Uma comparação de desempenho de algoritmos para criptografia pós-quântica

Pedro Rubbioli Amorim, Marco A. A. Henriques

Faculdade de Engenharia Elétrica e de Computação - Universidade Estadual de Campinas (UNICAMP) - Campinas, SP - Brasil

p204744@dac.unicamp.br, maah@unicamp.br

Abstract. *With the possible arrival of the first operational quantum computer that can break the security of traditional asymmetric cryptographic algorithms, entities that promote data security have been mobilizing themselves to offer a response to this advent. There are several proposals for a new standard of post-quantum cryptography, each one based on a different mathematical method. This work evaluates the main candidate proposals participating in the second round of NIST Post-Quantum Cryptography Standardization Process, showing their performance relative to each other. The aim of this paper is to help users make a more informed choice.*

Resumo. *Com a possível chegada do primeiro computador quântico operacional que poderá quebrar a segurança de algoritmos criptográficos assimétricos tradicionais, as entidades responsáveis por promover a segurança de dados têm se mobilizado a oferecer uma resposta para tal advento. Existem diversas propostas para um novo padrão de criptografia pós-quântica, cada uma baseada em um método matemático diferente. Este trabalho avalia as principais propostas que participam da segunda rodada do Processo de Padronização Criptográfica Pós-Quântica do NIST, apresentando as performances de umas em relação às outras. O objetivo deste artigo é ajudar usuários a fazer uma escolha mais informada.*

1. Introdução

Grande parte da comunicação digital atual faz uso de criptografia assimétrica para a proteção e integridade de seus dados e para garantir a autenticidade de suas origens. Sendo que, independente do esquema de criptografia tradicional empregado, tal segurança é assegurada pela dificuldade de computadores tradicionais executarem algoritmos eficientes para resolver um problema matemático em tempo computacionalmente viável [Paar e Pelzl 2009]. Tais problemas devem se espelhar às idealizadas funções de mão única, nas quais o cálculo da função num sentido é viável, mas no sentido oposto é inviável computacionalmente sem que se forneça algum parâmetro adicional. Por isso, elas possibilitam a cifração de dados com uma chave pública, mas não permitem a decifração de tal dado, a não ser com o auxílio de outro parâmetro: a chave privada correspondente.

Existem diferentes abordagens sobre qual problema matemático adotar como aproximação de uma função de mão única, tais como a fatoração de grandes números inteiros em seus fatores primos (RSA) [Rivest, Shamir e Adleman 1978] e a solução de

problemas de logaritmo discreto sobre curvas elípticas (ECC) [Koblitz 1987]. Tais abordagens são amplamente utilizadas atualmente, mas todas têm uma mesma fraqueza: são resolvidas rapidamente por um algoritmo de computação quântica conhecido como algoritmo de Shor [Shor 1994].

Uma vez que existem algoritmos quânticos capazes de solucionar problemas matemáticos da criptografia assimétrica tradicional, a segurança proporcionada por ela está com seus dias contados, pois depende apenas do surgimento do primeiro computador quântico com capacidade suficiente para lidar com os inteiros normalmente empregados, algo que parece estar cada vez mais próximo.

A solução para que toda a sociedade não tenha que abrir mão do mundo de possibilidades que a dinâmica de criptografia assimétrica lhe possibilita, é a troca dos problemas matemáticos tradicionais por outros, para os quais não se conhecem soluções implementáveis tanto em computadores tradicionais quanto quânticos. Estes problemas alternativos são a base para o que se passou a chamar de criptografia pós-quântica.

Dado o cenário descrito, somado aos esforços e avanços cada vez maiores no desenvolvimento da computação quântica, várias entidades da área de segurança de informações têm se mobilizado a fim de minimizar o impacto causado por esse grande avanço tecnológico. Dentre elas destaca-se o National Institute of Standards and Technology (NIST), dos Estados Unidos da América, que tem promovido debates e avaliações para seleção de novos padrões de algoritmos criptográficos de chave pública que sejam resistentes a ataques de computadores quânticos[1].

Neste contexto, o presente trabalho procura fazer uma ampla comparação entre os parâmetros de desempenho dos principais algoritmos de criptografia de chave pública pós-quânticos que estavam participando da segunda rodada de avaliações do NIST. A terceira rodada já foi iniciada, mas os dados aqui apresentados continuam válidos para auxiliar os potenciais usuários deste tipo de criptografia na escolha do algoritmo que melhor atenda suas necessidades.

2. Avaliação do NIST e suas propostas

O NIST tem, segundo sua própria página na web, como missão *"promover a inovação e competitividade industrial estadunidense [...] a fim de melhorar a segurança econômica e a qualidade de vida"*. Quando é considerado o espaço político que os EUA ocupam no mundo, é comum que as decisões adotadas pelo NIST impactem a forma como outros países definem seus próprios padrões, inclusive na área de segurança de informação.

O NIST já foi responsável por promover competições na área de segurança da informação, como as que elegeram o Keccak como o novo padrão de algoritmo de hash SHA-3 [Paar e Pelzl 2010] e o Rijndael como novo padrão de algoritmo de criptografia simétrica AES [Daemen e Rijmen 2002], e está realizando algo similar na área de criptografia pós-quântica, onde foram convidadas submissões de diversas implementações de criptografia assimétrica resistentes a ataques tradicionais e

[1] NIST (2020), Post-Quantum Cryptography PQC. Information Technology Laboratory Computer Security Resource Center. (disponível em: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography). Acesso em 31 de Julho de 2020.

quânticos a fim de padronizar um ou mais modelos [Chen 2016]. Esta avaliação é organizada em rodadas, as quais servem como peneira para as propostas, removendo as mais frágeis e devolvendo comentários, críticas e sugestões sobre o desempenho das restantes. No momento da realização desta edição do SBSeg a avaliação se encontra em sua terceira rodada.

O NIST incentivou que cada proposta de implementação apresentasse mais de uma configuração de parâmetros a fim de atender diferentes níveis de segurança que se baseiam na dificuldade de se quebrar a segurança de variantes do AES e do SHA-3. A Tabela 1 mostra esses níveis de segurança.

Tabela 1. Níveis de segurança para avaliação de algoritmos de criptografia pós-quânticos [2]

Nível	Descrição de Segurança
I	Tão difícil de quebrar quanto o AES128 (busca exaustiva)
II	Tão difícil de quebrar quanto o SHA256 (busca de colisão)
III	Tão difícil de quebrar quanto o AES192 (busca exaustiva)
IV	Tão difícil de quebrar quanto o SHA384 (busca de colisão)
V	Tão difícil de quebrar quanto o AES256 (busca exaustiva)

Considerando submissões tanto para assinaturas como para esquemas de cifração foram ao todo 69 submissões. Na segunda rodada, somente 17 propostas voltadas para a cifração de dados foram avaliadas. A maioria tem sua função de mão única sustentada por um dentre dois ramos da matemática: reticulados e códigos corretores de erros, mas há outros tipos de funções em análise também, como de criptografia isogênica.

3. Conceitos de Criptografia Pós-Quântica

No caso do RSA, a chave privada do usuário é protegida de inferência a partir da pública por um problema de fatoração de um grande número inteiro em seus fatores primos que, como já discutido, pode deixar de ser considerado um problema de difícil resolução com o surgimento do computador quântico de maior capacidade.

Criptografia pós-quântica também pode ser resumida à explicação de uma nova aproximação de função de mão única. Esta seção tem por objetivo explicar dois dos conceitos básicos por detrás de algumas das propostas. Ressalta-se que os algoritmos do [2]NIST não fazem uso exatamente das técnicas descritas a seguir, mas sim de versões otimizadas das mesmas, o que confere a cada proposta características que as diferem em questões de desempenho e eficiência.

[2] NIST (2016), Post-Quantum Cryptography Standardization: Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process, Computer Security Division, National Institute of Standards and Technology, EUA , 2016 (disponível em: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf). Acesso em 31 de Julho de 2020.

3.1. Criptografia baseada em reticulados

Um reticulado consiste em uma infinidade de pontos distribuídos em um espaço de n dimensões, de modo que seus pontos são gerados pelas possíveis combinações dentre um conjunto de vetores, denominados base do reticulado. Bases diferentes são capazes de dar origem aos mesmos reticulados. Uma base pode ser considerada boa ou ruim, a depender do tamanho e da ortogonalidade dentre os vetores que a compõem. Um conjunto de vetores pequenos e relativamente ortogonais compõem uma base considerada boa. Tanto vetores grandes quanto vetores não ortogonais são normalmente associados a bases ruins, já que exigem combinações complexas para produzir um mesmo reticulado.

Alguns problemas matemáticos podem ser propostos utilizando-se as estruturas de um reticulado. Um deles, o CVP (*closest vector problem*), propõe que se encontre, em um reticulado, o vetor pertencente a ele que seja o mais próximo a um outro vetor dado que não pertença a este reticulado. Em outras palavras, seria o problema de encontrar o melhor vetor do reticulado que representa um vetor fora deste.

Tal vetor dado pode ser originado por meio da multiplicação da base do reticulado por um vetor-externo originando um vetor-mensagem, seguido da adição de um pequeno vetor de ruído, a fim de retirar-se o resultado do conjunto de pontos pertencentes ao reticulado, transformando-o em um vetor-cifrado.

Uma das melhores maneiras de se resolver um CVP é por meio do algoritmo de Babai, o qual decompõe o vetor-cifrado (não pertencente ao reticulado) em uma composição dos vetores da base do reticulado, multiplicados por não inteiros. Em seguida o algoritmo aproxima esses multiplicadores não inteiros para os inteiros mais próximos e volta a multiplicar os vetores da base por esses números. O resultado será um vetor contido no reticulado que é a resposta do algoritmo para o CVP [Babai 1986]. Contudo, a efetividade do algoritmo de Babai está relacionada com a ortogonalidade dos vetores que compõem a base do reticulado; o algoritmo é eficiente somente para vetores ortogonais, ou seja para bases boas.

Um criptossistema que se baseia na teoria de reticulados, e é relativamente simples, é o GGH (Goldreich–Goldwasser–Halevi) [Goldreich, Goldwasser e Halevi 1997]. Ele elege como sua chave pública uma base ruim de um reticulado e como sua chave privada uma base boa para o mesmo reticulado, permitindo que qualquer vetor-mensagem se transforme em um vetor cifrado por meio de uma base, seja ela ruim ou boa. Entretanto apenas bases boas retornam vetores-mensagem corretos, pela utilização do algoritmo de Babai. A Fig. 1 ilustra (para duas dimensões) uma base boa (vermelha, com V1 e V2) e outra ruim (azul, com V1´ e V2´) que geram o mesmo reticulado de pontos, além de um exemplo de um vetor mensagem, m, e seu respectivo vetor-cifrado, m_enc, após a soma com um vetor de ruído r.

A maioria de propostas que implementam teorias de reticulados na utilização de criptografia, não faz uso direto do CVP, mas do chamado *learning with errors* (LWE) [Bernstein, Buchmann e Dahmn 2010]. Nele, a mensagem cifrada representa erros adicionados em um sistema de equações modulares (relacionado à chave pública), e para encontrar a mensagem original, faz-se uso da solução (relacionada à chave privada) do sistema. A função de mão única neste caso reside no fato que é fácil adicionar erros a

um sistema de equações modulares, mas encontrá-los é uma tarefa difícil. O LWE relaciona-se com a teoria de reticulados uma vez que o conjunto de equações modulares se assemelha a uma base e a tarefa de adicionar erros ao sistema equipara-se a deslocar o ponto-cifrado do reticulado em si.

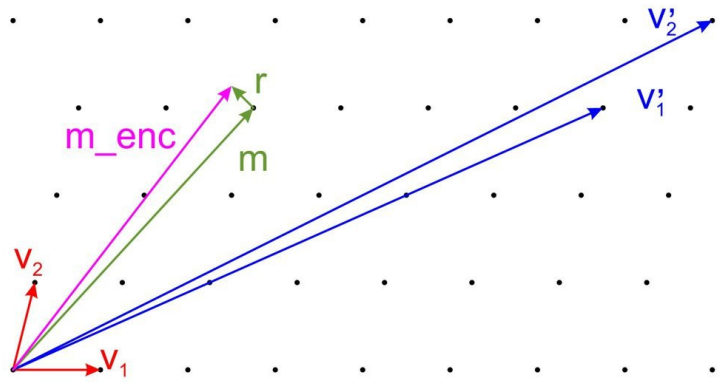


Fig. 1. Estruturas da criptografia de reticulados.

3.2. Criptografia Baseada em Códigos Corretores de Erro

Na teoria de códigos corretores de erros, um dos conceitos mais utilizados é a ampliação do tamanho de uma mensagem, a fim de conferir a possibilidade de detectar e corrigir erros na mensagem ampliada, caso ocorram durante sua transmissão. Detecções podem ocorrer de maneira simples, como pela adição de bits de paridade, e correções podem ser feitas pela simples repetição da mensagem ou usando decodificadores probabilísticos de canais.

Multiplicar o vetor-mensagem por uma matriz é outra maneira de expandir a mensagem a fim de nos possibilitar a correção de erros que podem ocorrer. Tal matriz, ou uma dual sua, pode ser utilizada em um código corretor de erros a fim de reaver a mensagem original. O quão fácil será a correção destes erros depende da complexidade da matriz escolhida. Matrizes que possibilitam uma fácil correção (boas), podem também ser transformadas em matrizes de difícil correção (ruins), quando multiplicadas por outras matrizes de embaralhamento. Entretanto obter a matriz boa a partir da ruim, sem o conhecimento das matrizes de embaralhamento, é tarefa difícil [Bernstein, Buchmann e Dahmn 2010].

Reside aí a viabilidade de códigos corretores de erros para a criptografia. Por meio da multiplicação, uma matriz ruim pode conferir a um vetor-mensagem a capacidade de ser corrigido, posteriormente, de erros que são adicionados à mensagem expandida, proveniente de tal multiplicação. Entretanto, a correção de tais erros apenas é possível a partir da utilização de uma matriz dual boa em um código corretor de erros. Relacionar, portanto, matrizes de difícil correção a chaves públicas e matrizes de fácil correção a chaves privadas é o cerne da criptografia baseada em códigos corretores de erros.

4. A biblioteca LIBOQS

O Projeto Open Quantum Safe (OQS) tem como seu objetivo principal "*oferecer suporte ao desenvolvimento e prototipagem da criptografia pós-quântica*", de acordo com sua página na web, e sua equipe disponibiliza e mantém uma biblioteca *open*

source em C, denominada LIBOQS [Stebila e Mosca 2016], que implementa algoritmos de criptografia pós-quântica presentes na avaliação promovida pelo NIST, e também disponibiliza a integração desta mesma biblioteca em um fork do OpenSSL.

A integração da LIBOQS com o OpenSSL permite executar (para diferentes níveis de segurança) uma comparação entre diversas propostas presentes na avaliação do NIST nas métricas de: velocidade de geração de pares de chaves e velocidades de cifração e decifração. Por outro lado, a utilização da biblioteca sem a integração com o OpenSSL permite que se extraia ainda mais dados de comparação dentre as propostas além das métricas acima: tamanhos de chave pública, de chave privada e de texto cifrado.

Durante este trabalho fizemos uso da biblioteca em suas duas formas, e para fins de divulgação, optamos por disponibilizar os resultados e discussões referentes aos testes da biblioteca não integrada ao OpenSSL, uma vez que a sua gama de métricas é maior e já que os resultados obtidos em ambas abordagens são praticamente idênticos e com diferenças desprezíveis.

As principais propostas de cifração, baseadas em teoria de códigos corretores de erros, participantes da segunda rodada da avaliação do NIST são: BIKE (códigos curtos de Hamming) e Classic McEliece (códigos Goppa). Enquanto as baseadas em reticulados são: CRYSTALS-KYBER (reticulados MLWE - Module Learning With Errors), FrodoKEM (reticulados LWE), NewHope (reticulados RLWE - Ring LWE), NTRU (reticulados NTRU), SABER (reticulados MLWR - Module Learning With Rounding) e ThreeBears (reticulados I-MLWE - Integer Module LWE) [Hamburg 2017]. Diversas destas premissas matemáticas estão detalhadas no trabalho de Barreto et al. [Barreto 2013]. Já a proposta SIKE tem seu sistema criptográfico baseado em grafos de isogenia supersingulares [Jao 2020], também resistente a ataques quânticos. Em 22/07/2020 o NIST publicou o resultado da segunda rodada de avaliação, no qual classifica como finalistas para a terceira rodada da avaliação os algoritmos Classic McEliece, CRYSTALS-KYBER, NTRU e SABER e coloca como candidatos alternativos os algoritmos BIKE, FrodoKEM, HQC, NTRU Prime e SIKE. Candidatos finalistas estão propensos a serem padronizados no final da terceira rodada enquanto que candidatos alternativos são passíveis de serem padronizados em uma quarta rodada, voltados para casos mais específicos a depender da proposta.

5. Condições de testes com a biblioteca LIBOQS

Os testes executados compararam as propostas com seus parâmetros ajustados para o mesmo nível de segurança, sendo eles os níveis 1, 3 ou 5, uma vez que estes foram os níveis priorizados pelos concorrentes. Entretanto, nem todas as propostas apresentam parâmetros para estes três níveis de segurança. São os casos das propostas BIKE, que não apresenta parâmetros para a segurança nível 5, e NewHope, que não apresenta parâmetros para o nível 3.

Comparando os desempenhos das propostas entre os diferentes níveis de segurança, notamos uma constância na diferença entre as propostas em todas as métricas. Isto é, um algoritmo que desempenha melhor que um outro em uma métrica no nível de segurança 1, mantém esse desempenho melhor, na mesma métrica, nos níveis 3 e 5. Isso se mostra útil, para estimarmos o desempenho de propostas que não apresentam parâmetros estabelecidos para todos os níveis de segurança, como é o caso de BIKE e NewHope.

Atentamos, também, para algumas especificidades de certas propostas, como o fato da proposta BIKE não ter segurança IND-CCA, isto é, não ser segura contra ataques de texto cifrado escolhido, e o caso da proposta SIKE apresentar duas implementações: uma original e outra denominada "*compressed*", voltada para a utilização em dispositivos IoT com pouca memória disponível.

Com exceção das propostas SIKE, SIKE-*compressed* e FrodoKEM, em todos os testes de cifração e decifração, atuou-se sobre um segredo de 32 bytes, representando assim o encapsulamento e desencapsulamento, respectivamente, de uma chave simétrica de 256 bits. Devido a definições internas da biblioteca LIBOQS, as exceções citadas neste parágrafo, agiram em processos de cifragem e decifragem sobre segredos de 16 bytes cada, comprometendo um pouco as comparações, já que as demais cifram um segredo de 32 bytes.

Os testes foram realizados em uma máquina Intel Core i7-6700HQ CPU @ 2.60ghz, com 16 GB de RAM e UBUNTU 18.04.2. Nela instalou-se uma máquina virtual VirtualBox versão 6.0.14, com um 4 CPUs dedicadas e 8192 MB de RAM. Apesar da utilização de máquinas virtuais impactar no desempenho dos algoritmos, o interesse deste trabalho reside na comparação relativa das propostas entre si e, ao executar os testes de todas no mesmo ambiente, esse objetivo está assegurado. Além disso, julgou-se interessante a execução de tais testes em um ambiente não físico separado para facilitar o gerenciamento dos mesmos e já que a utilização de máquinas virtuais é cada vez mais comum, tendo os constantes desenvolvimentos destas máquinas reduzido significativamente a diferença de desempenho das mesmas com máquinas reais.

6. Resultados e discussões

Com o objetivo de agregar mais informação às análises, adotamos os gráficos de círculo para a exposição dos resultados. Estes gráficos nos permitem analisar três métricas em duas dimensões, ao relacionar duas métricas com os eixos cartesianos e a terceira métrica com a área do círculo.

Cada métrica obtida nos permite analisar qual o impacto que cada implementação tem sobre o processo de comunicação criptografada. As métricas de tamanhos de chaves públicas e privadas nos informam a respeito da memória a ser consumida para guardar as chaves. A métrica de tamanho de texto cifrado nos informa a respeito do impacto que cada proposta apresenta sobre o tráfego de rede. Por fim, as métricas de velocidade de geração de chaves, de encapsulamento e desencapsulamento nos permitem analisar o consumo de processamento para tais atividades. Alguns gráficos têm seus eixos em escalas logarítmicas, entretanto as áreas dos círculos seguem sempre uma escala linear. A intenção é que os gráficos em escala logarítmica apresentem o cenário geral e que os em escala linear foquem na região com as propostas mais competitivas para facilitar o entendimento e enriquecer a análise. Para obter-se os valores exatos relacionados às áreas dos círculos o leitor pode recorrer a outros gráficos deste mesmo artigo, uma vez que uma métrica relacionada às áreas em um gráfico está atrelada a um eixo cartesiano em outro.

Devido a restrições de espaço, optou-se por apresentar os resultados obtidos para o nível 1 de segurança, mas como citado anteriormente constatou-se uma constância na diferença de performance dentre as propostas em diferentes níveis, de modo que uma

análise realizada sobre resultados do nível 1 é útil para estimar as diferenças de performances nos demais níveis.

Adicionou-se aos gráficos os resultados obtidos, na mesma máquina, métricas e condições, de testes com o algoritmo RSA da biblioteca OpenSSL a fim de comparar as propostas pós-quânticas com o mesmo. Para atender o nível de segurança 1 o tamanho escolhido para as chaves RSA foi de 3072 bits [Chandel 2019].

A primeira discussão dos resultados apresenta uma análise sobre os impactos das propostas do ponto de vista do lado que cifra as mensagens. Para tanto, foram eleitas as métricas de tamanho de texto cifrado, tamanho de chaves públicas e velocidade de encapsulamento. A Fig. 2, apresenta os resultados obtidos.

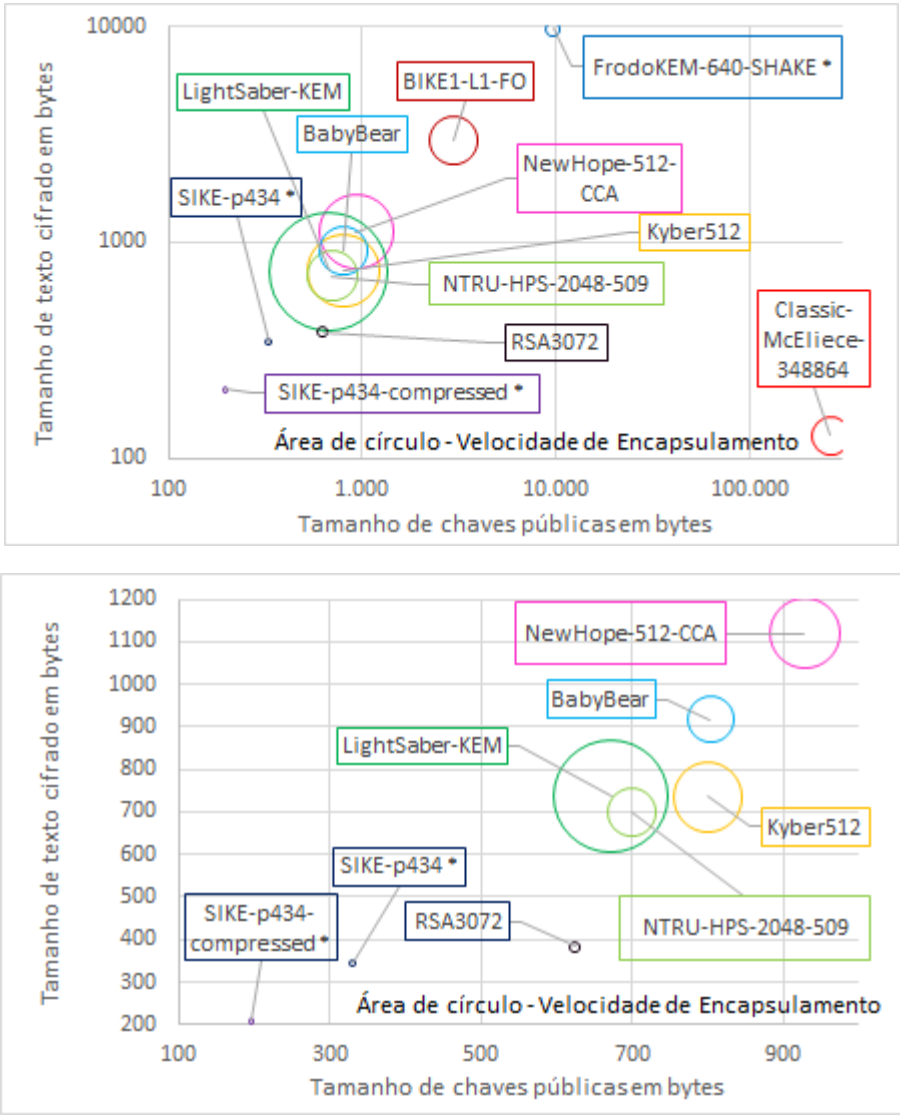


Fig. 2. SABER, NTRU e as implementações de SIKE apresentam os menores tamanhos de chave pública e texto cifrado. SABER se destaca em velocidade de encapsulamento.

Observando que as métricas de tamanho de arquivos encontram-se nos eixos, e a área dos círculos se refere à velocidade de encapsulamento, uma boa proposta deveria

ter seu círculo próximo da origem e com um raio grande. Ganham destaque nesta análise a propostas SABER e NTRU, que se mostraram mais equilibradas. As implementações da proposta SIKE, ganham destaque nas métricas de tamanhos tanto da chave pública e do texto cifrado, mas com a ressalva de um grande sacrifício na velocidade de encapsulamento, visto que é a mais lenta de todas as propostas nesta métrica.

A segunda discussão dos resultados apresenta uma análise sobre os impactos das propostas no ponto de vista do lado que decifra as mensagens. Para tanto, foram eleitas as métricas de tamanho de texto cifrado, tamanho de chaves privadas e velocidade de desencapsulamento. A Fig. 3, apresenta os resultados obtidos.

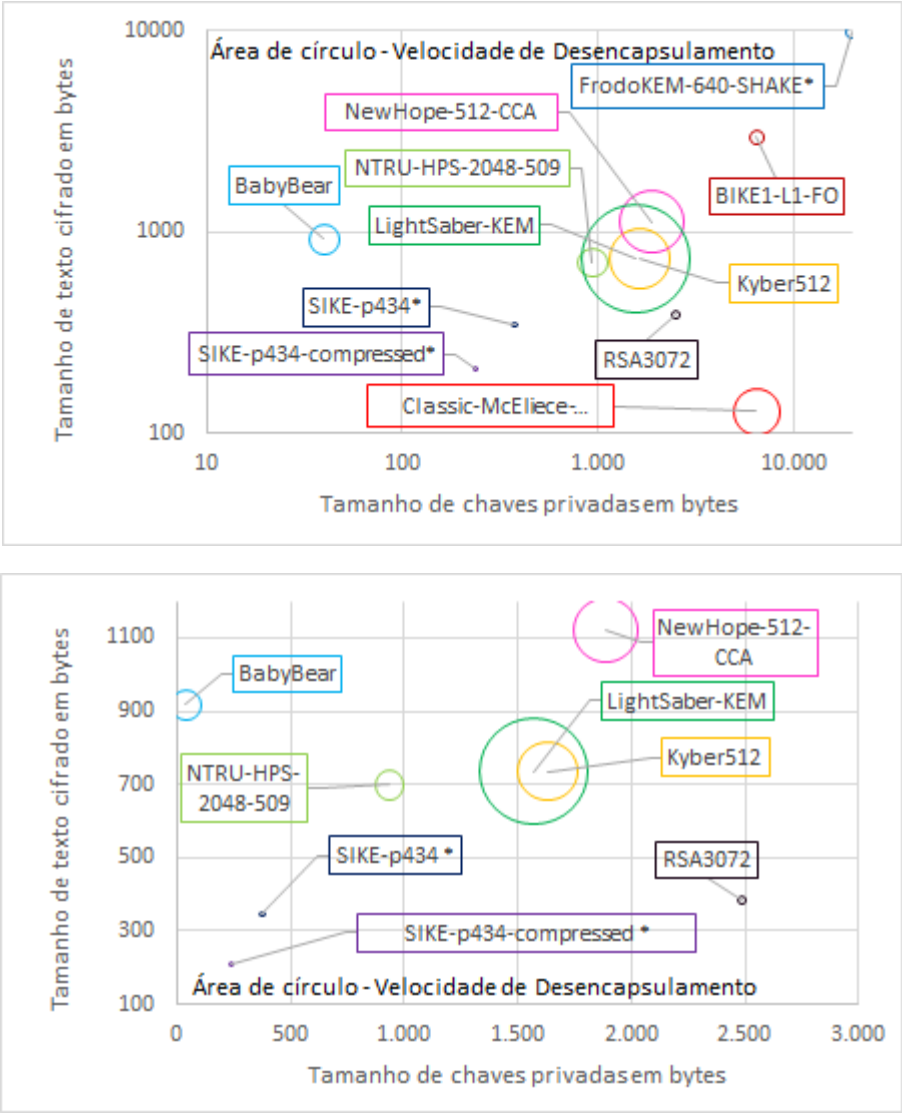


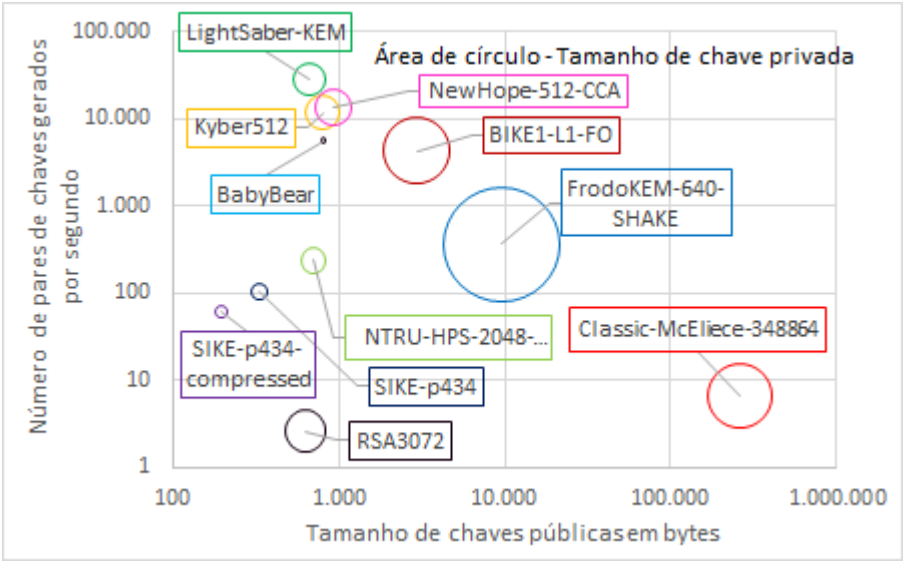
Fig. 3. ThreeBears, NTRU e as implementações de SIKE apresentam os menores tamanhos de chaves privadas e textos cifrado, mas SABER e Kyber oferecem um desempenho maior em desencapsulamento.

Ganham destaque nesta análise as propostas ThreeBears, SIKE e NTRU, que se mostraram as mais econômicas em termos de espaço de chave privada e texto cifrado. É interessante notar o tamanho reduzido da chave privada usada por ThreeBears e o bom

desempenho da proposta Classic McEliece nas métricas de tamanho de texto cifrado e velocidade de desencapsulamento, que podem ser mais relevantes que a métrica de tamanho de chave privada em algumas aplicações, uma vez que não é comum a posse de muitas chaves destas.

As implementações da proposta SIKE, ganham destaque nas métricas de tamanhos tanto da chave privada como do texto cifrado, mas novamente com a ressalva de uma perda significativa na velocidade de desencapsulamento, visto que é a mais lenta de todas as propostas nesta métrica.

A terceira discussão dos resultados apresenta uma análise sobre os impactos das propostas no ponto de vista de operações que envolvam a geração e o armazenamento do par de chaves. Para tanto, foram eleitas as métricas de velocidade de geração do par de chaves e tamanhos das chaves públicas e privadas. A Fig. 4 apresenta os resultados obtidos.



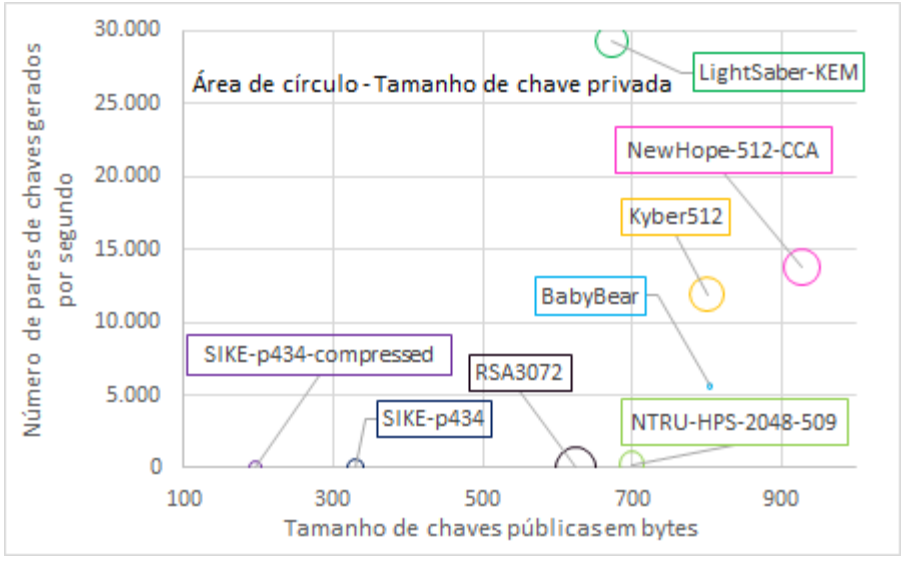


Fig. 4. Velocidade de SABER e Kyber ao gerar chaves se destacam, mas os tamanhos de chave e velocidade de ThreeBears não passam despercebidos.

A quarta discussão dos resultados apresenta uma análise sobre os impactos das propostas sobre uma visão geral da rede de comunicação. Para tanto, foram eleitas as métricas de velocidade de encapsulamento e desencapsulamento e tamanho de chaves públicas. A fim de priorizar a comparação das propostas que melhor desempenharam, excluímos os resultados das propostas Classic McEliece e FrodoKEM da exibição, uma vez que seus resultados foram muito discrepantes da média e, assim, dificultavam a visualização das outras propostas. Classic McEliece apresentou resultados medianos para a velocidade de desencapsulamento, mas pouco competitivos nas outras métricas, principalmente no tamanho de suas chaves públicas, que chegavam a 261 KB para esse nível de segurança. FrodoKEM apresentou resultados pouco competitivos em todas as métricas. A Fig. 5, apresenta os resultados obtidos.

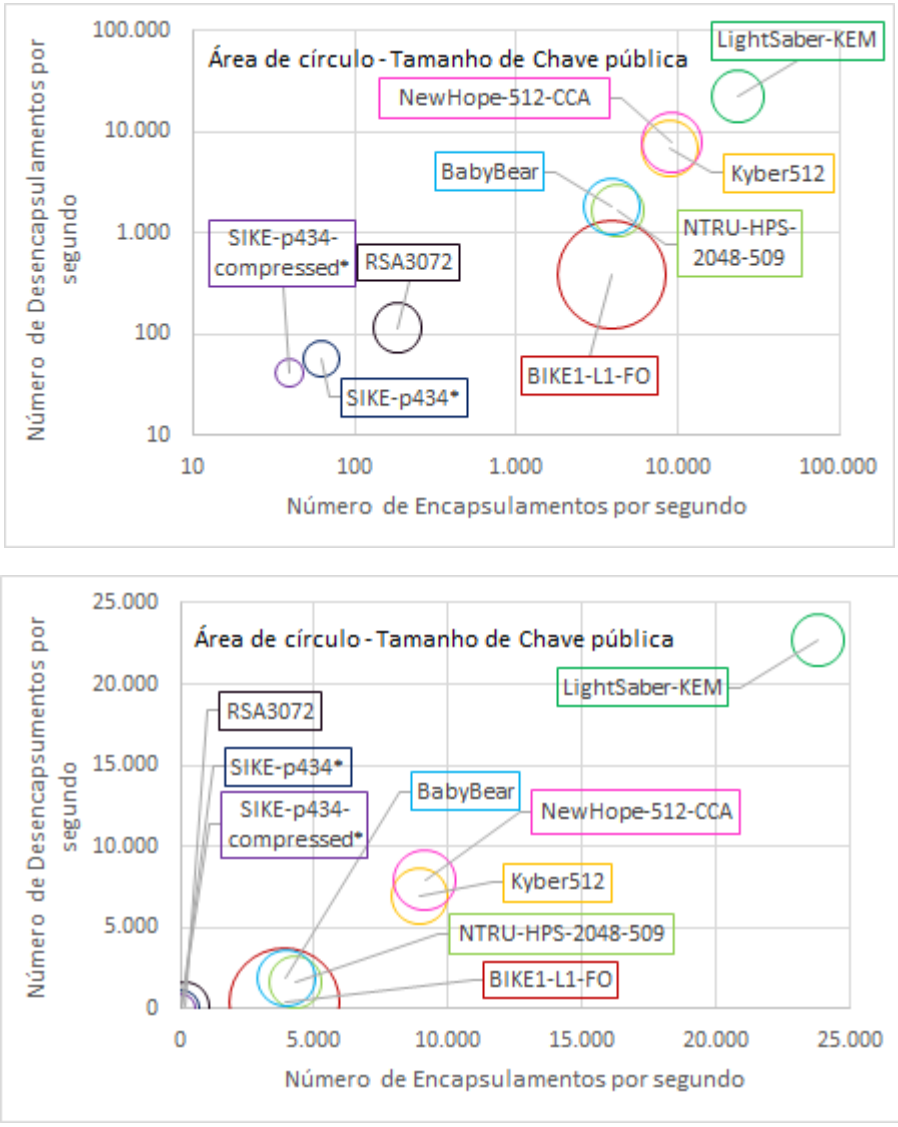


Fig. 5. SABER apresenta um desempenho bem superior aos demais algoritmos, sem, contudo, exigir uma chave pública acima da média.

Ganha destaque nesta análise a proposta SABER, que mostrou um desempenho acima dos demais e um tamanho de chave pública próximo da média.

A última discussão dos resultados apresenta outra análise sobre os impactos das propostas sobre uma visão geral da rede de comunicação. Para tanto, foram eleitas as métricas de velocidade de encapsulamento e de desencapsulamento e tamanho de texto cifrado. A Fig. 6, apresenta os resultados obtidos.

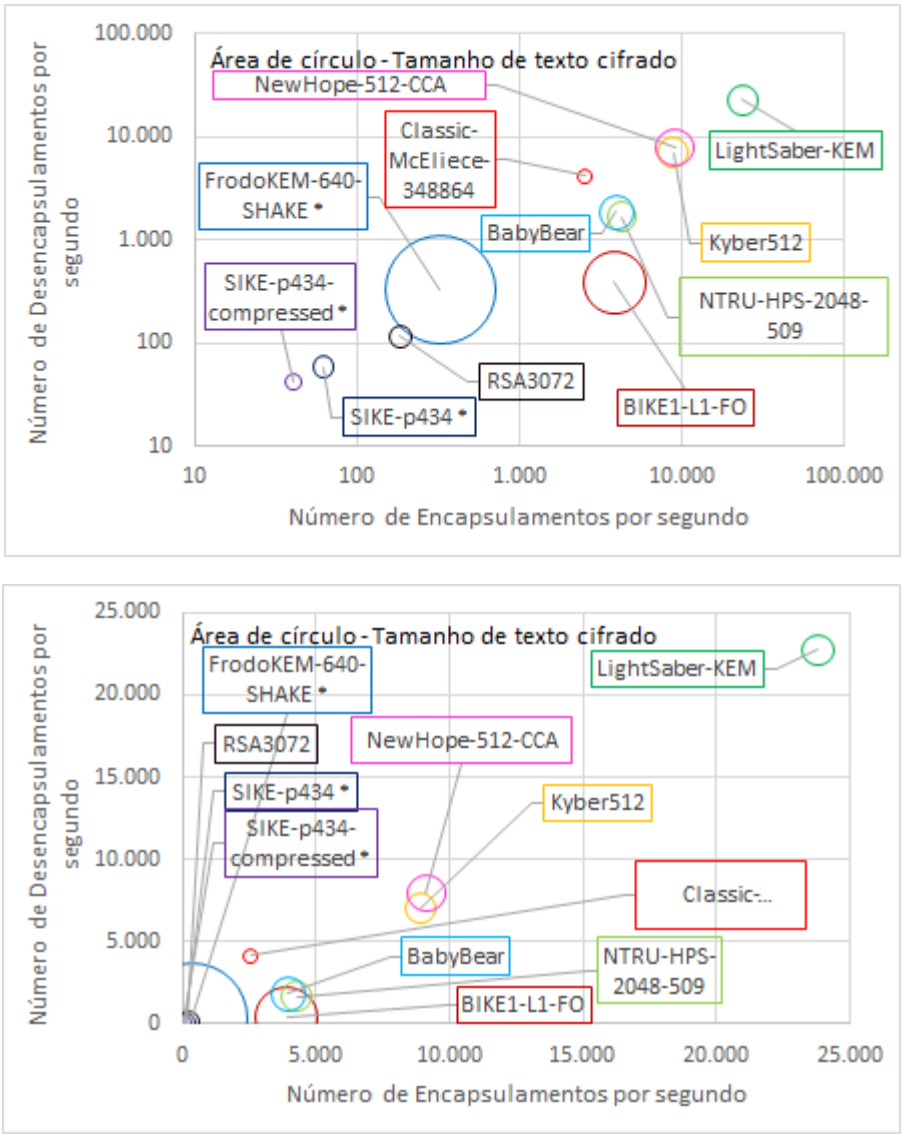


Fig. 6. SABER se destaca também em velocidade e produz um texto cifrado com tamanho próximo ao da média dos demais algoritmos.

Ganha destaque nesta análise a proposta SABER, que se mostrou a mais equilibrada das propostas nesta análise. Entretanto, para casos onde se busca arquivos cifrados menores em detrimento de melhores tempos de cifração e decifração, a proposta Classic McEliece se mostra uma alternativa interessante por apresentar os menores tamanhos de texto cifrado. Deve ser lembrado, contudo, que esta proposta apresenta chaves públicas 388 vezes maiores que as de SABER, não sendo recomendada para comunicações com restrições de memória para armazenamento de chaves públicas e certificados digitais.

7. Conclusões e trabalhos futuros

Pela análise dos resultados obtidos é possível notar que algumas propostas ocupam posições de destaque repetidamente e com métricas diferentes. É o caso da proposta SABER, que se mostrou como a alternativa mais equilibrada em todas as análises.

Entretanto, outras propostas também se mostram como fortes concorrentes à proposta SABER, de modo que, caso haja uma métrica preferida em detrimento de outras devido a especificidades da aplicação, tais propostas poderiam se mostrar como melhores opções. É o caso das propostas NTRU, que apresenta um balanço equilibrado como SABER, e das implementações de SIKE, que apresentam ótimas métricas de tamanhos de arquivos em detrimento das métricas de velocidades. Classic McEliece também mostrou-se como uma alternativa para certos casos em que o pequeno tamanho do texto cifrado é prioridade e os tamanhos grandes de sua chave pública e sua baixa velocidade de geração de pares não sejam empecilhos.

Ressaltamos que este trabalho almeja avaliar as diferenças de performance dentre as propostas, não avaliando por exemplo as premissas criptográficas adotadas pelas implementações. Algumas se baseiam em premissas conhecidas há mais tempo e que já foram mais estudadas e atacadas, provando assim a sua segurança. Um exemplo deste caso é Classic McEliece. O próprio NIST divulgou que, em sua peneira inicial, diferenças de desempenho não seriam tão decisivas na permanência de propostas na avaliação. Contudo, os resultados para a terceira rodada, com os algoritmos finalistas sendo Classic McEliece, Kyber, NTRU e SABER, mostraram que a avaliação começa a transitar para um campo de comparação de desempenho dentre as propostas, visto que as finalistas são propostas muito competitivas nas métricas aqui analisadas.

Destacamos também a relativa volatilidade da segurança criptográfica de novos algoritmos. Estudos e ataques são realizados constantemente a fim de se entender melhor a segurança e, por isso, propostas que se apresentam hoje como viáveis podem não ser amanhã.

Ao apresentar as diferenças relativas entre as métricas das principais propostas, este trabalho possibilita que usuários de criptografia pós-quântica possam analisar melhor tais propostas e escolher as que melhor atendam suas demandas em diferentes aplicações . Devido à decisão do NIST para a terceira rodada da avaliação, trabalhos futuros devem avaliar de forma mais aprofundada os desempenhos e diferenças entre as propostas Classic McEliece, CRYSTALS-KYBER, NTRU e SABER.

8. Agradecimentos

Ao Programa Institucional de Bolsas de Iniciação Científica (PIBIC) do CNPq, à Pró-Reitoria de Pesquisa da UNICAMP, à Faculdade de Engenharia Elétrica e de Computação (FEEC) - UNICAMP e a todos os membros do grupo de pesquisa ReGrAS (Research Group on Applied Security).

Referências

Barreto, P., et. al. (2013). Em Minicursos do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais — SBSeg 2013 Capítulo 2 Introdução à criptografia pós-quântica

Bernstein, D. J., Buchmann, J., & Dahmn, E. (2010). Post-quantum cryptography. Berlin: Springer.

Babai, L. On Lovász' lattice reduction and the nearest lattice point problem. Combinatorica 6, 1–13 (1986). https://doi.org/10.1007/BF02579403

Chandel S., Cao W., Sun Z., Yang J., Zhang B., Ni TY. (2020) A Multi-dimensional Adversary Analysis of RSA and ECC in Blockchain Encryption. In: Arai K., Bhatia R. (eds) Advances in Information and Communication. FICC 2019. Lecture Notes in Networks and Systems, vol 70. Springer, Cham. https://doi.org/10.1007/978-3-030-12385-7_67

Chen et. al. , Report on Post-Quantum Cryptography, Computer Security Division, National Institute of Standards and Technology, EUA, NISTIR 8105, 2016

Douglas Stebila, Michele Mosca. Post-quantum key exchange for the Internet and the Open Quantum Safe project. In Roberto Avanzi, Howard Heys, editors, Selected Areas in Cryptography (SAC) 2016, LNCS, vol. 10532, pp. 1–24. Springer, October 2017.

Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer. Belgium

Hamburg M., (2017). "Post-quantum cryptography proposal: ThreeBears." .

Jao D., Azarderakhsh R., Campagna M., Costello C., De Feo L., Hess B., Jalali A., Koziel B., LaMacchia B., Longa P., Naehrig M., Renes J., Soukharev V., and Urbanik D., (2017)."Supersingular Isogeny Key Encapsulation," Submission to the NIST Post-Quantum Standardization Project.

Goldreich O., Goldwasser S., Halevi S. (1997) Public-key cryptosystems from lattice reduction problems. In: Kaliski B.S. (eds) Advances in Cryptology — CRYPTO '97. CRYPTO 1997. Lecture Notes in Computer Science, vol 1294. Springer, Berlin, Heidelberg.

Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation 48:203–209

Paar, C., Pelzl, J. (2013). SHA-3 and The Hash Function Keccak An extension chapter for "Understanding Cryptography — A Textbook for Students and Practitioners" Springer.

Paar, C., Pelzl, J. (2009). Understanding Cryptography — A Textbook for Students and Practitioners. Springer.

Rivest R. L. , Shamir A., Adleman L. (1978). A method for obtaining digital signatures and public key cryptosystems, Commun. ACM 21

Shor P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA)