Assinaturas digitais pós-quânticas para dispositivos IoT (Internet of Things)

Aluno: Vitor Nagata
Email: nagatavit@gmail.com
Faculdade de Engenharia Elétrica e Computação - FEEC
Universidade Estadual de Campinas - UNICAMP

Orientador: Marco A. A. Henriques
Email: marco@dca.fee.unicamp.br
Faculdade de Engenharia Elétrica e Computação - FEEC
Universidade Estadual de Campinas - UNICAMP

***Resumo*—Grandes avanços no campo da computação quântica têm aumentado a preocupação com a quebra de algoritmos criptográficos atuais, como RSA e ECC. Para manter a segurança e dos protocolos atuais, já estão sendo pesquisados algoritmos resistentes a ataques quânticos. Neste artigo, apresentamos algumas das ideias por trás dos novos algoritmos de assinatura pós-quânticos e comparamos seus desempenhos em dois contextos: um em ambiente de desktop e outro voltado para aplicações IoT.**

I. Introdução

O crescente avanço no ramo da computação quântica nos últimos anos traz consigo uma grande preocupação com a segurança dos esquemas criptográficos atuais, especialmente os baseados em primitivas assimétricas como o problema da fatoração de números inteiros (RSA), logaritmo discreto (Diffie-Hellman, Elgamal, DSA) e curvas elípticas (ECDH, ECDSA), devido ao algoritmo de Shor [6]. De forma a prevenir os ataques possibilitados pela computação quântica, diversos esforços já estão sendo feitos, tais como, iniciativas de adoção de chaves maiores, propostas de novos protocolos baseados nas premissas atuais (Curvas Elípticas Supersingulares [3]) e principalmente, propostas de novas premissas criptográficas, os chamados Algoritmos Criptográficos Pós-Quânticos (*PQC - Post-Quantum Cryptography*).

No ramo da PQC, o principal esforço se concentra no processo de padronização sendo realizado pelo NIST [5] que, de forma similar aos processos realizados para o AES e SHA3, busca encontrar a(s) melhor(es) proposta(s) resistente(s) a ataques de algoritmos quânticos. Essas propostas contudo, possuem adversidades como grandes tamanhos de chaves e assinaturas, ou longos tempos de assinatura e verificação.

Em paralelo ao avanço da computação quântica, também estamos próximos de uma revolução em questão de conectividade com a proximidade de implementações das tecnologias 5G. Isso significa que cada vez mais, mais dispositivos com baixo poder computacional e capacidade armazenamento estarão conectados em rede, muitas vezes trafegando dados sensíveis que necessitam de autenticação como sensores de biometria ou controles de acesso, na chamada Internet das Coisas (*IoT - Internet of Things*).

Neste trabalho, apresentamos as principais ideias por trás dos novos algoritmos pós-quânticos e a realização de alguns ensaios para verificar as vantagens e desvantagens das propostas de assinaturas digitais pós-quânticas em cenários mais específicos como o de IoT. Alguns trabalhos na literatura já foram realizados para a medição de desempenho de algoritmos pós-quânticos como o trabalho de Hyeongcheol An [1] e de projetos como eBACS [2]. Nesses trabalhos o foco do estudo foi o desempenho geral das propostas ou sua viabilidade de uso em protocolos atuais. Nosso objetivo com este artigo é uma discussão de métricas práticas para o cenário de IoT como os requisitos mínimos necessários para que haja a viabilidade de implementação mas não será feita uma análise detalhada da segurança como está sendo realizado pelo NIST.

O artigo está estruturado da seguinte maneira: nas Seções II e III apresentamos uma breve contextualização do processo de padronização realizado pelo NIST e do ambiente a ser estudado; na Seção IV são detalhadas as ideias por trás das novas primitivas criptográficas, na Seção V apresentamos as ferramentas utilizadas e o ambiente de testes; por fim, nas Seções VI, VII e VIII temos a análise de resultados, conclusões e trabalhos futuros.

II. Chamada de contribuições NIST

Ao final de 2016, devido às perspectivas futuras para o avanço na computação quântica, o NIST resolveu iniciar seu processo de padronização para algoritmos pós-quânticos. A chamada pública foi motivada por dois fatores: uma rápida evolução da computação quântica nos últimos anos e a possível dificuldade de transição dos os algoritmos atuais para os pós-quânticos, dada as arquiteturas novas bem distintas das atuais.

A. Níveis de Segurança NIST

Na chamada de propostas do processo de padronização realizado pelo NIST [5], foi estabelecido um critério para o nível de segurança dos algoritmos a serem submetidos conforme a tabela I.

Por ser um ramo ainda em desenvolvimento, não é possível determinar a complexidade total dos ataques possibilitados

Tabela I: Níveis de Segurança (Adaptado de [5])

Nível de segurança	Descrição
I	Equivalente a um cifrador simétrico de 128 bits
II	Equivalente a colisão de um hash de 256 bits
III	Equivalente a um cifrador simétrico de 192 bits
IV	Equivalente a colisão de um hash de 384 bits
V	Equivalente a um cifrador simétrico de 256 bits

pela computação quântica, ou a existência de vulnerabilidades novas. Como um critério mais concreto, foram estimados custos computacionais equivalentes aos algoritmos simétricos atuais como AES128 e SHA256. Apesar da comparação com algoritmos simétricos, os níveis de segurança também são válidos para o cenário de assinaturas que será o nosso caso de estudo.

A recomendação inicial do NIST foi a de concentrar as submissões nos níveis de segurança I, II e III, os quais seriam suficientemente seguros para o futuro próximo mas, se possível, que fossem fornecidos parâmetros com provas de segurança acima do nível III para garantir a segurança no longo prazo. Além da segurança, outros critérios também serão julgados como a viabilidade em protocolos atuais como TLS e, para o caso de assinaturas, a formalização de *Existential Unforgeability under Chosen Message Attack*.

B. Candidatos da segunda rodada

No momento da escrita deste artigo, temos na segunda rodada do processo de padronização NIST, nove algoritmos PQC para assinaturas digitais. Não entraremos em detalhes neste artigo sobre o funcionamento de cada proposta, mas estão indicadas suas características principais na Tabela II. Para detalhes do funcionamento de cada uma, é necessário consultar a documentação respectiva submetida ao processo do NIST.

Tabela II: Candidatos da segunda rodada NIST PQC

Proposta	Características	Premissa
Crystals Dilithium	Heurística *Fiat-Shamir with aborts* Problema do *LWE*[1] modular	Reticulados
Falcon	Estrutura de dados: *Falcon tree* Baseada no reticulado do *NTRU*	Reticulados
qTesla	Baseada em LWE[1] sobre aneis	Reticulados
GeMSS	Problemas *Hidden Field Equations*	Polinômios Multivariados
LuoV	Baseada no problema do *UOV*[2]	Polinômios Multivariados
MQDSS	Problema *Multivariate Quadratic* Utiliza heurística de *Fiat-Shamir*	Polinômios Multivariados
Rainbow	Generalização do *UOV*[4] Camadas de sistema de equações	Polinômios Multivariados
Picnic	Baseada em *Zero Knowlegde Proof*	Funções hash e Primitivas simétricas
Sphincs+	Estruturas *WOTS+*[3]e *FORS*[4]	Funções hash

[1] *Learning With Errors*
[2] *Unbalanced Oil and Vinegar*
[3] *Winternitz one-time signature*
[4] *Forest Of Random Subsets*

III. Cenário de assinaturas em Internet das Coisas (*IoT - Internet of Things*)

Em um cenário de sistemas em Internet das Coisas, além da segurança, há uma grande preocupação com a dificuldade computacional de implementação da mesma. Devido às fortes restrições no processamento e capacidade de memória, há a necessidade do uso de algoritmos que economizem nos tamanhos ou tempos para assinatura e verificação a depender do que for mais crítico para a operação.

Um cenário muito característico em sistemas IoT consiste normalmente de diversos nós sensores / atuadores e um nó agregador central que realiza o processamento dos dados. Nesse cenário, tamanhos e tempos de assinatura são os fatores mais críticos pelo consumo de banda e pelas restrições de processamento dos sensores. Já chaves públicas e tempos de verificação são fatores menos críticos, já que pela natureza do ambiente, o nó central já estaria configurado com as chaves públicas ou só seria necessário o envio das chaves na primeira conexão. Além disso, o nó central possui um poder computacional maior do que os outros nós e, portanto, a exigência no processo de verificação pode ser mais alta. Este será nosso cenário base para discussão dos resultados obtidos.

IV. Premissas Criptográficas

Os algoritmos presentes na segunda rodada podem ser classificados em três categorias de primitivas criptográficas distintas:

- algoritmos baseados em reticulados;
- algoritmos baseados em polinômios multivariados;
- algoritmos baseados em hash ou primitivas simétricas.

Nelas, são explorados problemas matemáticos que são computacionalmente inviáveis de serem resolvidos mesmo com a presença de algoritmos quânticos conhecidos atualmente. Essas premissas são detalhadas em uma versão mais completa deste artigo submetido ao WTICG no SBSeg2020 com o nome de "Estudo comparativo de desempenho em Assinaturas Digitais Pós-Quânticas para plataformas de IoT" [4].

V. Avaliação de desempenho dos algoritmos da segunda rodada

Após estudar e entender as novas premissas criptográficas, buscamos avaliar o desempenho prático das propostas concorrendo a padronização NIST. Para tal, optamos pelo uso da biblioteca libOQS [7], que possui implementação dos principais algoritmos da segunda rodada e um conjunto de testes para medir a velocidade e tamanhos de chaves e assinaturas, o qual foi a base para os nossas discussões.

Apesar de facilitar o processo das medições de tempos, fornecendo um programa comum para os algoritmos implementados, o uso desta biblioteca possui algumas desvantagens, dentre elas: não implementar alguns dos candidatos do processo, ser uma biblioteca de uso geral, não específica para ambientes embarcados e não possuir testes para medição de tamanhos de chaves e assinaturas. As informações obtidas pelos testes do libOQS, são as especificadas nas respectivas

documentações dos algoritmos, e não os valores medidos na prática.

Antes da escolha dessa biblioteca para nossos testes, nossa primeira tentativa de estudo foi com o uso das implementações de referência submetidas ao NIST, já que gostaríamos de avaliar a performance dos algoritmos puros, sem a utilização de otimizações específicas, uma vez que este possivelmente seria o caso das plataformas em internet das coisas. Contudo, devido a heterogeneidade no formato das submissões, como o uso de algumas dependências externas, não foi possível a criação de um ambiente de testes comum a todas as submissões no período de nosso estudo.

A. *Ambiente de testes*

Como citado anteriormente, os testes foram realizados com o auxilio da libOQS em duas plataformas distintas. Os primeiros testes foram realizados com a seguinte configuração: Intel i7-8550U (1.8-4.0 GHz), 8 GB RAM, Arch Linux, libOQS (v0.4.0-dev) compilado com gcc (v10.1.0) e uso de funções auxiliares (AES, SHA-2 SHA-3) do OpenSSL (1.1.1g).

Os testes embarcados foram realizados em uma raspberry pi 3 B, com um processador ARM 64-bits, quad-core (1.2 GHz), 1 GB RAM, Raspbian (v8.0), com libOQS (v0.4.0) compilado sem optimizações de cpu (GCC 8.4.0), e sem funções do OpenSSL.

VI. Resultados

Os resultados do conjunto de testes da libOQS são mostrados a seguir. Os gráficos mostram a comparação dos algoritmos em seus diferentes níveis de segurança especificados pelo NIST. O teste é realizado medindo-se os tempos de assinatura para vetores aleatórios de 50 bytes. Alguns algoritmos estão ausentes nos gráficos da Raspberry por falta de implementação da própria biblioteca e no caso das medições no i7, o *Sphincs+* se encontra ausente pela falta de aprofundamento que tivemos durante nosso período de estudo, não conseguindo especificar os níveis de segurança dessa proposta para realizar uma comparação justa. Um ponto a ser destacado é que os gráficos estão em escala logarítmica dado que algoritmos de classes diferentes possuem resultados bem discrepantes.

De todos os parâmetros estudados, o tempo de geração de chaves é o menos relevante em nosso contexto dado o número de gerações muito inferior ao de assinaturas e verificações em um cenário IoT. Em nossos testes, observamos um ótimo desempenho no tempo de geração de chaves no Picnic, que se manteve abaixo dos 10 μs para testes no i7 e em torno dos 300 μs para raspberry em todos os níveis de segurança. Esse tempo reduzido muito possivelmente se dá ao uso de primitivas simétricas, facilitando sua geração. No outro espectro, vimos que o Rainbow possui os maiores tempos de geração, obtendo tempos entre 100 ms até a ordem de alguns segundos em seu último nível de segurança.

Além das medições de tempos de geração de chaves, outros parâmetros mais relevantes, como os tempos de assinatura e verificação, são mostrados nas Figuras 1 e 2. Ao comparar essas figuras, é possível observar que a maioria das propostas mantém consistentes seus tempos de assinatura e verificação, com a única exceção do Falcon, onde há uma assimetria. Essa assimetria nos tempos de assinatura e verificação pode ser útil em algumas situações onde a quantidade de assinaturas é muito inferior à de verificações como em aplicações cujo *payload* é de alto valor agregado. Para o nosso contexto, acreditamos que o desejável seja o oposto: menores tempos de assinatura com um possível *tradeoff* para a verificação. Isso considerando o cenário proposto na Seção III, onde há múltiplos nós assinando dados e apenas um nó central que os verifica.

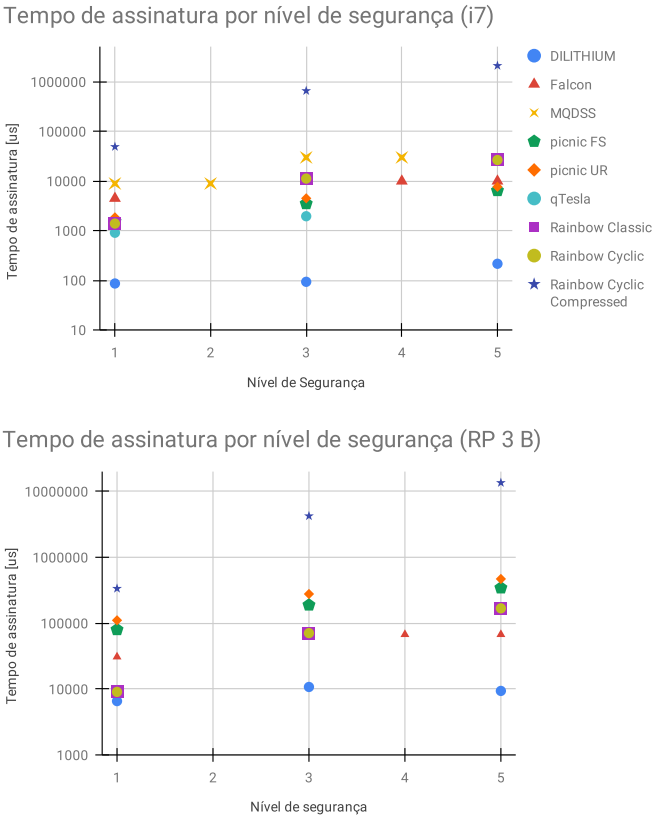

Figura 1: Menores tempos de assinatura em todos os níveis para DILITHIUM e maiores tempos para MQDSS, Falcon e Rainbow Cyclic Compressed

Vale destaque também para o algoritmo DILITHIUM que possui os menores tempos tanto para assinatura quanto para verificação. Ao mesmo tempo, vemos que os dois algoritmos multivariados presentes nos testes, são os mais lentos em ambas as categorias, o que pode ser crítico para determinadas aplicações em tempo real como por exemplo, em uma rede de sensores atrelado a um controlador de uma usina.

A partir das medições de tempos realizados no processador i7 e na rasberry pi, é possível traçar um gráfico da correlação entre eles para observar a relação entre a carga dos algoritmos e a diferença de tempo nas duas plataformas. Na Figura 3, temos a relação entre os tempos medidos em a escala *log-log*.

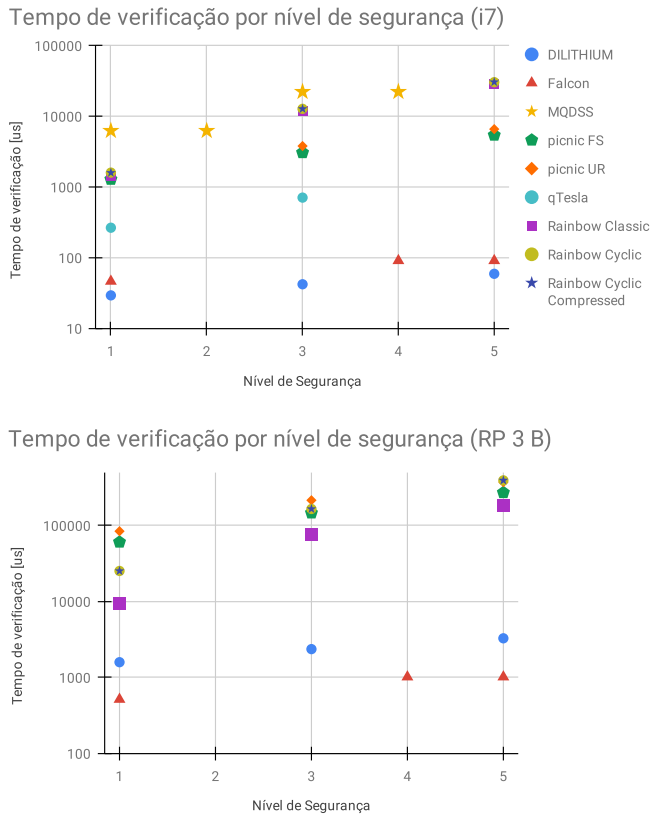

Figura 2: Menores tempos de verificação são dados pelo DILITHIUM e Falcon e maiores tempos pelo MQDSS, Rainbow e picnic (para o caso embarcado)

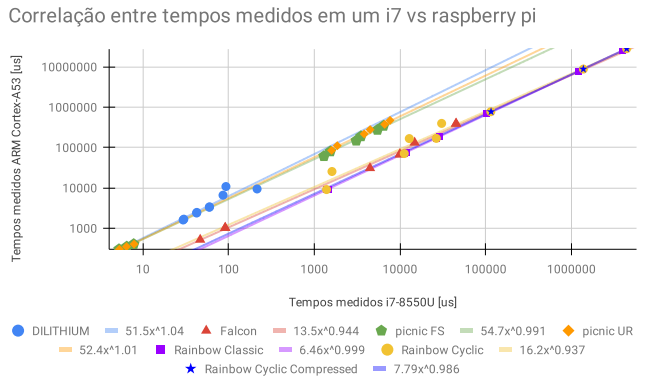

Figura 3: Regressão entre tempos medidos no i7 e na raspberry pi indicam uma característica quase linear, com expoentes variando em torno de um.

Na Figura 3 é possível observar a relação entre as medições nos dois ambientes, além das expressões para as curvas quase lineares que melhor aproximam os pontos de cada algoritmo. Os tempos mostrados nesse gráfico correspondem a todos os tempos medidos, ou seja, os tempos de geração, assinatura e verificação dos algoritmos implementados em ambos os ambientes, sempre considerando o mesmo nível de segurança.

Este gráfico traz alguns detalhes interessantes sobre os algoritmos pesquisados. Podemos constatar que para os algoritmos Falcon e Rainbow há uma redução de aproximadamente dez vezes na velocidade de execução quando trocamos o i7 pelo ARM mas, ao mesmo tempo, temos uma redução de quase cem vezes para os algoritmos Dilithium e Picnic. Isso mostra claramente outras limitações da plataforma restrita que vão além de sua frequência de clock mais baixa. Essa distinção possivelmente está relacionada com uma maior demanda de memória RAM por parte desses algoritmos e poderá ser estudada mais a fundo em trabalhos futuros que auxiliarão no entendimento das limitações em ambientes restritos quando comparados a um hardware mais robusto.

Duas últimas análises relevantes que podemos realizar são: a comparação entre as somas de tamanhos de chaves públicas e assinaturas e a comparação entre o tamanho de assinaturas e o tempo necessário para assinar.

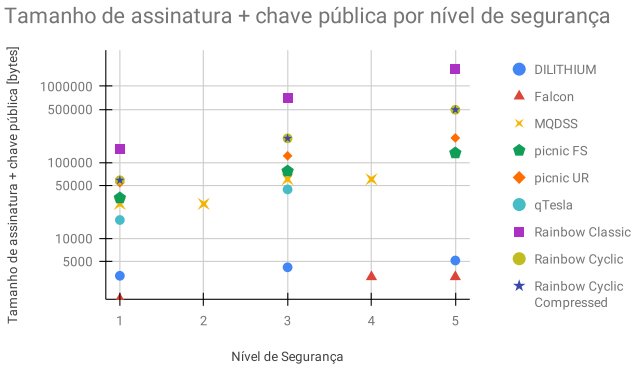

Figura 4: O Rainbow é custoso quando considerado o tamanho da chave pública junto a sua assinatura. Já o DILITHIUM e Falcon são os que possuem os menores tamanhos nessa métrica.

Pela Figura 4 é possível notar que, apesar do Rainbow possuir pequenas assinaturas em sua especificação, quando elas são somadas à sua chave pública ele se torna o pior nesta métrica. Contudo, como comentado na Seção III, em nosso cenário de estudo há um nó agregador central que já estaria configurado previamente com os certificados dos outros nós, permitindo portanto, que o Rainbow ainda seja viável neste cenário. Em outros cenários IoT onde não exista um nó centralizador, ainda é possível que o envio do certificado não seja um fator tão prejudicial, visto que o envio do certificado seria necessário apenas no início do estabelecimento da primeira conexão em situações com redes estáticas, como normalmente são as redes de sensoreamento locais.

A última análise a ser feita é baseada na Figura 5, onde é possível estudar eventuais fontes de gargalos em sistemas distribuídos em rede como arquiteturas IoT, uma vez que, nestes cenários, estamos preocupados com *overheads* tanto em tamanho de pacote, quanto em taxas de transmissão.

Podemos observar a partir da Figura 5 que há dois grandes destaques no cenário de IoT. A depender do fator mais crítico para cada aplicação, podemos optar pelo uso do DILITHIUM em cenários onde o tempo de assinatura deve ser baixo, mas o tamanho das assinaturas é aceitável, ou optar pelo uso do Rainbow onde o tempo não é crítico, mas é necessário uma assinatura menor. Dentre os piores desempenhos, estão o desempenho do Picnic e do MQDSS, mostrando um forte contraste com seus destaques anteriores por terem chaves pública e privada pequenas.

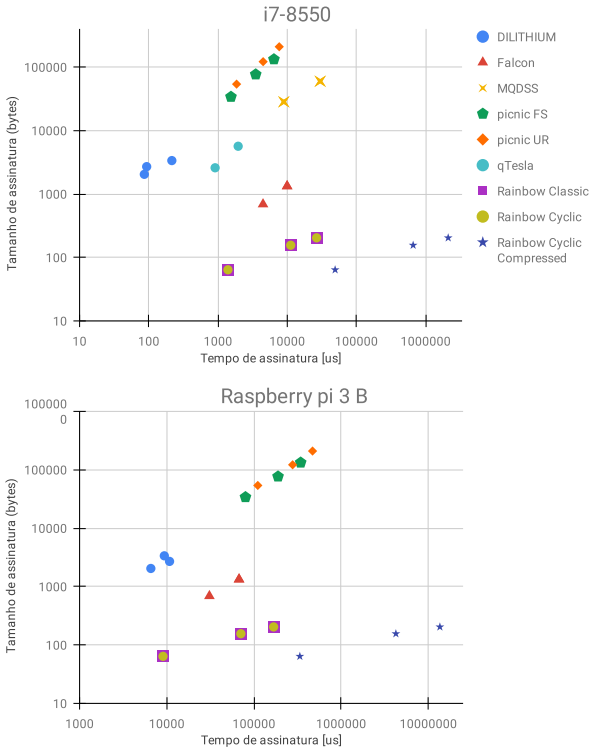

Figura 5: Em questão de gargalo para transmissão em redes, o DILITHIUM possui os melhores compromissos entre tamanho e tempo de assinatura. O Rainbow, por outro lado, possui as menores assinaturas, mas gastando um tempo considerável para criá-las.

VII. Observações finais

Pouco antes da finalização deste projeto de pesquisa, no dia (22/07/2020), foram publicados os candidatos escolhidos pelo NIST que avançaram para a terceira rodada do processo. Os escolhidos pelo NIST foram classificados em duas categorias: "finalistas" e "alternativos". A categoria "finalistas" corresponde aos que o NIST considera mais promissores e que possivelmente serão escolhidos como um dos padrões. Os finalistas estão: CRYSTALS-DILITHIUM, Falcon e Rainbow. Já os algoritmos "alternativos" são os algoritmos que ainda poderão ser padronizados, mas possivelmente não na terceira rodada. Nesta categoria, para assinatura digitais, constam: GeMSS, Picnic e SPHINCS+.

Nossa análise de desempenho também apontou o DILITHIUM e o Rainbow como opções promissoras para o cenário em estudo, especialmente dependendo da criticidade das aplicações. Dos algoritmos de assinaturas que ficaram fora da terceira rodada, temos: LUOV, MQDSS, qTESLA, já que em todos foram achadas falhas de segurança críticas.

VIII. Conclusão e Trabalhos futuros

Neste artigo apresentamos algumas das ideias por trás das novas premissas dos algoritmos criptográficos pós-quânticos para a realização de assinaturas digitais, bem como alguns testes de desempenho destes algoritmos em uma plataforma desktop (Intel i7) e em uma platafoma restrita (Raspberry pi 3).

Com o uso da biblioteca libOQS, comparamos o desempenho e os *tradeoffs* dos algoritmos de assinaturas implementados, com grande destaque para os tamanhos de chaves e tempos de assinaturas em reticulados, em especial do DILITHIUM. Para o cenário IoT, onde o envio de cadeias de certificados não costuma ser o padrão, vale destacar os tamanhos de assinaturas do Rainbow que, apesar de tempos e chaves maiores, pode possuir um espaço para aplicações IoT em certos cenários.

Em trabalhos futuros, pretendemos resolver algumas lacunas encontradas durante a realização deste trabalho, tais como o aprofundamento de algumas das propostas como Sphincs+ e Picnic, e a realização de testes e implementações em ambientes IoT completos para medição de performance em sistemas com condições mais próximas às reais, bem como com a presença de atrasos na rede e limitação de banda. Também serão buscadas formas de otimizar os códigos para ambientes IoT a fim de amenizar a queda de desempenho quando comparado a um ambiente desktop.

Agradecimentos: Agradeço o Programa Institucional de Bolsas de Iniciação Científica - PIBIC coordenado pela Universidade Estadual de Campinas - UNICAMP e financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq, processo número 124609/2019-8 pelo financiamento parcial desta pesquisa.

Referências

[1] Hyeongcheol An, Rakyong Choi, Jeeun Lee, and Kwangjo Kim. Performance evaluation of liboqs in open quantum safe project (part i). In *2018 Symposium on Cryptography and Information Security (SCIS 2018)*. IEICE Technical Committee on Information Security, 2018.

[2] Daniel J Bernstein and Tanja Lange. ebacs: Ecrypt benchmarking of cryptographic systems, 2019. URL: bench.cr.yp.to/, Acessado em 13/09/2020.

[3] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *International Workshop on Post-Quantum Cryptography*, pages 19–34. Springer, 2011.

[4] Vitor Nagata and Marco Aurelio Amaral Henriques. Estudo comparativo de desempenho em assinaturas digitais pós-quânticas para plataformas de iot. In *SBSeg 2020 - WTICG ()*, Virtual, oct 2020.

[5] NISTPQC. Submission requirements and evaluation criteria for the post-quantum cryptography standardization process. *https://csrc.nist.gov*, Dec 2016.

[6] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[7] Douglas Stebila and Michele Mosca. Post-quantum key exchange for the internet and the open quantum safe project. In *International Conference on Selected Areas in Cryptography*, pages 14–37. Springer, 2016.