Post-Quantum Cryptography for Big Data: A Comparative Performance Evaluation of NIST-Selected Post-Quantum Cryptographic Schemes

Arnab Ghosh

November 19, 2023

Abstract

Post-quantum cryptography has developed significantly in response to the acceleration of the possibility of a quantum computer capable of running Shor's algorithm, which theoretically may break the current state-of-the-art cryptographic standards based on RSA (factorization) and ECC (elliptic curve) cryptography. Currently, the projected cryptographic standard by the National Institute for Standards in Technology (NIST) has identified four lattice-based learning-with-errors cryptographic algorithms as the likely successors for a quantum-resistant cryptographic standard. However, LWE and Lattice-based cryptographic algorithms are known to be more memory inefficient than their state-of-the-art counterparts. This paper measures the comparative performance of the 4 NIST-selected post-quantum cryptographic algorithms: Dilithium, Kyber, Falcon, and SPHINCS to the current state-of-the-art in traditional cryptography using large encryption payloads and strict performance constraints.

1 Introduction

1.1 Modern Cryptography

Cryptography describes the study of creating systems for encoding or decoding data; since the advent of digital computation even in its most primitive forms, it has become a primarily computational discipline. Cryptography is among the most important modern disciplines for maintaining the massive digital infrastructure network of the modern world. Databases, passwords, authentication, secure communication, website usage, financial transactions, and more all rely on cryptography to secure and protect from malicious third parties.

Within cryptography, there exist many requirements for certain algorithms, each with unique use cases. Public-key cryptography, for example, describes the secure transmission of messages between two parties while guaranteeing security even if a third party has full knowledge of the exchange and may intercept the encrypted message. HTTPS, the primary protocol by which data on the internet is exchanged, relies on robust public-key cryptography to guarantee security versus standard HTTP. Hashing algorithms describe an algorithm that takes a given input and outputs a corresponding ciphertext. Effective hashing algorithms do

not allow third-parties to take a hashed message and derive the original input. As such, one needs not compare the direct plaintext of a message (which is vulnerable to interception), but rather the hash, which theoretically is useless to any intercepting third party. Hashing algorithms are essential parts of nearly every branch of cryptography, including authentication and the storage of passwords as well as the abstract implementation of secure and fast database systems such as the Log-Structured-Merge-Tree or the Bloom Filter.

1.2 RSA

RSA is a form of public-key encryption. Modern cryptography primarily relies on mathematical approaches, identifying a mathematical problem that is trivial with certain parameters given, but virtually impossible without. These are also called intractable problems.[1] The most commonly used state-of-the-art encryption scheme in use currently descends from Rivest-Shamir-Adleman (RSA), a cryptosystem created in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at the Massachusetts Institute of Technology. RSA relies on the difficulty of a certain mathematical problem within number theory, the branch of mathematics focusing on the study of numbers. More particularly, RSA uses the prime number factorization problem.

RSA is generally described in its vanilla form in Schneier's *Applied Cryptography* as follows,[2] beginning with key generation (λ is Caramichel's totient function):

$$\begin{gathered}\exists p, q \in \mathbb{P} \\ n \coloneqq pq \\ \exists e \in \mathbb{Z} \mid 2 < e < \lambda(n) \text{ and } \gcd(e, \lambda(n)) = 1 \\ d \coloneqq e^{-1} \bmod \lambda(n)\end{gathered}$$

Here, d is the private key and (n, e) is the public key. Usually, to guarantee security, p, q are chosen to be very large and far from each other. Now that a key is generated, both parties know the key. Define the public key as follows, where A is a set containing the message:

$$\begin{gathered}h : A \to \mathbb{Z} \\ m \coloneqq h(\text{message}) \mid 0 \leq m < n \\ \text{publickey} = (n, e) \\ c \coloneqq m^e \bmod n\end{gathered}$$

Where c is the encrypted ciphertext to be distributed. The message can be decrypted as follows:

$$c^d \equiv m^{e^d} \equiv m \bmod n$$

1. Kwok-Yan Lam et al., eds., *Cryptography and Computational Number Theory* [in en] (Basel: Birkhäuser, 2001), ISBN: 978-3-0348-9507-1 978-3-0348-8295-8, accessed September 22, 2023, https://doi.org/10.1007/978-3-0348-8295-8, https://link.springer.com/10.1007/978-3-0348-8295-8.

2. Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* [in English], 2nd edition (New York: Wiley, October 1996), ISBN: 978-0-471-11709-4.

Where the decrypting party knows the secret key, d. RSA in the form presented does contain certain vulnerabilities; however, a litany of security layers are added in modern implementations which guarantee that RSA is virtually secure via classical methods. Without the given secret key, it is extremely difficult to compute the message given purely the public key (which may be intercepted) and the ciphertext (which also may be intercepted).

1.3 Elliptic Curves

Elliptic Curve Cryptography (ECC) takes advantage of another intractable mathematical problem; namely, that of discrete logarithms.[3] Discrete logarithms are defined with the following, given a group G and generator $g \in G$ and element $h \in G$:[4]

$$\log_g(h) = x \iff \exists x \in \mathbb{Z} \mid g^x = h$$

While numerical methods exist when $x \in \mathbb{R}$, finding a given *integer* $x \in \mathbb{Z}$ is known to be an intractable problem. Elliptic curves can provide more security to the discrete logarithm problem by defining G as the group of all points in the elliptic curve, complexifying the requirements for a brute-force solution. ECC is often preferred over traditional RSA due to the smaller key size requirements while guaranteeing equivalent security standards. ECC is used most prominently for public-key encryption[5] and IoT security measures[6] for this reason.

1.4 Quantum Computing

Here, we make the distinction between Classical and Quantum computing models. Virtually all currently used digital infrastructure and the vast majority of developed applications run on classical computing models. Mathematically, classical computing models use binary bits to store and process data, where each bit stores a 0 or 1. Quantum Computing takes advantage of certain quantum mechanical properties, which emerged in the 1950s as an alternative to classical physics. The principal difference between quantum and classical computing models is data storage: rather than bits, quantum computers use qubits. Qubits also alternate between 0 and 1; however, due to the quantum mechanical property of superposition, a qubit may be both 0 and 1 simultaneously.[7] Various other quantum mechanical properties such as entanglement[8] have consequences for qubit measurement, allowing one to observe the state of many qubits at once due to their "linked" nature.

3. Schneier, *Applied Cryptography*.

4. Schneier.

5. Parwinder Kaur Dhillon and Sheetal Kalra, "Elliptic curve cryptography for real time embedded systems in IoT networks," in *2016 5th International Conference on Wireless Networks and Embedded Systems (WECON)* (October 2016), 1–6, https://doi.org/10.1109/WECON.2016.7993462.

6. Harsh Durga Tiwari and Jae Hyung Kim, "Novel Method for DNA-Based Elliptic Curve Cryptography for IoT Devices" [in en], *ETRI Journal* 40, no. 3 (2018): 396–409, ISSN: 2233-7326, accessed August 18, 2023, https://doi.org/10.4218/etrij.2017-0220, https://onlinelibrary.wiley.com/doi/abs/10.4218/etrij.2017-0220.

7. Ray LaPierre, *Introduction to Quantum Computing* [in en], The Materials Research Society Series (Cham: Springer International Publishing, 2021), ISBN: 978-3-030-69317-6 978-3-030-69318-3, accessed September 23, 2023, https://doi.org/10.1007/978-3-030-69318-3, https://link.springer.com/10.1007/978-3-030-69318-3.

8. Jeffrey Bub, "Quantum Entanglement and Information," Last Modified: 2023-05-02, August 2001, accessed September 23, 2023, https://seop.illc.uva.nl/entries/qt-entangle/.

Quantum computers are thus able to solve certain problems much more efficiently than classical computers due to the superposition of states on qubits and the parallel power afforded by entanglement. However, because quantum computers differ in such a fundamental manner from classical computing models, the array of problems that each can solve is limited. Quantum entanglement and superposition lead to multiple complexities when performing certain computations, as they are much more susceptible to noise and error. On classical computing models, measuring the position of a bit is a trivial operation. However, on quantum computing models, measuring the position of a qubit may be a tricky matter. While entanglement may allow for the optimization of certain tasks, it also complicates the behavior of others due to random behavior, which is unfortunately fundamental to quantum particles.[9] Additionally, the very act of measurement for quantum particles, including qubits, contains the possibility of changing the state and thus polluting the result.

1.5 Shor's Algorithm

Among the most early, and applicable, applications of quantum computing come from Shor's algorithm. Shor's algorithm describes a theoretical model for efficient polynomial-time (of order $O(\log n)$) of factorization into large prime numbers.[10] Further iterations and extrapolations of Shor's original algorithm have revealed that it may also be used to solve the discrete logarithm problem. The former two applications of the algorithm stand as a threat to most modern cryptography, which relies on the intractability of the discrete logarithm and factorization problem. The intractability of the aforementioned problems guarantees virtually complete security; however, given Shor's algorithm, one may theoretically solve each problem in a matter of days given a sufficiently powerful quantum computer. While the estimates for a quantum computer large enough to compute Shor's algorithm for realistically complex inputs to break encryption do estimate a generous time allocation before such possibilities, the development of quantum computing has grown exponentially (partially due to the desire to break RSA/Elliptic Curve Cryptography).

The primary purpose of Shor's algorithm is to solve the aforementioned factorization problem. Let us define it as follows: *Find the integer factors* (p_i, m) *of a composite integer* N. Note that m denotes the multiplicity of a given prime p_i in the prime factorization of N. Shor's algorithm aims to solve a slightly modified version of this problem which may be trivially extrapolated to the original:[11] *Find two nonzero integer factors* p, q *of* N. Shor's algorithm takes the approach of reducing this problem to the order-finding problem, and then solves the order-finding problem using a quantum algorithm. The order-finding problem is defined as follows:

$$\mathrm{ord}_a = r \iff a^r \equiv 1 \bmod N$$

To solve this problem, Shor's algorithm first picks a random $a \mid 1 < a < N$.[12] Using the

9. Bub, "Quantum Entanglement and Information."

10. Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," Publisher: Society for Industrial and Applied Mathematics, *SIAM J. Comput.* 26, no. 5 (October 1997): 1484–1509, ISSN: 0097-5397, accessed August 18, 2023, https://doi.org/10.1137/S0097539795293172, https://epubs.siam.org/doi/10.1137/S0097539795293172.

11. Shor.

12. Lam et al., *Cryptography and Computational Number Theory*.

Euclidean algorithm:

$$x = \gcd(a, N)$$

If $x \neq 1$, then we have found a factor of N and can thus compute, with each factor as integers:

$$N = x \cdot \frac{N}{x}$$

If $x = 1$, then using a quantum algorithm, we compute:

$$r = \mathrm{ord}_a$$

. If r is odd, we pick a random a as in the beginning and retry. Otherwise, we compute:

$$g = \gcd(N, a^{\frac{r}{2}} + 1)$$

Should $g \neq 1$, we have found a non-trivial calculation; otherwise, we continue choosing random a. Shor's paper proves that this iteration runs a trivially finite amount of iterations and thus will eventually work.[13]

As alluded to before, Shor's algorithm does not present as large of a threat to current state-of-the-art cryptography as one may seem in part due to additional complications that arise from the quantum order-finding algorithm.[14] However, rapidly advancing quantum computing technology in addition to problems posed by the SDNL (Store-now, decrypt-later) scheme provide additional urgency to the problem of *Post-Quantum Cryptography.*

1.6 Post-Quantum Cryptography

It is important to make a distinction between Post-Quantum Cryptography (PQC)[15] and Quantum Cryptography (QC).[16] Post-quantum cryptography describes the development and implementation of cryptographic schemes resistant to attacks posed by Shor's algorithm and its derivatives. Quantum Cryptography alludes to the field of cryptography emerging from certain quantum mechanical properties such as entanglement. While this paper will give a short overview of the state of QC in the race for efficient, practical PQC, it is important to note that the primary focus of this paper will be studying PQC.

Currently, the most optimal mathematical problem identified for PQC is known as the Learning with Errors (LWE) problem, also known as Lattice-based cryptography.[17] It is important to note that by all indications, though certain intractibile problems may be trivially

13. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer."

14. Martin Roetteler et al., "Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms" [in en], in *Advances in Cryptology – ASIACRYPT 2017*, ed. Tsuyoshi Takagi and Thomas Peyrin, Lecture Notes in Computer Science (Cham: Springer International Publishing, 2017), 241–270, ISBN: 978-3-319-70697-9, https://doi.org/10.1007/978-3-319-70697-9_9.

15. Iván Blanco-Chacón, *Ring Learning with Errors: A Crossroads Between Post-Quantum Cryptography, Machine Learning and Number Theory* (February 2019).

16. S. Pirandola et al., "Advances in quantum cryptography" [in EN], Publisher: Optica Publishing Group, *Adv. Opt. Photon., AOP* 12, no. 4 (December 2020): 1012–1236, ISSN: 1943-8206, accessed August 18, 2023, https://doi.org/10.1364/AOP.361502, https://opg.optica.org/aop/abstract.cfm?uri=aop-12-4-1012.

17. Blanco-Chacón, *Ring Learning with Errors*.

broken in polynomial time by quantum computers, NP-hard problems appear to be immune from such concerns. It follows, then, that should one identify a suitable mathematical NP-hard problem, you may develop an effective PQC cipher. The problem arises from the fact that finding a suitable NP-hard problem is extremely difficult under the required parameters, particularly given the efficient use of such an algorithm.[18] Several candidates such as the Jacobians of hyperelliptic curves are not feasible solutions for this reason.

Lattice-based cryptography derives its security from the closest-vector problem (CVP) and the smallest vector problem (SVP). Note: the length of an n-dimensional vector v is defined as the euclidean length, where v_i denotes the magnitude of v in the i-th dimension:

$$||v|| = \sqrt{\sum_{i=1}^{n} v_i^2}$$

Given a lattice L, SVP is defined as finding a vector $x \in L$ as below:[19]

$$x \in L : \forall y \in L, ||x|| \leq ||y||$$

CVP is a quite similar problem.[20] Given a point y in $\mathbb{R}^n$, x_y is as follows:

$$x_y \in L : \forall x \in L, ||y - x_y|| \leq ||y - x||$$

Because both SVP and CVP are NP-hard, LWE is also NP hard, and is thus a theoretically viable PQC scheme.[21]

2 Literature Review

2.1 Viability of Post-Quantum Cryptography

Fortunately, the development of lattice-based LWE cryptography has significantly accelerated since the identification of Shor's algorithm as a credible threat to state-of-the-art cryptography. Prior to the early 2010s, the development of PQC standards suffered due to a limited knowledge of the true threat it presented. It was not believed that a large enough quantum computer would be developed in time for the identified problem to pose a major threat. However, the significant acceleration of quantum-computing based developments shifted the timeline for the potential arrival of capable quantum computers by a magnitude of decades; while an exact estiamte is not currently known, NIST has, in response, identified post-quantum cryptography as a critical security crisis.[22] In 2016, the National Institute of

18. Blanco-Chacón, *Ring Learning with Errors*.
19. Blanco-Chacón.
20. Blanco-Chacón.
21. Vinod Vaikuntanathan, "Advanced Topics in Cryptography: Lattices" (Massachusetts Institute of Technology, October 2015).
22. Information Technology Laboratory Computer Security Division, *Post-Quantum Cryptography | CSRC | CSRC* [in EN-US], technical report (National Institute for Standards in Technology, January 2017), accessed September 29, 2023, https://csrc.nist.gov/projects/post-quantum-cryptography.

Standards in Technology (NIST) held a competition to begin the standardization of a robust, secure, and efficient PQC scheme.[23] While developments had been made prior to the introduction of a formal standard, NIST's announcement began the formal process and continued accelerating development. Submissions were closed in late 2017; while a large variety of potential mathematical problems were studied, typically, algorithms featuring lattice-based cryptography generally fared better than others. As recently as August 2023, NIST enshrined three federal information processing standards as the United States' post-quantum cryptographic standard for the forseeable future:[24] FIPS 203, FIPS 204, FIPS 205.

NIST has selected four algorithms to lay at the foundation of the future post-quantum security framework: CRYSTALS-Kyber for general encryption; and CRYSTALS-Dilithium, FALCON, SPHINCS for digital signatures. These four algorithms comprise the aforementioned brand new Federal Information Processing Standards (FIPS).[25] FIPS 203 describes a post-quantum key encapsulation mechanism (KEM) called ML-KEM, which dictates how the private or public key may be transmitted securely from party to party for purposes of verification. ML-KEM utilizes a variation of the LWE problem called the Module Learning with Errors problem, which is similarly NP-hard and thus is secure against Shor's algorithm. FIPS 203 includes three parameter sets for ML-KEM: ML-KEM-512, ML-KEM-768, and ML-KEM-1024 in increasing order of security and resource usage.[26] FIPS 204 specifies the standards for post-quantum key establishment and digital signature schemes. FIPS 204 packages three selected post-quantum algorithms from the NIST competition under ML-DSA, each of which can be used to verify digital signatures. Similar to FIPS 203, FIPS 204 contains three parameter sets for ML-DSA: ML-DSA-44, ML-DSA-65, ML-DSA-87; once again, in increasing order of security and resource usage.[27] FIPS 205[28] describes a post-quantum stateless digital signature standard, based on the SPHINCS+ algoritm selected at the conclusion of the NIST PQC competition.[29]

23. *Public-Key Post-Quantum Cryptographic Algorithms: Nominations | CSRC* [in EN-US], technical report (National Institute for Standards in Technology, December 2016), accessed September 29, 2023, https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms.

24. *Three Draft FIPS for Post-Quantum Cryptography | CSRC* [in EN-US], technical report (National Institute for Standards in Technology, August 2023), accessed September 29, 2023, https://csrc.nist.gov/News/2023/three-draft-fips-for-post-quantum-cryptography.

25. "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms" [in en], Last Modified: 2022-07-07T12:51-04:00, *NIST*, July 2022, accessed September 29, 2023, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

26. *Module-Lattice-Based Key-Encapsulation Mechanism Standard* [in en], technical report Federal Information Processing Standard (FIPS) 203 (Draft) (U.S. Department of Commerce, August 2023), accessed September 29, 2023, https://doi.org/10.6028/NIST.FIPS.203.ipd, https://csrc.nist.gov/pubs/fips/203/ipd.

27. *Module-Lattice-Based Digital Signature Standard* [in en], technical report Federal Information Processing Standard (FIPS) 204 (Draft) (U.S. Department of Commerce, August 2023), accessed September 29, 2023, https://doi.org/10.6028/NIST.FIPS.204.ipd, https://csrc.nist.gov/pubs/fips/204/ipd.

28. *Stateless Hash-Based Digital Signature Standard* [in en], technical report Federal Information Processing Standard (FIPS) 205 (Draft) (U.S. Department of Commerce, August 2023), accessed September 29, 2023, https://doi.org/10.6028/NIST.FIPS.205.ipd, https://csrc.nist.gov/pubs/fips/205/ipd.

29. "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms."

2.2 Performant Post-Quantum Cryptography

While PQC has undoubtely made significant leaps in performance even for significant restraints[30] over the prior decades, post-quantum cryptography is relatively raw in development[31] compared to current state-of-the-art cryptographic, though that is to be expected. Lattice-based LWE PQC encryption schemes are much more mathematically complex than their state-of-the-art counterparts: while ECC ciphers often excel in low performance scenarios[32] even with smaller key-sizes in low-performance environments such as the Internet of Things (IoT), LWE PQC algorithms often require much more memory.[33] For this reason, while LWE has been identified as feasible on IoT devices[34] by performance metrics, memory requirements damper the potential of PQC on smaller, performance-constrained devices.[35] In addition, the additional memory requirements often complicate the integration of PQC into existing technology.

Notably, while there is a significant amount of research output on the performance and viability of PQC on IoT and other small devices, in addition to significant benchmarking on traditional workloads, there is a lack of data on the performance of the NIST selected post-quantum algorithms in scenarios with large payloads. During the inevitable final transition away from traditional state-of-the-art encryption measures, large databases will benefit from the ability to quickly transition existing encrypted data to quantum-resistant standards. However, the high memory requirements of current post-quantum cryptographic algorithms dictate that such a transition will likely be difficult. This paper aims to analyze the current capabilities of the NIST-selected PQC algorithms with large payloads compared to that of traditional state-of-the-art cryptography and identify areas of potential improvement for new cryptographic standards.

30. Oscar M. Guillen et al., "Towards post-quantum security for IoT endpoints with NTRU," in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, ISSN: 1558-1101 (March 2017), 698–703, https://doi.org/10.23919/DATE.2017.7927079.

31. Sajimon P C, Kurunandan Jain, and Prabhakar Krishnan, "Analysis of Post-Quantum Cryptography for Internet of Things," in *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, ISSN: 2768-5330 (May 2022), 387–394, https://doi.org/10.1109/ICICCS53718.2022.9787987.

32. Dhillon and Kalra, "Elliptic curve cryptography for real time embedded systems in IoT networks."

33. Maximilian Schöffel et al., "On the Energy Costs of Post-Quantum KEMs in TLS-based Low-Power Secure IoT," in *Proceedings of the International Conference on Internet-of-Things Design and Implementation*, IoTDI '21 (New York, NY, USA: Association for Computing Machinery, May 2021), 158–168, ISBN: 978-1-4503-8354-7, accessed August 18, 2023, https://doi.org/10.1145/3450268.3453528, https://dl.acm.org/doi/10.1145/3450268.3453528.

34. Sedat Akleylek and Meryem Soysaldı, "A new lattice-based authentication scheme for IoT," *Journal of Information Security and Applications* 64 (February 2022): 103053, ISSN: 2214-2126, accessed August 18, 2023, https://doi.org/10.1016/j.jisa.2021.103053, https://www.sciencedirect.com/science/article/pii/S2214212621002398.

35. Riste Ristov and Saso Koceski, "Quantum Resilient Public Key Cryptography in Internet of Things," in *2023 12th Mediterranean Conference on Embedded Computing (MECO)*, ISSN: 2637-9511 (June 2023), 1–4, https://doi.org/10.1109/MECO58584.2023.10154994.

3 Method

In this paper, we aim to demonstrate the comparative performance of NIST-selected post-quantum cryptographic algorithms to current state-of-the-art cryptography; particularly, in situations requiring large data throughput in which performance considerations beyond simple feasibility require consideration.

3.1 Virtualization

In line with previous performance benchmarks of a similar nature,[36] we opt to test each algorithm via a virtualized approach using equivalent performance constraints and same underlying infrastructure. We decide not to test performance on raw metal as to standardize the process and remove as much entropy from results as possible. Docker is selected as the platform for virtualization; while there have been documented instances of Docker performance overhead, the comparative nature of this paper allows us to ignore this consideration. Docker is chosen primarily for configurability; utilizing Docker's featureset, we are able to automate the generation of constraint configurations, affording us greater ability to adjust experimental parameters.

3.2 Approach

Recall that we may categorize cryptographic communication methods into two categories: public-key encryption and private-key encryption. Public-key encryption mechanisms are often implemented in the form of Key Exchange Mechansims (KEM). We define a KEM as a triplet of functions:

References

Akleylek, Sedat, and Meryem Soysaldı. "A new lattice-based authentication scheme for IoT." *Journal of Information Security and Applications* 64 (February 2022): 103053. ISSN: 2214-2126, accessed August 18, 2023. https://doi.org/10.1016/j.jisa.2021.103053. https://www.sciencedirect.com/science/article/pii/S2214212621002398.

Blanco-Chacón, Iván. *Ring Learning with Errors: A Crossroads Between Post-Quantum Cryptography, Machine Learning and Number Theory.* February 2019.

Bub, Jeffrey. "Quantum Entanglement and Information." Last Modified: 2023-05-02, August 2001. Accessed September 23, 2023. https://seop.illc.uva.nl/entries/qt-entangle/.

36. Zhe Liu and Hwajeong Seo, "IoT-NUMS: Evaluating NUMS Elliptic Curve Cryptography for IoT Platforms," Conference Name: IEEE Transactions on Information Forensics and Security, *IEEE Transactions on Information Forensics and Security* 14, no. 3 (March 2019): 720–729, ISSN: 1556-6021, https://doi.org/10.1109/TIFS.2018.2856123.

Computer Security Division, Information Technology Laboratory. *Post-Quantum Cryptography | CSRC | CSRC* [in EN-US]. Technical report. National Institute for Standards in Technology, January 2017. Accessed September 29, 2023. https://csrc.nist.gov/projects/post-quantum-cryptography.

Dhillon, Parwinder Kaur, and Sheetal Kalra. "Elliptic curve cryptography for real time embedded systems in IoT networks." In *2016 5th International Conference on Wireless Networks and Embedded Systems (WECON)*, 1–6. October 2016. https://doi.org/10.1109/WECON.2016.7993462.

Guillen, Oscar M., Thomas Pöppelmann, Jose M. Bermudo Mera, Elena Fuentes Bongenaar, Georg Sigl, and Johanna Sepulveda. "Towards post-quantum security for IoT endpoints with NTRU." In *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, 698–703. ISSN: 1558-1101. March 2017. https://doi.org/10.23919/DATE.2017.7927079.

Lam, Kwok-Yan, Igor Shparlinski, Huaxiong Wang, and Chaoping Xing, eds. *Cryptography and Computational Number Theory* [in en]. Basel: Birkhäuser, 2001. ISBN: 978-3-0348-9507-1 978-3-0348-8295-8, accessed September 22, 2023. https://doi.org/10.1007/978-3-0348-8295-8. https://link.springer.com/10.1007/978-3-0348-8295-8.

LaPierre, Ray. *Introduction to Quantum Computing* [in en]. The Materials Research Society Series. Cham: Springer International Publishing, 2021. ISBN: 978-3-030-69317-6 978-3-030-69318-3, accessed September 23, 2023. https://doi.org/10.1007/978-3-030-69318-3. https://link.springer.com/10.1007/978-3-030-69318-3.

Liu, Zhe, and Hwajeong Seo. "IoT-NUMS: Evaluating NUMS Elliptic Curve Cryptography for IoT Platforms." Conference Name: IEEE Transactions on Information Forensics and Security, *IEEE Transactions on Information Forensics and Security* 14, no. 3 (March 2019): 720–729. ISSN: 1556-6021. https://doi.org/10.1109/TIFS.2018.2856123.

Module-Lattice-Based Digital Signature Standard [in en]. Technical report Federal Information Processing Standard (FIPS) 204 (Draft). U.S. Department of Commerce, August 2023. Accessed September 29, 2023. https://doi.org/10.6028/NIST.FIPS.204.ipd. https://csrc.nist.gov/pubs/fips/204/ipd.

Module-Lattice-Based Key-Encapsulation Mechanism Standard [in en]. Technical report Federal Information Processing Standard (FIPS) 203 (Draft). U.S. Department of Commerce, August 2023. Accessed September 29, 2023. https://doi.org/10.6028/NIST.FIPS.203.ipd. https://csrc.nist.gov/pubs/fips/203/ipd.

"NIST Announces First Four Quantum-Resistant Cryptographic Algorithms" [in en]. Last Modified: 2022-07-07T12:51-04:00, *NIST*, July 2022. Accessed September 29, 2023. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

P C, Sajimon, Kurunandan Jain, and Prabhakar Krishnan. "Analysis of Post-Quantum Cryptography for Internet of Things." In *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 387–394. ISSN: 2768-5330. May 2022. https://doi.org/10.1109/ICICCS53718.2022.9787987.

Pirandola, S., U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, et al. "Advances in quantum cryptography" [in EN]. Publisher: Optica Publishing Group, *Adv. Opt. Photon., AOP* 12, no. 4 (December 2020): 1012–1236. ISSN: 1943-8206, accessed August 18, 2023. https://doi.org/10.1364/AOP.361502. https://opg.optica.org/aop/abstract.cfm?uri=aop-12-4-1012.

Public-Key Post-Quantum Cryptographic Algorithms: Nominations | CSRC [in EN-US]. Technical report. National Institute for Standards in Technology, December 2016. Accessed September 29, 2023. https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms.

Ristov, Riste, and Saso Koceski. "Quantum Resilient Public Key Cryptography in Internet of Things." In *2023 12th Mediterranean Conference on Embedded Computing (MECO)*, 1–4. ISSN: 2637-9511. June 2023. https://doi.org/10.1109/MECO58584.2023.10154994.

Roetteler, Martin, Michael Naehrig, Krysta M. Svore, and Kristin Lauter. "Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms" [in en]. In *Advances in Cryptology – ASIACRYPT 2017*, edited by Tsuyoshi Takagi and Thomas Peyrin, 241–270. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017. ISBN: 978-3-319-70697-9. https://doi.org/10.1007/978-3-319-70697-9_9.

Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C* [in English]. 2nd edition. New York: Wiley, October 1996. ISBN: 978-0-471-11709-4.

Schöffel, Maximilian, Frederik Lauer, Carl C. Rheinländer, and Norbert Wehn. "On the Energy Costs of Post-Quantum KEMs in TLS-based Low-Power Secure IoT." In *Proceedings of the International Conference on Internet-of-Things Design and Implementation*, 158–168. IoTDI '21. New York, NY, USA: Association for Computing Machinery, May 2021. ISBN: 978-1-4503-8354-7, accessed August 18, 2023. https://doi.org/10.1145/3450268.3453528. https://dl.acm.org/doi/10.1145/3450268.3453528.

Shor, Peter W. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." Publisher: Society for Industrial and Applied Mathematics, *SIAM J. Comput.* 26, no. 5 (October 1997): 1484–1509. ISSN: 0097-5397, accessed August 18, 2023. https://doi.org/10.1137/S0097539795293172. https://epubs.siam.org/doi/10.1137/S0097539795293172.

Stateless Hash-Based Digital Signature Standard [in en]. Technical report Federal Information Processing Standard (FIPS) 205 (Draft). U.S. Department of Commerce, August 2023. Accessed September 29, 2023. https://doi.org/10.6028/NIST.FIPS.205.ipd. https://csrc.nist.gov/pubs/fips/205/ipd.

Three Draft FIPS for Post-Quantum Cryptography | CSRC [in EN-US]. Technical report. National Institute for Standards in Technology, August 2023. Accessed September 29, 2023. https://csrc.nist.gov/News/2023/three-draft-fips-for-post-quantum-cryptography.

Tiwari, Harsh Durga, and Jae Hyung Kim. "Novel Method for DNA-Based Elliptic Curve Cryptography for IoT Devices" [in en]. *ETRI Journal* 40, no. 3 (2018): 396–409. ISSN: 2233-7326, accessed August 18, 2023. https://doi.org/10.4218/etrij.2017-0220. https://onlinelibrary.wiley.com/doi/abs/10.4218/etrij.2017-0220.

Vaikuntanathan, Vinod. "Advanced Topics in Cryptography: Lattices." Massachusetts Institute of Technology, October 2015.