JOURNAL OF
EMERGING INVESTIGATORS

Article

A meta-analysis on NIST post-quantum cryptographic primitive finalists

Steven Benny[1], Ishaan Desai[2], Leah Uriarte[3], Isaac Tsai[4], Larry McMahan[5]

[1] Foothill High School, Pleasanton, California
[2] Monta Vista High School, Cupertino, California
[3] Lynbrook High School, San Jose, California
[4] Burlingame High School, Burlingame, California
[5] Computer Science & Engineering, ASDRP, Fremont, California

SUMMARY

The advent of quantum computing will pose a substantial threat to the security of classical cryptographic methods, which could become vulnerable to quantum-based attacks. In response to this impending challenge, the field of post-quantum cryptography has emerged, aiming to develop algorithms that can withstand the computational power of quantum computers. This study addressed the pressing concern of classical cryptographic methods becoming vulnerable to quantum-based attacks due to the rise of quantum computing. The emergence of post-quantum cryptography has led to the development of new resistant algorithms. Our research focused on four quantum-resistant algorithms endorsed by America's National Institute of Standards and Technology (NIST) in 2022: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+. This study evaluated the security, performance, and comparative attributes of the four algorithms, considering factors such as key size, encryption/decryption speed, and complexity. Comparative analyses against each other and existing quantum-resistant algorithms provided insights into the strengths and weaknesses of each program. This research explored potential applications and future directions in the realm of quantum-resistant cryptography. Our findings concluded that the NIST algorithms were substantially more effective and efficient compared to classical cryptographic algorithms. Ultimately, this work underscored the need to adapt cryptographic techniques in the face of advancing quantum computing capabilities, offering valuable insights for researchers and practitioners in the field. Implementing NIST-endorsed quantum-resistant algorithms substantially reduced the vulnerability of cryptographic systems to quantum-based attacks compared to classical cryptographic methods.

INTRODUCTION

The field of post-quantum cryptography (PQC) has emerged within computer science as a response to the formidable challenges presented by quantum computers to conventional cryptographic methods. Cryptography, the practice of securing communication and data through codes, relies on the computational difficulty of specific mathematical problems. Quantum computers, which leverage the principles of quantum mechanics to process information in ways that classical computers cannot, possess distinct problem-solving capabilities. These capabilities allow quantum computers to potentially compromise the security of prevalent classical encryption techniques like RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) (1).

In general, there are two main foundational structures for cryptography: lattice-based and hash-based signature schemes. Lattice-based signature schemes rely on the shortest vector problem (SVP) and the closest vector problem (CVP) (2). The SVP looks to find a nonzero vector in a lattice, which is defined as a mathematical structure composed of a set of elements that each have a unique upper and lower bound. Meanwhile, the CVP asks to find the closest lattice point to the target, given a particular lattice and a target point. While both problems are NP-hard, meaning they are computationally intensive and believed to be intractable to solve exactly in polynomial time, there are numerous algorithms used to find approximate answers to them (2). However, they still remain extremely challenging problems even for quantum computers to solve, making the SVP and CVP schemes fairly secure. Lattice-based signature schemes have many different advantages over traditional cryptographic methods, such as smaller key sizes (requiring less storage space), efficient signature verification and signing algorithms (faster processing times), and strong resistance to side-channel attacks (a method of exploiting the indirect effects of the system or its hardware). One major drawback that remains is that these security schemes are relatively new and have not been studied extensively, making it unclear how vulnerable they are to attacks compared with other schemes. Moreover, lattice-based signature schemes can be slower than other signature schemes, such as elliptic curve–based ones (3). Some common examples of lattice-based signature schemes are FALCON and CRYSTALS-Dilithium (4). FALCON is known for its compact signatures and high efficiency, making it suitable for applications requiring quick verification. Two common variants of FALCON are considered in this investigation. FALCON 512 and FALCON 1024 are both lattice-based cryptographic algorithms designed for digital signatures. FALCON 1024 offers higher security due to its larger polynomial degree, whereas FALCON 512 provides faster performance and smaller signature sizes, making it suitable for resource-constrained environments. In contrast, CRYSTALS-Dilithium offers strong security guarantees and robustness, even in environments with limited resources.

https://doi.org/10.59720/23-233

In contrast, hash-based signature schemes rely on the security of cryptographic hash functions. Hash functions are mathematical functions that convert some input data into a particular size output, called a hash. One real-life example of hash functions is online passwords. When you enter your password, the system compares its hash to a list of stored hashes to verify if the password is correct. Hash-based signature schemes are resistant to quantum attacks, meaning they are a good choice for post-quantum cryptography. The security of a hash-based signature scheme relies on its underlying hash function and is determined by its pre-image resistance, second pre-image resistance, and collision resistance. Pre-image resistance refers to how hard it is to find an input for some output in the hash space such that . The second pre-image resistance refers to how hard it is, given an input , a second input such that . Similar to the second pre-image resistance, collision resistance is a measure of how hard it is to find a pair of inputs such that . Although a preimage attack implies a collision attack, the reverse is not necessarily true. Hash-based signature schemes have a couple of advantages, such as fast signing and verification times, meaning they are instrumental in areas such as the stock market, where many financial transactions are made per second. However, they do have some limitations, such as larger signature sizes and a requirement for frequent vital updates. Also, a possible pitfall is if the hash function underlying the signature scheme is not built correctly, as this can lead to vulnerabilities such as collision attacks or preimage attacks, compromising the integrity of the signatures and potentially undermining the security of the entire system. A common example of a hash-based signature scheme is SPHINCS+, a stateless hash-based signature scheme known for its strong security guarantees and resistance against quantum attacks. It achieves these properties through the use of tree-based structures and hash functions, making it suitable for various applications requiring robust digital signatures (5).

Recognizing this imminent threat, the U.S. National Institute of Standards and Technology (NIST) initiated a standardization process in 2016 to address the vulnerability of current cryptographic systems in the face of quantum computing (6). In a collaborative effort with the cryptographic community, NIST called for algorithm submissions with the aim of identifying and establishing quantum-resistant algorithms capable of becoming industry standards for safeguarding data transmissions. As such, the central objective of this research was to comprehensively evaluate and compare CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+. These evaluations encompassed the algorithms' overall resilience against quantum attacks, their efficiency, and their adaptability across diverse applications. In response to the urgent need for secure cryptographic solutions, our research specifically aimed to identify and establish the most resilient and efficient post-quantum cryptographic algorithm. We hypothesized that a thorough evaluation and comparison of lattice-based and hash-based signature schemes would provide evidence supporting the superiority of post-quantum cryptographic algorithms and potentially lead to the identification of a quantum-resistant algorithm that can serve as an industry standard for safeguarding data transmissions in the face of advancing quantum technologies. The successful achievement of this objective will address the urgent need for secure cryptographic solutions and provide actionable guidance to policymakers, industry professionals, and researchers, thereby contributing substantially to enhancing digital security in the modern era.

In line with our hypothesis, our findings revealed that both lattice-based and hash-based signature schemes exhibited promising attributes in terms of resilience against quantum attacks. The comparative analysis highlighted the strengths and weaknesses of each approach, shedding light on their efficiency and adaptability across diverse applications. Importantly, our investigation showed the imperative nature of post-quantum cryptographic algorithms in the modern era, emphasizing their potential to outperform classical cryptographic algorithms.

RESULTS

We conducted a comprehensive meta-analysis focusing on post-quantum cryptographic primitives or fundamental cryptographic algorithms, particularly the NIST PQC finalists. Our meta-analysis focused on evaluating the performance and security of NIST-endorsed quantum-resistant algorithms, namely CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+. Our results intended to prove the superiority of post-quantum cryptographic algorithms.

In the realm of cryptographic algorithms, the efficiency of various schemes plays a pivotal role in determining their practical applicability. In our analysis of the four prominent PQC algorithms—CRYSTALS-Dilithium, CRYSTALS-Kyber, SPHINCS+, and FALCON—distinct patterns emerged when considering the ratios of public key size (the length of the data a receiver uses to verify your message) and private key size (the length of the data you keep secret to decrypt messages) to encryption time (the amount of time it takes to encrypt a message). (**Figures 1 & 2**) CRYSTALS-Dilithium stood out as the most efficient in terms of the public key size to encryption time ratio, displaying the smallest footprint and fastest encryption time. This makes it ideal for applications where quick data verification is essential, such as secure online communications or real-time data processing. SPHINCS+ followed closely, showcasing a good balance between key size and encryption speed, making it suitable for scenarios

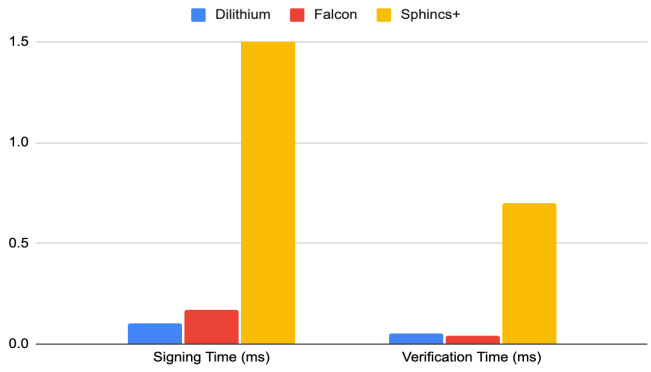

Figure 1: Ratio of Public Key Size and Encryption Time for the CRYSTALS-Dilithium, FALCON-512, FALCON-1024, and SPHINCS+ cryptographic algorithms. This figure presents the ratio of public key size to encryption time for four prominent post-quantum cryptographic algorithms: CRYSTALS-Dilithium, FALCON-512, FALCON-1024, and SPHINCS+. The public key size is measured in bytes, while the encryption time is measured in milliseconds (ms).

https://doi.org/10.59720/23-233

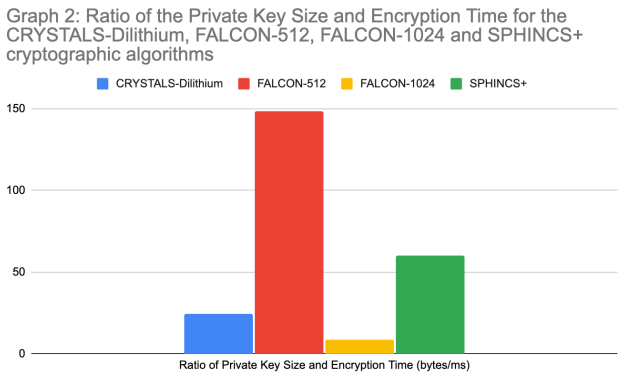

Figure 2: Ratio of the Private Key Size and Encryption Time for the CRYSTALS-Dilithium, FALCON-512, FALCON-1024, and SPHINCS+ cryptographic algorithms. This figure illustrates the ratio of private key size to encryption time for four leading post-quantum cryptographic algorithms: CRYSTALS-Dilithium, FALCON-512, FALCON-1024, and SPHINCS+. The private key size is measured in kilobytes (kB), and the encryption time is measured in milliseconds (ms).

where both security and performance are important, such as in financial transactions or secure messaging apps. **(Figure 1)**. When evaluating the private key size to encryption time ratio, FALCON 1024 claimed the top spot, indicating superior efficiency in scenarios where minimizing the private key size is crucial. This could be beneficial in environments with limited storage capacity or devices that prioritize security, like smart cards or IoT devices. CRYSTALS-Dilithium continued to demonstrate its prowess by securing the second position, making it a versatile option for both public and private key efficiency. SPHINCS+ ranked third, followed by FALCON 512 in fourth place. These algorithms balance security and efficiency, making them suitable for applications where both are needed but storage or speed is less of a constraint. Notably, CRYSTALS-Kyber was the only algorithm among the finalists that functions as a key encapsulation mechanism (KEM), which is intended for secure key transmission. The other three were digital signature schemes, which verify the authenticity of transmitted messages. Therefore, CRYSTALS-Kyber was not able to be compared with the other three finalists in this regard. This diversity emphasizes the need for standardization to facilitate accurate algorithm comparisons.

Critical determinants of algorithm efficiency also included overall key size and implementation complexity. Key size, which influences security and computational overhead, varied among the NIST PQC finalists (18). CRYSTALS-Dilithium's modest key size suited mobile devices and other resource-constrained environments, while CRYSTALS-Kyber struck a balance between security and performance (**Figure 3**). When compared to other KEM algorithms, such as NTRU (a lattice-based public key cryptosystem), CRYSTALS-Kyber had a higher total bandwidth and a lower cycle count, indicating its ability to process more data in a given time frame and its superior efficiency in resource usage (**Figures 4 & 5**). FALCON prioritized security, and SPHINCS+ emphasized security at the cost of efficiency (**Figure 3**). However, variations in performance metrics were observed due to differences in platforms, cryptographic libraries, and parameter configurations.

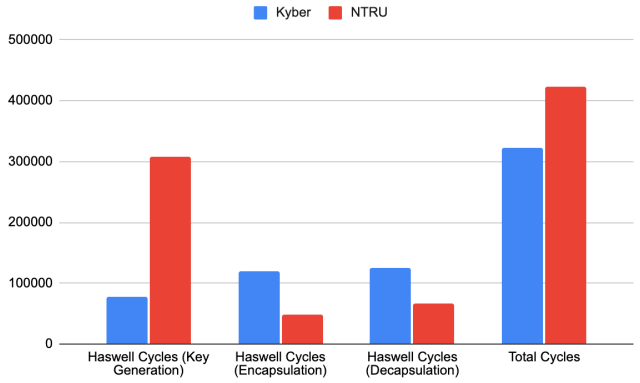

Figure 3: Bandwidth comparison of CRYSTALS-Dilithium, FALCON, and SPHINCS+ algorithms. This figure compares the bandwidth requirements of CRYSTALS-Dilithium, FALCON, and SPHINCS+ algorithms by showing the sizes of the ciphertext, private key, and public key for each algorithm at NIST security level 1. The sizes are measured in bytes.

DISCUSSION

Our meta-analysis aimed to assess the performance and security attributes of NIST PQC finalists, focusing on CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+. The primary hypothesis was that the implementation of these NIST-endorsed quantum-resistant algorithms would effectively enhance security against quantum-based attacks compared to classical cryptographic methods. The dominance of lattice-based schemes, particularly evident in CRYSTALS-Kyber and CRYSTALS-Dilithium, underscored their resilience and adaptability. Our results supported the hypothesis, revealing substantial resistance against quantum attacks among the NIST PQC finalists. The delicate balance between security and efficiency highlighted the importance of meticulous algorithm selection, with CRYSTALS-Dilithium standing out as the most efficient option for low-latency applications.

Our standardized evaluation methodologies played a crucial role in providing a unified understanding for

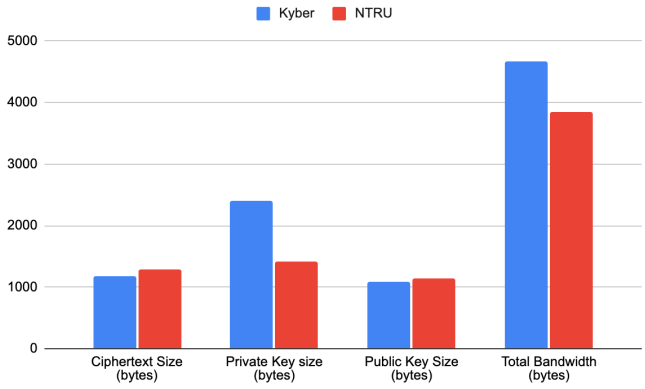

Figure 4: Bandwidth comparison of CRYSTALS-Kyber and NTRU algorithms. This figure presents a bandwidth comparison between CRYSTALS-Kyber and NTRU algorithms by showing the sizes of the ciphertext, private key, and public key for each algorithm at NIST security level 1. The sizes are measured in bytes.

https://doi.org/10.59720/23-233

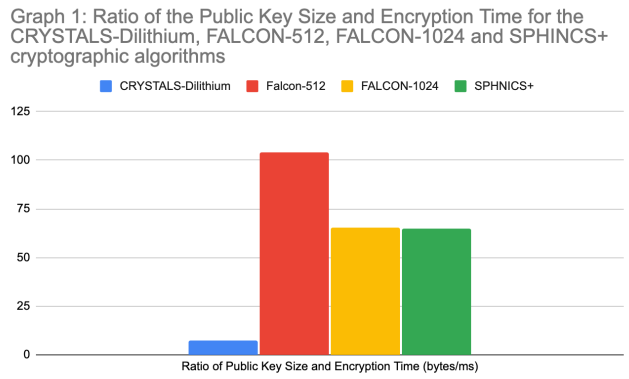

Figure 5: Cycle times of CRYSTALS-Kyber and NTRU key encapsulation algorithms. This figure compares the cycle times of CRYSTALS-Kyber and NTRU key encapsulation algorithms on a Haswell processor, specifically measuring the cycles required for key generation, encapsulation, and decapsulation at NIST security level 1.

practitioners, researchers, and policymakers. However, caution is necessary in interpreting results due to potential biases, study heterogeneity, and underlying assumptions. Quality variations in research studies, evolving dynamics in the field, and potential publication biases could impact conclusions drawn from the analysis. These variations contributed to the observed differences in performance metrics among the studies. The spectrum of capabilities exhibited by the NIST PQC finalists in performance assessments revealed distinct attributes defining their suitability in various contexts. CRYSTALS-Dilithium's compactness, CRYSTALS-Kyber's balance between security and efficiency, FALCON's emphasis on security, and SPHINCS+'s high security at the cost of speed highlighted the diversity of options available. These findings aligned with the hypothesis that the NIST-endorsed quantum-resistant algorithms provide a range of solutions catering to different application requirements. However, the absence of a unanimous "best" algorithm emphasizes the need for

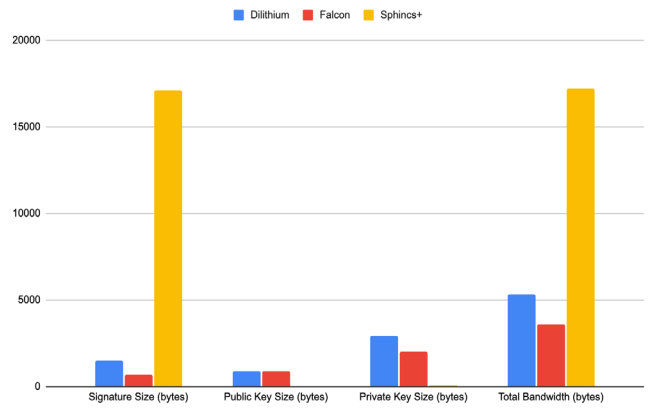

Figure 6: Speed of CRYSTALS-Dilithium, FALCON, and SPHINCS+ algorithms. This figure compares the signing and verification times of CRYSTALS-Dilithium, FALCON, and SPHINCS+ algorithms at NIST security level 1. The times are measured in milliseconds (ms).

continuous evaluation and refinement in the face of emerging threats and challenges. Lingering vulnerabilities, as indicated in our analysis, showed the necessity for proactive research to address evolving threats. The ongoing adaptability of NIST PQC finalists to various cryptographic scenarios showcased the comprehensive nature of current research efforts in the field.

In conclusion, our meta-analysis supported the hypothesis that the implementation of NIST-endorsed quantum-resistant algorithms enhances security against quantum-based attacks compared to classical cryptographic methods, as suggested by previous studies (18). The NIST PQC finalists, with their diverse strengths and limitations, provide valuable options for different cryptographic scenarios. Although our study did not directly compare these quantum-resistant algorithms to classical cryptographic algorithms, the findings align with existing research indicating that classical methods are vulnerable to quantum attacks. This highlights the importance of adopting post-quantum cryptographic solutions.

MATERIALS AND METHODS

Relevant peer-reviewed studies from 2016 to early 2023 were carefully curated for this meta-analysis. Selection criteria encompassed factors such as relevance to post-quantum cryptography and alignment with NIST's algorithm investigations. The quality of publications was determined based on their impact factor, the reputation of the publishing journal, the number of citations, and the rigor of the peer-review process. This focus on trusted sources increases the credibility of our findings. Academic databases, journals, conferences, and reputable online repositories were thoroughly searched using specific terms like "post-quantum cryptography," "quantum-resistant algorithms," and the names of NIST PQC finalists. The resulting collection of studies was refined through a systematic process, which involved removing duplicates, assessing title and abstract relevance, and performing a comprehensive full-text analysis. Primary sources were obtained from platforms such as IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, arXiv, and official NIST publications.

Pertinent information, including algorithm specifics, performance metrics, security analysis, implementation details, and use cases, was meticulously extracted from the finalized selection of studies. The security criteria used to measure the algorithms are as follows: resistance to Shor's algorithm, resistance to Grover's algorithm, resistance to side-channel attacks, and resistance to man-in-the-middle attacks. A coding schema was employed to systematically organize the gathered data. Notably, performance metrics and algorithm implementation details were coded to facilitate streamlined comparisons. Effect sizes were computed for performance metrics, providing a measurable foundation for comparing differences among PQC algorithms. To enhance clarity, visual representation was achieved through the construction of a forest plot. Additionally, a meta-regression analysis was conducted to explore potential sources of heterogeneity across the studies.

Received: September 09, 2023
Accepted: April 17, 2024
Published: September 21, 2024

https://doi.org/10.59720/23-233

REFERENCES

1. Mahto, Dindayal, and Dilip Kumar Yadav. "RSA and ECC: a comparative analysis." *International journal of applied engineering research* 12.19 (2017): 9053-9061.
2. "Shortest Vector Problem (SVP)." *UCSD CSE*,cseweb.ucsd.edu/~daniele/LatticeLinks/SVP.html
3. Davenport, Amanda, and Sachin Shetty. "Comparative analysis of elliptic curve and lattice based cryptography." *2021 Annual Modeling and Simulation Conference (ANNSIM)*. IEEE, 2021. DOI: 10.23919/ANNSIM52504.2021.9552144
4. Beckwith, Luke, Duc Tri Nguyen, and Kris Gaj. "Hardware Accelerators for Digital Signature Algorithms Dilithium and FALCON." *IEEE Design & Test* (2023). DOI: 10.1109/MDAT.2023.3305156
5. Aumasson, Jean-Philippe, et al. *Sphincs*. Stanford Univ., Tech. Rep, 2019.
6. "Post-Quantum Cryptography." *NIST Computer Security Resource Center*, csrc.nist.gov/projects/post-quantum-cryptography
7. Hülsing, Andreas, et al. "High-speed key encapsulation from NTRU." *International Conference on Cryptographic Hardware and Embedded Systems*. Cham: Springer International Publishing, vol. 10529, Aug. 2017.
8. Maram, Varun, and Keita Xagawa. "Post-quantum anonymity of Kyber." *IACR International Conference on Public-Key Cryptography*. Cham: Springer Nature Switzerland, 2023.
9. Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC press, 2018. doi.org/10.1201/9780429466335
10. Rieffel, Eleanor G., and Wolfgang H. Polak. *Quantum computing: A gentle introduction*. MIT press, 2011.
11. Fouque, Pierre-Alain, et al. "Falcon: Fast-Fourier lattice-based compact signatures over NTRU." *Submission to the NIST's post-quantum cryptography standardization process* 36.5 (2018): 1-75.
12. Schwabe, Peter, and James Mann. "Dilithium." *CRYSTALS*, 16 February 2021, pq-crystals.org/dilithium/index.shtml.
13. Schwabe, Peter, and James Mann. "Kyber." *CRYSTALS*, 23 December 2020, pq-crystals.org/kyber/index.shtml.
14. Avanzi, Roberto, et al. "CRYSTALS-Kyber algorithm specifications and supporting documentation." *NIST PQC Round* 2.4 (2019): 1-43.
15. Zeydan, Engin, et al. "Recent advances in post-quantum cryptography for networks: A survey." *2022 Seventh International Conference On Mobile And Secure Services (MobiSecServ)*. IEEE, 2022. DOI: 10.1109/MobiSecServ50855.2022.9727214
16. Ducas, Léo et al. "CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation." (2017).
17. Bernstein, Daniel J., and Tanja Lange. "Post-quantum cryptography." *Nature* 549.7671 (2017): 188-194. doi.org/10.1038/nature23461
18. Nejatollahi, Hamid, et al. "Post-quantum lattice-based cryptography implementations: A survey." *ACM Computing Surveys (CSUR)* 51.6 (2019): 1-41. doi.org/10.1145/3292548