EAI Endorsed Transactions
on Internet of Things

Research Article EAI.EU

A Survey about Post Quantum Cryptography Methods

Jency Rubia J*,[1], Babitha Lincy R[2], Ezhil E Nithila[1], Sherin Shibi C[3] and Rosi A[1]

[1]Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, India
[2]Sri Eshwar College of Engineering, Coimbatore, India
[3]SRM Institute of Science and Technology, Kattankulathur. Tamil Nadu, India

Abstract

Cryptography is an art of hiding the significant data or information with some other codes. It is a practice and study of securing information and communication. Thus, cryptography prevents third party intervention over the data communication. The cryptography technology transforms the data into some other form to enhance security and robustness against the attacks. The thrust of enhancing the security among data transfer has been emerged ever since the need of Artificial Intelligence field came into a market. Therefore, modern way of computing cryptographic algorithm came into practice such as AES, 3DES, RSA, Diffie-Hellman and ECC. These public-key encryption techniques now in use are based on challenging discrete logarithms for elliptic curves and complex factorization. However, those two difficult problems can be effectively solved with the help of sufficient large-scale quantum computer. The Post Quantum Cryptography (PQC) aims to deal with an attacker who has a large-scale quantum computer. Therefore, it is essential to build a robust and secure cryptography algorithm against most vulnerable pre-quantum cryptography methods. That is called 'Post Quantum Cryptography'. Therefore, the present crypto system needs to propose encryption key and signature size is very large.in addition to careful prediction of encryption/decryption time and amount of traffic over the communication wire is required. The post-quantum cryptography (PQC) article discusses different families of post-quantum cryptosystems, analyses the current status of the National Institute of Standards and Technology (NIST) post-quantum cryptography standardisation process, and looks at the difficulties faced by the PQC community.

Keywords: quantum computing, cryptography, post quantum cryptography, nist post quantum cryptography, lattice-based, multivariant, hash based, and code based

Received on 29 November 2023, accepted on 02 February 2024, published on 12 February 2024

doi: 10.4108/eetiot.5099

1. Introduction

Communication plays a major role from an early stage of civilization to modern civilization. Modern society harnessed Internet as a primary source to enable any interaction between two parties. Hence, there is a need of ensuring safe and secure communication between them for maintaining their privacy. Cryptography is a field of cryptology which deals with the design of algorithms for guarantee to maintain the secrecy between authenticity of messages. Many researchers work on the cryptographic algorithm and propose several methods for ensuring the privacy and integrity of data between both the ends. A new revolution on computing has been developed slowly in the form of quantum computers. The Quantum computer definitely uses different capabilities which take over the classical computer [1]. Because the quantum computer has an ability to perform some computation which are not probable by at existing superior performance multicore systems. The impression behind the concept of quantum computing is purely associated with quantum physics. Quantum physics deals with sub-atomic level. Understanding the sub-atomic level mechanism has been

*Corresponding author. Email: jencyrubia@gmail.com initiated by some significant scientists like Schrodinger, Bohr, Heisenberg and Einstein at an early 20th century. Then in 1980s researchers were tried to implement quantum physics and its mathematics to model computer. Surprisingly which performs the computations with high rate than the traditional computer [2].

Furthermore, quantum computer supports qubits as their inputs and outputs. Moreover, the rules of quantum mechanics have been involved for computing purpose. A qubit, the fundamental building block of quantum information, can represent either a 0 or a 1 or a superposition of the two states. Unlike a classical bit, a qubit can exhibit quantum phenomena such as interference and entanglement, which enable quantum computing to solve certain problems much faster than classical computing. A qubit can be realized by various physical systems, such as trapped ions, photons, atoms, or quasiparticles. A quantum computer has the ability to solve problems quickly and within a set time limit that are intractable to traditional computers. Additionally, a quantum computer can resolve the most challenging, unsolved supercomputer challenge of our time. There are innumerable uses and applications for quantum computers. Some of the applications are physics research, seismology, pharmaceuticals, financial modelling, electronic material invention and so on. in addition to that, Quantum computing brings massive revolution on artificial intelligence in terms of computation power [3]. Though Quantum computing provides solution for the complex problem at different dimensions within a short span of time, it may turn into powerful hazard for us in convinced circumstances. One such case is cryptanalysis.

The study of decrypting a message without having access to the sender's or receiver's secret key is known as cryptanalysis. It is officially referred to as code breaking. The uncomfortable reality is that quantum computers can solve the challenging mathematical puzzles that support our current cryptography techniques. The encryption techniques frequently utilised in digital communication will be simple to break as a result. There are two distinct categories of cryptographic algorithms. Advanced Encryption Standard (AES) and 3DES (Data Encryption Standard) are typically utilized as symmetric cryptographic methods. But the Grover's algorithm [4] can mitigate the reliability level into half. Similar to this, RSA, Diffie-Hellman, and ECC are asymmetric cryptosystems that rely heavily on challenging mathematical issues like discrete logarithm and prime factorization. However, a quantum computer will be able to quickly answer such challenging calculations. The security of asymmetric cryptosystems is gravely compromised by these characteristics [5].

Post-quantum cryptography is the research of innovative cryptosystems that neither quantum nor classical computers are able to crack. According to the security-related issues they have, the cryptosystem can be split into many families. It is believed that neither quantum nor contemporary computers can solve cryptography-related security problems. Multivariate cryptography, framework-based encryption, isogeny-based digital signatures, non-commutative encryption, code-based digital encryption, and hash-based cybersecurity are just a few of the prominent families that make up cryptography [6]. By recommending quantum-secure algorithms, the cryptographic standard association called National Institute of Standards and Technology has taken action to improve the reliability of cryptographic algorithms. Currently, the NIST is working towards establishing standard specifications for post-quantum cryptography.

In this work, the security of several cryptographic algorithms against quantum adversaries and analyse the consequences of quantum computers were remarked. It also looks at some widely studied methods (post-quantum cryptography) that would be challenging for even a quantum adversary to break. The paper concludes with recommendations for additional post-quantum cryptography research as well as an assessment of the most promising NIST standard contenders. This paper also identifies and outlines the most difficult issues in post-quantum cryptography for all families [7]. Utilising significant basic cryptosystems, each family is discussed. The study's conclusion highlights a number of active research areas.

2. Cryptography – General Outline

Cryptography is a field of cryptology which deals with the design of algorithms for guarantee to maintain the secrecy between authenticity of messages, says William Stallings a famous author of Computer network related books. The cryptography is turning normal text into unreadable format that cannot access the original text by non-authorized persons. The developed security mechanism should attain three golden objectives called CIA (Confidentiality, Integrity and Availability) Tried. The CIA Triad encompasses three objectives: confidentiality, integrity, and availability, which are vital for information system resources such as hardware, software, firmware, information, and telecommunications [8] The evolution of cryptography can be divided into three distinct periods: the classical (manual) era, the modern era, and the quantum era. The classical way of encryption methods includes some manual computation. Hence, those methods experienced slow in process and possibility of attacks is more.

Nowadays the security of information shared has been secured with modern cryptographic methods. The modern cryptographic methods are broadly classified as symmetric and asymmetric algorithms. The symmetric method of cryptographic algorithm contains same key for encryption and decryption [9]. This method is called as private key crypto system. The asymmetric cryptographic method utilizes a couple of keys, one for encoding and the other for decoding. The other name of asymmetric method termed as public key cryptosystem. The term cryptanalysis actually is a way of breaking security system by knowing secret key or simple text without knowing secret value. The term cryptanalysis is otherwise called as an attack. Simple text, ciphertext, a private key, an encryption method and a decryption algorithm are all included in Figure 1's portrayal of a conventional encryption scheme.

The encryption algorithm receives the plaintext, which is the source message in a decipherable format. The ciphertext, in contrast, designates a scrambled communication in an unintelligible format. The decryption algorithm uses the ciphertext, which is a yield of the encoding algorithm, as an input to restore the unique message. The ciphertext is created by the encryption algorithm by applying a series of operations to the plaintext. Both the basic text and the concealed key are inputs into the encryption process, which results in the ciphertext. The decryption algorithm, on the other hand, performs a sequence of operations to obtain the original plaintext as output, reversing the encryption process [10]. The cypher text and secret key are inputs to the decryption algorithm, which outputs the plaintext.

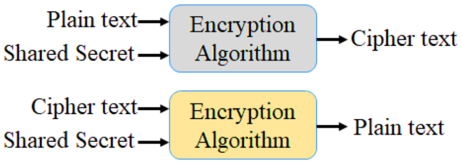

Figure 1. General Architecture of Cryptosystem

The secret key is crucial to ensuring the confidentiality of the original text because it is utilized as an input in both the ciphering and deciphering processes. Notably, using two different secret keys for the same plaintext will generate two distinct ciphertexts. The ciphertext in a symmetric key cryptography can be produces using plaintext and secret key as follows.

$$C=E\_k\ (P) \qquad (1)$$

Then the same secret key is used to compute original text (plain text) out of cipher text and secret key during decryption algorithm.

$$P=D\_K\ (C) \qquad (2)$$

Where P stands for plaintext and E denotes encryption. Also, D refers decryption and C signifies ciphertext. And K stands for secret key. Based on the aforementioned terms and techniques many modern encryption and decryption algorithms were devised in the literature and even in practice. However, depending upon the key size the possibility of attacks may be reduced. But increase in key size, mitigate the compactness of the system. Moreover, the third-party intrusion cannot be known to sender or receiver.

3. Preface about Quantum Cryptography

Quantum Cryptography is a next generation or another dimension of the cryptography era. It is a prominent technology in which two parties can transmit data securely abide by the rules of quantum physics. Generally, it termed as Quantum Key Distribution (QKD) which transmit photons on four random quantum states. The advantage of Quantum cryptography over modern cryptography method is there will be an acknowledgement when there is an unauthorized intrusion. But it failed in modern cryptography methods. Moreover, the speed of assuming or tackling the prime number combination is maximum in Quantum cryptography. The paper is structured as follows: Section 2 offers the foundational math needed for the cryptographic techniques. The section 3 explains the modern cryptographic methods and examples. And the section 4 illustrates the classification and some important algorithms of modern cryptographic schemes. Section 5 reveals some basic concepts and algorithms of Quantum cryptography. Section 6 explains the comparison analysis of some significant cryptography methods stated in a literature and section 7 concludes the paper with open research directions.

4. Rudiments of Mathematical Concepts

The strength of the cryptographic algorithms formally associated with the secret key size. The computation of secret keys is relying on prime number and the calculation of biggest prime number is purely depends on residue number system (RNS). The robustness against possible attacks have been improved by computing very big prime numbers. Because the cryptosystems are following discrete mathematics. The discrete mathematics computes the operation in a simple manner in one direction. The other direction of the operation is very complicated. That is the required operation of cryptography algorithm. Because the encryption is one direction of the operation that is simple to do. On the other hand, the other direction of the operation denotes the decryption process. The decryption operation should be more complicated than encryption. Then only, the secure communication can be withstood for a long period. Thus, the cryptography follows discrete mathematics and since it relies on residue number system, modular arithmetic has been used to calculate prime number. The required fundamental mathematical concepts and theorems for the cryptography will be discussed.

4.1. Modular Arithmetic

Modular arithmetic is resembling as division relationship ($b=q\times c+r$) where b and c are two inputs and q and r are two outputs such as quotient and reminder. However, only the remainder r is of interest in modular arithmetic. The quotient q is irrelevant to modular arithmetic. On the other hand, when the input and is divided by n, the modular arithmetic demands the value of the reminder r. The preceding connection, which only has two inputs (b and c) and one output (r), is then modified as a result.

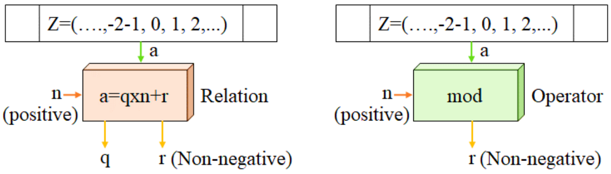

Figure 2. The relation between Division and Modulo Operator

Modulo Operator: A binary operator known as a modulo operator is represented by the symbol mod. As a modulus, the second input (c) is referred to. The residue is referred to as the output r. The distinction between the division and modulo operators is clearly shown in Figure 2.

Figure 2 illustrates how the modulo operator computes a positive modulus (c) and an integer (b) from the collection Z. The operator then produces a residue that is not negative (r). As a result, the modified relation is,

$$b \bmod c = r \tag{3}$$

Based on the outcomes of the modulo operation, the collection of residues was created. An integer between 0 and $c-1$ is always the outcome of a modulo operation with regard to modulus c. The result must also be a nonnegative integer and less than c. The modulo operation results in a set of least residues modulo c or Z_c.

4.2. Congruence

In place of equality, the philosophy of congruence is frequently applied in cryptography. It is not a one-to-one operation to map from the set Z to the set Z_c. It is possible to map many members of the set Z to just one or the same member of the set Z_c. 2 mod = 2, 12 mod = 2, 22 mod 2 = 2, and so forth are examples of outputs. Congruent mod 10 describes integers like 2, 12, and 22 in modular mathematics. The general notation of the congruency between two integers as using congruence operator (≡). The value of the modulus ($mod\ c$) should be incorporated to the right of the congruence operator that makes the relationship standard. There is some of the dissimilarity between equality and congruence operator. A member of Z is translated to a member of Z_e via a congruence operator, as opposed to an equality operator, which moves a member of Z to itself. Second, even if the congruence operator behaves as a many-to-one mapping, it still operates as a one-to-one mapping for the equality operator.

Congruence has the following properties:

1. $c \equiv d\ (mod\ n)$ if $n\ |(c-d)$┤
2. $c \equiv d\ (mod\ n)$ implies $d \equiv c\ (mod\ n)$
3. $c \equiv d\ (mod\ n)$and $d \equiv e\ (mod\ n)$ imply $c \equiv e\ (mod\ n)$

4.3. Inverses

The computation of modular arithmetic often involves contrary operation of a number related to the modular process. In general, there are two types of inverse operations: multiplicative inverse and additive inverse. The multiplicative negation connected to a multiplication action, whereas the additive inverse related to an addition action.

Additive Inverse: In the language of modular arithmetic, every integer has an additive inverse. The sum of an integer and its additive inverse is congruent to 0 modulo n. There is only one additive inverse for any number. The number itself, however, can be the number's opposite. In Z_n, two numbers a and b are additive inverse of each other if

$$c+d \equiv 0 \text{ (mod n)} \tag{4}$$

Multiplicative Inverse: In modular arithmetic, an integer may or may not have a multiplicative inverse. When it does, the product of the integer with its multiplicative inverse is identical to 1 modulo n. In Z_n, two numbers a and b are the multiplicative inverse of each other if

$$c \times d \equiv 1 \text{(mod n)} \tag{5}$$

The input a has a multiplicative inverse in Z_n if and only if $gcd\ (n,c)=1$. In this case, a and n are said to be relatively prime.

5. Modern Cryptography

Cryptography is utilized to protect data stored in storage devices, ensuring security even in the presence of physical access. In computer networks, cryptographic techniques find diverse applications such as document time stamping, user digital signatures, and authentication. In internet payment systems like Google Payments and Paytm, which rely on cryptological methods to secure bank account credentials, cryptography is essential for protecting sensitive information. Emails, messaging services like WhatsApp, and social networking platforms like Instagram and Facebook all use encryption and decryption. The modern cryptographic algorithms consist of two types namely symmetric and asymmetric in nature.

5.1. Symmetric Cryptography

Symmetric cryptography is a cryptosystem that employs a solitary significant for both encryption and decryption processes. With sufficiently large and random key lengths, brute force attacks on such systems are not feasible with existing computer capabilities. The secure transmission of the key from sender to receiver is paramount in symmetric cryptography, as the entire encryption and decryption rely on this shared key.

Data Encryption Standard (DES): One sort of symmetric algorithm and widely used algorithm is The Data Encryption Standard. This algorithm already proven to be weakened for the brutal force attack in a pre-quantum cryptographic method. But if the key size increased, the vulnerability of the algorithm can be overcome. If not, 2 or 3 keys can be utilised with the modified form of DES (Triple/3 DES). As a result, an exhaustive search involves exponentially more processes. DES follows Feistel-Round structure, where the message frame will get break into two halves and perform different kind of operations for each iteration [11]. Each message block in the DES encryption process consists of 64 bits, with 32 bits processed every round. For successive processing cycles, the unpretentious bits are switched with the processed bits after the output of the Feistel function is XORed with the first 32 bits. The DES algorithm consists of 16 such rounds. The iteration starts with initial permutation and ends with final permutation. By employing S-boxes and P-boxes in this manner, DES generates random output while providing adequate confusion and dispersion. By using brute force, the random output can only be broken. However, as mentioned earlier, DES acts as very fragile against brute force. Thus, DES not recommended for use.

To increase the robustness of DES, a computational trial has been enhanced through increasing the key length. That is called 3DES algorithm.

Triple - Data Encryption Standard (3-DES): The DES security vulnerabilities are addressed by Triple-DES. Because DES algorithm uses very small key length of 56 bits. But, in the case of 3-DES, uses three different keys of each length 56 bits. Hence the name called Triple – Data Encryption Standard. Thus, totally three layers of encryption method has been used for the security enhancement. The sequence of encryption, decryption, and encryption is shown here. The process begins by encrypting the plaintext using key K1. The encoded message can then be decoded using the Data Encryption Standard (DES) and key K2. Subsequently, the resulting data is encrypted again using key K3, resulting in ciphertext. The security level of Triple Data Encryption Standard (3DES) relies on the strength and complexity of its key size. Utilising three different values for the keys K1, K2, and K3 is the only way to enhance the time complexity of brute force after that. From the analysis, for the key length of 168 bits, the 3DES algorithm gives maximum security level. The short block size, which increases the likelihood of collisions, makes the 3DES algorithm susceptible. The sweet32attack [12] defeated the 3DES algorithm. In that collision attack was found at 2^(72) trials.

Advanced Encryption Standard (AES): The AES algorithm [13] is frequently used as a symmetric encryption technique. AES's standard of reliability is realized by the random number of ciphertext generated by repeated iterations of a conventional substitution-permutation network. The AES method will use a variety of critical sizes, such as 128-bit, 192-bit, or 256-bit keys. The AES algorithm also frequently uses 10, 12, or 14 rounds, each with four stages. To maintain a look-up table that has enough subkeys for each round, a straightforward key schedule should be used. After many times of mixing and substitution process, sufficient number of confusion and diffusion operations can be achieved. The AES algorithm is composed of four stages in each round: SubByte, ShiftRows, MixColumns, and AddRoundKey. All the rounds are computed within a Galois Field of order 2^8. The reverse order of a same algorithm with same number of rounds will be the steps of decryption process.

Vulnerabilities that can be exploited have been identified in both the presence of repeated character sequences in the message and the selection of inappropriate keys. However, these attacks do not significantly reduce the calculation time needed to make brute force searches feasible. AES is 'secure' as long as it is limited by available computational power. The most extensively used symmetric key cypher for both wired and wireless security protocols is AES.

5.2. Asymmetric Cryptography

A public key and a private key are used in asymmetric cryptoanalysis to encrypt data. The communication is encrypted using the public key, which can be exchanged between the sender and the recipient. On the other side, data decryption requires the private key. The sender provides the recipient's private key to facilitate decryption. This cryptographic method guarantees the message's confidentiality and integrity.

RSA (Rivest-Shamir-Adleman) Algorithm: A well-known public cryptosystem with the goal of offering the highest level of data security is RSA. Ron Rivest, Adi Shamir, and Leonard Adleman created the RSA algorithm, which saw usage for the first time in 1977. The basic concept of RSA algorithm is prime factorization of a number. In a traditional computer, exponential complexity provides a solution for the prime factorization problem. This benefit is utilised by the RSA algorithm for encryption. This makes the algorithm secure in terms of computation. The one-way function is used as a benefit by the RSA algorithm. It is difficult to invert such functions because they are very easy to compute. Because factoring is difficult, yet multiplying the numbers is quite simple.

No effective approach for resolving the issue has been discovered for big RSA key sizes (1024 bits and above). The prime factorization of large numbers serves as the foundation for all RSA cracking techniques [14]. With today's computing power, it is impossible to crack RSA with a 2048-bit key size in a reasonable amount of time due to the exponential nature of the complexity. Many different systems that require asymmetric cryptography use RSA extensively.

Diffie Hellman Key Exchange: The discrete logarithm issue is the sole foundation of the Diffie-Hellman protocol. Another one-way function problem is the discrete logarithm problem. Though easy to compute, that problem is challenging to reverse. For the discrete logarithmic problem, N must be a large prime. The discrete logarithm issue has an exponentially complicated solution. The strength of the protocol is derived from its exponential difficulty to be compromised, which is attributed to the security proof of the Diffie-Hellman Key Conversation based on the challenging discrete logarithm problem. However, it is important to note that the Diffie-Hellman key exchange mechanism does not require additional authentication, rendering it susceptible to potential "Man in the Middle Attacks." The essence of the Diffie-Hellman method lies in the complication of the isolated logarithm problem it relies on, which is known for its challenging nature.

As a result, the eavesdropper can play the role of the opposing party in an attack where both parties successfully drag a guy into the middle. It can generate a special shared key for Bob and Alice. Then, by assuming the roles of Alice for Bob and Bob for Alice, it can accurately decode and alter each message transmitted between parties. The resilience of the Diffie-Hellman infrastructure and its associated algorithms depends on their continuous strengthening, ensuring they remain as robust as the challenging discrete logarithm problem they rely on.

Elliptic Curve Cryptography: The basis of elliptic curve encryption lies in the fundamental concept of the elliptic curve, which possesses the remarkable property of being intersected by a line at precisely three points. This characteristic is harnessed to create one-way functions, playing a vital role in cryptographic operations. Operation A leverages this idea. A is defined [15]. To achieve this result, the computation needs to do n times operation. Computing Y is very simple but finding number of times is very hard. In the group, this math problem is challenging. The maximum setting for ECC limits the group's overall point total. It looks a lot like modular arithmetic since it helps with wrapping around the lines. The maximum value is determined by the key's size. Due to the fact that ECC's security-related key sizes are substantially less than those of its RSA rival, it has attracted a lot of attention recently. The security offered by a 256-bit elliptic curve is comparable to that of a 3072-bit RSA key. Popular platforms at the moment include Whatsapp, Tor, and Bitcoin [16].

The task of resolving the isolated logarithm problem within elliptic curve groups lies at the heart of Elliptic Curve Cryptography's (ECC) complexity. To facilitate ECC systems, NIST has designated several elliptic curves for use. In the case of a ciphertext-only attack on ECC, the only viable approach to compromise it is by devising an algorithm accomplished of cracking the isolated logarithm problem. The problem still hasn't been solved in a method that can be calculated in an acceptable length of time.

6. Post Quantum Cryptography

The advancement of cryptographic techniques that can withstand attacks from both quantum and classical computers is the aim of post-quantum cryptanalysis. Depending on the unique security problems they address, these cryptographic systems are split into a number of families that are supposed to be beyond the reach of both classical and quantum computers. Some of the well-known families of cryptography include multidimensional cryptography, lattice-based digital signatures, isogeny-based digital encryption, non-commutative digital encryption, code-based digital signatures, and hash-based computing [6]. By making a variety of adjustments, the National Institute of Standards and Technology (NIST) has improved the security of cryptographic algorithms. NIST has suggested quantum-secure algorithms to create standards for post-quantum cryptography. Table 1 provides the family of cryptosystems and their algorithm used.

Table 1. Post Quantum Cryptography

S.No	Family	Algorithm
1	Lattice based Cryptosystem	NTRU Ring LWE BLISS
2	Multivariate Encryption method	Rainbow
3	Hash based Digital signature	Lamport Signature Merkle Signature
4	Code based Encryption	McEllice Niederreiter

6.1. Lattice based Cryptography

The hard mathematics lattice problem serves as the sole foundation for the security level of framework-based cryptography. Thus, this variety of cryptography implemented the family of lattice issues. The survey work evaluates the significance of lattice-based encryption in terms of security using worst-case scenarios. The typical situation heavily influences the security level of the cryptosystem [17]. Lattice is generally structured as a grid of points which are spaced at equal distance. The lattice has a property of stretching out to infinity. A small point in a lattice is termed as a vector which is responsible for the coordination of a point. The other name of the vector is called as a tuple. The origin of a tuple is referred as all 0's [18]. If a vector locate away from the origin is called far vector. And if the vector situated near to the origin is termed as a short vector. Since it comprises a small number of vectors and serves to represent the entire lattice space, a basis continues to be a crucial part of vector data representation. A lattice has numerous bases. Several significant issues with hard lattices include the following:

Short Vector Problem: A short vector problem is one in which the attacker must locate a grid point in the supplied lattice L that as closely resembles the source as feasible.
Brief Basis Problem: An extended basis for a framework L will be specified, the attacker will find short basis among L.
Contiguous Vector Problem: An extended basis for a framework L will be given. Moreover, the challenging point P will be given in the L. The identification of the nearest point to the P within the given L.

While the mentioned challenges may seem relatively simple in a limited context, cryptography deals with lattice spaces of enormous dimensions. The given issues can be resolved with ease for a small base value. However, the provided issues will be challenging to resolve for a large basis value. Since the issue was deemed a challenging mathematical issue. Since the 1800s, mathematicians have studied lattices. Knowing what is possible and what is not with lattice is a result of this insight. This makes sense while asymmetric algorithms are built on the lattice problems. Hence lattice reduction algorithm such as LLL (Lenstra–Lenstra–Lovász) commonly used in the attacker side. To determine the small basis for the long basis of a given lattice space, the LLL polynomial technique is employed. Ajtai-Dwork [17] created a shortest vector problem-based cryptosystem in 1997. In 1998, Nguyen and Ster succeeded [19]. The Closest Vector Problem serves as the foundation for the Goldreich-Goldwasser-Halevi algorithm [20], which was released. This was discovered in 1999 by Nguyen [21]. NTRU [22] was published in 1996. The NTRU encryption technology has become a strong contender for the NIST Standardization process after years of development and improvement. Two different second-round NTRU candidates were combined to create the present NTRU version.

6.2. Hash-based Cryptography

Hash-based digital signature techniques take the place of current digital signature methods. The asymmetric algorithms like RSA are used in the digital signature algorithm. However, hash-based cryptography relies on two crucial properties of hash functions: resistance to collision and resistance to preimages. Preimage resistance is the measure of how difficult it is to find an input x given the output y of a hash function, written as y = H(x). Because of the poor collision resistance H, it is challenging to calculate the following message m2 such that H(m1)=H(m2) for a given message mi. Messages 1 and 2 can be found using the same hash function with a significant collision resistance so that H(m1)=H(m2). If the hash algorithm is reliable, locating collisions and preimages can be difficult. It is difficult to find a suitable quantum algorithm to address this problem. Therefore, in the post-quantum era, authentication can be done via a hash-based digital signature mechanism. The fact that each digital signature algorithm can only be used once has an impact on them.

In 1979 [23], Lamport invented the hash digital signature system. Witernitz introduced a highly efficient One Time Signature scheme, surpassing Lamport's technique in terms of key and signature size. By creating the Merkle Signature Method, which combines Witernitz's technique with binary trees, Merkle improved this field even further. SPHINCS+, a rival proposal for digital signatures, includes the Forest of Random Subsets signature scheme, the Witernitz One-Time Signature Plus Scheme, and Merkle hash trees.

6.3. Code-based Encryption

Error-correcting codes serve as the foundation of code-based cryptography [6]. For the past four decades computer scientist were being studying and working on these. As above-mentioned already, error correcting codes are widely used in data communication to correct the transmission error. Any data that is submitted into an error-correction coding block will have random error added to it before being transferred. Code-based cryptosystems like the McEliece algorithm are frequently employed [24].

Table 2. Overall Performance Assessment of Post-Quantum Algorithms

Properties	BLISS [27] 128-bit security	Ring LWE [28] (More than 156-bit security)	NTRU (80-bit security)	Lamport	Lamport with Merkle (80-bit security)	Rainbow [29]	McEllice	Neidrreiter [30] 80-bit security
Public key (KB)	7	***	2	12	0.09	135.2	505	76.082
Private key (KB)	2	***	1	10	255	98.4	1003	5.335
Signature size	8.245	***	***	***	***	7.21	***	***
Signature time	330 ms	***	***	***	***	167.2 ms	***	***
Verification time	89 ms	***	***	***	***	293.2 ms	***	***
Encryption time	***	69 ms	***	***	***	***	***	1.8 ms/op
Decryption time	***	19.3 ms	***	***	***	***	***	185 ms/op
Possible attacks	***	***	***	***	***	***	***	***
Platform	Atmel ATxmega – 128 A1	Atmel ATxmega – 128 A1	PC (not specified)	PC (not specified)	PC (not specified)	Atmel ATxmega – 128 A1	PC (not specified)	Atmel ATxmega – 256 A1

The linear error correction codes, which are based on matrix multiplication, are how the McEliece algorithm operates. The effective error-correction code used by the receiver is multiplied by two blind matrices to create a defective correction code. This flawed correction code acts as the public key, shared among both senders and receivers. When the sender transmits the message, it is accompanied by a flawed error correction code. Based on the overhead, additional mistakes are made, leading to a dispersed final ciphertext. Decryption takes place at the receiver's end using a trustworthy error correction code applied to the ciphertext. Nobody has found a bug in the McEliece algorithm since it was released in 1978 [25]. The size of the public key is the fundamental barrier preventing its practical application. It is far bigger than asymmetric alternatives like RSA.

6.4. Multivariate Cryptography

The complex mathematical challenge of solving a system of multivariate polynomials serves as the foundation for multivariate cryptosystems. Multivariate cryptography is mostly built on multivariate quadratic maps [26]. The quadratic map contains a sequence of *a=(a_1,….a_n)∈F_y^n* and gives the output *b=(x_1 (a),…x_m (a))∈F_y^m*. The quadratic map equation consists of *x_i (a)* are multivariant quadratic polynomials for *i=1,…m* and the coefficients of the polynomials are in *F_y*. A multivariant quadratic map P with m components and n variables is what the map is known as. The MQ issue, a complex multivariate cryptography task, is regarded as being problematic even for quantum computers.To solve this problem, strategies like the Grobner basis can be used. To address the MQ problem, a number of Grobner basis-like algorithms, including F4/F5 and XL, have recently been created [31]. Numerous digital signature solutions have been put forth by researchers with the goal of resolving the MQ issue. The Oil and Vinegar plan is one of them and is extensively used. The digital signature system Rainbow, a finalist in the NIST competition, is based on the Unbalanced Oil and Vinegar method. The overall performance of the post quantum algorithms has been tabulated in Table 2.

7. Conclusion

The area of quantum cryptography is new and expanding quickly. Businesses worldwide invest substantially to enhance the comprehension and expertise in post-quantum security. Given the widespread interest and extensive research conducted across various regions, it is crucial to grasp the present focus on quantum security and the latest progress made in this domain. In this survey, various post-quantum cryptography techniques have been compared and analysed as the comparative study. Lattice-based cryptography schemes show good promise even when implemented in a restricted microcontroller, as shown by the comparison table, as they require the least time for multiple operations and use the least memory. However, a more thorough investigation must be done before it can be said with certainty that Lattice-based encryption is the best among post-quantum cryptography. The development and study of post-quantum cryptography algorithms in software simulation and limited devices will be included in future studies.

References

[1] Karthikeyan BG, Leurent. On the Practical (In-)Security of 64-Bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security; 2016. p. 1-6.

[2] Sehgal SK, Gupta R. Quantum Cryptography and Quantum Key. Proceedings of International Conference on Industrial Electronics Research and Applications: 2021. p. 1-5.

[3] Pan Y, Deng Y. A Ciphertext-Only Attack Against the Cai-Cusick Lattice-Based Public-Key Cryptosystem. IEEE Transactions on Information Theory. 2011; vol. 57: p. 1780-1785.

[4] Lee Y, Cho J, Kim YS. Cryptanalysis of the Ivanov-Kabatiansky-Krouk-Rumenko Cryptosystems. IEEE Communications Letters. 2020; vol. 24: p. 2678-2681.

[5] Mariot L, Picek S, Yorgova R. On McEliece-Type Cryptosystems Using Self-Dual Codes With Large Minimum Weight. IEEE Access. 2023; vol. 11: p. 43511-43519.

[6] Ji X, Wang B, Hu F, Wang C, Zhang H. New advanced computing architecture for cryptography design and analysis by D-Wave quantum annealer. Journal of Tsinghua Science and Technology, 2022; vol. 2: p. 751-759.

[7] Shahid F, Ahmad I, Imran M, Shoaib M. Novel One Time Signatures (NOTS): A Compact Post-Quantum Digital Signature Scheme. IEEE Access. 2020; vol. 8: p. 15895-15906.

[8] Odin Hashemi SH, Hodtani GA. A Modified McEliece Public-Key Cryptosystem Based On Irregular Codes Of QC-LDPC and QC-MDPC. Proceddings of 27th Iranian Conference on Electrical Engineering: 2019. p. 1373-1376.

[9] Choi P, Kim JH, and Kim DK. Fast and Power-Analysis Resistant Ring Lizard Crypto-Processor Based on the Sparse Ternary Property. IEEE Access. 2019; vol. 7: p. 98684-98693.

[10] Eka Pratama P, Gusti I . Post Quantum Cryptography: Comparison between RSA and McEliece. Proceddings of International Conference on ICT for Smart Society; 2022. p. 01-05.

[11] Fernández-Caramès TM, and Fraga-Lamas P.Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. IEEE Access. 2020; vol. 8: p. 21091-21116.

[12] Oder, Tobias, Thomas P, Tim G. Beyond ECDSA and RSA: Lattice-based digital signatures on constrained devices: Proceedings of the 51st Annual Design Automation Conference; 2014. p 1-8.

[13] Pppelmann, Thomas, Tobias Oder, Tim Gneysu. High-performance ideal lattice-based cryptography on 8bit ATxmega microcontrollers: Proceedings of

International Conference on Cryptology and Information Security in Latin America; Springer International Publishing; 2015. p 1-7.

[14] Kumar et al A. Survey of Promising Technologies for Quantum Drones and Networks. IEEE Access. 2021; vol. 9: p. 125868-125911.

[15] Sutradhar K and Om H. A Generalized Quantum Protocol for Secure Multiparty Summation. IEEE Transactions on Circuits and Systems II: Express Briefs. 2020; vol. 67: p. 2978-2982.

[16] Lella E. Cryptography in the Quantum Era: Proceedings of IEEE 15th Workshop on Low Temperature Electronics; 2022. p. 1-4.

[17] Giroti I, Malhotra M. Quantum Cryptography: A Pathway to Secure Communication. Proceddings of 6th International Conference on Computation System and Information Technology for Sustainable Solutions: 2022. p. 1-6.

[18] Chen ACH. Post-Quantum Cryptography Neural Network. Proceedings of International Conference on Smart Systems for applications in Electrical Sciences: 2023. p. 1-6.

[19] Cohen A, D'Oliveira G L, Salamatian S, Médard M. Network Coding-Based Post-Quantum Cryptography. IEEE Journal on Selected Areas in Information Theory. 2021; vol. 2: p. 49-64.

[20] Putranto R, Wardhani H, Larasati T , Kim H. Space and Time-Efficient Quantum Multiplier in Post Quantum Cryptography Era. IEEE Access. 2023; vol. 11: p. 21848-21862.

[21] Jain R, Miller C A, Shi Y. Parallel Device-Independent Quantum Key Distribution. in IEEE Transactions on Information Theory. 2020; vol. 66 (9) : p. 5567-5584.

[22] Cohen A, D'Oliveira R G L, Salamatian S Médard M. Network Coding-Based Post-Quantum Cryptography. in IEEE Journal on Selected Areas in Information Theory. 2021; vol. 2: p. 49-64.

[23] Jain R, Miller CA Shi Y. Parallel Device-Independent Quantum Key Distribution. IEEE Transactions on Information Theory. 2020; vol. 66: p. 5567-5584.

[24] Yano H, Suzuki Y, Itoh KM, Raymond R, Yamamoto N. Efficient Discrete Feature Encoding for Variational Quantum Classifier. IEEE Transactions on Quantum Engineering. 2021; vol. 2: p. 1-14.

[25] Lee Y, Cho J, Kim YS. Cryptanalysis of the Ivanov-Kabatiansky-Krouk-Rumenko Cryptosystems. IEEE Communications Letters.2020; vol. 24: p. 2678-2681.

[26] Harn L, Hsu CF, Xia Z, He Z. Lightweight Aggregated Data Encryption for Wireless Sensor Networks (WSNs). IEEE Sensors Letters. 2021; vol. 5 (4): p. 1-4.

[27] Kaffah FM, Gerhana YA, Huda IM. E-Mail Message Encryption Using Advanced Encryption Standard (AES) and Huffman Compression Engineering: Proceedings of 6th International Conference on Wireless and Telematics; 2020. p. 1-6.

[28] Zhang X, Wang X. Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem. IEEE Access. 2018; vol. 6: p. 70025-70034.

[29] Mehrabi MA, Doche C, Jolfaei A. Elliptic Curve Cryptography Point Multiplication Core for Hardware Security Module. IEEE Transactions on Computers. 2020; vol. 69: p. 1707-1718.

[30] Yu S, Huang Q. Hard Reliability-Based Ordered Statistic Decoding and Its Application to McEliece Public Key Cryptosystem. IEEE Communications Letters. 2022; vol. 26: p. 490-494.

[31] Althobaiti OS, Dohler M. Quantum-Resistant Cryptography for the Internet of Things Based on Location-Based Lattices. in IEEE Access. 2021; vol. 9: p. 133185-133203.