento futuro devido a segurança dos algoritmos estar baseada em problemas que poderiam ser resolvidos rapidamente por computadores quânticos [Barreto et al. 2013].

Uma vertente da criptografia é a chamada criptografia assimétrica que, sucintamente, é uma classe de algoritmos que requerem duas chaves, sendo uma pública e uma privada, onde através de cálculos com as chaves é possível se verificar a integridade e autenticidade das mensagens. Algoritmos de criptografia baseada em chave pública são indispensáveis para os dias de hoje, viabilizam vários serviços na Internet e estão relacionados com aplicações importantes para a economia, segurança, entre outros [Chen et al. 2016]. E uma das aplicações mais utilizadas para essa categoria está relacionada com a assinatura digital.

Consequentemente, pesquisadores têm buscado algoritmos de assinatura digital que possam ser resistentes a ataques que usam computadores quânticos para a substituição dos algoritmos utilizados atualmente. Desde 2016, o National Institute of Standards and Technology tem promovido o concurso *Post-Quantum Cryptography Standardization* (PQCS), que visa avaliar e padronizar um ou mais algoritmos de criptografia de chave pública pós-quânticos, que sejam seguros no contexto da tecnologia atual e que sejam resistentes a computadores quânticos [NIST 2018]. O concurso se encontra atualmente em disputa, com diversos algoritmos submetidos e em análise. Existem diferentes classes de algoritmos de assinatura digital, dentre eles destacam-se os baseados em reticulados, que em geral possuem demonstrações formais de segurança, além de implementações eficientes e relativamente simples de serem compreendidas [Chen et al. 2016].

Estes algoritmos possuem vantagens e desvantagens, considerando-se os diversos critérios usuais para avaliação, como a aplicação do algoritmo (protocolos, por exemplo), segurança (resistência a ataques de mensagem escolhida – EUF-CMA) e eficiência [NIST 2016], apenas para citar alguns exemplos.

Este trabalho visa realizar um levantamento de propriedades e analisar os algoritmos de assinatura digital baseada em reticulados que estão participando do PQCS. Esta análise se fundamenta em questões relacionadas ao custo e à eficiência dos algoritmos, como tamanho dos parâmetros (chaves e assinatura), tempo de geração de chaves, de assinatura e verificação.

2. Algoritmos de assinatura digital e sua Segurança

Um reticulado, de acordo com [Regev 2006], é um conjunto de pontos em um espaço de n-dimensional com estrutura periódica como ilustrado na figura 1. De uma maneira mais formal, dado n vetores linearmente independentes $v_1, v_2, \ldots, v_n \in \mathbb{R}^n$, o reticulado gerado por eles é o conjunto de vetores

$$L(v_1, \ldots, v_2) := \left\{ \sum_{i=1}^{n} \alpha_i v_i \;\middle|\; \alpha_i \in \mathbb{Z} \right\}. \tag{1}$$

Os vetores $v_1, \ldots, v_n$ são conhecidos como base do reticulado. Ou seja, um reticulado é um espaço vetorial discretizado, isto é, existem analogias com conceitos de álgebra linear, tais como, módulo, dimensão, ortogonalidade, transformação linear, entre outros [Barreto et al. 2013].

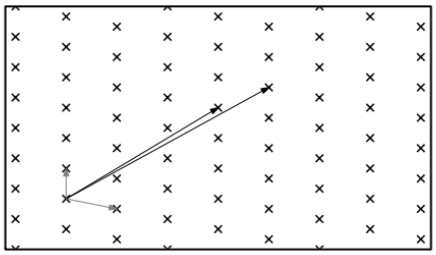

Figura 1. Reticulado em $\mathbb{R}^2$ e duas de suas bases. Retirado de [Regev 2006]

O estudo sobre reticulados no contexto da criptografia surgiu com os resultados obtidos por [Ajtai 1996], onde ele descobriu que os reticulados não somente poderiam ser usados como ferramenta para criptanálise, mas também podem ser utilizados para se construir primitivas criptográficas [Regev 2006].

A segurança de algoritmos baseados em reticulados está associada a problemas computacionais como o chamado *Shortest Vector Problem (SVP)*. No SVP, dada uma base de um reticulado, quer se encontrar o menor vetor não-nulo no reticulado [Regev 2006]. Porém, na prática, é utilizado um fator de aproximação $\gamma(n)$ para o problema SVP, ou seja, deseja-se encontrar um vetor cujo módulo seja inferior ao menor vetor multiplicado pelo fator γ [Barreto et al. 2013].

Existem outros problemas computacionais sobre reticulados de interesse, dentre os quais pode-se destacar:

(a) Problema do vetor de distância mínima (*Closest Vector Problem - CVP*): dados um reticulado $L(v_1, \ldots, v_n)$ e um vetor $t \in \mathbb{R}^m$, o objetivo é encontrar um vetor $v \in L$ que seja mais próximo de t [Barreto et al. 2013];

(b) Problema de vetores independentes mínimos (*Shortest Independent Vector Problem - SIVP*): dada uma base $B \in \mathbb{Z}^{m \times n}$, o problema consiste em encontrar n vetores linearmente independentes que pertençam ao reticulado tais que o módulo entre os vetores v_i seja mínima [Barreto et al. 2013].

2.1. Tipos de ataques sobre Assinatura Digital

O objetivo principal de um atacante (adversário) nesse tipo de esquema de criptografia é falsificar assinaturas, isto é, produzir assinaturas válidas, passando-se por outra entidade, em qualquer um dos três níveis a seguir [Menezes et al. 1996]:

- Quebra total: o adversário pode tanto calcular a chave privada do signatário quanto encontrar algoritmo eficiente que gera assinaturas válidas e se equivalha ao algoritmo original;
- Falsificação seletiva: o adversário está apto a criar assinaturas válidas para mensagens particulares ou classes de mensagens escolhidas;
- Falsificação existencial: o adversário é capaz de falsificar a assinatura para pelo menos uma mensagem.

Existem duas classes de ataques contra esquemas de assinatura digital de chave pública:

(a) Ataque de chave (*key-only attack*): o adversário conhece somente a chave pública do signatário;

(b) Ataque de mensagens (*message attack*): neste tipo de ataque, o adversário consegue examinar assinaturas correspondentes a mensagens conhecidas ou mensagens escolhidas. Podemos subdividir em duas categorias:

   i. Ataque de mensagem conhecida (*known-message attack*): o adversário tem conhecimento da chave de verificação e de um conjunto de pares mensagem-assinatura [Canetti 2008];

   ii. Ataque de mensagem escolhida (*chosen-message attack*): o adversário tem conhecimento da chave de verificação possui a habilidade de gerar mensagens e receber suas respectivas assinaturas válidas. Observe que o mesmo não possui nenhuma informação da chave secreta do signatário [Canetti 2008].

2.2. Níveis de Segurança do NIST para Assinatura Digital Pós-quântica

Para a segurança, o NIST propõe uma abordagem em níveis, diferentemente da criptografia clássica moderna (baseda em bits de segurança). Isto acontece porque existe incerteza em estimar a segurança de criptossistemas pós-quânticos. Assim, essa abordagem está separada em categorias, mais fácil de se analisar as métricas e, consequentemente, comparar os algoritmos. As categorias definidas pelo NIST estão separadas de acordo com os seguintes requisitos:

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. Post-Quantum Cryptography Standardization (PQCS)

Os algoritmos escolhidos para análise neste trabalho são os que foram submetidos para a primeira rodada do PQCS, no final de 2017. Ao todo, participam 23 algoritmos de assinatura digital, onde cinco deles são baseados em reticulados. São eles: Crystals-Dilithium, DRS, Falcon, pqNTRUSign e qTesla.

3. Resultados Preliminares

Os resultados preliminares da análise dos algoritmos podem ser vistos na Tabela 1, onde dados relacionados ao tamanho dos parâmetros e o nível de segurança foram retirados da documentação dos algoritmos. A geração de chaves, dada em quilociclos de CPU foram retirados de [SAFEcrypto 2018], onde estes testes foram realizados em uma máquina Intel x64 com Windows e Linux com compilador GCC instalado.

4. Conclusões

A análise inicial dos algoritmos foi realizada baseada na documentação oficial submetida ao NIST. Como o concurso de padronização está em andamento, um levantamento bibliográfico se torna mais difícil, visto que testes ainda estão sendo feitos.

Vale ressaltar que este trabalho está em andamento, ou seja, outros aspectos relevantes, como segurança formal e problema computacional associado ou eficiência para assinar e verificar, ainda estão em avaliação.

Tabela 1. Comparação dos algoritmos da primeira rodada do PQCS de Assinatura Digital baseada em reticulados.

	Versão	Chave Pública (bytes)	Assinatura (bytes)	Geração de Chave (10^{3} ciclos de CPU)	Nível de Segurança NIST
CRYSTALS-Dilithium	medium	1184	2044	1.185,462	1
	recommended	1472	2701	2.753,772	2
	very high	1760	3366	2.293,141	3
DRS	128	5.094.433	8550	62.867,536	1
	192	8.410.001	11020	95.622,249	3
	256	14.402.026	14421	148.424,947	5
FALCON	512	897	617,38	8.359,971	1
	768	1441	993,91	13.058,641	3
	1024	1793	1233,29	19.884,364	5
pqNTRUSign	Gaussian-1024	2048	1408	349.028,118	5
	Uniform-1024	2048	2048	202.185,303	5
qTESLA	128	2976	2720	2.020,404	1
	192	6176	5664	9.899,854	3
	256	6432	5920	8.143,869	5

5. Referências

[Ajtai 1996] 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 et al. 2013] 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*.

[Canetti 2008] Canetti, R. (2008). Lecture 8: Digital signatures. Último acesso em 22 ago 2018.

[Chen et al. 2016] 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*.

[Menezes et al. 1996] 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.

[NIST 2016] NIST (2016). Submission requirements and evaluation criteria for the post-quantum cryptography standardization process. *https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography//call-for-proposals-final-dec-2016.pdf*. Último acesso em em 08 jul 2018.

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

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

[SAFEcrypto 2018] SAFEcrypto, S. A. o. F. E. C. (2018). Nist software performance tests - signatures. *https://www.safecrypto.eu/pqclounge/software-analysis-signatures/*. Último acesso em 11 nov 2018.

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