Evaluation and Comparison of Lattice-based Cryptosystems for a Secure Quantum Computing Era

Maria Sabani *, Ilias K. Savvas, Dimitrios Poulakis, Georgia Garani, Georgios Makris

Posted Date: 8 May 2023

doi: 10.20944/preprints202305.0515.v1

Keywords: Quantum Computing; Lattice-based cryptosystems; Post-Quantum Cryptography

Article

Evaluation and Comparison of Lattice-Based Cryptosystems for a Secure Quantum Computing Era

Maria E. Sabani [1,†,‡*], Ilias K. Savvas [1,‡], Dimitrios Poulakis [2,‡], Georgia Garani [1,‡] and Georgios C. Makris [1,‡]

[1] Dept. of Digital Systems, University of Thessaly, Greece; masampani@uth.gr, isavvas@uth.gr, garani@uth.gr, makris@uth.gr
[2] Dept. of Mathematics, Aristotle University of Thessaloniki, Greece; poulakis@math.auth.gr
* Correspondence: masampani@uth.gr
† Current address: Dept. of Digital Systems, University of Thessaly, Geopolis Campus, Larissa-Trikala Ring-Road, 415 00, Larissa, GREECE.
‡ These authors contributed equally to this work.

Abstract: The rapid development of quantum computing devices promises powerful machines with capabilities that solve a wide range of problems that traditional computers cannot. Therefore, quantum computers generate new threats at unprecedented speed and scale and specifically pose an enormous threat to encryption. Lattice-based cryptography is considered to be the rival to a quantum computer attack and the future of post-quantum cryptography. So, cryptographic protocols based on lattices have a variety of benefits, like security, efficiency, lower energy consumption, and speed. In this work, we study the most well-known lattice-based cryptosystems while a systematic evaluation and comparison is presented also.

Keywords: quantum computing; lattice-based cryptosystems; post-quantum cryptography

1. Introduction

Quantum computing constitutes a critical issue as the impact of theirs advent and development, will be present in every cell of our technology and therefore our life. Quantum computational systems use the qubit (QUantum BIT) instead of the typical bit, which has a unique property; it can be in basic states $|0\rangle$, $|1\rangle$ or in any linear combination of these two states, such that $a|0\rangle + b|1\rangle, a, b \in \mathbb{C}, \wedge a^2 + b^2 = 1$ [67]. This is an algebraic-mathematical expression of quantum superposition which claims, that two quantum states can be added and their sum can be also a valid quantum state [57]. Regardless of superposition, quantum computers' power and capability, are based on quantum mechanics and specifically on the phenomenon of quantum entanglement and the no-cloning system. The odd phenomenon of quantum entanglement states that there are particles that are generated, interact and connected, regardless the distance or the obstacles that separate them [66]. This fundamental law of quantum physics allows us to know or to measure the state of one particle if we know or measure the other particles.

A programmable quantum device is able to solve and overcome problems that a classical computer is unable to solve in any logical amount of time. A quantum computer can perform operations with enormous speed, in a flash of an eye, process and store an extensive number of information. This huge computational power which makes quantum computers superior than classical computers, was described in 2012 by John Preskill with the term quantum supremacy [61]. Quantum Mechanics provides us a fascinating theorem, the no-cloning theorem. As an evolution of no-go theorem by James Park, the no-cloning theorem states that the creation of identical copies of an arbitrary unknown quantum state is forbidden [57]. This is a fundamental theorem of quantum physics and quantum cryptography.

Cryptography is the science of secure communication that implements complex mathematics into cryptographic protocols and algorithms [62] The cryptosystems, they appear in every electronic

 doi:10.20944/preprints202305.0515.v1

transaction and communication in our everyday life. The security, the efficiency and the speed of these cryptographic methods and schemes, are the main issue of interest and study. The contemporary cryptosystems are considered to be vulnerable to a quantum computer attack. In the 1994, the American mathematician and cryptographer professor Peter Shor presented an algorithm [70], which dumbfound the scientists. Shor in his work argued that with the implementation of the proposed algorithm in a quantum device, there is no more security in current computational systems. This was a real revolution for the science of computing and a great motivator for the design and construction of quantum computational devices. Post-quantum cryptography refers to cryptographic algorithms that are thought to be secure against an attack by a quantum computer. Post-quantum cryptography studies and analyzes the preparation for the era of quantum computing by updating existing mathematical-based algorithms and standards [12].

Lattice-based cryptographic protocols attract the interest of researchers for an amount of reasons. Firstly, the algorithms that are applied to lattice-based protocols are simple and efficient. Additionally, they have proven to be secure protocols and create a multitude of applications.

In this review, we examine the cryptographic schemes that are developed for a quantum computer. The following research questions were answered:

- How much the science of Cryptography is affected by quantum computers ?
- What cryptosystems are efficient and secure for the quantum era?
- Which are the most known lattice-based cryptographic schemes and how do they function?
- How can we evaluate NTRU, LWE and GGH cryptosystem?
- Which are their strengths and weaknesses ?

The rest of the paper is organized as follows. In Section 2 we present the changes and the challenges due to quantum devices in cryptography and in Section 3 are described the cryptographic schemes in quantum era. In Section 4 we present some basic issues about lattice theory. In Sections 5 and 6 we present the lattice based cryptographic schemes NTRU, LWE and GGH correspondingly, while is given a discrete implementation of them. In addition, the GGH cryptosystem is described in Section 7. Results and comparisons are given in Section 8 while some future work directions are presented in Section 9. Finally, Section 10 concludes this work.

2. The evolution of Quantum Computing in Cryptography

Cryptography is an indispensable tool for protecting information in computer systems and modern cryptographic algorithms are based on hard mathematical problems, such as the factorization of large prime numbers and the discrete logarithm problem. We can divide the cryptographic protocols in two broad categories: symmetric cryptosystems and asymmetric (public key cryptosystems) cryptosystems [62].

Symmetric cryptosystems use the same key for encryption and decryption and despite their speed and their easy implementation, they have certain disadvantages. One main issue of this type of cryptosystems is the secret key distribution between two parties that want to communicate safely. Another drawback of symmetric cryptographic schemes is that, the private keys which are being used must be changed frequently in order not to be known by a fraudulent user. If we can ensure the existence of an efficient method to generate and exchange keys, symmetric encryption and decryption methods are considered to be secure.

Asymmetric cryptographic schemes use a pair of keys, private and public key, for encryption and decryption. This type of cryptosystems relies on mathematical problems that are characterized as hard to be solved. Some of the most widely known and implemented public key cryptosystems are RSA [63], the Diffie-Helman protocol, ECDSA and others. Since the early 1990's all these cryptographic schemes were believed to be effective and secure but Shor's algorithm changed things up.

Peter Shor proved with his algorithm, that a quantum computer could quickly and easily compute the period of a periodic function in polynomial time [68]. Since 1994, when Shor's protocol was presented, has been a great amount of study, analysis and implementation of the algorithm both in

 doi:10.20944/preprints202305.0515.v1

classical and quantum computing devices. Shor's method solves the factorization problem and the discrete logarithm problem, that are the basis of the current cryptographic schemes and therefore the public key cryptosystems are insecure and vulnerable to a quantum attack [70].

2.1. Quantum Cryptography

In 1982, for the first time was recommended the term "Quantum Cryptography" but the idea of quantum information was appeared for the first time in the decade of 1970's, from Stephen Wiesner and his work about quantum money [77]. Quantum Cryptography is the science that uses the main principles of quantum physics to transfer or store data in complete security. In general, in Quantum Cryptography the transmission and the encryption procedure is performed with the aid of Quantum Mechanics [75]. Quantum cryptography exploits the fundamental laws of Quantum Mechanics like superposition and quantum entanglement, and constructs cryptographic protocols advanced and more efficient.

A basic problem in classical cryptographic schemes is the key generation and exchange, as this process is endangered and unsafe when takes place in an insecure environment. When two different parties want to communicate and transfer data, they exchange information (i.e. key, message) and this procedure occurs in a public channel, so their communication could be vulnerable to an attack by a third party [11]. The most fascinating and also useful discovery and widely used method of Quantum Cryptography is the Quantum Key Distribution.

2.2. Quantum Key Distribution

Quantum Key Distribution (QKD) utilizes the laws of Quantum Physics in the creation of a secret key through a quantum channel. With the principles of Quantum Physics, in QKD a secret key is being generated and a secure communication between two (or more parties) is been established. The inherent randomness of the quantum states and the results accrue from their measurements have as a result a total randomness in the generation of the key. Quantum Mechanics, solves the problem of key distribution - the main challenge in cryptographic schemes - with the aid of quantum superposition, quantum entanglement and the Uncertainty Principle of Heisenberg. Heisenberg's Principle argues that two quantum states cannot be measured simultaneously [66] . This principle has as consequence, the detection of someone who tries to eavesdrop the communication between two parties. If a fraudulent user tries to change the quantum system, he will be detected and the users abort the protocol.

Let us suppose that we have two parties that they want to communicate and use a Quantum Key Distribution protocol to generate a secret key. A quantum key distribution scheme has two phases and for its implementation it is necessary the existence of a classical and a quantum channel. In the quantum channel, it is generated and reproduced the private key and in the classical channel takes place the communication of the two parties. Into the quantum channel are sent polarized photons and each one of the photons has a random quantum state. Both the two parties have in their possession a device that collects and measures the polarization of these photons. Due to Heisenberg's principle, the measurement of the polarized photons can reveal a possible eavesdropper as in his effort to elicit information, the state of the quantum system changes and the fraudulent user is being detected.

In 1984, Charles Bennett and Gilles Brassard proposed the first Quantum Key Distribution protocol, the BB84 protocol, named by its developers and the year it was published [10]. BB84 is the most studied, analyzed and implemented QKD protocol and since then have been proposed various QKD protocols. B92 and SARG04 that are known as variants of BB84, and E91 that exploits the phenomenon of quantum entanglement, are a few of the widely known quantum key distribution protocols [67]. All these QKD protocol are in theory well designed and structured and are proved to be secure, but in practice, in their implementation, there are imperfections. Loopholes, as unwell constructed detectors or defective optical fibers, and generally imperfections in devices and the practical QKD system, make

 doi:10.20944/preprints202305.0515.v1

the QKD protocols vulnerable to attacks. Exploiting these weaknesses of the system, one can perform certain types of attacks and this is the basic issue of research and study, the QKD security.

3. Cryptographic Schemes in Quantum Era

The advances in computer processing power and the evolution of quantum computers for many people, seem to be a threat in the distant future. On the other hand, researchers and security technologists are anxious about the capabilities of a quantum computational device to threat the security of contemporary cryptographic algorithms. Shor's algorithm consists of two parts, a classical part and a quantum part and with the aid of a quantum routine could break modern cryptographic schemes, like RSA and the Diffie-Hellman cryptosystem[23]. These type of cryptosystems are based on hard mathematical problems like the factorization problem and the discrete logarithm problem, the cornerstone of modern cryptographic schemes.

From that moment and after, it is widely known in the scientific and technological community, that with the arrival of a sufficiently large quantum computer there is no more security in ours encryption schemes. Therefore, post-quantum data encryption protocols are the basic topic of research and work, with main goal to construct cryptosystems resistant to quantum computers' attacks [12]. Subsequently, we present certain cryptographic schemes that have been developed and there are secure under an attack of a quantum computer.

3.1. Code-Based Cryptosystems

Coding Theory is an important scientific field which study and analyze linear codes that are being used for digital communication. The main subject of research in Coding Theory is finding a secure and efficient data transmission method. In the process of data transmission, often, data are lost due to errors owing to noise, interference or other reasons and the main subject of study of coding theory is to minimize this data loss [74]. When two discrete parties want to communicate and transfer data, they add extra information to each message which is transferred to enable the message to be decoded despite the existing errors.

Code-based cryptographic schemes are based on the theory of error correcting codes and are considered to be prominent for the quantum computing era. These cryptosystems are considered to be reliable and their hardness relies on hard problems of coding theory, such as the syndrome decoding (SN) and learning parity with noise (LPN).

In 1978 Robert McEliece, proposed the first code-based cryptosystem based on the hardness of decoding random linear codes, a problem which is considered to be NP-hard [44]. The main idea of McEliece is to use an error-correcting code, for which it is known a decoding algorithm and which is capable to correct up to t errors to generate the secret key. The public key is constructed by the private key, covering up the selected code as a general linear code. The sender creates a codeword using the public key that is disturbed up to t errors. The receiver performs error correction and efficient decoding of the codeword and decrypts the message.

McEliece's cryptosystem and Niederreiter cryptosystem that was proposed by Harald Niederreiter in 1986 [53], can be suitable and efficient for encryption, hashing and signature generation. McEliece cryptosystem has a basic disadvantage, the large size of the keys and ciphertexts. In modern variants of McEliece cryptosystem has been an effort to reduce the size of the keys. However, these type of cryptographic schemes are considered to be resistant to quantum attacks and this make them prominent for post-quantum cryptography.

3.2. Hash-Based Cryptosystems

Hash based cryptographic schemes in general, generate digital signatures and relies on the security of cryptographic hash functions, like SHA-3. In 1979, Ralph Merkle proposed a public key signature scheme based on one-time signature (OTS) and Merkle signature scheme is considered to

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

be the simplest and the most widely known hash-based cryptosystem [45]. This digital signature cryptographic scheme converts a weak signature with the aid of a hash function to a strong one.

The Merkle signature scheme is a practical development of Leslie Lamport's idea of OTS that turn it into a many times signature scheme, a signature process that could be used multiple times. The generated signatures are based on hash functions and their security is guaranteed even against quantum attacks.

Many of the reliable signature schemes based on hash functions have the drawback, that the person who signs must keep a record of the exact number of previously signed messages, and any error in this record will create a gap in their security. Another disadvantage of these schemes is that it can be generated certain number of digital signatures and if this number increases indefinitely, then the size of the digital signatures is very large. However, hash-based algorithms for digital signatures are regarded as safe and strong against a quantum attack and can be used for post-quantum cryptography.

3.3. Multivariate Cryptosystems

In 1988 T. Matsumoto and H. Imai [42] presented a cryptographic scheme which is based on multivariate polynomials of degree two over a finite field, for encryption and for signature verification. In 1996 J. Patarin [59] implemented a cryptosystem that relies its security on difficulty of solving systems of multivariate polynomials in finite fields.

The multivariate quadratic polynomial problem states that given m quadratic polynomials $f_1, ..., f_m$ in n variables $x_1, ..., x_n$ with their coefficients to be chosen from a field $\mathbb{F}$, is requested to find a solution $z \in \mathbb{F}^n$ such that $f_i(z) = 0$, for $i \in [m]$. The choice of the parameters make the cryptosystem reliable and safe against attacks, so this problem is considered to be NP - hard.

This type of cryptographic schemes are believed to be efficient and fast, with high speed computations process and proper for implementation on smaller devices. The need of new, stronger cryptosystems with the evolution of quantum computers created various candidates for secure cryptographic schemes based on the multivariate quadratic polynomial problem [12]. These type of cryptosystems are considered to be an active issue of research due to their quantum resilience.

3.4. Lattice-Based Cryptosystems

Cryptographic schemes that are based on lattice theory gain the interest of the researchers and perhaps is the most famous of all candidates for post-quantum cryptography. Let imagine a lattice like a set of points in a n dimensional space with periodic structure. The algorithms which are implemented in lattice based cryptosystems are characterized by simplicity and efficiency and highly parallelizable [56].

Lattice-based cryptographic protocols are proved to be secure, as rely their strong security on well-known lattice problems such as the Shortest Vector Problem (SVP) and the Learning with Errors problem (LWE). Additionally, they create powerful and efficient cryptographic primitives, such as fully homomorphic encryption and functional encryption [39]. Moreover, lattice-based cryptosystems create several applications, like key exchange protocols and digital signature schemes. For all these reasons, lattice based cryptographic schemes are believed to be the most active field of research in the post-quantum cryptography and the most prominent and promising one.

4. Lattices

Lattices are considered to be a typical subject in both cryptography and cryptanalysis and an essential tool for future cryptography, especially with the transition to quantum computing era. The study and the analysis of the lattices goes back to the 18th century, when C.F. Gauss and J.L. Lagrange used lattices in number theory and H. Minkowski with his great work "geometry of numbers" arised the study of lattice theory [60]. In the late 1990s, a lattice was used for the first time in a cryptographic scheme and the latest years the evolution in this scientific field has been enormous, as there are

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

lattice-based cryptographic schemes for encryption, digital signatures, trapdoor functions and much more.

A lattice is a dicrete subgroup of points in n-dimensional space with periodic structure. Any subgroup of $\mathbb{Z}^n$ is a lattice, which is called integer lattice. It is appropriate to describe a lattice using its basis [56]. The basis of a lattice is a set of independent vectors in $\mathbb{R}^n$ and by combining them, the lattice can be generated.

Definition 1. A set of vectors $\{b_1, b_2, ..., b_n\} \subset \mathbb{R}^m$ is linearly independent if the equation

$$c_1 b_1 + c_2 b_2 + ... + c_n b_n = 0, \text{where } c_i \in \mathbb{R} (i = 1, ..., n)$$

accepts only the trivial solution $c_1 = c_2 = ... = c_n = 0$.

Definition 2. Given n linearly independent vectors $b_1, b_2, ..., b_n \in R^m$, the lattice generated by them is defined as

$$\mathcal{L}(b_1, b_2, ..., b_n) = \{\sum x_i b_i / x_i \in \mathbb{Z}\}.$$

Therefore, a lattice consists of all integral linear combinations of a set of linearly independent vectors and this set of vectors $\{b_1, b_2, ..., b_n\}$ is called a lattice basis. So, a lattice can be generated by different bases as it is seems in Figure 1.

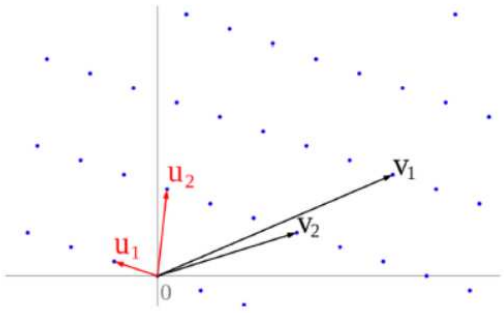

Figure 1. Bases of a lattice

Definition 3. The same number $dim(\mathcal{L})$ of elements of all the bases of a lattice $\mathcal{L}$ it is called the dimension (or rank) of the lattice, since it matches the dimension of the vector subspace $span(\mathcal{L})$ spanned by $\mathcal{L}$.

Definition 4. Let $\mathcal{L}$ be a lattice with dimension n and $B = \{b_1, b_2, ..., b_n\}$ a basis of the lattice. We define as fundamental parallelepiped as the set:

$$\mathcal{P}(b_1, b_2, ..., b_n) = \{t_1 b_1, t_2 b_2, ..., t_n b_n : 0 \leq t_i < 1\} = \sum_{j=1}^{n} [0, 1) b_j$$

Not every given set of vectors forms a basis of a lattice and the following theorem give us a criterion.

Theorem 1. *Let $\mathcal{L}$ be a lattice with rank n and $\{b_1, b_2, ..., b_n\} \in \mathcal{L}$, n linearly independent lattice vectors. The vectors $\{b_1, b_2, ..., b_n\}$ form a basis of $\mathcal{L}$ if and only if $\mathcal{P}(b_1, b_2, ..., b_n) \cap \mathcal{L} = \{0\}$.*

Definition 5. A matrix $U \in \mathbb{Z}^{n \times n}$ is called unimodular if $detU = \pm 1$.

For example, the matrix

$$\begin{pmatrix} 4 & 5 \\ 13 & 16 \end{pmatrix}$$

with $det(U) = -1$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

Theorem 2. *Two bases $B_1, B_2 \in \mathbb{R}^{m\times n}$ generate the same lattice if and only if there is an umimodular matrix $U \in \mathbb{R}^{n\times n}$ such that $B_2 = B_1U$.*

Definition 6. Let $\mathcal{L} = \mathcal{L}(\mathcal{B})$ be a lattice of rank n and let B a basis of $\mathcal{L}$. We define the determinant of $\mathcal{L}$ denoted $det(\mathcal{L})$, as the n-dimensional volume of $\mathcal{P}(\mathcal{B})$.

We can write

$$det(\mathcal{L}(\mathcal{B})) = vol(P) \text{ and also}$$

$$det(\mathcal{L}) = \sqrt{det(B^TB)}.$$

An interesting property of the lattices is that the smaller the determinant of the lattice is, so the denser the lattice is.

Definition 7. For any lattice $\mathcal{L} = \mathcal{L}(\mathcal{B})$, the minimum distance of $\mathcal{L}$ is the smallest distance between any two lattice points:

$$\lambda(\mathcal{L}) = inf\{\|x - y\| : x, y \in \mathcal{L}/x \neq y\}$$

It is obvious that the minimum distance can be equivalently defined as the length of the shortest nonzero lattice vector:

$$\lambda(\mathcal{L}) = inf\{\|v\| : v \in \mathcal{L},\ \{0\}\}$$

4.1. Shortest Vector Problem (SVP)

The Shortest Vector Problem (SVP) is a very interesting and extensively studied computational problem on lattices. The Shorter Vector Problem states that given a lattice $\mathcal{L}$ should be found the shortest nonzero vector in $\mathcal{L}$.

That is to say, given a basis $B = \{b_1, b_2, ..., b_n\} \in \mathbb{R}^{m\times n}$, the shortest vector problem is to find a vector $\vec{v}$ satisfying

$$\|\vec{v}\| = \min_{\vec{u}\in\mathcal{L}(\mathcal{B})\ /0} = \lambda(\mathcal{L}(\mathcal{B}))$$

A variant of Shortest Vector Problem is computing the length of the shortest nonzero vector in $\mathcal{L}$ (e.g. $\lambda(\mathcal{L})$) without necessarily finding the vector.

Theorem 3. ***Minkowski's first theorem.*** *The shortest nonzero vector in any n-dimensional lattice $\mathcal{L}$ has length at most $\gamma_n det(\mathcal{L})^{1/n}$, where γ_n is an absolute constant (approximately equals to $\sqrt{n}$) that depend only of the dimension n and $det(\mathcal{L})$ is the determinant of the lattice.*

Two great mathematicians J. Lagrange and C.F.Gauss where the first ones that had studied the lattices and knew an algorithm to find the shortest nonzero vector in two dimensional lattices. In 1773, Lagrange proposed an efficient algorithm to find a shortest vector of a lattice and Gauss, working independently, made a publication with his proposal for this algorithm in 1801 [60].

A g-approximation algorithm for SVP is an algorithm that on input a lattice $\mathcal{L}$, outputs a nonzero lattice vector of length at most g times the length of the shortest vector in the lattice. The LLL lattice reduction algorithm is capable to approximate SVP within a factor $g = O((2/\sqrt{3})n)$ where n is the dimension of the lattice. Micciancio proved that the Shortest Vector Problem is NP-hard even to approximate within any factor less than $\sqrt{2}$ [48]. SVP is considered to be a hard mathemarical problem and can be used as cornerstone for the construction of provably secure cryptographic schemes, like lattice based cryptography.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

4.2. Closest Vector Problem (CVP)

The Closest Vector Problem (CVP) is a computational problem on lattices that relates closely to Shortest Vector Problem. CVP states that given a target point $\vec{x}$, should be found the lattice point closest to the target.

Let $\mathcal{L}$ be a lattice and a fixed point $t \in \mathbb{R}^n$, we define the distance:

$$d(t, \mathcal{L}) : min_{x \in \mathcal{L}} \|x - t\|.$$

CVP can be formulated as following : Given a basis matrix B for the lattice $\mathcal{L}$ and a $t \in \mathbb{R}^n$, compute a non-zero vector $v \in \mathcal{L}$ such that $\|t - v\|$ is minimal. So, we search a non-zero vector $v \in \mathcal{L}$, such that $\|v\| = d(t, \mathcal{L})$.

Another version of the CVP is computing the distance of the target from the lattice, without finding the closest vector of the lattice and many applications only demand to find a lattice vector that is not too far from the target, not necessarily the closest one.

The most famous polynomial-time algorithms to solve the Chortest Vector Problem are Babai's algorithm and Kannan's algorithm which are based on lattice reduction. Below we present the first algorithm which was proposed by Lazlo Babai in 1986 [4].

Algorithm 1 Babai's Round-off Algorithm

Input: basis $B = \{b_1, b_2, ..., b_n\} \in \mathbb{Z}^n$, target vector $c \in \mathbb{R}$
Output: approximate closest lattice point of c in $L(B)$
1: procedure RoundOff
2: Compute inverse of $B : B^{-1} \in \mathbb{Q}^n$
3: $v := B[B^{-1}c]$
4: return v
5: end procedure

CVP is considered to be NP-hard to solve approximately within any constant factor and is the cornerstone for many cryptographic schemes of lattice cryptography where the decryption procedure corresponds to a CVP computation [49]. Besides cryptography, CVP has various applications in computer science and the problem to find a good CVP approximation algorithm with approximation factors that grow as a polynomial in the dimension of a lattice is an active open problem in lattice theory.

4.3. Lattice reduction

Lattice reduction or else Lattice Basis Reduction is about finding an interesting, useful basis of a lattice. Such a requested useful basis, from a mathematical point of view, satisfies a few strong properties. A lattice reduction algorithm is an algorithm that takes as input a basis of the lattice and returns a simpler basis which generates the same lattice. For computing science we are interested in computing such bases in a reasonable time, given an arbitrary basis. In general, a reduced basis is composed from vectors with good properties, such as being short or being orthogonal.

In 1982 Arjen Lenstra, Hendrik Lenstra and Laszlo Lovasz published a polynomial-time basis reduction algorithm, LLL, which took its name from the initials of their surnames [36]. The basis reduction algorithm approaches the solution of the smallest vector problem in small dimensions, especially in two dimensions, the shortest vector is too small that can be computed in a polynomial time. On the contrary, in large dimensions there is no algorithm known which solves the SVP in a polynomial time. With the aid of the Gram-Schmidt orthonormalization method we define the base reduction method LLL .

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

5. The NTRU cryptosystem

NTRU is a public key cryptosystem that was presented in 1996 by Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman [32]. Until 2013, the NTRU cryptosystem was only commercially available but after, it was released into the public domain for public use. The NTRU is one of the fastest public key cryptographic schemes, it uses polynomials rings for the encryption and decryption of data, and it is based on the shortest vector problem in a lattice. NTRU is more efficient than other current cryptosystems like RSA, and is believed to be resistant to quantum computers attacks and this make it prominent post quantum cryptosystem.

To describe the way NTRU cryptographic scheme operates, firstly we have to give some definitons.

Definition 8. Fix a positive integer N. The ring of convolution polynomials (of rank N) is the quotient ring

$$R = \frac{\mathbb{Z}[X]}{(X^N - 1)}. \tag{1}$$

Definition 9. The ring of convolution polynomials (modulo q) is the quotient ring

$$R_q = \frac{(\mathbb{Z}/q\mathbb{Z})[x])}{(X^N - 1)}. \tag{2}$$

Definition 10. We consider a polynomial $a(x)$ as an element of R_q by reducing its coefficients mopulo q. For any positive integers d_1 and d_2, we let

$$\mathcal{L}(d_1, d_2) = a(x) \in R : \left\{ \begin{array}{c} a(x) \text{ has } d_1 \text{ coefficients equal to } 1 \\ a(x) \text{ has } d_2 \text{ coefficients equal to } -1 \\ a(x) \text{ has all other coefficients equal to } 0 \end{array} \right\} \tag{3}$$

Polynomials in $\mathcal{L}(d_1, d_2)$ are called ternary (or trinary) polynomials. They are analogous to binary polynomials, which have only 0's ans 1's as coefficients.

We assume we have two polynomials $a(x)$ and $b(x)$. The product of these two polynomials is given by the formula

$$a(x) \star b(x) = c(x) \text{ with } c_k = \sum_{i=0}^{k} a_i b_{k-i} + \sum_{i=k+1}^{N-1} a_i b_{N+k-i} = \sum_{i+j \equiv k \bmod N} a_i b_j \tag{4}$$

We will denote the inverses by F_q and F_p, such that

$$F_q \star f \equiv 1 (\bmod q) \text{ and } F_p \star f \equiv 1 (\bmod p) \tag{5}$$

5.1. Description

The NTRU cryptographic scheme is based firstly on three well chosen parameters (N, p, q), such that N is a fixed positive large integer, p and q, is not necessary to be prime but are relatively prime, e.g. $gcd(p, q) = 1$ and q will be always larger than p [32]. Secondly, NTRU depends on four sets of polynomials $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_\phi$ and $\mathcal{L}_m$ with integer coefficients of degree $N - 1$ and works on the ring $R = \frac{\mathbb{Z}[X]}{X^N - 1}$.

Every element $f \in R$ is written as a polyonomial or as vector $f = \sum_{N-1}^{i=0} f_i x^i = [f_0, f_1, ..., f_{N-1}]$. We assume that there are two parties, Alice and Bob, that they want to transfer data, to communicate, with security. A trusted party or the first party selects public parametres (N, p, q, d) such that N,p are prime numbers, $gcd(p, q) = gcd(N, q) = 1$ and $q > (6d + 1)p$.

- Alice chooses randomly two polynomials $f(x) \in \mathcal{L}_(d + 1, d)$ and $g(x) \in \mathcal{L}_(d, d)$. These two polynomials are Alice's private key.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

- Alice computes the inverses polynomials

$$F_q(x) = f(x)^{-1} \in R_q \text{ and } F_p(x) = f(x)^{-1} \in R_p \tag{6}$$

- Alice computes $h(x) = F_q(x) \star g(x) \in R_q$ and the polynomial $h(x)$ is Alice's public key. Alice's private key is the pair $(f(x), F_p(x))$ and by only using this key, she can decrypt messages. Otherwise, she can store , which is probably intertible $\bmod q$ and compute $F_p(x)$ when she needs it.

  Alice publishes her key h.
- Bob wants to encrypt a message and chooses his plaintext $m(x) \in R_p$. The $m(x)$ is a polynomial with coefficients m_i such that $-\frac{1}{2}p \leq m_i \leq \frac{1}{2}p$.
- Bob chooses a random polynomial $r(x) \in \mathcal{T}(d,d)$, which is called ephemeral key, and computes

$$e(x) \equiv ph(x) \star r(x) + m(x) (\bmod q) \tag{7}$$

  and this is the encrypted message that Bob sends to Alice.
- Alice computes

$$a(x) \equiv f(x) \star e(x) (\bmod q) \tag{8}$$

- Alice chooses the coefficients of a in the interval from $-q/2$ to $q/2$ (center lifts $a(x)$ to an element of R).
- Alice computes

$$b(x) \equiv F_p(x) \star a(x) (\bmod p) \tag{9}$$

  and she recovers the message m as if the parameters have been chosen correctly, the polynomial $b(x)$ equals to the plaintext $m(x)$.

Depending on the choise of the ephemeral key $r(x)$ the plaintext $m(x)$ can be encrypted with many ways, as its possible encryptions are $ph(x) \star r(x) + m(x)$. The ephemeral key should be used one time and only, e.g. it shouldn't be used to encrypt two different plaintexts. Additionally, Bob shouldn't encrypt the same plaintext by using two different ephemeral keys.

5.2. Discrete implementation

- Assume the trusted party chooses the parametres $(N, p, q, d) = (11, 3, 61, 2)$. As we can see $N = 11$ and $p = 3$ are prime numbers, $gcd(3, 61) = gcd(11, 2) = 1$ and the condition $q > (6d + 1)p$ is satisfied as it is $61 > (6 \cdot 2 + 1)3 = 39$.
- Alice chooses the polynomials

$$f(x) = x^{10} - x^8 - x^6 + x^4 + x^2 + x + 1 \in \mathcal{L}(3, 2)$$
$$g(x) = x^9 - x^8 - x^6 + x^4 + x^2 + 1 \in \mathcal{L}(2, 2)$$

  These polynomials, f, g is the private key of Alice.
- Alice computes the inverses

$$F_{61}(x) = f(x)^{-1} \bmod 61 =$$

$$= 45x^{10} + 49x^9 + 26x^8 + 40x^7 + 53x^6 + 47x^5 + 21x^4 + 24x^3 + 60x^2 + 32x + 31 \in R_{61}$$
$$F_3(x) = f(x)^{-1} = x^9 + x^7 + x^5 + 2x^4 + 2x^3 + 2x^2 + x \in R_3$$

  Alice can store $(f(x), F_3(x))$ as her private key.
- Alice computes

$$h(x) = F_{61}(x) \star g(x) =$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

$$= 11x^{10} + 49x^9 + 26x^8 + 46x^7 + 28x^6 + 53x^5 + 31x^4 + 36x^3 + 30x^2 + 5x + 50$$

and publishes her public key $h(x)$.

- Bob decides to encrypt the message $m(x) = x^7 - x^4 + x^3 + x + 1$ and uses the ephemeral key $r(x) = x^9 + x^7 + x^4 - x^3 + 1$.
- Bob computes and sends to Alice the encrypted message

$$e(x) \equiv ph(x) \star r(x) + m(x) (\mathrm{mod}\, q)$$

that is

$$e(x) = 11x^{10} + 49x^9 + 52x^8 + 35x^7 + 30x^6 + 25x^5 + 35x^4 + 32x^3 + 18x^2 + 56x + 28 (\mathrm{mod}\, 61)$$

.

- Alice receive the ciphertext $e(x)$ and computes

$$f(x) \star e(x) =$$

$$= 58x^{10} + 60x^9 + 60x^8 + 4x^7 + 56x^5 + 6x^4 + 55x^2 + 3x + 6 \in R_{61}$$

- Therefore Alice centerlifts modulo 61 to obtain

$$a(x) = -3x^{10} - x^9 - x^8 + 4x^7 + 5x^5 + 6x^4 - 6x^2 + 3x + 6 \in R_{61}$$

- She reduces $a(x)$ modulo 3 and computes

$$F_3(x) \star a(x) = x^7 + 2x^4 + x^3 + x + 1 \in R_3$$

and recovers Bob's message $m(x) = x^7 - x^4 + x^3 + x + 1$

5.3. Security

NTRU is one of the most fast public key cryptosystems which is based on lattice theory and it is used for encryption (NTRU-Encrypt) and digital signatures (NTRUSign). For the moment that NTRU was presented, in 1996, NTRU security has been a main issue of interest and research. NTRU hardness relies on the hard mathematical problems in a lattice, such as the Shortest Vector Problem [56].

The authors of NTRU in their paper [32] argue that the secret key can de recovered by the public key, by finding a sufficiently short vector of the lattice that is generated in NTRU algorithm. D. Coppersmith and A. Shamir proposed a simple attack against the NTRU cryptosystem. In their work argued that the target vector $f||g \in \mathbb{Z}^{2N}$ (the symbol $||$ denotes vector concatenation) belongs to the natural lattice:

$$L_{CS} = \{F||G \in \mathbb{Z}^{2N} | F \equiv h \star G \bmod q \text{ where } F, G \in \mathbb{R}\}.$$

It is obvious that L_{CS} is a full dimension lattice in $\mathbb{Z}^{2N}$, with volume q^N. The target vector is the shortest vector of L_{CS}, so the SVP-oracle should heuristically output the private keys f and g. Hoffstein et al. claimed that if one chooses the number N reasonably, the NTRU is sufficient secure as all these type of attacks are exponential in N. These type of attacks are based on the difficulty of solving certain lattice problems, such as SVP and CVP. Lattice attacks can be used to recover the private key of an NTRU system, but they are generally considered to be infeasible for the current parameters of NTRU. It is important that the key size of the NTRU protocol is $O(N \log q)$ and this fact makes NTRU a promising cryptographic scheme for post-quantum cryptography.

Furthermore, the cryptanalysis of NTRU is an active area of reasearch and they have been developed other type of attacks against NTRU cryptosystem. We refer to some of them as detailed below.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

- Brute-Force Attack. In this type of attack, are being tested all possible values of the private key until the correct one is found. Brute-force attacks are generally not practical for NTRU, as the size of the key space is very large.
- Key Recovery Attack. This type of attack relies on exploiting vulnerabilities in the key generation process of NTRU. For example, if the random number generator used to generate the private key is weak, a fraudulent user may be able to recover the private key.
- Side-channel Attack. This type of attack take advantage of the weaknesses in the implementation of NTRU, such as timing attack, power analysis attack, and fault attack. Side-channel attacks require physical access to the device running the implementation.

To protect NTRU against these types of attacks and avoid the leak of secret data and information, researchers use various techniques to ensure its security, such as parameter selection, randomization, and error-correcting codes.

6. The LWE cryptosystem

In 2005, O. Regev presented a new public key cryptographic scheme, the Learning with Errors cryptosystem and for this work, Regev won in 2018 the Godel Prize [64]. LWE is one of the most famous lattice-based cryptosystems and one of the most widely studied in recent years. It is based on the Learning with Errors problem and the hardness of finding a random linear function of a secret vector modulo a prime number. The LWE public key cryptosystem is a probabilistic cryptosystem, which relies on a high probability algorithm. Since LWE proved to be secure and efficient, it becomes one of the most contemporary and innovational research topics in both lattice- based cryptography and computer science.

6.1. The Learning with Errors Problem

Firstly, we have to introduce the Learning with Errors problem (LWE). Assuming that we have a secret vector $s = (s_1, s_2, ..., s_n) \in \mathbb{Z}^n$ with coefficients integer numbers and n linear equations such that

$$\begin{aligned} a_{11}s_1 + a_{12}s_2 + ... + a_{1n}s_n &\approx a \\ a_{21}s_1 + a_{22}s_2 + ... + a_{2n}s_n &\approx b \\ &\vdots \\ a_{m1}s_1 + a_{m2}s_2 + ... + a_{mn}s_n &\approx m \end{aligned}$$

We use the symbol "≈" to claim that the value approaches the real answer to within a certain error. This problem is a difficult one as by multiplying and adding rows together, the errors in every different equation will compound, so the final row reduced state will be worthless and the answer will be faraway from the real value.

Definition 11. Let $s \in \mathbb{Z}_q^n$ be a secret vector and χ be a given distribution on $\mathbb{Z}_q$. An LWE distribution $A_{s,n,q,\chi}$ generates a sample $(a, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ or $(A, b) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$ where $a \in \mathbb{Z}_q^n$ is uniformly distributed and $b = \langle a, s \rangle + e$, where $e \leftarrow \chi$ and $\langle a, s \rangle$ is the inner product of a and s in $\mathbb{Z}_q$.

We call $A_{s,n,q,\chi} = (a, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ the LWE distribution, s is called the private key and e is called the error distribution. If $b \in \mathbb{Z}_q$ is uniformly distributed, then is called the uniform LWE distribution.

Definition 12. Fix $n \geq 1$, $q \geq 2$ and an error probability distribution χ on $\mathbb{Z}_q$. Let s be a vector with n coefficients in $\mathbb{Z}_q$. Let $A_{s,\chi}$ on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ be the probability distribution choosing a vector $a \in \mathbb{Z}_q$ uniformly at random, choosing $e \in \mathbb{Z}_q$ according to χ and outputting $(a, \langle a, s \rangle + e)$ where additions are performed in $\mathbb{Z}_q$. We say an algorithm solves LWE with modulus q and error distribution χ if for any $s \in \mathbb{Z}_q^n$ given enough samples from $A_{s,\chi}$ it outputs s with high probability.

Definition 13. Suppose we have a way of generating samples from $A_{s,\chi}$ as above, and also generating random uniformly distributed samples of (a, b) from $\mathbb{Z}_q^n \times \mathbb{Z}_q$. We call this uniform distribution U. The decision-LWE problem is to determine after a polynomial number of samples, whether the samples are coming from $A_{s,\chi}$ or U .

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

Simplifying the definition and formulated in more compact matrix notation, if we want to generate a uniformly random matrix A with coefficients between 0 and q and two secret vectors s, e with coefficients drawn from a distribution with small variance, the LWE sample can be calculated as: $(A, b = As + e \bmod q)$. The LWE problem states that is hard to recover the secret s from such a sample.

Definition 14. For $a > 0$, the family Ψ_a is the (uncountable) set of all elliptical Gaussian ditributions D_r over a number field $K_{\mathbb{R}}$ in which $r \geq a$.

The choise of the parametres is crucial for the hardness of this problem. The distribution is a Gaussian distribution or a binomial distribution with variance 1 to 3, the lenght of the secret vector n is such that $2^9 < n < 2^{10}$ and the modulus q is in the range 2^8 to 2^{16}.

6.2. Description

Assuming $n \geq 1$, $q \geq 2$ are positive integers and χ is a given probability distribution in $\mathbb{Z}_q$. The LWE cryptographic scheme is based on LWE distribution $A_{s,\chi}$ and is being described below.

The parametres of the LWE cryptosystem are of great importance for the security of the protocol. So, let n be the security parameter of the system, m, q are two integers numbers and χ is a probability distribution on $\mathbb{Z}_q$.

The security and the correctness of the cryptosystem are based on the following parametres, which are be chosen appropriately.

- Choose q a prime number between n^2 and $2n^2$.
- Let $m = (1 + \epsilon)(n + 1) \log q$ for some arbitary constant $\epsilon > 0$.
- The probability distribution is chosen to be $\chi = \Psi_{a(n)}$ for $a(n) \in O(1/\sqrt{n} \log n)$

We suppose that are two parties, Alice and Bob, who want to transfer informations securily. The LWE cryptosystem has the typical structure of a cryptographic scheme and its steps are the following.

- Alice chooses uniformly at random $s \in \mathbb{Z}_q^n$. s is the private key.
- Alice generates a public key by choosing m vectors $a_1, a_2, ..., a_m \in \mathbb{Z}_q^n$ independently from the uniform distribution. She also chooses elements (error offsets) $e_1, e_2, ..., e_m \in \mathbb{Z}_q^n$ independently according to χ. The public key is $(a_i, b_i)_{i=1}^m$, where $b_i = \langle a_i, s \rangle + e_i$.

  In matrix form, the public key is the LWE sample $(A, b = As + e \bmod q)$, where s is the secret vector.
- Bob in order to encrypt a bit, chooses a random set S uniformly among all 2^m subsets of $[m]$. The encryption is $(\sum_{i \in S} a_i, \sum_{i \in S} b_i)$ if the bit is 0 and $(\sum_{i \in S} a_i, \lfloor \frac{q}{2} \rfloor + \sum_{i \in S} b_i)$ if the bit is 1.

  In matrix form, Bob can encrypt a bit m by calculating two LWE problems : one using A as random public element, and one using b. Bob generates his own secret vectors s', e' and e and make the LWE samples $(A, b' = A^T s' + e' \bmod q)$, $(b, v' = b^T s' + e'' \bmod q)$. Bob has to add the message that wants to encrypt to one of these samples, where v' is a random integer between 0 and q. The encrypted message of Bob consists of the two samples $(A, b' = A^T s' + e' \bmod q)$, $(b, v' = b^T s' + e'' + \frac{q}{2} m \bmod q)$.
- Alice wants to decrypt Bob's ciphertext. The decryption of a pair (a, b) is 0 if $b - \langle a, s \rangle$ is closer to 0 than to $\lfloor \frac{q}{2} \rfloor$ modulo q. In other case the decryption is 1.

  In matrix form, Alice firstly calculates $\Delta v = v' - b'^T s$. As long as $e^T s' + e'' - s^T e'$ is small enough, Alice recovers the message as $mes = \lfloor \frac{2}{q} \Delta v \rceil$.

6.3. Discrete implementation

We choose $n = 4$ and $q = 13$.

- Alice chooses the private key $s = [2, 5, 0, 6]$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

- Let $m = 3$ so Alice generates the public key with the aid of three vectors $a_i, i = 1, 2, 3$ and three elements $e_i, i = 1, 2, 3$ (error terms). She chooses : $a_1 = [1, 6, 2, 4]$ and $e_1 = 1$, $a_2 = [0, 3, 5, 1]$ and $e_2 = 0$ and $a_3 = [2, 1, 6, 3]$ and $e_3 = -1$. Therefore, Alice's public key is:

$$\{([1, 6, 2, 4], 4), ([0, 3, 5, 1], 8), ([2, 1, 6, 0], 0)\}$$

- Bob wants to encrypt 0 so he takes the subset $S = \{1, 2\}$. So he computes

$$(\sum_{i \in S} a_i, \sum_{i \in S} b_i) = ([1, 6, 2, 4] + [0, 3, 5, 1], 4 + 8) = ([1, 9, 7, 5], 12)$$

- Alice performs the decryption algorithm by computing

$$b - \langle a, s \rangle = 12 - \langle [1, 9, 7, 5], [2, 5, 0, 6] \rangle = 12 - 12 = 0$$

and obviously the decryption is 0 since the output value is closer to 0 (in this case equal to 0) than to $\lfloor \frac{13}{2} \rfloor$ modulo 13.

Therefore, the encryption scheme worked correctly.

6.4. Implementations and Variants

The Learning with Errors (LWE) cryptosystem is a popular post-quantum cryptographic scheme that relies on the hardness of solving certain computational problems in lattices. There are several variants of the LWE cryptosystem, including the Ring-LWE, the Dual LWE, the Module-LWE, the Binary-LWE, the Multilinear LWE and others.

6.4.1. The RING-LWE cryptosystem

This variant of LWE uses polynomial rings instead of the more general lattices used in standard LWE. Ring-LWE has a simpler structure, which makes it faster to implement and more efficient in terms of memory usage. In 2013, Lyubashevsky et al [41] presented a new public key cryptographic scheme that is based in LWE problem.

The Ring-LWE cryptosystem structure.

Lyubachevsky et al proposed a well analyzed a cryptosystem that uses two ring elements for both public key and ciphertext and it is an extension of the public key cryptograsystem on plain lattices.

The two parties that they want to communicate, agree on complexity value of n, the highest co-efficient power to be used. Let $R = \frac{\mathbb{Z}[X]}{(X^n+1)}$ be the fixed ring and it is chosen an integer q, such as $q = 2n - 1$. The steps of the RING-LWE protocol are described below.

- A secret vector s with n length is chosen with modulo q integer entries in ring R_q, where $q \in \mathbb{Z}^+$. This is the private key of the system.
- It is chosen an element $a \in R_q$ and a random small element $e \in R$ from the error distribution and we compute $b = a\dot{s} + e$.

The public key of the system is the pair (a, b).

- Let m be the n bit message that is for encryption.

1. The message m is considered as an element of R and the bits are used as coefficients of a polynomial of degree less than n
2. The elements $e_1, e_2, r \in R$ are generated from error distribution.
3. It is computed the $u = a \cdot r + e_1 \bmod q$.
4. It is computed the $v = b \cdot r + e_2 + \cdot \lfloor \frac{q}{2} \rceil \cdot m \bmod q$ and it is send $(u, v) \in R_q^2$ to receiver.

- The second party receives the payload $(u, v) \in R_q^2$ and computes $r = v - u \cdot s = (r \cdot e - s \cdot e_1 + e_2) + \lfloor \frac{q}{2} \rceil \cdot m \bmod q$. It is evaluated each r_i and if $r_1 \approx \frac{q}{2}$ then the bits are recovered back to 1, or else 0.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

Ring-LWE cryptographic scheme is similar to LWE cryptosystem was proposed by Regev. Their difference is that the inner products are replaced with ring products, so the result is new ring structure, increasing the efficiency of the operations.

6.5. Security

Learning with Errors (LWE) is a computational problem that is the basis for cryptosystems and especially for cryptographic schemes of post-quantum cryptography. It is considered to be a hard mathematical problem and as a consequence the cryptosystems that are based on LWE problem are of high security as well. LWE cryptographic protocols are a contemporary and active field of research and therefore their security is studied and analyzed continually and steadily.

There are a various of attacks can be performed against the cryptosystems which are based in LWE problem. We can say that these types of attacks are in general, those attacks that that exploit weaknesses in the LWE problem itself, and those attacks that exploit weaknesses in the specific implementation of the cryptosystem. Below we present some of these types of attacks that can be launched against LWE-based cryptographic schemes.

- Dual Attack. This type of attack is based on the dual lattice and is most effective against LWE instances with small size of plaintext messages.

  Thus, hybrid dual attacks that are appropriate for spare and small secrets and in a hybrid attack one guesses part of the secret and performs some attacks on the remaining part [13] Since guessing reduces the dimension of the problem, the cost of the attack on the part of the secret that remains it is reduced. In addition,0 the lattice attack component can be reused for multiple guesses. The optimal attack is achieved when the cost of guessing equals to the cost of the lattice attack and we define where the lattice attack component is a primal attack as the hybrid primal attack, and respectively, the hybrid dual attack.
- Shieving Attack. This type of attack is relied on the idea of sieving, which claims to find linear combinations of the LWE samples that reveal information about the secret. Sieving attacks can be used to solve the LWE problem with fewer samples than its original complexity.
- Algebraic attack. This type of attack is based on the idea of finding algebraic relations between the LWE samples that let put secret data information. Algebraic attacks can be suitable for solving the LWE problem with fewer samples than the original complexity as well.
- Side-channel attack. This type of attack exploits weaknesses in the implementation of the LWE-based scheme, such as timing attack and others. Side-channel attacks are generally easier to mount than attacks against the LWE problem itself, but they require physical access to the device running the implementation.
- Attack that use the BKW algorithm. This is a classic attack, is considered to be sub-exponential and is most effective against small or small structured LWE instances.

To mitigate these attacks, LWE-based schemes typically use various techniques such as parameter selection, randomization, and error-correcting codes. These techniques are designed to make the LWE problem harder to solve and to prevent attackers from taking advantage of vulnerabilities in the implementation.

7. The GGH cryptosystem

In 1997 Oded Goldreich, Shafi Goldwasser and Shai Halevi proposed a cryptosystem (GGH) [30] based on algrebraic coding theory and can be seen as a lattice analogue of the McEliece cryptosystem [44]. In both GGH and McEliece schemes, a ciphertext is the addition of a random noise vector corresponding to the plaintext [56]. At GGH cryptosystem the public and the private key is a representation of a lattice and at MCEliece the public and the private key is a representation of a linear code. The basic distinction between these two cryptographic schemes is that the domains in which the operations take place are different. The main idea and structure of GGH cryptographic scheme is characterized by simplicity and it is based on the difficulty to reduce lattices.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

7.1. Description

The GGH public key encryption scheme is formed by the key generation algorithm K, the encryption algorithm E and the decryption algorithm D. It is based on lattices in $\mathbb{Z}^n$, a key derivation function $h : \mathbb{Z}^n \times \mathbb{Z}^n \rightarrow K_s$ and a symmetric cryptosystem (K_s, P, C, E_s, D_s), where K is the key generation algorithm, P the set of plain texts, C the set of ciphertexts, E_s the encryption algorithm and D_s the decryption algorithm.

- The key generation algorithm K generates a lattice L by choosing a basis matrix V that is nearly orthogonal. An integer matrix U it is chosen which has determinant $det(U) = \pm 1$ and the algorithm computes $W = UV$. Then, the algorithm outputs $ek = W$ and $dk = V$.
- The encryption algorithm E receives as input an encryption key $ek = W$ and a plain message $m \in P$. It chooses a random vector $u \in \mathbb{Z}^n$ and a random noise vector u. Then it computes $x = uW$, $z = x + r$ and encrypts the message $w = E_s(h(x, r), m)$. It outputs the ciphertext $c = (z, w)$.
- The decryption algorithm D takes as input a decryption key $dk = V$ and a ciphertext $c = (z, w)$. It computes $x = \lfloor zV^{-1} \rceil V$ and $r = z - x$ and decrypts as $m = D_s(h(x, r), w)$. If D_s algorithm outputs the symbol $\perp$ the decryption fails and then D outputs $\perp$, otherwise the algorithm outputs m.

We assume that exist two users, Alice and Bob, that they want to communicate secretly. The main (classical) process of GGH cryptosystem is being decribed below.

1. Alice chooses a set of linearly independent vectors $v_1, v_2, ..., v_n \in \mathbb{Z}^n$ which form the matrix $V = [v_1, v_2, ..., v_n], v_i \in \mathbb{Z}^n, 1 \leq i \leq n$. Alice, by calculating the Hadamard Ratio of matrix V and verifying that is not too small, checks her vector's choice. This is Alice's private key and we let L be the lattice generated by these vectors.
2. Alice chooses an $n \times n$ unimodular matrix U with integer coefficients, that satisfies $det(U) = \pm 1$.
3. Computes a bad basis $w_1, w_2, ..., w_n$ for the lattice L, as the rows of $W = UV$, and this is Alice's public key. Then, she publishes the key $w_1, w_2, ..., w_n$.
4. Bob chooses a plaintext that he wants to encrypt and he chooses a small vector m (e.g. a binary vector) as his plaintext. Then he chooses a small random "noise" vector r which acts as a random element and r is been chosen randomly between $-\delta$ and δ, where δ is a fixed public parameter.
5. Bob computes the vector $e = mW + r = \sum_{i=1}^{n} m_i w_i + r = x_1 w_1 + x_2 w_2 + ... + x_n w_n + r$ using Alice's public key and sends the ciphertext e to Alice.
6. Alice, with the aid of Babai's algorithm, uses the basis $v_1, v_2, ..., v_n$ to find vector in L that is close to e. This vector is the $a = mW$, since the "noise" vector r is small and since she uses a good basis. Then, she computes $aW^{-1} = mWW^{-1}$ ans she recovers m.

Supposing there is an eavesdropper, Eve, which wants to obtain information of the communication between Alice and Bob. Eve has in her possession the message e that Bob sends to Alice and therefore tries to find the closest vector to e, solving the CVP, using the public basis W. As she uses vectors that are not reasonably orthogonal, Eve will recover a message $\hat{e}$ which probably will not be near to m.

7.2. Discrete implementation

- Alice chooses a private basis $\vec{v_1} = (48, 1)$ and $\vec{v_2} = (-1, 48)$ that it is a good basis since $\vec{v_1}$ and $\vec{v_2}$ are orthogonal vectors, e.g. it is $\langle \vec{v_1}, \vec{v_2} \rangle = 0$. The rows of the matrix $V = \begin{pmatrix} 48 & 1 \\ -1 & 48 \end{pmatrix}$ is Alice's private key. The lattice L spanned by $\vec{v_1}$ and $\vec{v_2}$ has determinant $det(L) = 2305$ and the Hadamard ratio of the basis is $\mathcal{H} = (det(L)/|\vec{v_1}||\vec{v_2}|)^{1/3} \simeq 1$
- Alice chooses the unimodular matrix U that its determinant is equal to 1, such as $U = \begin{pmatrix} 5 & 8 \\ 3 & 5 \end{pmatrix}$ with $det(U) = +1$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

- Alice computes the matrix W, such that $W = UV = \begin{pmatrix} 232 & 389 \\ 139 & 243 \end{pmatrix}$. Its rows are Alice's bad basis $\vec{w}_1 = (232, 389)$ and $\vec{w}_2 = (139, 243)$, since it is $cos(\vec{w}_1, \vec{w}_2) \simeq 0,99948$ and these vectors are nearly parallel and so they are suitable for a public key.
- It is very important the noise vector to be selected carefully and that it is not shift where the nearest point is located. For Alice's basis that generates the lattice L, $\vec{r}$ is chosen that $|\vec{r}| < 20$. So, it is choosen the vector $\vec{r}$ to be (r_x, r_y) with $-10 \leq r_x$ and $r_y \leq 10$.
- Bob wants to encrypt the message $m = (35, 27)$. The message can be seen as a linear combination of the basis $\vec{w}_1, \vec{w}_2$, such as $35\vec{w}_1 + 25\vec{w}_2$ and the noise vector $\vec{r}$ can be added.
- The corresponding ciphertext is $e = mW + r = (35, 27) \begin{pmatrix} 232 & 389 \\ 139 & 243 \end{pmatrix} + (-9, 1) = (19285, 17064) + (-9, 1) = (19276, 17065)$ and Bob sends it to Alice.
- Alice using the private basis, she applies Babai's algorithm and finds the closest lattice point. So, she solves the equation $a_1(48, 1) + a_2(-1, 48) = (19276, 17065)$ and finds $a_1 \simeq 463.02$ and $a_2 \simeq 345.8$. So, the closest lattice point is $a_1(48, 1) + a_2(-1, 48) = 463(48, 1) + 346(-1, 48) = (21878, 17071)$ and this lattice vector is close to e.
- Alice realizes that Bob must have computed $(21878, 17071)$ as a linear combination of the public basis vectors and then solving the linear combination again $m_1(232, 389) + m_2(139, 243) = (21878, 17071)$ she finds $m_1 = 35$ and $m_2 = 27$ and recovers the message $m = (m_1, m_2) = (35, 27)$.

Eve has in her possesion the encrypted message $(19276, 17065)$ that Bob had send to Alice and tries to solve the CVP using the public basis. So, she is solving the equation $m_1(232, 389) + m_2(139, 243) = (19276, 17065)$ and finds the incorrect values $m_1 \simeq 1003.1$, $m_2 \simeq -1535.5$ and recovers the incorrect encryption $m' = (m_1, m_2) = (1003, -1535)$.

In 1999 and in 2001 D. Micciancio proposed a simple technique to reduce both the size of the key and size of the ciphertext of GGH cryptosystem without decreasing the level of its security [50], [46].

7.3. Security

In GGH cryptographic scheme, if a security parameter n is chosen, the key size and the encryption time can take $O(n^2 \log n)$ and it is more effiecient than other cryptosystems like AD.

There are some natural ways to perform an attack to the GGH cryptographic scheme.

1. Leak information and obtain the private key V from the public key W.

   For this type of attack, it is performed a lattice basis reduction (LLL) algorithm on the public key, the matrix W. It is possible that the output is a basis W' that is good enough to allow the efficient solution of the required closest vector instances. If the dimension of the lattice is large enough, is very difficult for this attack to succeed.
2. Try to obtain information about the message from the ciphertext e, assuming that the error vector r is small.

   For this type of attack, it is useful that in the ciphertext $e = mW + r$, the error vector r is a vector with small entries. An idea is to compute $eW^{-1} = mWW^{-1} + rW^{-1}$ and try to deduce possible values for some entries of rW^{-1} . For example, if the j-th column of W^{-1} has particularly small norm, then one can deduce that the j-th entry of rW^{-1} is always small and hence get an accurate estimate for the j-th entry of m. To defeat this attack one should only use some low-order bits of some entries of m to carry information, or use an appropriate randomised padding scheme
3. Try to solve the Closest Vector Problem of e with respect to the lattice that is being generated by W, for example by performing the Babai's nearest plane algorithm or the embedding technique.

Moreover, certain types of attacks can be performed against GGH, which are being discussed below like Nguyen's attack and Lee and Hahn attack.

Goldreich, Goldwasser and Halevi claimed that increasing the key size compensates for the decrease in computation time [56]. When presented their paper, the three authors, published five

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

numerical challenges corresponding to increase the value of the parameters n in higher dimensions with the aim to support their algorithm. In each challenge were given a public key and a ciphertext and was requested to recover the plaintext.

In 1999, P.Nguyen exploited the weakness specific to the way the parametres are chosen and developed an attack against the GGH cryptographic scheme [54]. The first four challenges, for $n = 200, 250, 300, 350$ were broken since then GGH is considered to be broken, partially in its original form. Nguyen argued that the choice of the error vector is its weakness and make it vulnerable to a possible attack. The error vectors used in the encryption of the GGH algorithm must be shorter than the vectors that generate the lattice. This weakness makes Closest Vector Problem instances arising frim GGH easier than general CVP instances [56].

The other weakness of GGH cryptosystem is the choice of the error vector e in the encryption algorithm procedure. The e vector is in $\{\pm\sigma\}^n$ and it is chosen to maximize the Euclidean norm under requirements on the infi

nity norm. Nguyen takes the ciphertext $c = mB + e$ modulo $sigma$, where m is the plaintext and B the public key, and the e disappears from the equation. This is because $e \in \{\pm\sigma\}^n$ and every choice is 0 mod σ. So, this leaks information about the message $m(\mathrm{mod}\sigma)$ and increasing the modulus to 2σ and adding an all $-\sigma$ vector s to the equation. If this equation is solved for m, it leaks information for $m(\mathrm{mod}2\sigma)$. Nyguen also demonstrated that in most cases this equation it could be easily solved for m.

In 2006 Nguyen and Regev performed an attack at GGH signatures scheme, transforming a geometrical problem to a multivariate optimization problem [55]. The final numerical challenge for $n = 400$ was solved by M.S. Lee and S.G. Hahn in 2010 [35]. Therefore, GGH has weaknesses and trapdoors such that it is vulnerable to certain type of attacks, as one attack that allows a fraudulent user to recover the secret key using a small amount of information about the ciphertext. Specifically, if an attacker can obtain the two smallest vectors in the lattice, they can give information and recover the secret key using Coppersmith's algorithm. As a result, GGH has a limited practical use and has been largely superseded by newer and more secure lattice-based cryptosystems. So, while GGH had an important early contribution to the field of lattice-based cryptography, it is not currently considered a practical choice for secure communication due to its limitations in security.

8. Evaluation, Comparison and Discussion

We have presented a few of the main cryptographic schemes that are based on the hardness of lattice problems and especially based on the Closest Vector Problem. GGH is a public key cryptosystem which is based in algebraic coding theory. A plaintext is been added with a vector noise and the result of this addition is a ciphertext. Both the private and the the public key is a depiction of a lattice and the private key has a specific structure. The Nguyen's attack [54] revealed the weakness and vulnerability of the GGH cryptosystem and for many researchers, after that considered GGH to be unusable [52,54]

Therefore, in 2010, M.S. Lee and S.G. Hahn presented a method that solved the numerical challenge of the highest dimension 400 [35]. Applying this specific method Lee and Hann, lead to the conclusion that the decryption of the ciphertext can be accomplished using partial information of the plaintext. Thus, this methods requires some knowledge of the plaintext and can't be performed in actually real cryptanalysis circumstances. At the other side, in M. 2012 Yoshino and N. Kunihiro and C. Gu et al in 2015, have presented a few modifications and improvements in GGH cryptosystem claiming that made it more resistant in these attacks [78].

The same year C.F. de Barros and L.M. Schechter with their paper "GGH may not be dead after all", proposed certain improvements for GGH and finally a variation of the GGH cryptographic scheme [8]. De Barros and Schecher by reducing the public key, in order to find a basis with the aid of Babai's algorithm perform a direct way to attack to GGH. They increase the length of the noise vector $\vec{r}$ setting a new parameter k that modified the GGH cryptographic algorithm. Their modifications resulted in a variation of GGH more resistant to cryptanalysis, but with slower decrytpion process of the

 doi:10.20944/preprints202305.0515.v1

algorithm. In 2015, Brakerski et al., described certain types of attacks against some variations of GGH cryptosystem and rely on the linearity of the zero-testing procedure [16].

GGH was a milestone in the evolution of post quantum cryptography, was one of the earliest lattice based cryptographic schemes and it is based on the hardness of the Shortest Vector Problem. Even though is considered to be one of the most important lattice-based cryptosystems and still has a theoretical interest, it is not recommended for practical use due to its security weaknesses. GGH is the less efficient than other lattice-based cryptosystems. The process to encrypt and decrypt a message requires a large amount of computations and this fact makes the GGH cryptosystem obviously slower and less practical than other lattice-based cryptosystems.

Thus, GGH protocol is vulnerable to certain attacks, such as Coppersmith's attack and Babai's nearest plane algorithm and it is considered not to be strong enough. These attacks disputed the security of the GGH and make it less preferable than newer, stronger and more secure lattice-based cryptosystems. Evaluating the efficiency of GGH cryptographic protocol, GGH is relatively inefficient to other lattice-based cryptosystems like NTRU, LWE and others and especially in the key generation and for large key length. As GGH cryptosystem is based in multiplications of matrices, when we choose large keys, it requires a computationally expensive basis reduction algorithm for the encryption and decryption procedure.

Moreover, GGH is considered to be a complex crypographic scheme which requires concepts and knowledge of lattices and linear algebra to study, analyze and implement. GGH also has one more drawback that is the lack of standardization and this makes hard the comparison of its functionality, security and connectivity with other cryptographic schemes. GGH was one of the first cryptogrpahic schemes that were developed and are based on lattice theory and cryptography. In spite of the fact that GGH certainly has interesting theoretical basis and properties, GGH is not used in practice due to its limitations in security, efficiency, and complexity.

NTRU is a public key cryptographic scheme that is based on the Shortest Vector Problem in a lattice and was first presented in the 1990s. It is one of the most well studied and analyzed lattice-based cryptosystems and have been many cryptanalysis studies og NTRU algorithms, including NTRU signatures. NTRU has a high level of security and efficiency and it is a promising protocol for the post-quantum cryptography. Moreover, NTRU cryptographic algorithm uses polynomial multiplication as its basic operation and it is notable for its simplicity.

A main advantage of NTRU cryptosystem is its speed and has been used in certain commercial applications, where speed is a priority. NTRU has a fast implementation compared with other lattice-based cryptosystems, such as GGH, LWE and Ajtai-Dwork. For this reason, NTRU is preferable for applications that require fast encryptions and decrytpion, such as in IoT devices or in embedded systems. In addition to its speed, NTRU uses smaller key sizes compared to other public key cryptosystems, while still maintaining the same level of security. This makes it ideal for applications or environments with limited memory and processing power.

NTRU is considered to be a secure cryptographic scheme against various types of attacks. It is designed to be resistant against attacks such as lattice basis reduction, meet-in-the-middle attacks and chosen ciphertext attacks. NTRU is believed to be a strong cryptographic scheme for the quantum era, meaning that is considered to be resistant against attacks by quantum computers.

NTRU has become famous and widely usable after 2017, because since then it was under a patent it was difficult for the researchers to use it and modificate it. Thus, NTRU is not widely used or standardized in the industry, making it difficult to assess its interoperability with other cryptosystems. Furthermore, NTRU is considered to be a public key cryptohraphic protocol with a relative complexity and its analysis and implementation requires a good understanding of lattice-based cryptography and ring theory. NTRU is a promising lattice-based cryptosystem for post quantum cryptography that offers fast implementation and strong security guarantees.

Learning with Errors (LWE) is a widely used and well studied public key cryptographic scheme that is based in lattice theory. LWE is considered to be secure against both classical and quantum

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

attacks and indeed, is consedered to be among the most secure and efficient of these schemes, while NTRU has limitations in terms of its security. LWE depends its hardness on the difficulty of finding a random error vector in a matrix product and this makes it a resistant cryptosytem against various types of attacks, the same types of attacks with NTRU. It considered to be a strongly secure cryptosystem and post-quantum secure which it means, that is resistant to attacks by a quantum computer.

LWE uses keys with small length size comparing with other cryptographic schemes that are designed for the quantum era, like code-based and hash-based cryptosystems. Just like NTRU, LWE is appropriate for implementation in resource-constrained environments, such as in IoT devices or in embedded systems. A basic advantage of LWE cryptosystem is its flexibility as it is a versatile cryptographic scheme that can be suitable in a variety of cryptographic methods such as digital signatures, key exchange and encryption. LWE can also be used as a building block for more complex cryptographic protocols and from LWE were developed other variations of it.

LWE can be vulnerable to certain type of attacks, like side-channel attacks, i.e. timing attacks or power analysis attacks, if we wouldn't take the right countermeasures. Just like NTRU, LWE is not considered to be standardized and widely adopted by the computing industry and this makes it difficult to assess its interoperability with other cryptosystems and the comparison with them. Moreover, LWE cryptographic protocol is characterized with complexity and its understanding and modification becomes challenging.

Undoubtedly, both NTRU and LWE are fast, efficient and secure cryptographic schemes. NTRU uses smaller keys sizes and that makes it suitabale for applications where memory and computational power are limited. Both LWE and NTRU are considered to be strong and resistant to various types of attacks and are considered to be prominent for post-quantum cryptography. Thus, LWE is an adaptable cryptographic protocol and can be used in a wide range of cryptographic tasks and methods, while NTRU is primarily used for encryption and decryption.

In summary, LWE and NTRU are both promising lattice-based cryptosystems that offer strong security guarantees and are resistant to quantum attacks. NTRU is known for its fast implementation and smaller key sizes, while LWE offers more flexibility in cryptographic primitives and is currently undergoing standardization. Ultimately, the choice between LWE and NTRU will depend on specific use cases and implementation requirements.

Overall, each lattice-based cryptosystem has its own strengths and weaknesses depending on the specific use case. Choosing the right one requires careful consideration of factors such as security, efficiency, and ease of implementation.

9. Lattice-based Cryptographic Implementations and Future Research

Quantum research over the past few years has been particularly transformative, with scientific breakthroughs that will allow exponential increases in computing speed and precision. In 2016, the National Institute of Standards and Technology (NIST) has announced an invitation to researchers to submit their proposals for developed public - key post-quantum cryptographic algorithms. At the end of 2017, when was the initial submission deadline, there were submitted 23 signature schemes and 59 encryption - key encapsulation mechanism (KEM) schemes, in total 82 canditates' proposals.

In July 2022, the NIST has finished the third round of selection and has chosen a set of encryption tools designed to be secure against attacks by future quantum computers. The four selected cryptographic algorithms are regarded as an important milestone in securing the sensitive data against the possibility of cyberattacks from a quantum computer in the future [58].

The algorithms are created for the two primary purposes for which encryption is commonly employed: general encryption, which is used to secure data transferred over a public network, and digital signatures, which are used to verify an individual's identity. Experts from several institutions and nations collaborated to develop all four algorithms which are presented below.

- **CRYSTALS-Kyber**

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 May 2023 doi:10.20944/preprints202305.0515.v1

This cryptographic scheme is being selected by NIST, for general encryption and is based on the module Learning with Errors problem. CRYSTALS-Kyber is similar to Ring-LWE cryptographic scheme but it is considered to be more secure and flexibile. The parties that communicate can use small encrypted keys and exchange them easily with high speed.

- **CRYSTALS-Dilithium**

  This algorithm is recommended for digital signatures and relies its security on the hardness of lattice problems over module lattices. Like other digital signature schemes, the Dilithium signature scheme allows a sender to sign a message with their private key, and a recipient to verify the signature using the sender's public key but ilithium has the smallest public key and signature size of any lattice-based signature scheme that only uses uniform sampling.
- **FALCON**

  FALCON is cryptographic protocol which is proposed for digital signatures. Falcon cryptosystem is based on the theoretical framework of Gentry et al [28]. It is a promising post-quantum algorithm as it provides fast signature generation and verification capabilities. FALCON cryptographic algorithm has strong advantages such as security, compactness, speed, scalability and RAM Economy.
- **SPHINCS+**

  SPHINCS plus is the third digital signature algorithm that was selected by NIST. SPHINCS + uses hash functions and is considered to be a bit larger and slower than FALCON and Dilithium. It is regarded as an improvement of the SPHINCS signature scheme, which was presented in 2015, as it reduces the size of the signature. One of the key points of interest of SPHINCS+ over other signature schemes is its resistance to quantum attacks, by depending on the hardness of a one-way function.

10. Conclusions

Significant progress has been made in recent years, taking us beyond classical computing and into a new era of data called quantum computing. Quantum research over the past few years has been particularly transformative, with scientific breakthroughs that will allow exponential increases in computing speed and precision. Research on post-quantum algorithms is active and huge sums of money are being invested for this reason, because it is necessary the existence of strong cryptosystems.

It is considered almost certain that both the symmetric key algorithm and hash functions they will continue to be used as tools of post quantum cryptography. A various of cryptographic schemes have been proposed for the quantum era of computing and this is an active research topic. The development and the standardization of an efficient post-quantum algorithm is the challenge of the academic community. What was once considered a science fiction fantasy is now a technological reality. The quantum age is coming, it will bring enormous changes, therefore we have to be prepared.

References

1. Albrecht, M. ; Ducas, L. Lattice Attacks on NTRU and LWE: A History of Refinements. Cambridge University Press, 2021.
2. Alkim, E. ; Dukas, L. ; Pöppelmann, T. ; Schwabe, P. Post-quantum Key Exchange – A New Hope. In USENIX Security Symposium 2016 , Austin, TX, 2016, (10-12 August 2016), https://eprint.iacr.org/2015/1092.pdf.
3. Ashur, T.; Tromer, E. Key Recovery Attacks on NTRU and Schnorr Signatures with Partially Known Nonces. In the 38th Annual International Cryptology Conference, 2018.
4. Babai, L.On Lovasz' lattice reduction and the nearest lattice point problem. *Combinatorica* **1986**, *6*, 1–13.
5. Bai, S.; Gong, Z.; Hu, L. Revisiting the Security of Full Domain Hash. In 6th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, 2013.
6. Bai, S.; Chen, Y.; Hu, L. Efficient Algorithms for LWE and LWR. In Proceedings of the 10th International Conference on Applied Cryptography and Network Security, 2012.
7. Balbas, D. The Hardness of LWE and Ring-LWE: A Survey *Cryptology ePrint Archive* **2021**.

8. Barros, C.; Schechter, L.M. GGH may not be dead after all. In Proceedings of the Congresso Nacional de Matemática Aplicada e Computacional, 2015.
9. Bennett, C.H. ; Brassard, G.; Breidbart, S. ; Wiesner, S. Quantum cryptography, or Unforgeable subway tokens. *Advances in Cryptology: Proceedings of Crypto '82* **1982**, 267-275.
10. Bennett, C.H. ; Brassard, G. Quantum Cryptography : Public Key Distribution and Coin Tossing. In International Conference in Computer Systems and Signal Processing, 1984.
11. Bennett, C.H. ; Brassard, G.; Ekert, A. Quantum cryptography. *Scientific American* **1992**, 50-57.
12. Berstein, D.J.; Buchmann, J. ; Brassard, G. ; Vazirani, U. *Post-Quantum Cryptography*. Publisher: Springer, 2009.
13. Bi, L.; Lu, X. ; Luo, J.; Wang, K. ; Zhang, Z. Hybrid dual attack on LWE with arbitrary secrets. *Cryptology ePrint Archive* **2022**.
14. Brakerski, Z.; Gentry, C.; Vaikuntanathan, V. New Constructions of Strongly Unforgeable Signatures Based on the Learning with Errors Problem. In Proceedings of the 48th Annual ACM Symposium on Theory of Computing, 2016.
15. Brakerski, Z.; Langlois, A. ; Regev, O.; Stehl, D. Classical Hardness of Learning with Errors. In Proceedings of the 45th Annual ACM Symp. on Theory of Computing (STOC), 2013. 575-584.
16. Brakerski, Z., Gentry, C., Halevi, S., Lepoint, T., Sahai, A., Tibouchi, M. Cryptanalysis of the quadratic zero-testing of GGH. *IACR Cryptology ePrint Archive*, **2015**, *845*.
17. Bonte, C. ;Iliashenko, I.; Park, J.; Pereira, H.V.; Smart, N. FINAL: Faster FHE instantiated with NTRU and LWE *Cryptology ePrint Archive* **2022**.
18. Bos, W.; Costello, C. ; Ducas, L. l; Mironov, I. ; Naehrig, M. ; Nikolaenko, V. ; Raghunathan, A. ; Stebila, D. Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE. In CCS 2016, Vienna, Austria, 2016, https://eprint.iacr.org/2016/659.pdf.
19. Buchmann, J; Dahmen, E.; Vollmer, U. Cryptanalysis of the NTRU Signature Scheme. In Proceedings of the 6th IMA International Conference on Cryptography and Coding, 1997.
20. Buchmann, J. ; Dahmen, E. ; Vollmer, U. Cryptanalysis of NTRU using Lattice Reduction *Journal of Mathematical Cryptology* **2008**.
21. Chunsheng, G. Integer Version of Ring-LWE and its Applications *Cryptology ePrint Archive* **2017**.
22. Coppersmith, D. ; Shamir, A. Lattice attacks on NTRU. *advances in Cryptology—EUROCRYPT'97* **1997**.
23. Diffie, W. ; Hellman, M. New Directions in Cryptography. In *IEEE Transactions in Information Thery*, **1976**, 644-654.
24. Dubois, V. ; Fouque, P.A. ; Shamir, A. ; Stern, J. Practical cryptanalysis of sflash. In *Advances in Cryptology CRYPTO 2007***2007**, volume 4622 of Lecture Notes in Computer Science, pages 1–12.
25. Faugere, J.; Otmani, A. ; Perret, L. ; Tillich, J. ; Sendrier, N. Cryptanalysis of the Overbeck-Pipek Public-Key Cryptosystem. *Advances in Cryptology – ASIACRYPT 2010* **2010**.
26. Faugère, J.C.; Otmani, A.; Perret, L.; Tillich, J.P. On the Security of NTRU Encryption. *Advances in Cryptology – EUROCRYPT 2010* **2010**.
27. Galbraith, S. *Mathematics of Public Key Cryptography*, Publisher: Cambridge University Press , 2012.
28. Gentry, C. ; Peikert, C.; Vaikuntanathan, V. Trapdoors for Hard Lattices and New Cryptographic Constructions. *Cryptology ePrint Archive* **2007**.
29. Gentry, C. Fully Homomorphic Encryption Using Ideal Lattices. In Proceedings of the 41st Annual ACM Symp. on Theory of Computing (STOC), 169-178.
30. Goldreich, O. ; Goldwasser, S. ; Halive, S. Public-Key cryptosystems from lattice reduction problems. *Crypto '97* **1997**, *10*, 112-131.
31. Gu, C. ; Yu, Z. ; Jing, Z. ; Shi, P. ; Qian, J. Improvement of GGH Multilinear Map. In IEEE Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Krakow, Poland: IEEE; 407-411.
32. Hoffstein, J. ; Pipher, J. ; Silverman, J. NTRU: A ring-based public key cryptosystem. *Algorithmic Number Theory (Lecture Notes in Com- puter Science* **1998**, *1423*, New York, NY, USA: Springer-Verlag, 267–288.
33. Kannan, R. Algorithmic Geometry of Numbers. In *Annual Reviews of Computer Science*; Annual Review Inc., Palo Alto, CA, 1987, 231–267.
34. Komano, Y.; Miyazaki, S. On the Hardness of Learning with Rounding over Small Modulus. In Proceedings of the 21st Annual International Conference on the Theory and Application of Cryptology and Information Security, 2015.

35. Lee, M.S. ; Hahn, S.G. Cryptanalysis of the GGH Cryptosystem.*Mathematics in Computer Science* **2010**, 201-208.
36. Lenstra, A.K. ; H.W. Lenstra, Jr. ; L. Lovasz. Factoring polynomials with rational coefficients.*Mathematische Annalen* **1982**, *261*, 513-534.
37. Lyubashevsky, V.; Micciancio, D. Generalized Compact Knapsacks Are Collision Resistant. In Proceedings of the 33rd International Colloquium on Automata, Languages and Programming., 2006, 144-155.
41. Lyubashevsky, V.; Peikert, C. ; Regev, O. On Ideal Lattices and Learning with Errors over Rings. *Advances in Cryptology – EUROCRYPT 2010* **2010**.
39. Lyubashevsky, V. A Decade of Lattice Cryptography. *Advances in Cryptology – EUROCRYPT 2015* **2015**.
40. Martinet, G.; Laguillaumie, F.; Fouque, P.A. Cryptanalysis of NTRU using Coppersmith's Method. *Cryptography and Communications* **2011**.
41. Lyubashevsky, V.; Peikert, C.; Regev, O. On Ideal Lattices and Learning with Errors over Rings. *ACM* **2013**, *60*, 43:1–43:35.
42. Matsumoto, T ; Imai, H. Public quadratic polynomials-tuples for efficient signature verification and message encryption. *Advances in cryptology -EURO-CRYPT '88* **1988**, *330*, 419-453.
43. May, A.; Peikert, C. Lattice Reduction and NTRU. In Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science, 2005.
44. McEliece, R. A public key cryptosystem based on alegbraic coding theory. *DSN progress report* **1978**, *42-44*, 114-116.
45. Merkle, R. A certified digital signature. *Advances in Cryptology – CRYPTO'89* **1989**, Springer: Berlin/Heidelberg, Germany, 218–238.
46. Micciancio, D., Improving Lattice Based Cryptosystems Using the Hermite Normal Form. In *Cryptography and Lattices Conference*; Springer, 2001.
47. Micciancio, D., Regev, O. Lattice-based cryptography. In *Post-quantum cryptography*; Germany, Editor Publishing House: Springer, 2009.
48. Micciancio, D. On the Hardness of the Shortest Vector Problem. PhD thesis, Massachusetts Institute of Technology, USA, 1998.
49. Micciancio, D. The shortest vector problem is NP-hard to approximate within some constant. In 39th FOCS IEEE, California, USA. Available at [47] as TR98-016.
50. Micciancio, D. Lattice based cryptography: A global improvement. Technical report. *Theory of Cryptography Library* **1999**, *99-05*.
51. Micciancio, D. The hardness of the closest vector problem with preprocessing. *IEEE Trans. Inform. Theory* **2001**, *47(3)*.
52. Minaud, B., Fouque, P. A. Cryptanalysis of the New Multilinear Map over the Integers. *IACR Cryptology ePrint Archive* **2015**, *941*.
53. Niederreiter, H. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory. Problemy Upravlenija I Teorii Informacii.* **1986**, *15*, 159–166.
54. Nguyen, P.Q. Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from crypto'97. In Annual International Cryptology Conference , Santa Barbara, USA, 1999; CA: Springer, pages: 288-304.
55. Nguyen P. Q. Regev, O. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. *Journal of Cryptology* **2009**, *22*, 139-160.
56. Nguyen P.Q. ;Stern, J. The two faces of Lattices in Cryptology. In Proceedings of International Cryptography and Lattices Conference, Rhode, USA, 29-30 March 2001; pages : 146-180.
57. Nielsen, M., ; Chuang, I. *Quantum computation and quantum information*, Publisher: Cambridge, England: Cambridge University Press, 2011.
58. Post-Quantum Cryptography. Available online: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms
59. Patarin, J. Hidden field equations and isomorphism of polynomials *Eurocrypto '96* **1996**.
60. Peikert, C. Lattice-Based Cryptography: A Primer. *IACR Cryptology ePrint Archive* **2016**.
61. Preskill, J. Quantum computing and the entanglement frontier. **2012**.
62. Poulakis, D. *Cryptography, the science of secure communication*, 1st ed.; Publisher: Ziti Publications, Thessaloniki Greece, 2004.
63. Rivest, R.L.; Shamir, A.; Adleman, A. Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Journal of the ACM* **1978**, *21*, 120-126.

64. Regev, O. On lattices, learning with errors, random linear codes, and cryptography *Journal of the ACM* **2009**, *56(6)*, 1-40.
65. Regev, O. The Learning with Errors Problem: Algorithms and Applications. *Foundations and Trends in Theoretical Computer Science* **2015**.
66. Sabani, M.; Savvas I.K.; Poulakis, D.; Makris, G.; Butakova, M. The BB84 Quantum Key Protocol and Potential Risks. In 8th International Congress on Information and Communication Technology (ICICT 2023), London, UK, 20-23 February 2023.
67. Sabani, M.; Savvas I.K.; Poulakis, D.; Makris, G. Quantum Key Distribution: Basic Protocols and Threats. In 256th Pan-Hellenic Conference on Informatics (PCI 2022), Greece, November 2022 , pages: 383-388, ACM, New York, USA, 2022.
68. Sabani, M.; Galanis, I.P.; Savvas I.K.; Garani G. Implementation of Shor's Algorithm and Some Reliability Issues of Quantum Computing Devices. In 25th Pan-Hellenic Conference on Informatics (PCI 2021), Volos, Greece, 26-28 November 2021 , pages: 392-296, ACM, New York, USA, 2021.
69. Scherer, W. *Mathematics of Quantum Computing, An Introduction*. Publisher: Springer, 2019.
70. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *J Comput. SIAM* **1997**, *26*, 1484–509.
71. Silverman, J.H.; Piher, J. ;Hoffstein, J. *An introduction to Mathematical Cryptopraphy*, 1st ed.; Publisher: Springer, USA, 2008.
72. Susilo, W.; Mu, Y. *Information Security and Privacy*. Publisher: Springer, 2014.
73. Takagi, T.; Kiyomoto, S. Improved Sieving Algorithms for Shortest Lattice Vector Problem and Its Applications to Security Analysis of LWE-based Cryptosystems. In Proceedings of The 23rd Annual International Conference on the Theory and Applications of Cryptographic Techniquesthe Name of the Conference, 2004.
74. Trappe, W. ; Washington, L.C. *Introduction to Cryptography with Coding Theory*. Publisher: Pearson Education, USA, 2006.
75. Van Assche, G. *Quantum Cryptography and Secret-Key Distillation*, 3rd ed.; Publisher: Cambridge University Press, New York, 2006.
76. Wang, Q. ; Jin, Z. ; Dong, X. Survey of Lattice-based Cryptography: Attacks, Constructions, and Challenges *IEEE Communications Surveys Tutorials* **2019**.
77. Wiesner, S. Conjugate coding. *Sigact News*, **1983**, *15*, 78-88.
78. Yoshino, M.; Kunihiro, Improving GGH Cryptosystem for Large Error Vector. In International Symposium on Information Theory and its Applications, Honolulu, Hawaii, USA, 2012 (28-31 October 2012), 416-420.
79. Zheng, Z., ; Tian, K. ; Liu, F. *Modern Cryptography Volume 2 A Classical Introduction to Informational and Mathematical Principle*, Publisher: Springer, Singapore, 2023.