Quantum Cryptography Analysis for Secure Data Communication in Multi-Core Environment

Govindu Surla[1*] and R Lakshmi[2]

[1] Research Scholar, Pondicherry University, Department of Computer Science, Pondicherry, India. govindu561@gmail.com
2 Associate Professor, Pondicherry University, Department of Computer Science, Pondicherry, India.

prof.rlakshmi@gmail.com

Abstract. Compared to traditional computing methods, quantum computing's performance is a direct result of its foundation in quantum theory. It's a real benefit to academia and will cut computing times in half, from years to hours or minutes. Thus, quantum computers represent a significant risk to encryption because they create new dangers at an unparalleled pace and scale. When confronted by a quantum computer, conventional cryptographic techniques fail. However, particularly in a multi-core setting, there is a need for the design as well as development of cryptographic algorithms, which are safe from or resistant to the effects of quantum computing. In this paper, the advantages and disadvantages of the most popular quantum-safe cryptographic algorithms are described with an analysis of their performance on a multi-core machine. In this research, the efficiency of many possible quantum-safe algorithms, including multivariate, code-based, hash-based, and lattice-based algorithms, is analyzed. Most of quantum-safe algorithms need longer execution times and larger key sizes. In order to safeguard computers and networking in the post-quantum age, this work compares and analyses the performance of several post-quantum cryptographic methods.

Keywords: Post Quantum Cryptography, Quantum Computing, Code Based Cryptography, Multivariate Cryptography.

1 Introduction

In most fields, including medicine, defense, social media, and more, quantum computers are no longer science fiction [1-3]. [11-15]. There are several ways in which quantum computers diverge from their binary electrical predecessors. In contrast to the binary digits, which can only ever be in one of two states (0 or 1) used in traditional digital calculations, quantum bits (qubits) may be in a superposition of states and are used to handle information in quantum computers. The idea of quantum computing, first introduced in 1982 by Richard Feynman, was the topic of much research ever

C. Kiran Mai et al. (eds.), *Proceedings of the Fourth International Conference on Advances in Computer Engineering and Communication Systems (ICACECS 2023)*, Atlantis Highlights in Computer Sciences 18,
https://doi.org/10.2991/978-94-6463-314-6_20

since, and is frequently considered the foundation of modern asymmetric cryptography [9]. A global arms race is taking place to see who can master quantum technology first. Therefore, secure cryptographic methods that are immune to quantum-computing-based assaults are urgently required. The current encryption protocols are vulnerable to quantum computing attacks [4]. Existing information technology infrastructure will be rendered fully vulnerable during the transition to the quantum computer, necessitating the creation of quantum-safe or quantum-resistant cryptographic techniques. However, designing and developing cryptographic algorithms that are secure or resistant to the impacts of quantum computing is necessary, especially in a multi-core scenario. In this research, we compare and contrast several widely used quantum-safe cryptographic algorithms in the context of a parallel computing architecture. In this research, the efficiency of many possible quantum-safe algorithms, including multivariate, code-based, hash-based, and lattice-based algorithms, is analyzed. Most quantum-safe algorithms need longer execution times and bigger keys [6].

After this section, the remainder of the paper will have the following structure. The essential methods and concepts are laid down in Section 3. In Section 4, we demonstrate the ideas behind post-quantum cryptography. Section 4 has the comparison. In Section 5, the findings and interpretations are presented. The research is summarized in Section 6.

2 Related work

Interest in quantum computing increased significantly with the publication of "Simulating Physics with Computer" by American theoretical physicist Feynman [8]. Feynman proposed using quantum states in his essay. To create a more precise and cost-effective quantum computer, researchers throughout the globe are tackling a wide range of difficult problems [5][12]. A 20 million-qubit quantum computer, as reported by MIT Technology Review [19], could factor a 2048-bit number in around 8 hours. Peter Shor invented a quantum computer technique for factoring integers in polynomial time in 1994. The demonstration of the superiority of the Quantum Computer over a conventional computer was a major step forward [7][10]. The time needed to find a prime factor may be drastically cut using Shor's method. If Shor's method were successfully implemented, it would pose a serious threat to public-key cryptosystems for example RSA, ECC (Elliptic Curve Cryptography), and Diffie-Hellman. Several Post Quantum Cryptosystems, proposed by NIST and other authors [13][8][10], have been proposed as potential successors to RSA and ECC. As can be shown below, NTRU encryption techniques are lattice-based cryptosystems, and the NSA (National Security Agency) has already stated intentions to convert its cryptographic standards to post-quantum cryptography [2]. Two hash-based signature techniques are now being considered for industry-wide adoption. SPHINCS “Stateless Practical Hash-based Incredibly Nice Collision-resilient Signatures” [4] are stateless although the stateful Extended Merkle Signature Scheme (XMSS) is widely used. According to [9], there have been several efforts to develop multivariate polynomial-based asymmetric public key encryption

systems. To solve this issue, [12] introduced a novel efficient multivariate technique based on matrix multiplication called Simple Matrix (ABC).

3 Post Quantum Cryptography

The main objective of post-quantum cryptography is to design cryptographic systems, which cannot be broken by quantum computers while yet being backwards-compatible with existing technologies.[4]. As shown in Figure 1, PQC (Post-Quantum Cryptography) techniques are predicted to be secure even after the widespread deployment of fully operational, large-scale quantum computing systems [6]. Hash-based signature algorithms, multivariate cryptography protocols, code-based cryptography, and lattice-based cryptography are the most common implementations of the PQC algorithms described in Figure 1. The PQC algorithms are shown in great depth in the picture.

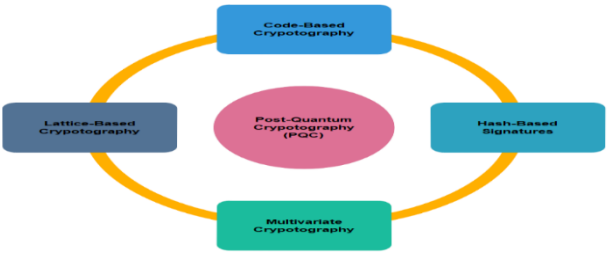

Fig. 1. The Post-Quantum Cryptography Types and Algorithms

3.1 Lattice – Based Cryptography

Cryptographic methods developed on lattices are based on challenging mathematical issues. This cryptography relies on the lattice problems family. Security based on worst-case situations is a distinguishing aspect of lattice-based encryption. When it comes to security, most other cryptosystems just consider the most common of scenarios. A lattice as shown in Figure 2 is an infinitely large grid of equally spaced points. In this lattice, a vector represents a point as a tuple of coordinates. A tuple always begins with a value of 0. A vector that is distant from the origin is said to be "far," whereas a vector that is near to the origin is said to be "short". If the line between the origin and a chosen point is not shared by any other points in the set, then N vectors are chosen as the basis for the lattice in dimension n. This process might be used to build a structure.

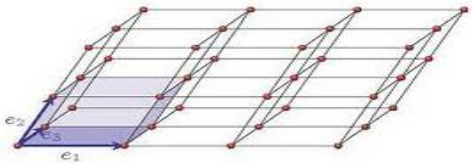

Fig. 2. Lattice Diagram

Key Encapsulation Mechanism (KEM) / Encryption Systems that are based on Lattices are the most researched because of their adaptability. Digital signatures, key exchange, and completely homomorphic encryption are all possible using them. Despite the advanced mathematics required for optimization and security proofs, lattice cryptosystem has a base in elementary linear algebra. The algebraic math is shown down below.

$$\begin{aligned} a_{0,0}x_0+a_{0,1}x_1+\ldots+a_{0,n}x_n &= y_0 \\ a_{1,0}x_0+a_{1,1}x_1+\ldots+a_{1,n}x_n &= y_1 \\ &\vdots \\ a_{n,0}x_0+a_{n,1}x_1+\ldots+a_{n,n}x_n &= y_n \end{aligned} \quad (1)$$

The Gaussian elimination approach makes rapid work of solving for in a standard linear algebra problem. This problem may also be addressed using a "mystery function."

$$f_x(a)=a_0x_0+a_1x_1+\cdots+a_nx_n \quad (2)$$

In the case where "a" is a vector, the answer to ax is shown, while x remains unknown. When this function is called often enough, we can pick up f useful information quickly (by solving the system of equations above). The aforementioned linear algebra problem may be recast as a problem in machine learning. We may reduce our algebraic function to a modulo a (medium-sized) prime q by adding an error term e to the product of x. If so, this is what our noisy mystery function entails:

$$f_x(a)=a_0x_0+a_1x_1+\cdots+a_nx_n+\in mod\ q \quad (3)$$

Learning this noisy function is a formidable mathematical challenge. The error term grows when the noisy function is used in each iteration of the Gaussian elimination procedure. As we keep going around in the loop, the error term grows and grows until it completely obscures the noisy function. In the context of a Lattice Cryptographic system, this method is known as the Learning with Errors (LWE) Problem. Because obtaining the smallest vector is an NP-hard task, cryptosystems for the LWE are sometimes referred to as lattices. A lattice is, in essence, a tiling of n-dimensional space.

3.2 Hash-based Digital Signatures

Alternatives to conventional digital signature systems that rely on asymmetric algorithms like RSA include hash-based digital signature techniques as shown in figure 3. They rely on two characteristics of the hash function: its resilience to collisions and its resistance to preimages.

Fig. 3. Hash-based Digital Signatures

To be preimage resistant, a hash function H must make it hard to discover an input x such that the hash function's output y Equals H (x). A hash function H with low collision resistance means that, given any message m1, it is hard to find a message m2 such that H(m1) = H(m2). Strong collision resistance of a hash function H implies finding messages m_1 and m_2 such that $H(m_1) = H(m_2)$. The birthday paradox makes it more convenient to take use of high collision resistance. Whereas preimage resistance and poor collision resistance both need a $\Theta(2^{n-1})$ search, strong collision resistance requires $o(2^{n/2})$ search as a consequence of the birthday paradox. After the advent of the quantum computer, these hash-based digital signature methods might be put to use in the authentication process. However, every digital signature may only be used once, which is a severe limitation.

3.3 Code-Based Cryptography

Error-correcting codes are crucial in code-based cryptography [3]. Over the last 40 years, computer scientists have been trying to solve this problem. It is common practice in the communications industry to apply error correction codes in order to remedy transmission faults. The text is converted into an error-correcting code before transmission. Then, some erroneous data is intentionally supplied to the output. If you have a single bit, you can change the value of 0 to 000 and the value of 1 to 111. This manner, if the intended receiver receives 101, they will know that 111 was really sent. The receiver will follow the lead of the majority and calculate zero instead of one. Since a linear code may be represented by a k× n matrix, wherein k is the length of the original message and n is the length of the encoded message, it is one of the most frequently utilized error-correcting codes. Deciphering messages often requires knowledge of the corresponding linear code. The McEliece public key cryptosystem is only as safe as how difficult it is to use. McEliece uses public key encryption and key encapsulation with caution.

3.4 Code-Based Cryptography

In multivariate cryptography, the key mathematical difficulty is to solve multivariate polynomials system. The quadratic map takes a sequence $x = (x_1, x_2, \ldots, x_n) \in F_q^m$ and returns an output $y = (p_1(x), p_2(x), \ldots, p_m(x)) \in F_q^n$ where $p_i(x)$ define as multivariate quadratic polynomials for $i = 1,2,\ldots,m$ whereas F_q are polynomials coefficients. The map has m components and m variables, making it a multivariate quadratic map P. Assumed $P: F_q^n \mapsto F_q^m$ a multivariate quadratic map and a target $t \in F_q^m$ search for a number such that $P(s) = t$. This is so difficult that not even quantum computers can solve it. The MQ Problem is already seen widespread application of Grobner basis-like algorithms, including XL and F4/F5 [16-19]. On top of the MQ issue, digital signature systems are often developed. Most people think of the Oil and Vinegar Scheme when they think about digital signatures in multivariate cryptography. Comparison of Post-Quantum Cryptography Algorithms is given in table 1.

Table 1. Comparison of Post-Quantum Cryptography Algorithms

Properties	Hash-based	Code-based	Multivariate based	Lattice-based
Schemes	Signature	Signature Encryption Hash	Signature Encryption	Signature Encryption, Hash Identity-based Encryption.
Algorithms	SPHINCS,XMSS,	McEliece, HQC, BIKE	--	CRYSTALS-Kyber CRYSTALS-Dilithium
Security Reduction	Collision Resistance	Code invertibility	Solving multivariate equation system	Finding good basis for Lattice Solving Lattice problems in special Lattices
Advantages	Extremely fast with good security	Mature with first scheme remaining secure	Fast Small key sizes	Excellent security reductions
Disadvantages	Only signature relies on secure hash function	Secure variants have extensive memory requirements	Low security Confidence due to many systems broken	Not fully understood”

4 Result Analysis

Present-day research is focused on post-quantum computing in multi-core environment. Steps must be carefully considered while making the transition from a single core to a multi-core environment in the post-quantum era. This section compares the efficiency of pre-quantum public-key encryption as well as digital signature systems with the most promising post-quantum alternatives in a multi-core setting. A 2.80GHz Intel(R) Core(TM) i7-1165G7 was used to do the tests on all of the strategies. The method for post-quantum cryptography was executed in a multi-core environment, and the results are shown in Table 2-5 and Figure 4-7. Table 6 below presents the execution time of the Lattice based cryptography algorithm in three different file sizes. From the results shown in both Figure.4 and Table.2, it is known that HQC took long time to perform the key operations i.e., Keygen=19269, Encryption=13476 and Decryption=9676 Seconds with maximum file size 358 KB respectively. The lowest time took by BIKE in all the operations i.e., Keygen=4172, Encryption=29010 and Decryption=1830 Seconds with file size 173 KB respectively.

Table 2. Runtime Analysis of Open Quantum Code based Cryptographic Algorithms

Algorithm	File Size(KB)	Keygen	Encaps	Decaps
BIKE	173	4172	29010	1830
BIKE	291	6345	30686	4049
BIKE	358	7902	31756	5652
Classic-McEliece	173	6218	53261	17594
Classic-McEliece	291	7421	53409	18455
Classic-McEliece	358	8843	54797	20542
HQC	173	15579	9786	5986
HQC	291	17924	12131	8331
HQC	358	19269	13476	9676

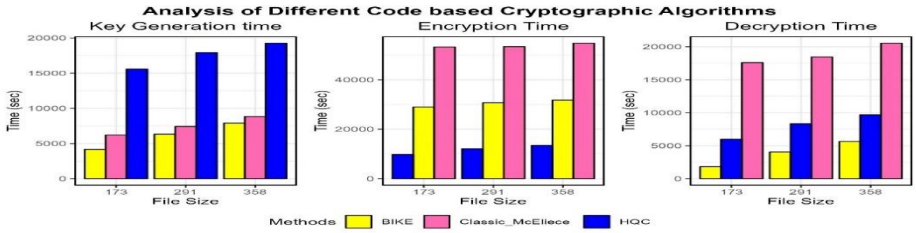

Fig. 4. Runtime Analysis of Open Quantum Code based Cryptographic Algorithms

Rainbow-Classic, and Rainbow-Compressed are two algorithms in Multivariate cryptography. The runtime performance of these two algorithms over three different files of sizes173 kb, 291 kb and 358kb is shown in Table.3 and Figure.5.

From the results shown in both Table and Figure, it is known that Rainbow-Classic took long time to perform the key operations i.e., Keygen=16, Signature=524 and Verification=543 seconds with maximum file size 358 KB respectively. The slowest time took by Rainbow-Compressed in all the operations i.e., Keygen=6, Signature =115 and Verification =465 Seconds with minimum file size 173 KB respectively.

Table 3. Runtime Analysis of Open Quantum Multi-variate Cryptographic Algorithms

Algorithm	File Size(KB)	Keygen(sec)	Sign(sec)	Verify(sec)
Rainbow-Classic	173	8	489	501
Rainbow-Classic	291	11	493	512
Rainbow-Classic	358	16	524	543
Rainbow-Compressed	173	6	115	465
Rainbow-Compressed	291	9	121	489
Rainbow-Compressed	358	13	132	508

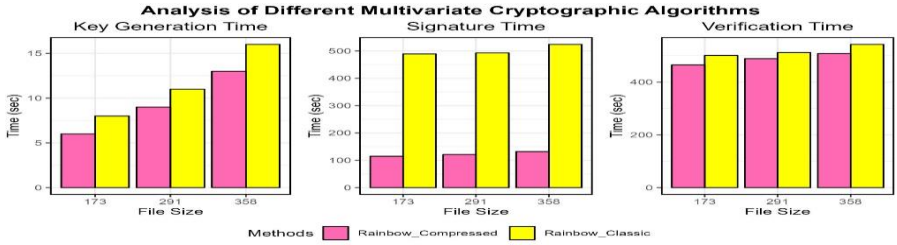

Fig. 5. Runtime Analysis of Open Quantum Multivariate Cryptographic Algorithms

Table 4. Runtime Analysis of Open Quantum Safe Hash Based Cryptographic Algorithms

Algorithm	File Size(KB)	Keygen	Sign	Verify
SPHINCS	173	2987	132	549
SPHINCS	291	3152	145	867
SPHINCS	358	3879	201	349
SPHINCS_SHA	173	975	45	246
SPHINCS_SHA	291	1087	56	284
SPHINCS_SHA	358	1178	68	212
SPHINCS_SHAKE	173	482	19	149
SPHINCS_SHAKE	291	514	25	151
SPHINCS_SHAKE	358	597	37	187

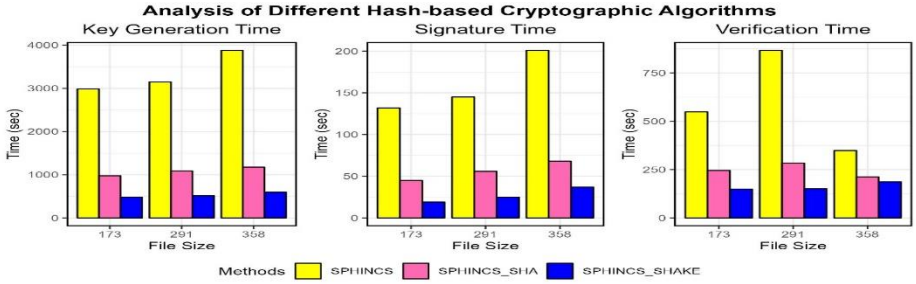

Fig. 6. Runtime analysis of Open Quantum Safe Hash-based Cryptographic Algorithms

The runtime behavior of SPHINCS and its variants is shown in Table 4 and Figure 5. From the results, it is known that SPHINCS took long time to perform the key operations i.e., Keygen=3879, Signature=201 and Verification=349 Seconds with maximum file size 358 KB respectively. The lowest time took by SPHINCS_SHAKE in all the operations i.e., Keygen=482, Signature =19 and Verification =149 Seconds with minimum file size 173 KB respectively.

Table.5 and Figure.7 provide the execution time results for files of 173 kb, 291 kb, and 358 kb for each of the three approaches. Both Table.6 and Figure.6 reveal that NTRU required considerable time to complete the essential procedures i.e., Keygen=21478, Encryption=85791 and Decryption=86975 Seconds with maximum file size 358 KB respectively. The lowest time took by BLISS method in all the operations i.e., Keygen=2621, Encryption=22524 and Decryption=22428 Seconds with minimum file size 173 KB respectively.

Table 5. Runtime analysis of open quantum safe Lattice-based cryptographic algorithms

Algorithm	File Size(KB)	Keygen	Encaps	Decaps
NTRU	173	15548	62579	72495
NTRU	291	16875	69825	74851
NTRU	358	21478	85791	86975
RING	173	34268	30187	40527
RING	291	38975	34521	43512
RING	358	42567	40479	43826
BLISS	173	2621	22524	22428
BLISS	291	2798	22665	22564
BLISS	358	2802	22795	22698

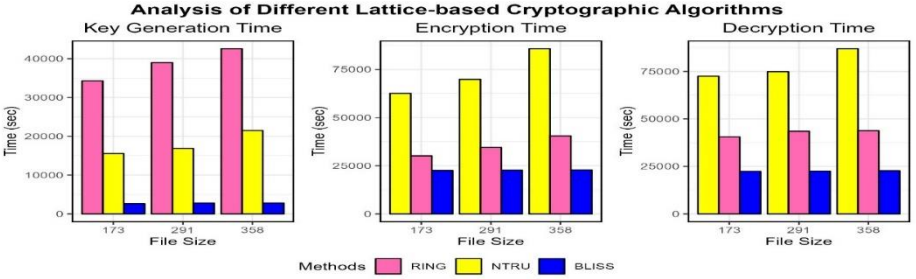

Fig. 7. Runtime Analysis of Open Quantum Safe Lattice-based Cryptographic Algorithms

5 Conclusion

The field of computing has advanced significantly in recent years, allowing us to go beyond "classical" computing and into the "quantum" age of data. Scientific discoveries in quantum computing over the last several years will allow for exponential gains in computer speed and accuracy. Our primary goal in writing this work was to investigate and dissect the four classes of cryptosystems that we consider to be quantum-resistant in order to encourage more investigation in this promising field. In light of this, it is important that any upgrades made to preexisting post-quantum cryptosystems be implemented in a manner that does not significantly compromise system security. But before we can conclude for sure that Lattice-based encryption is better than other kinds of post-quantum cryptography, further in-depth study is needed. Post-quantum Cryptography algorithms will need to be rigorously implemented and analyzed in Software simulation and in limited hardware in future research.

References

1. Alagic G, Apon D, Cooper D, Dang Q, Dang T, Kelsey J, Licht Inger J, Miller C, Moody D, Peralta R, Perlne R, Robinson A, Smith-Tone D, Liu Y-K. Status report on the third round of the NIST post-quantum cryptography standardization process. NIST Publications; 2022.

2. arXiv. Emerging technology from the. How a Quantum Computer Could Break 2048-Bit RSA Encryption in 8 Hours 2 Apr. 2020.
3. Balamurugan Chithralekha, et al. Code-based post-quantum cryptography. 2021.
4. Baldi Marco, et al. post-quantum cryptography based on codes: state of the art and open challenges. 2017 AEIT International Annual Conference 2017.
5. Beullens W, D'Anvers J-P, Hülsing AT, Lange T, Panny L, de Saint Guilhem C, Smart NP. Post-Quantum Cryptography: current state and quantum mitigation. ENISA; 2021.
6. Chen Jiajun. Review on quantum communication and quantum computation. J Phys Conf 2021;1865(2):02200.
7. Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inf Theor 1976; 22(6):644–54 Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehl´e, D. (2018).
8. CRYSTALS-dilithium: a lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(1), 238–268.
9. Grover Lov K. A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on theory of computing - STOC '96; 1996.
10. Joseph D, Misoczki R, Manzano M, Tricot J, Pinuaga FD, Lacombe O, Leichenauer S, Hidary J, Venables P, Hansen R. Transitioning organizations to post-quantum cryptography. Nature 2022;605(7909):237–43.
11. K. Lavanya, G.V.Suresh," An Additive Sparse Logistic Regularization Method for Cancer Classification in Microarray Data", The International Arab Journal of Information Technology, Vol. 18, No. 2, March 2021.https://doi.org/10.34028/iajit/18/10, ISSN: 1683- 3198E-ISSN: 2309-4524, Impact Factor is 0.654.
12. K. Lavanya, Devireddy Syamala, Kotha Vineetha Vani, Choragudi Gipsy," A Novel SVM-KNN Classifier for Cervical Cancer Diagnosis using Feature Reduction and Imbalanced Learning Techniques", International Journal of Psychosocial Rehabilitation, Vol.24, Issue 6, pp:5151-5161,2020.ISSN 1475-7192.
13. KAMPA LAVANYA, Pemula Rambabu, Vijay Suresh, Rahul Bhandari, " Gene Expression Data Classification with Robust Sparse Logistic Regression using Fused Regularization", International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC), Inderscience Publishers, Vol 42,No.4,20 April 2023.
14. G.N. Basavaraj, K. Lavanya, Y Sowmya Reddy, B. Srinivasa Rao, Reliability-driven time series data analysis in multiple-level deep Learning methods utilizing soft computing methods,Measurement: Sensors,Volume 24,2022,100501,ISSN 2665-9174.
15. LaMacchia B. The long road ahead to transition to post-quantum cryptography. Commun ACM 2022;65(1):28–30.
16. Lei X, Liao X. NTRU-KE: a lattice-based public key exchange protocol. 2013, March 11. Retrieved, https://eprint.iacr.org/.
17. Micciancio Daniele, Regev Oded. Lattice-based cryptography. Post-Quantum Cryptography 2009:147–91.
18. Sendrier N. Code-based cryptography: state of the art and perspectives. IEEE Security & Privacy 2017;15(4):44–50
19. Roma, Crystal Andrea, et al. "Energy efficiency analysis of post-quantum cryptographic algorithms." IEEE Access, vol. 9, 2021, pp. 71295–71317. Crossref, doi:10.1109/access.2021.3077843.