Computer Communications 218 (2024) 176–187

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

A physical layer security scheme for 6G wireless networks using post-quantum cryptography

Walid Abdallah [*]

University of Carthage, Higher School of Communication of Tunis (SUP' COM),LR11TIC04, Communication Networks and Security Research Lab. & LR11TIC02,Green and Smart Communication Systems Research Lab., Tunisia
Borj El Amri Aviation School, Tunisia

ARTICLE INFO

Keywords:
6G networks
Physical layer security
OFDM
Lattice-based cryptography

ABSTRACT

The sixth generation (6G) of mobile networks is poised to revolutionize communication capabilities with its infinite-like reach. These networks will feature an ultra-dense topology, accommodating a wide range of devices, from macro devices like satellites to nano-devices integrated within the human body. However, the extensive data traffic handled by 6G networks, a significant portion of which is sensitive in nature, presents a security challenge. This paper presents the design and implementation of an encryption scheme that ensures the confidentiality of data transmission in the physical layer of 6G networks. The proposed physical layer security architecture relies on lattice cryptography, wherein each user is associated with a pair of bases (a public basis and a private basis) and a set of orthogonal sub-carriers. The encryption process involves projecting the vector of the transmitted data's quadrature amplitude modulation (QAM) symbols onto the user's public basis. A random error vector is then added before applying the inverse Fourier transform of the orthogonal frequency division multiplexing (OFDM) technique. The security of this encryption scheme hinges on the complexity of the closest vector problem in an integer lattice. To evaluate its efficacy, we analyze the security of our lattice-based physical layer encryption concerning the properties of the base pairs and error vectors. Our findings indicate that the proposed scheme offers satisfactory security protection against eavesdropping attacks by significantly enhancing the confidentiality of the transmitted signal. Furthermore, we assess the performance of our design through numerical experiments, demonstrating its resilience against various security attacks.

1. Introduction

The sixth generation of wireless mobile networks will encompass a diverse range of nodes, spanning from nano-devices implanted in the human body to macro communication devices integrated into high-altitude platform systems (HAPS) or satellites. The evolution from 5G to 6G networks is expected to further enhance the concept of the Internet of Everything (IoE), ensuring consistent performance across devices, environments (air, space, land, sea), and providing ubiquitous connectivity [1–4]. The forthcoming 6G standard will witness an intensified distribution of network deployment, reflecting its distributive nature. The establishment of autonomous and infinite-like connectivity, facilitated by this emerging technology, will be supported by recent advancements in artificial intelligence, machine learning, and modern signal processing techniques. These techniques include compressive sensing, random finite matrix theory, simulated annealing, among others.

Due to the vast amount of sensitive data that will be handled by this new generation of ultra-dense networks, ensuring privacy and security will be of utmost importance [5,6]. In this regard, physical layer security (PLS) techniques can play a significant role in 6G networks security by offering a bottom-up approach to ensure confidentiality across different communication architecture layers. PLS leverages the physical characteristics of the transmission environment to gain a security advantage against passive and active attacks that aim to compromise data confidentiality. There has been a recent surge of interest in designing and developing efficient physical layer security techniques for data transmission privacy in 6G networks. Implementing security measures at the physical layer can enhance transmission rates and maintain protocol and data format transparency. However, this presents a challenging task due to the disruptive connectivity paradigm expected in 6G networks, which will increase vulnerabilities and attacks targeting the communication infrastructure. Additionally, the anticipated integration of quantum computing-based processing

[*] Correspondence to: University of Carthage, Higher School of Communication of Tunis (SUP' COM),LR11TIC04, Communication Networks and Security Research Lab. & LR11TIC02,Green and Smart Communication Systems Research Lab., Tunisia.
E-mail address: walid.abdallah@supcom.tn.

https://doi.org/10.1016/j.comcom.2024.02.019
Received 19 July 2023; Received in revised form 28 January 2024; Accepted 20 February 2024
Available online 21 February 2024

and searching algorithms [7–9] will further amplify the number of threats. Classical cryptographic algorithms that rely on the hardness of discrete logarithm and prime factorization problems, such as RSA and Diffie–Hellman, will become obsolete [10]. Furthermore, security approaches based on quantum cryptography [11] are currently limited to key distribution procedures. The security of this approach is based on the fact that observing a quantum system unavoidably disturbs its state, facilitating the detection of eavesdropping attacks. However, it also introduces increased system complexity and cost.

In this paper, we propose a physical layer security scheme that leverages post-quantum encryption to enhance communication security in 6G networks. This scheme is based on a public key cryptosystem that exploits the computational hardness of lattice point problems to encrypt data streams. Unlike current public encryption schemes such as RSA or ElGamal, which are based on average case hardness, lattice-based encryption schemes offer best security by relying on worst-case hardness [12]. The proposed encryption scheme is particularly suitable for physical layer communications in 6G networks because it can satisfy the signal processing efficiency and high transmission capacity requirements of these networks. The encryption procedure assumes that each user possesses a private basis and a public basis composed of integers. The physical layer communication employs orthogonal frequency division multiplexing (OFDM) technique. The transmitter initially maps the data bit stream to a vector of quadrature amplitude modulated (QAM) symbols. It then projects this vector onto the receiver's public basis, adds a random "error vector", and applies the inverse fast Fourier transform of the OFDM process. The receiver recovers the transmitted data by projecting the encrypted modulated stream onto its private basis, finding the closest vector and applying demodulation procedure of the OFDM technique.

To enhance the performance of the asymmetric cryptosystem, we study the requirements related to the error vector generated and added to the encrypted modulated data stream. We demonstrate that the proposed lattice-based encryption technique is well-suited for the physical layer transmission constraints and offers an acceptable level of security when specific parameters concerning the lattice-based encryption procedure are appropriately selected. Furthermore, the different operations performed by the encryption/decryption processes are quadratic (mainly based on matrix multiplication), which can be tailored to real-time constraints of the physical layer communication in 6G networks.

In addition, the security of the scheme is based on the complexity of the closest vector problem in lattices, which is believed to be quantum computing resistant when specific parameters such as the dimension of the lattice and the generation procedure of the error vector are appropriately selected. Nevertheless, it is worth noting that the proposed scheme can be applied to any multi-carrier-based transmission, particularly OFDM, which exhibits enhanced spectral efficiency and robust immunity to fading and intersymbol interference. Also, to the best of our knowledge, our work is the first to propose the use of lattice-based encryption schemes to secure data stream transmission in the physical layer of wireless networks.

The remainder of the paper is structured as follows: Section 2 presents a review of major works related to physical layer security techniques; Section 3 introduces the mathematical concepts related to lattice-based cryptography; Section 4 presents the physical layer security scheme that utilizes OFDM and the lattice-based encryption technique; Section 5 is dedicated to the security analysis and performance evaluation of the proposed physical layer security scheme using a simulation framework; and finally, Section 6 concludes the paper and discusses future extensions for this work.

2. Related work

Physical layer security (PLS) has been recognized for decades as a front-line defense that can provide security even for devices with limited resources [13]. PLS is considered a valuable complement to cryptography techniques in protecting wireless networks. While cryptography relies on the limited computational power of adversaries, PLS leverages the asymmetry in reception quality between the legitimate receiver and the attacker, taking advantage of channel propagation models and environmental conditions to gain security advantages.

Several recent works have provided overviews of physical layer security techniques. In [14]authors present a classification and application of PLS techniques. The paper [15] discusses open research issues and future visions for applying PLS in next-generation networks. In [16] physical layer security techniques and their deployment in securing 6G networks are explored. Furthermore, in [17] the potential of physical layer security in providing security for 6G access networks is investigated. The principles of physical layer security, as well as techniques for single and multi-antenna communication systems, multi-user environments, and relaying technology deployment, are discussed in [18]. The challenges of wireless communication security, particularly at the physical layer, are described in [19]. Authentication and handover security approaches for 5G heterogeneous networks (HetNet) using software-defined networks (SDN) are depicted in [20]. The paper [21]explores the opportunities and challenges of utilizing device transceiver fingerprinting for authentication and privacy in the physical layer. An overview of user identification and authentication in wireless networks using non-cryptographic physical layer security techniques is presented in [22]. PLS techniques using multiple-input multiple-output (MIMO) and error coding techniques are detailed in [23,24] respectively. Additionally, exploiting channel uncertainty to design effective PLS solutions is discussed in [25]. A comprehensive review of physical layer authentication and trading technologies is achieved in [26].

Many physical layer security schemes relying on orthogonal frequency division multiplexing (OFDM) and multiple input multiple output (MIMO) techniques have emerged in recent years as solutions to provide data transmission confidentiality in the new generation of communication networks. These two technologies can ensure large capacity transmission with higher spectral efficiency, flexible resource allocation, low cost, and resilience against inter-symbol interference and fading phenomena.

In [27] two OFDM-based physical layer security schemes were proposed. The first one uses time domain pre-coding that employs interleaving and scaling, and the second one uses a random cyclic prefix length to randomize the OFDM symbol period. Both techniques are performed according to a secret key pre-shared between the legitimate parties.

The work published in [28] proposed an OFDM-based physical layer security scheme for cognitive radio networks. The scheme considers relaying transmission where one relay node will forward the data packet, and another relaying node will generate random noise to prevent an eavesdropper from correctly receiving the transmitted information. This is achieved by optimizing power allocation and sub-carriers in the source node and the relaying node.

A compressed sensing-based physical layer security scheme for Internet of Things (IoT) systems was presented in [29]. In this scheme, a secret key is dynamically derived from channel measurements and is used to encipher the OFDM transmitted signal. Wireless steganography was also investigated in [30] to ensure security in the physical layer of IoT networks by hiding the secret OFDM signal in a Discrete Fourier Transform (DFT)-precoded OFDM cover signal. Authors in [31] attempted to improve physical layer communication security using the channel shortening technique. The basic concept is to make the channel less or equal to the cyclic prefix (CP) at the legitimate users, while it will appear longer than the CP at the attacking user. The recent work published in [32] addressed the design of a flexible physical layer security scheme that can secure both data and pilot transmission to prevent channel estimation by the attacker. Physical layer security schemes guaranteeing secure low-latency transmission in beyond 5G networks were described in [33]. Authors in this work demonstrate that it is possible to perform two-way transmission privacy with reduced latency by using a protocol that can optimize time–frequency resource usage. Artificial pilot noise generation to combat signal eavesdropping and ensure secure OFDM communication was investigated in [34]. Additionally, the work in [35] exploits the phase error insertion technique to enhance OFDM transmission. This is achieved by rotating the constellation mapping of the M-PSK modulated symbols using a pre-shared key and leveraging the channel fading of the sub-carriers to introduce phase error in the encoded symbol according to the channel state. The design of an unmanned aerial vehicle embedded transceiver to enable full-duplex secure communication between the mobile user and the terrestrial base station was presented in [36]. The proposed communication system employs an intertwining logistic map (ILM)-cosine transform-aided encryption algorithm combined with artificial noise enhancing physical layer security (PLS) to ensure secure zero-padded OFDM signal transmission.

Several other papers have been interested in using encryption techniques to provide physical layer security. The work published in [37] focuses on improving physical layer security in wavelength division multiplexing (WDM) orthogonal frequency division multiplexing (OFDM) based passive optical networks (PONs). The proposal envisions an elliptic curve-based Diffie–Hellman key exchange protocol for secure key distribution between the optical line terminal (OLT) and the optical network unit (ONU). Advanced Encryption Standard (AES) is then employed to encrypt transmitted data, with encryption applied to partial data of the I/Q channel to reduce processing time. The successful transmission of a 16-QAM modulated OFDMA encrypted signal over a distance of 100 km within acceptable values of the peak-to-average power ratio is achieved. Furthermore, a physical layer encryption scheme using frequency induction for OFDM based transmission systems was introduced in [38]. The transceiver design was implemented on a Virtex-7 FPGA and consists of a secret key-based frequency shift module and an encryption module. The decryption operation is performed by a modified synchronizer that is configured with the same key.

Chaotic-based physical layer security approaches have been discussed in some papers. The work in [39] proposed the design of a multi-input multi-output (MIMO) communication system using chaos-based time-varying unitary matrices. Practical physical layer security was achieved through differential encoding without using channel estimation. Authors in [40] addressed the enhancement of physical layer security in MIMO OFDM systems using a multilevel chaotic encryption technique. This is performed by firstly scrambling the modulated symbol using a pre-coding matrix generated with a unique chaotic sequence, and then a second level of encryption is achieved by phase scrambling based on selective mapping and a chaotic sequence. In another recent work [41], a physical layer security scheme using time reversal pre-coding technique combined with artificial noise injection was proposed for Differential Chaos Shift Keying (OFDM-DCSK) based communication systems to ensure higher transmission capacity with enhanced confidentiality and reliability.

The use of visible light communication (VLC) technology is considered a form of physical layer security because it enables the confinement of the transmitted signal within the area covered by the light-based access point. A physical layer security scheme for OFDM-based VLC networks using chaotic encryption was proposed in [42]. In this scheme, ciphertext was dynamically generated by leveraging the random nature of chaotic keys and transmitted data. Sub-carrier allocation in time and frequency domains is achieved according to a chaotic permutation and reversal of sub-carriers. The authors show that their VLC-based communication system can resist known and chosen plaintext cryptanalysis attacks. In [43] the design of an optical backhaul solution for light fidelity (LiFi) networks is studied. This proposal presents a LiFi access point structure that implements orthogonal frequency division multiplexing (OFDM) and optical encoding techniques to provide multi-user access and enable all-optical processing and transmission in the backhaul network. Additionally, a tunable optical encoding/decoding technique based on delaying optical pulses in a vector of optical delay line (ODL) loops is designed to facilitate efficient mapping of the OFDM-based access and data forwarding in the optical backhaul network.

Although the aforementioned works constitute valuable contributions to the design of efficient and reliable physical layer security schemes, they, however, present some limits. Firstly, most of the proposed schemes rely on accurate knowledge of the channel propagation model and the positions of the sender, receiver, and attacker. In many cases, these assumptions are not practical, especially in a mobile scenario where the different parties are moving at very high speeds. In addition, encryption techniques used to provide confidentiality in these physical layer security approaches are based on symmetric key encryption algorithms, which require the pre-sharing of encryption keys between the transmitter and the receiver. This is challenging to manage and less secure than when using dynamic exchange and establishment of encryption keys using public key encryption algorithms. Finally, existing encryption procedures employed in the described PLS schemes are not resistant to quantum computer-based processing, and most of them will be eliminated from usage when the upcoming quantum era begins.

Consequently, many recent works have focused on the implementation of lattice-based post-quantum encryption schemes. In [44] ASIC implementations of two post-quantum cryptographic algorithms, NTRU, and TTS, are presented. The main objective is to leverage the hardware processing efficiency of these algorithms to secure machine-to-machine communication systems. Furthermore, in [45] the use of lattice-based cryptography in the era of quantum computing is discussed for securing the Internet of Things (IoT). A comprehensive overview of lattice-based post-quantum encryption schemes can be found in [46]. This paper provides a detailed exploration of lattice-based cryptographic algorithms and their applications in the context of post-quantum cryptography. Additionally, [47] presents an ultra-fast FPGA-based implementation of arithmetic operations used in post-quantum encryption algorithms. The paper focuses on accelerating the computation of cryptographic operations required for lattice-based schemes, leveraging the capabilities of FPGA technology to achieve high-performance implementations. In our previous work published in [48,49], we proposed a lattice-based public key encryption scheme to secure optical code division multiple access (OCDMA) transmission. We demonstrated that this scheme outperforms existing solutions in terms of robustness against cryptanalysis attacks. This approach helps reduce the processing overhead typically observed in classical public key approaches and enhances the efficiency of encrypted signal transmission.

Our main objective in this work is to develop a secure communication scheme that offers enhanced confidentiality for wireless data transmission at the physical layer. To this end, we have devised an encryption scheme that utilizes lattice-based public key cryptosystems [12, 50–53]. In the proposed scheme, the OFDM modulated transmission pattern is protected by projecting it onto the public basis of the receiver and adding a pseudo-random noise-like vector generated according to specific rules. The receiver can recover the transmitted message by deciphering the received signal using its private base (private key) and performing OFDM demodulation operations.

Compared to existing approaches, the proposed PLS scheme does not require any knowledge about either the channel propagation characteristics or the positions of evolved entities. Furthermore, no secret key should be pre-shared between the transmitter and the receiver to initiate secure communication. Indeed, in this work, the lattice-based public key encryption is executed directly on the data stream and not used to securely exchange symmetric keys, as implemented in most security protocols (IPsec, SSL/TLS, etc.). We also believe that the designed scheme can remain secure even when quantum computing becomes practically available, provided that some parameters, namely the dimension of the lattice and the error noise vector, are appropriately selected.

In addition, it is worthy to note that the designed PLS scheme can be used to secure any multi-carriers (OFDM)-based communication. However, the main target of our work is to enhance security in 6G wireless networks because they are intended to enable high transmission capabilities and seamless integration of very heterogeneous devices.

3. Background on lattice-based encryption

In this section, we provide the mathematical background of the proposed lattice-based encryption scheme used to provide physical layer security (PLS) in 6G networks. We begin by introducing the theoretical aspects related to lattices. Lattices are mathematical structures that play a crucial role in the design of lattice-based encryption schemes. Next, we describe the hard problems that are utilized in the design of lattice point-based public key encryption schemes. These problems form the foundation of the security of lattice-based cryptography and involve computational challenges that are believed to be difficult to solve efficiently. By leveraging these hard problems, lattice-based encryption schemes offer a promising approach to achieve secure communication in 6G networks. It is worthy noting that in this section, lemmas and theorems are presented without proofs, most of which can be found in [54].

3.1. Mathematics for integer lattice

We introduce theoretical aspects concerning mathematical objects called integer lattices. Thus, we begin by providing definitions and discussing interesting properties of these objects.

An integer lattice can be defined as a discrete set of points in a multi-dimensional space, where each point has integer coordinates. It can be represented as a grid structure with points located at the intersection of integer coordinates. The lattice extends infinitely in all directions. Formally, a lattice is a set of points in n-dimensional space with a periodic structure that is defined as follows:

Definition 1 (*Lattice*). Given n-linearly independent vectors, $b_1, b_2, \dots, b_n \in \mathbb{R}^m$, the lattice generated by them is defined as

$$L(B) = \{v = \sum_{i=1}^{n} \alpha_i b_i, \alpha_i \in \mathbb{Z}\} \tag{1}$$

where B is a $m \times n$ matrix whose columns are $b_1, b_2, \dots, b_n$. We say that the rank of the lattice is n and its dimension is m. If $n = m$, the lattice is called full-rank lattice. In our work we will only consider full-rank lattices.

Hereinafter, the term “basis” will be used to refer both to the matrix B and the vector collection $b_1, b_2, \dots, b_n$. One peculiarity of a lattice is that it has multiple bases. It can be observed that a lattice is similar to a vector space, with the distinction that the vectors in a lattice are constrained to be multiplied by integers. Despite this seemingly minor restriction, it gives rise to numerous intriguing and subtle problems.

One initial problem we can pose is how to determine whether a given set of vectors forms a basis. Therefore, it becomes necessary to introduce some additional concepts.

Definition 2 (*Span*).The span of a lattice $L(B)$ is a linear space spanned by its vectors,

$$span(L(B)) = span(B) = \{By,\ y \in \mathbb{R}^n\} \tag{2}$$

Definition 3 (*Fundamental Parallelepiped*). For any lattice basis B we define the fundamental parallelepiped as :

$$P(B) = \{Bx,\ x \in \mathbb{R}^n, \forall i : 0 \le x_i < 1\} \tag{3}$$

We should notice that the fundamental parallelepiped, $P(B)$ depends on the basis B. Moreover, a tiling of the entire $span(L(B))$ can be obtained by placing one copy of $P(B)$ at each lattice point in $L(B)$. Consequently, to verify if a set of n linearly independent vectors forms a basis of a given lattice, we can prove that this set must satisfy the condition given by the following lemma.

Lemma 1. *Let L be a lattice of rank n, and let $b_1, b_2, \dots, b_n \in L$ be n linearly independent lattice vectors. The set of vectors $b_1, b_2, \dots, b_n$ forms a basis of L if and only if $P(b_1, b_2, b_3, \dots, b_n) \cap L = \{0\}$. Where $P(b_1, b_2, \dots, b_n)$ is the fundamental parallelepiped constructed using vectors $b_1, b_2, \dots, b_n$ as previously defined.*

Another important question concerning lattice bases is how to determine if two bases belong to the same lattice. To address this, we need to introduce the notion of a unimodular matrix.

Definition 4 (*Uni-Modular Matrix*). A matrix $U \in \mathbb{Z}^{n \times n}$ is called unimodular, if its determinant verifies, $det(U) = \pm 1$

The following lemma asserts an important propriety of unimodular matrix is that its inverse is also uni-modular. Consequently, the set of unimodular matrices forms a group under matrix multiplication.

Lemma 2. *if U is a uni-modular matrix then U^{-1} is also uni-modular, in particular $U^{-1} \in \mathbb{Z}^{n \times n}$*

Hence, we can prove that two bases generate the same lattice if they satisfy the following condition.

Theorem 1. *Two bases B and C are equivalent if and only if $C = BU$, where U is a unimodular matrix.*

A main parameter that characterizes a given lattice is its determinant defined as follows:

Definition 5 (*Lattice Determinant*). Let $L(B)$ be a full-rank lattice of rank n. The determinant of L, denoted $det(L)$ is defined as the n-dimensional volume of $P(B)$, and we have $det(L) =\mid det(B) \mid$.

We can notice that the determinant of the lattice is independent of the choice of the basis B, since by applying theorem 1 all the bases of a given lattice have the same determinant (up to the sign).

Moreover, we will see that in the proposed encryption schemes, we need to create basis with a high degree of orthogonality. The Hadamard ratio is a parameter that measure how much the vectors of a basis are orthogonal. It is defined as follows:

Definition 6 (*Hadamard Ratio*). if B is a real non-singular $n \times n$ matrix. The Hadamard ratio of B is defined as:

$$\mathcal{H}(B) = \left[\frac{\mid det(B) \mid}{\prod_i \|b_i\|}\right]^{\frac{1}{n}} \tag{4}$$

where $\|b_i\|$ is the Euclidean norm of the i’th column in B.

The columns of B are orthogonal to one another if and only if $\mathcal{H}(B) = 1$;otherwise 0< $\mathcal{H}(B) < 1$. When comparing different bases of the same lattice in $\mathbb{R}^n$, we only care about the product of the $\|b_i\|$’s since $det(B)$ is the same for all the bases and serves just as a normalized factor.

We can notice that orthogonality is one of the major concern when constructing a basis. Consequently, a useful technique used in lattice theory is the Gram–Schmidt orthogonalization. This procedure takes n linearly independent vectors, and creates a set of n orthogonal vectors. It performs a projection of each vector on the space orthogonal to the span of the previous vectors. The following theorem gives a formal description of the construction procedure

Theorem 2. *Given a sequence of n linearly independent vectors $b_1, b_2, \dots, b_n$, we can construct n orthogonal vectors $\tilde{b}_1, \tilde{b}_2, \dots, \tilde{b}_n$ by the following procedure :*

$$\tilde{b_1} = b_1,\ for\ i = 2...n,\ \tilde{b_i} = b_i - \sum_{j=1}^{i-1} \mu_{ij}\tilde{b_j}\ where\ \mu_{ij} = \frac{\langle b_i, \tilde{b_j}\rangle}{\|\tilde{b_j}\|^2}$$

It is easy to verify that $span(b_1, b_2, \dots, b_n) = span(\tilde{b_1}, \tilde{b_2}, \dots, \tilde{b_n})$ and $det(L(B = b_1, b_2, \dots, b_n)) = \prod_{i=1}^{n} \|\tilde{b_i}\|$

3.2. Hard problems in lattices

The two fundamental computational problems associated to a lattice are those of finding a shortest nonzero vector and a vector in the lattice that is the closest to a given non-lattice vector. The security of the adopted public key algorithm is based on the intractability of these two computational problems in lattices.

- The shortest vector problem (SVP): Given a lattice $L(B)$, find the shortest nonzero vector of the lattice, i.e find the nonzero vector $v \in L$ that minimizes the norm $\|v\|$. Minkowski gives an upper bound of the length of the shortest vector that is $\sqrt{n}(det(L(B)))^{\frac{1}{n}}$ but he does not give us an algorithm to find such vector.
- The Closest Vector Problem (CVP): Given a basis B for a lattice in $\mathbb{R}^n$ and another vector $v \in \mathbb{R}^n$ the problem of finding the closest vector in $L(B)$ is NP-hard for any norm in $\mathbb{R}^n$.

Both SVP and CVP are profound problems, and both become computationally difficult as the dimension n of the lattice grows. It is proved that these two problems are NP-hard. There are many important variants of SVP and CVP that arise both in theory and in practice. We describe a few of them that are useful in the construction of the cryptosystem.

- The Smallest Basis Problem (SBP): Given a basis B for a lattice in $\mathbb{R}^n$, the goal is to find the smallest basis B' for the same lattice. There are many variants of this problem, depending on the exact meaning of the smallest. In this context we care about bases with high Hadamard ratio. Thus we consider the version in which we look for the basis B' of $L(B)$ which has a Hadamard ratio very close to 1.
- Approximate Shortest Vector Problem (apprSVP) : Let $f(n)$ be a function of n. In a lattice $L(B)$ of dimension n, find a nonzero vector that is no more than $f(n)$ times longer than a shortest nonzero vector. In other words, if v_s is a shortest nonzero vector in L, find a nonzero vector $v \in L(B)$ satisfying $\|v\| \leq f(n)\|v_s\|$. Each choice of function $f(n)$ gives a different apprSVP.
- Approximate Closest Vector Problem (apprCVP): This is the same as apprSVP, but now we are looking for a vector that is an approximate solution to CVP, instead of an approximate solution to SVP.

These problems have no known polynomial-time algorithms and the best polynomial-time approximation algorithm for theme is the LLL algorithm and its variants [55]. The description of these algorithms will be given in the next sub-section.

3.3. Algorithms for solving lattice problems

Some polynomial time algorithms are developed in the literature to give an approximate solution to lattice hard problems. The approximation factors of these algorithm is γ^n, where γ is a constant that could be very little and n is the dimension of the lattice. Thus, these algorithms are inefficient when the dimension of the lattice increases. The two algorithms that will be presented in this section are the Babai's algorithm that is used for solving apprCVP and the LLL algorithm used for solving the apprSVP and the SBP.

3.3.1. Babai's algorithm for solving the apprCVP

This algorithm is based on the observation that if a lattice $L \subset \mathbb{R}^n$ has an orthogonal basis $b_1, b_2, \dots, b_n$, it is easy to solve the CVP . It is tempting to try a similar procedure with an arbitrary basis of L. If the vectors in the basis are reasonably orthogonal to one another, then we are likely to be successful in solving the CVP; but if the basis vectors are highly non-orthogonal, then the algorithm does not work well. Thus we can use the following theorem to find the closest lattice point to any element of $\mathbb{R}^n$.

Theorem 3. *Let $L \subset \mathbb{R}^n$ be a lattice with basis $b_1, b_2, \dots, b_n$ and let $v \in \mathbb{R}^n$ be an arbitrary vector. If the vectors in the basis are sufficiently orthogonal to one another, then the following algorithm solves the CVP.*

Write v as a linear combination of $b_1, b_2, \dots, b_n$, $v = a_1 b_1 + a_2 b_2 + a_3 b_3 + \dots + a_n b_n$ where $a_1, a_2, \dots, a_n \in \mathbb{R}$

for $i = 1, 2, \dots, n$, set $u_i = \lceil a_i \rfloor$ where $\lceil \rfloor$ is the ceiling operator.

Return vector $w = u_1 b_1 + u_2 b_2 + \dots + u_n b_n$

In general, if the vectors in the basis are reasonably orthogonal to one another, then the algorithm solves some version of apprCVP, but if the basis vectors are highly non-orthogonal, then the vector returned by the algorithm is generally far from the closest lattice point vector to v.

3.3.2. The LLL lattice reduction algorithm

LLL is an algorithm used to find the shortest vector in a lattice and to reduce lattice basis. Suppose that we are given a basis $B = \{b_1, b_2, \dots, b_n\}$ for a lattice L. The objective of this algorithm is to transform this basis in a better basis in the sense that its vectors are as short as possible and are more orthogonal to each other. It is obvious that finding such basis and applying the Babai's algorithm will give a better solution to the apprCVP. This algorithm is based on the following definition

Definition 7 (*LLL Reduced*)**.** Let $B = \{b_1, b_2, \dots, b_n\}$ be a basis for a lattice L and let $\tilde{B} = \{\tilde{b_1}, \tilde{b_2}, \dots, \tilde{b_n}\}$ be the associated Gram–Schmidt orthogonal basis as described by Theorem 2. The basis B is said to be LLL reduced if it satisfies the following two conditions :

1. Size condition $|\mu_{ij}| = \frac{|b_i \tilde{b_j}|}{\|\tilde{b_j}\|^2} \leq \frac{1}{2}$ $\quad for\ all\ 1 \leq j < i \leq n$
2. Lovasz condition $\|\tilde{b_i}\|^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2)\|\tilde{b}_{i-1}\|^2$ $\quad for\ all\ 1 < i \leq n$

The fundamental result of the LLL algorithm is the following theorem

Theorem 4. *Let L be a lattice of dimension n. any LLL reduced basis $\{b_1, b_2, \dots, b_n\}$ for L has the following properties :*

$\prod_{i=1}^{n} \|b_i\| \leq 2^{\frac{n(n-1)}{4}} det(L)$

$\|b_j\| \leq 2^{\frac{(i-1)}{2}} \|\tilde{b}_i\|$ *for all* $1 \leq j \leq i \leq n$

Further, the first vector in an LLL reduced basis satisfies

$\|b_1\| \leq 2^{\frac{(n-1)}{4}} |det(L)|^{\frac{1}{n}}$ *and* $\|b_1\| \leq 2^{\frac{(n-1)}{2}} min(\|b\|)$ $\quad for\ all\ b \neq 0$ *and* $b \in L$

Thus an LLL reduced basis solves apprSVB to within a factor of $2^{\frac{n-1}{2}}$. It is clear that this problem becomes intractable when the lattice dimension is very large.

3.4. Lattice-based cryptosystem

Several public key encryption algorithms that exploit the hardness of SVP and CVP in a lattice L are introduced. The most important of these are Ajtai–Dwork cryptosystem [12], the NTRU cryptosystem proposed by Hoffstein, Pipher, and silverman [51], and the GGH cryptosystem [50] of Goldreich, Goldwasser, and Halevi. In our work we selected the latter cryptosystem to ensure physical layer security in 6G networks. Our choice is justified by the simplicity and the low encryption overhead of the GGH algorithm. In fact, this algorithm is based on the observation that the best known algorithm for solving

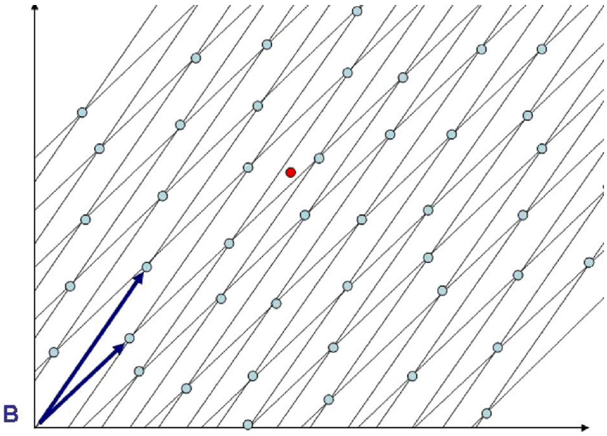


Fig. 1. Projection of point on the public basis.

apprCVP could not be efficient if a "bad" basis is selected to solve this problem. A bad basis is a basis whose vectors are not orthogonal and a good basis is a basis whose vectors are almost orthogonal and that gives a good approximation of the CVP problem. The principle of encryption process as follows:

A user that wants to receive secure message begins by choosing a set of linearly independent vectors

$\{r_1, r_2, \dots, r_n\} \in \mathbb{Z}^n$

that are reasonably orthogonal to each others. This set of vectors are the user's private key. Let R is the $n \times n$ matrix whose column are $r_1, r_2 ..., r_n$ and L is the lattice generated by these vectors.

Next the user should select a unimodular matrix U and then computes

$$B = UR \tag{5}$$

the column vectors of B noted $b_1, b_2, \dots, b_n$ form a new basis of L and they are the user's public key and is transmitted to all other users that want to communicate with this user.

When a transmitter wants to send a confidential message to that user, he transforms its plain text message into a vector m. He also selects a small error vector e that acts as an ephemeral key and then computes the vector c

$$c = E_B(m, e) = Bm + e = \sum_{i=1}^{n} b_i m_i + e \tag{6}$$

c is the cipher text. We should mention that c is not a lattice point of L, but it is close to the lattice point Bm because e is very small.

An example of the construction and the projection on the basis B (in the simple case where the points are in a two-dimensional space) is shown in Fig. 1. The encryption process transforms a lattice point into a non-lattice point by adding a small error vector e. Whereas our example shows a lattice of dimension 2, it can be noticed that it is difficult to find the original lattice point by projecting the non-lattice point on the public basis.

The decryption function is performed using Babai's round-off algorithm with the private basis R to find a vector in L that is close to c. As it has been previously described, this is done by representing c as a linear combination of the columns of R and then round the coefficients of this linear combination to the nearest integers to get a lattice point. Since R is a good basis and the error e is small the lattice point is Bm. Thus, multiplying this vectors by B^{-1}recovers the plain text m. Formally, if we denote $T = B^{-1}R$, then $m = T\left\lceil R^{-1}c \right\rfloor$, and $e = c - Bm$, where $\lceil \rfloor$ the ceiling operator.

Fig. 2 shows the projection of the non-lattice point on the private basis. It is clear that recovering the original lattice point by using the private basis is more easy and efficient than using the public basis. This is due to the fact that the vectors of the private basis are shorter and more orthogonal to each other than the vectors of the public basis.

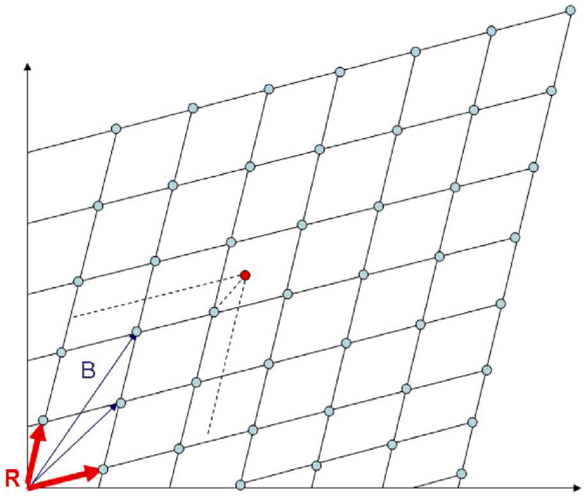


Fig. 2. Projection of point on the private basis.

4. Physical layer security scheme description

In this section, we will describe the proposed physical layer security scheme. We will begin by providing an overview of the scheme's architecture. Subsequently, we will present the various secure processing functions employed for the signal. Finally, we will conduct a security analysis of the proposed encryption procedure.

4.1. General architecture

In this sub-section, we describe the architecture of the proposed physical layer security system. As depicted in Figs. 3 and 4 the system is composed of two parts: the transmitter and the receiver. We will now provide a detailed explanation of the functions performed by the transmitter and the receiver.

The transmitter is composed of three processing blocks: data modulation, encryption, and OFDM processing. The user begins by generating a sequence of bits that are mapped into a sequence of modulation symbols. In practical applications, quadrature amplitude modulation (QAM-M) is commonly used for OFDM, where M represents the number of states of the QAM modulation and $p = log_2(M)$ is the length of the bit sequence represented by each state. Consequently, each sequence of p bits is mapped to a complex symbol $x_i = a_i + jb_n$ where $a_i, b_i \in \{\pm 1, \pm 3, \dots, \pm\sqrt{M} - 1\}$.

Before modulation, a serial-to-parallel conversion is applied to form a vector of N sequences of p bits. N represents the rank of the lattice used for encryption and also corresponds to the number of sub-carriers used in the OFDM process. Thus, the input to the encryption process is a vector of N complex symbols, $\left[S_0, S_1, \dots, S_{N-1}\right]^T$ where S_k represents the QAM symbol representing a transmitted bit sequence and corresponds to a specific constellation point. The lattice-based encryption process is then applied to this vector, generating an encrypted complex vector, $\left[C_0, C_1, \dots, C_{N-1}\right]^T$. Further details of this encryption process will be explained in an upcoming subsection. In the next step, the OFDM process is executed to generate a discrete time-domain signal $c = [c_0, c_1, \dots, c_{N-1}]$ using the inverse discrete Fourier transform, as indicated by the following formula:

$$c_n = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} C_i \exp(j2\pi n f_i), \quad 0 \le n \le N-1 \tag{7}$$

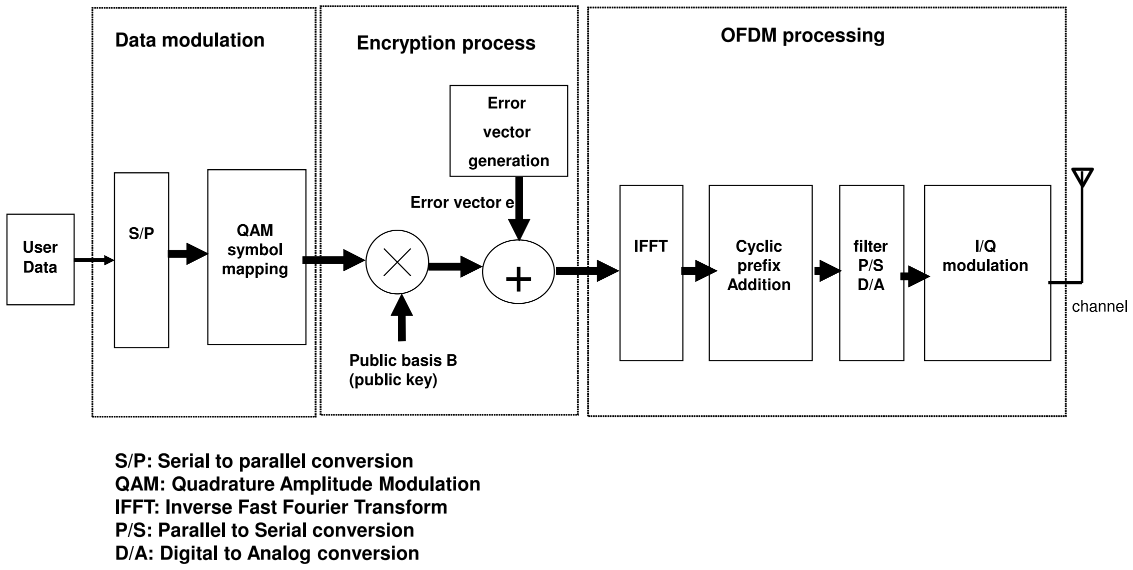

Data modulation
Encryption process
OFDM processing
User Data
S/P
QAM symbol mapping
Error vector generation
Error vector e
Public basis B (public key)
IFFT
Cyclic prefix Addition
filter P/S D/A
I/Q modulation
channel
S/P: Serial to parallel conversion
QAM: Quadrature Amplitude Modulation
IFFT: Inverse Fast Fourier Transform
P/S: Parallel to Serial conversion
D/A: Digital to Analog conversion

Fig. 3. Transmitter architecture.

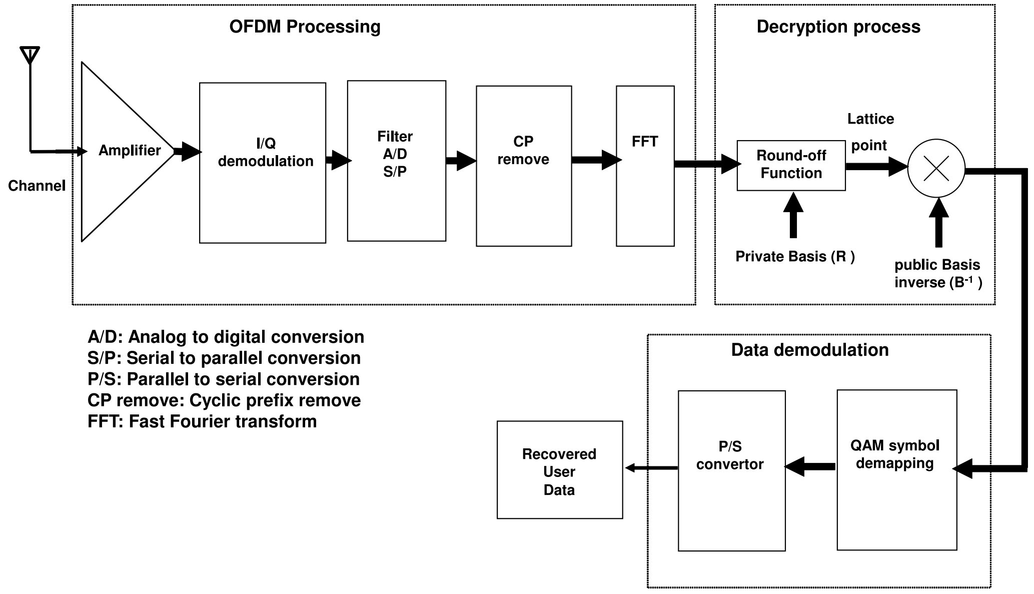


Fig. 4. Receiver Architecture.

Where $\{f_0, f_1, \dots, f_{N-1}\}$ is the set of sub-carrier frequencies assigned to the user. The remaining steps of the OFDM processing involve adding a cyclic prefix to mitigate inter-symbol interference, converting the parallel IFFT symbols to serial form, and converting the resulting signal to analog form. Finally, the signal is modulated using I/Q QAM modulation technique and transmitted through the wireless channel.

On the other hand, the receiver initially performs the inverse operations of the OFDM processing. It amplifies the received signal, converts it from analog to digital, and transforms it from serial to parallel. The receiver then removes the cyclic prefix and executes the fast Fourier transform to recover the encrypted message. After applying the decryption operation, the resulting vector is mapped to the corresponding QAM symbols and converted into a serial stream to recover the data bit stream. In the sequel, we will provide a detailed description of the encryption and decryption processes.

4.2. Signal encryption/decryption processes

In this subsection, we will provide a detailed explanation of the encryption and decryption processes executed by the transmitter and the receiver to ensure secure physical layer communication. The first step is to generate a pair of private and public keys for the destination user.

4.2.1. Private and public keys generation

To secure OFDM encoded data every user should get a private and a public keys (bases). These bases should be previously generated in the corresponding device and must satisfy some important proprieties. Algorithm 1 describes the different steps of the bases construction process that is executed in every device of the wireless network.

- Private basis (key) generation, R: The private basis is the most sensitive element of the encryption scheme and must be securely generated and stored within the device. Additionally, to enable data restoration using this basis, it should be a good basis in the sense that it can efficiently resolve the closest vector problem (CVP) using Babai's round-off algorithm. Consequently, the private basis denoted by R should be composed of a set of vectors that are short and nearly orthogonal to each other. The private basis R must have a Hadamard ratio that is very close to 1, indicating high orthogonality among the vectors. To generate the private basis R, we randomly select vectors from $\mathbb{Z}_+^N \times \mathbb{Z}_+^N$, where N is the dimension of the lattice. The Hadamard ratio of the generated basis is then calculated and compared to a predefined threshold denoted as $GoodTh$. If the Hadamard ratio of the basis falls below the defined threshold, the generation procedure is repeated.
- Generating the public basis (key), B: Once we have constructed the private basis R, we transform R into B by multiplying it with a unimodular matrix U. It is important to note that the public key B should be a "bad" basis in the sense that it does not provide an accurate solution to the CVP problem. This means that the vectors in B should not be orthogonal to each other, and consequently, the Hadamard ratio of B should be close to zero. To generate the public key B from the private basis R, we iteratively generate an unimodular matrix U at each step and multiply it with the public basis generated in the previous step. The procedure continues until the Hadamard ratio of B falls below a predefined threshold denoted as $BadTh$. . It is worth mentioning that in the first step, we initialize B with the value of R.
- Public basis (key) transmission: In order to enable the encryption of data generated at the transmitter, it is necessary for the component to possess the public bases of all users within the network. Therefore, once the public basis is generated, it should be transmitted by the respective users to the other users. This transmission can be achieved using conventional transmission techniques, typically utilizing a dedicated control channel for this purpose.

In our case, we have set the Hadamard ratio thresholds of the private basis and public basis to 0.8 and 0.001, respectively. This decision is based on tests conducted during the implementation of the encryption/decryption procedures, which indicate that these two values can be used to generate private and public bases without inducing transmission errors. However, it is important to note that the values of the two thresholds $GoodTh$ and $BadTh$, will affect the security and the efficiency of the key generation process. More precisely, the closer the chosen value of the Hadamard ratio of the good base is to 1, the less will be the error recovery at the receiver. Similarly, the closer the Hadamard ratio of the bad base is to 0, the more secure will be the encryption procedure against cryptanalysis attacks that attempt to recover the good base. Nevertheless, this will cause a longer delay for the private and public basis generation processes. Consequently, a trade-off between security and efficiency must be achieved in selecting these two thresholds. Learning approaches could be investigated in the future to reach this objective.

4.2.2. Data encryption

The data encryption process is described by algorithm 2. This procedure is executed by the transmitter and its objective is to provide security for the transfer of the bit stream between the transmitter and the receiver. Thus, when the transmitter decides to send encrypted data to a specific receiver, it generates and constructs a data vector $S = [S_0, S_1, \dots, S_{N-1}]$ by mapping each sequence of p bits into a QAM-M symbol where $M = 2^p$. An eventual padding can be added to the vector S to reach the selected lattice size. Using the public basis, B, of the corresponding receiver and an error vector E, the transmitter transforms the vector S to the integer vector $C = BS + E$. The error vector E is chosen randomly from the set $\{-\sigma; +\sigma\}^N$ and σ is a positive integer that must be selected according to a rule that will be evaluated later. Afterwards, the transmitter will apply the fast Fourier transform to the integer vector C to generate a discrete-time vector c. This vector will be transmitted to the corresponding receiver through the channel after adding the cyclic prefix. The vector is then converted from parallel to serial and from digital to analog. Finally, an I/Q modulation is performed using the carrier frequency

Algorithm 1 Private/public bases generation.

```
Inputs:
$N = 2^n$ : Dimension of the lattice,
$GoodTh = 0.8$: Hadamard ratio threshold for a "good" basis
$BadTh = 0.001$: Hadamard ratio threshold for a "bad" basis
Outputs
$R$ : Private (good) basis
$B$ : Public (bad) basis
  1. repeat
      (a) randomly generate $NxN$ matrix $R$ where elements are
          selected from $\{0, 1, 2, ..., N-1\}$
      (b) calculate the Dadamard ratio of $R$, $Hadamardratio(R)$
  2. until $Hadamardratio(R) \geq GoodTh$
  3. return $R$
  4. initiate $B$ with the value of $R$, $B = R$
  5. repeat
      (a) generate an unimodular matrix $U$
      (b) $B = B.U$
      (c) calculate the Hadamard ratio of $B$, $Hadamardratio(B)$
  6. until $Hadamardratio(B) \leq BadThreshol$
  7. return $B$
```

4.2.3. Data decryption

The decryption process begins by recovering the encrypted vector from the received OFDM signal through demodulation, sampling, and fast Fourier transform operations. As described by algorithm 3, the receiver uses its private basis R to recover the received QAM-encoded data vector $\hat{S}$ and extract the transmitted data. To invert the encryption function, we can use Babai's Round-off algorithm [55]. This involves representing the received encrypted vector $\hat{C}$ as a linear combination on the columns of R and rounding the coefficients to the nearest integers, resulting in a lattice point. The representation of this lattice point as a linear combination on the columns of B^{-1} gives us the vector $\hat{S}$. To prevent statistical cryptanalysis, an additional parameter can be used to randomize the generation of the vector E. Formally, if we denote $T = B^{-1}R$, then $\hat{S} = T \lceil R^{-1}C \rfloor$, where $\lceil \rfloor$ the ceiling operator.

4.2.4. Correctness of the scheme

In this subsection, we discuss the correctness of the scheme, which pertains to its ability to recover the original message without error. It should be noted that no inversion error occurs if $\lceil R^{-1}E \rfloor = 0$. We will now demonstrate that in order to satisfy this condition, the error vector must be very limited. Specifically, we require that $\sigma < \frac{1}{2\rho}$, where ρ denote the maximum L_1norm of R^{-1}.

Let $d = R^{-1}E$ and r'_i is the ith raw in R^{-1}. For every element d_i of d, we have $d_i = \sum_{j=1}^{N} r'_{ij} e_j$, e_j is the jth entry of E. To recover the plain text without errors we should have $|d_i| < 1/2$

Nevertheless, $|d_i| = |\sum_{j=1}^{N} r'_{ij} e_j| \leq \sum_{j=1}^{N} |r'_{ij}|.|e_j|$. According to the generation procedure of the error vector, we have $|e_j| = \sigma \; \forall j$ so,

Algorithm 2 OFDM signal encryption

```
inputs:
$B$: Matrix $NxN$ the public key of the destination user,
$Binary - data$: clear text a very long sequence of bits
$M$: number of QAM states
$\sigma$ :error element
$p = log_2(M)$ : the length of the bit sequence that will be mapped to a QAM-M symbol
outputs : encrypted OFDM signal

  1. Covert every sequence of $p$ bits of the $binary-data$ into a QAM-M symbol
  2. reshape the sequence of QAM-M symbols into column vectors of $N$ elements
  3. $for$ every vector $S = [S_0, S_1, ..., S_N]$ of $QAM - M$ symbols $do$
       (a) randomly generate an error vector $E \in \{\pm\sigma\}^N$
       (b) Calculate the vector $C = BS + E$
       (c) Calculate the vector $c$ the inverse of fast Fourier transform of $C$ using formula (7)
       (d) add cyclic prefix
       (e) transform the vector to serial
  4. end for
  5. transform the digital signal to analog and perform the classical I/Q modulation using the carrier signal
  6. transmit the encrypted OFDM signal through the wireless channel
```

Algorithm 3 OFDM signal decryption

```
inputs:
$R$: Matrix $NxN$ the private key of the destination user,
$B$: Matrix $NxN$ the public key of the destination user,
Sampled OFDM encrypted signal
Output
binary clear data

  1. covert the samples of the encrypted OFDM signal into a blocs of discrete time vectors of $N$ elements, $\hat{c}$
  2. $for$ every vector $\hat{c}$ of $N$ elements $do$
       (a) calculate the encrypted vector $\hat{C}$ by applying the fast Fourier transform on $\hat{c}$
       (b) apply the Babai's algorithm and calculate $\hat{S} = B^{-1}R\lceil \hat{C}R^{-1}\rfloor$
       (c) map the QAM-M recovered symbols into a binary sequence
  3. end $for$
```

$\sum_{j=1}^{N}|r'_{ij}|.|e_j| = \sigma\sum_{j=1}^{N}|r'_{ij}| \leq \sigma\rho$ where ρ is the maximum L_1 norm of the raws of R^{-1}. Therefore, if we chose $\sigma \leq \frac{1}{2\rho}$ then $|d_i| < 1/2\ \forall i$ and we can recover the encrypted vector without error.

4.3. Security analysis of the proposed scheme

The objective of the lattice encryption-based physical layer security scheme is to securely transmit the OFDM encoded signal from a transmitter to a receiver. For each individual stream, a private and public key pair is used to encrypt the transmitted data. The data stream is represented as an integer vector of N elements, which is beneficial when applying the proposed lattice-based physical layer security scheme. This representation enables the application of the GGH lattice-based public key algorithm to encrypt the QAM modulated codes. The dimension of the lattice plays a crucial role in the security of the encryption scheme. A higher dimension enhances the security of the encryption algorithm. It is essential to select the lattice dimension in a way that prevents the best-known basis reduction algorithm from providing a good solution for the Shortest Vector Problem (SVP).

As previously mentioned, each device in the network should be assigned two bases. It is indicated in [50] that the best basis reduction algorithm becomes inefficient when the lattice dimension exceeds 100, and a recommended range for this parameter is between 250 and 300. Additionally, a cryptanalysis conducted in [56,57] demonstrated a security attack on the GGH and NTRU signature schemes, where a reduced basis can be constructed by selecting a given number of linearly independent lattice points. The authors proposed that to guarantee the security of the lattice-based encryption scheme, the lattice dimension should be greater than 350. Also, it is clear from the study published in [58] that, until now, using a lattice dimension of 400 and more can resist major cryptanalysis attacks. This security requirement will be largely guaranteed in the proposed physical layer security scheme. Indeed, according to this scheme, the dimension of the lattice used is the same as the number of sub-carriers allocated to the user. Very high capacity is one of the key characteristics of 6G communication infrastructure. This can only be satisfied by allocating a significantly high number of sub-carriers to the user, typically more than 512 sub-carriers. In addition, the security of the proposed scheme can be further enhanced by combining the encryption process with other physical security layer processes that consider the environmental conditions of the transmission, making it more challenging for attackers to recover transmitted data [14]. This can be achieved by reducing the signal-to-noise ratio available to the attacker.

On the other hand, higher lattice dimensions increase the length of the keys, thereby escalating the storage and computational capacity required to perform the encryption and decryption processes. Thus, a trade-off between resource requirements and security must be considered. This challenge can be addressed by improving the storage capacity of the communicating devices. Notably, memory capacities of devices are increasing every year, and it is expected that most devices in 6G networks will be capable of supporting the key length required for post-quantum encryption schemes.

Another security enhancement that can be envisioned for the proposed scheme is the encryption of the real part and the imaginary part of the encoded vector by two different public keys. This will harden the recovery of the encrypted data even for a medium dimension lattice. Furthermore, authors in [59–61] proposed enhanced variants of the lattice-based encryption algorithm that can ensure an acceptable security level with reduced key lengths.

Another issue that needs to be addressed is how to ensure secure public key distribution and management. Specifically, security schemes should be designed to ensure the connection between the public key and the identity of the device or user. For this purpose, a post-quantum public key infrastructure (PKI) and authentication mechanisms could be considered to facilitate trusted management of public/private key pairs. Although this topic is beyond the scope of this work, it presents an intriguing perspective.

5. Numerical simulation and performance evaluation

This section is dedicated to evaluating the performance of the physical layer security scheme based on lattice encryption. We implemented the proposed lattice encryption-based PLS scheme using the Matlab software, utilizing the Mapel tool integrated within it for key generation and matrix manipulation. Our scenario consists of a transmitter that sends an encrypted OFDM signal to a receiver.

To begin, we generate the private key (base) and public key (base) of the receiver using the aforementioned procedure. Next, the transmitted message is encoded with QAM symbols and encrypted using the

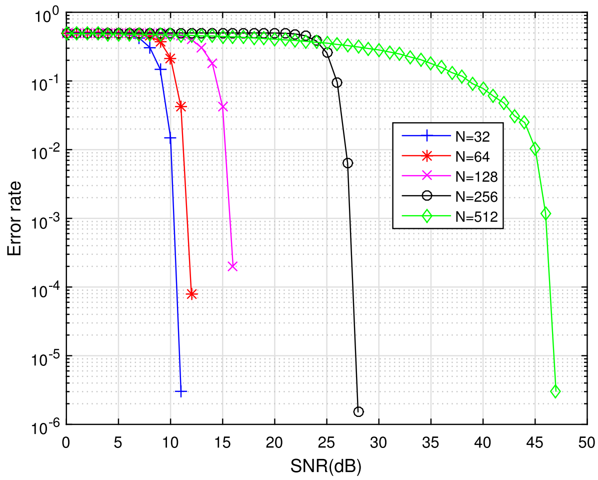


Fig. 5. SNR vs dimension of the Lattice.

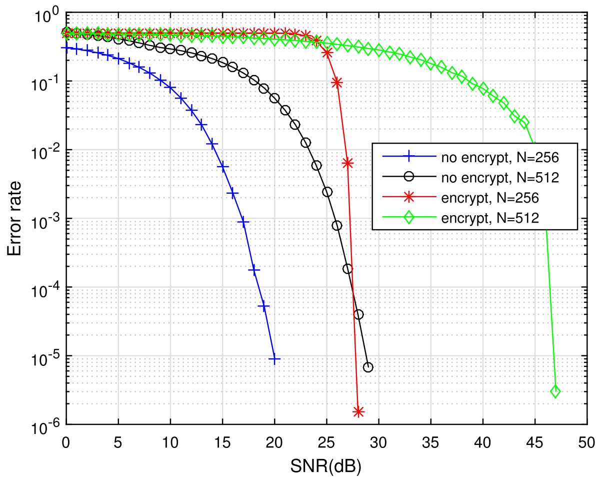


Fig. 6. SNR of encrypted vs not encrypted transmission.

receiver's public key. Subsequently, the OFDM process is applied before transmitting the encrypted signal through the channel. Each OFDM encoded message is appended with an eight-symbol cyclic prefix.

In our simulation framework, we create a message composed of a randomly generated sequence of bits. We consider an additive white Gaussian noise (AWGN) wireless channel model between the transmitter and the receiver. Each simulation is repeated until a confidence interval of 98% is reached. Through our work, we observed that repeating the simulations five times is sufficient to achieve this threshold.

Fig. 5 illustrates the average bit error rate variation with the signal-to-noise ratio (SNR) for different lattice dimensions. It is important to note that the lattice dimensions also determine the number of sub-carriers allocated for transmission. In our simulations, we considered five lattice dimensions: 32, 64, 128, 256 and 512. The transmitted message is modulated using QAM-16.

As it has been mentioned in the security analysis sub-section, to ensure the security of the scheme the lattice dimension must be typically greater than 350. In our simulations, we extended the dimension of the lattice to 512 in order to study the parameter's impact on communication performance. We observe that the SNR requirement for achieving an acceptable bit error rate increases with the lattice dimension, particularly for N = 512, where the SNR must be above 46 dB.

In Fig. 6 we evaluate the impact of applying lattice encryption to the OFDM signal in terms of SNR and bit error rate. Specifically, we compare the SNRs required for transmitting clear (non-encrypted) and encrypted OFDM signals for two dimensions of the lattice: 256 and 512. The results show that the encryption process increases the SNR by approximately 7 dB when the dimension of lattice is 256 and about 16 dB when it is 512.

Another set of simulations is dedicated to studying the influence of the number of QAM states on the performance of the physical layer security scheme employing lattice-based encryption. Fig. 7 illustrates the variation of the bit error rate as a function of the SNR for three values of the *M* parameter: 16, 64, and 256. We observe that the scheme achieves the best performance when utilizing QAM-16 modulation. This can be argued by the fact that when we increase the number of states in the QAM modulation, the error probability tends to increase. In other words, as the complexity of the modulation scheme increases, it becomes more susceptible to errors, resulting in a higher bit error rate.

To validate the security of the encryption process, we present in Fig. 8 the constellations of the transmitted signal (a), the encrypted signal (b), and the recovered signal (c). It is evident that the encryption process introduces significant confusion among the different states of the QAM-16 modulation. This further demonstrates the effectiveness of the encryption in enhancing the security of the transmitted data.

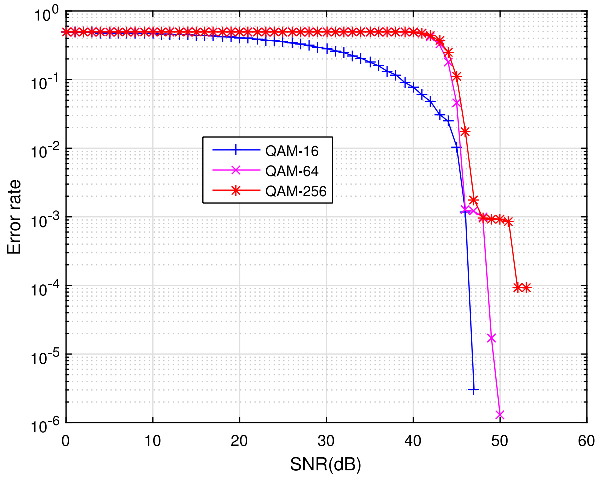


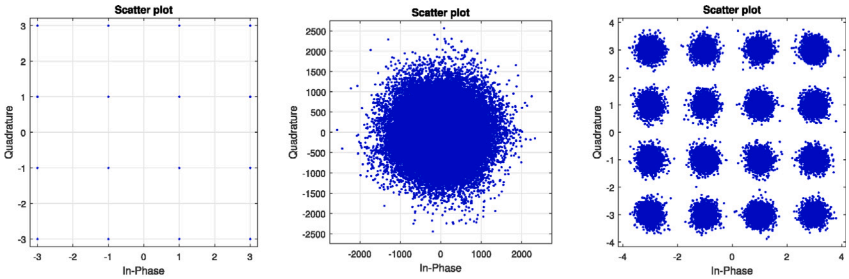
Fig. 7. Error rate for different QAM states.

In Fig. 9 we demonstrate the transmission of a multimedia message, specifically a standard image. We showcase the transmitted image (a), the encrypted image (b), and the recovered image (c). It is evident that without decrypting the intercepted signal using the correct credentials (i.e., the private key of the receiver), an eavesdropper will be unable to gather any information about the transmitted image. This emphasizes the robustness of the encryption scheme in preserving the confidentiality of the transmitted data.

6. Conclusion

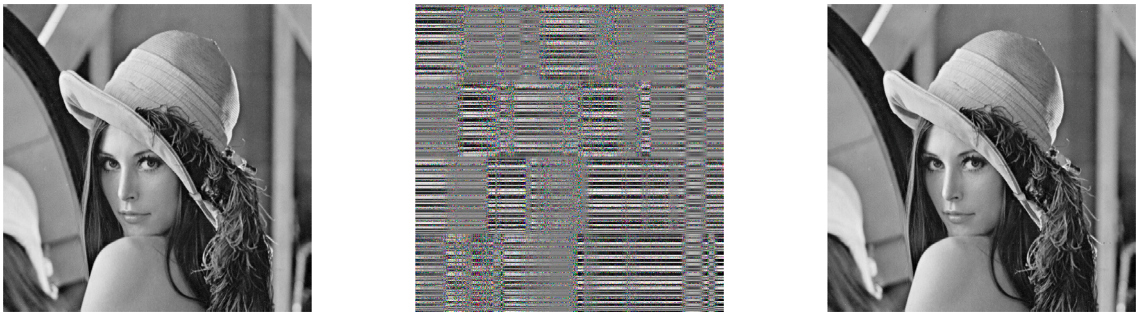
In this paper, we have introduced a physical layer security scheme for 6G wireless networks based on lattice encryption technique. Our scheme ensures confidentiality of OFDM modulated data by encrypting the vector of QAM symbols through projection onto the destination user's public base (key). We then introduce an error vector with reduced amplitude before performing the inverse fast Fourier transform of the OFDM procedure.

The performance evaluation tests reveal that the encryption process imposes an increasing cost in terms of signal-to-noise ratio. However, our physical layer security scheme demonstrates robustness in providing privacy for signals transmitted over 6G wireless networks, especially when the lattice dimension is sufficiently large. In 6G networks, this requirement is anticipated to be met due to the substantial number of sub-carriers allocated for each user, thereby satisfying the capacity requirement.



(a) (b) (c)

Fig. 8. Transmission constellations: (a) transmitted data, (b) encrypted data, (c) received data.



(a) (b) (c)

Fig. 9. Image Transmission : (a) transmitted image, (b) encrypted image, (c) received image.

CRediT authorship contribution statement

Walid Abdallah: Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] G. Gui, M. Liu, F. Tang, N. Kato, F. Adachi, 6G: Opening new horizons for integration of comfort, security, and intelligence, IEEE Wirel. Commun. 27 (5) (2020) 126–132.

[2] M.Z. Chowdhury, M. Shahjalal, S. Ahmed, Y.M. Jang, 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions, IEEE Open J. Commun. Soc. 1 (2020) 957–975.

[3] L.U. Khan, I. Yaqoob, M. Imran, Z. Han, C.S. Hong, 6G wireless systems: A vision, architectural elements, and future directions, IEEE Access 8 (2020) 147029–147044.

[4] L. Bariah, L. Mohjazi, S. Muhaidat, P.C. Sofotasios, G.K. Kurt, H. Yanikomeroglu, O.A. Dobre, A prospective look: Key enabling technologies, applications and open research topics in 6G networks, IEEE Access 8 (2020) 174792–174820.

[5] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, W. Zhou, Security and privacy in 6G networks: New areas and new challenges, Digit. Commun. Netw. 6 (3) (2020) 281–291, URL https://www.sciencedirect.com/science/article/pii/S2352864820302431.

[6] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T.H. Nguyen, F. Liu, T. Hewa, M. Liyanage, A. Ijaz, J. Partala, R. Abbas, A. Hecker, S. Jayousi, A. Martinelli, S. Caputo, J. Bechtold, I. Morales, A. Stoica, G. Abreu, S. Shahabuddin, E. Panayirci, H. Haas, T. Kumar, B.O. Ozparlak, J. Röning, 6G white paper: Research challenges for trust, security and privacy, 2020, arXiv:2004.11665.

[7] P. Botsinis, D. Alanis, Z. Babar, H.V. Nguyen, D. Chandra, S.X. Ng, L. Hanzo, Quantum search algorithms for wireless communications, IEEE Commun. Surv. Tutor. 21 (2) (2019) 1209–1242.

[8] V. Hassija, V. Chamola, V. Saxena, V. Chanana, P. Parashari, S. Mumtaz, M. Guizani, Present landscape of quantum computing, IET Quantum Commun. 1 (2020) 42–48.

[9] S.K. Satpathy, V. Vibhu, B.K. Behera, S. Al-Kuwari, S. Mumtaz, A. Farouk, Analysis of Quantum Machine Learning Algorithms in Noisy Channels for Classification Tasks in the IoT Extreme Environment, IEEE Internet Things J 11 (3) (2024) 3840–3852.

[10] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, M. Ylianttila, Security for 5G and beyond, IEEE Commun. Surv. Tutor. 21 (4) (2019) 3682–3722.

[11] C. Elliott, Quantum cryptography, IEEE Secur. Priv. 2 (4) (2004) 57–61.

[12] M. Ajtai, Generating Hard Instances of Lattice Problems (Extended Abstract), in: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC '96, Association for Computing Machinery, New York, NY, USA, 1996, pp. 99–108.

[13] Y.-S. Shiu, S.Y. Chang, H.-C. Wu, S.C.-H. Huang, H.-H. Chen, Physical layer security in wireless networks: a tutorial, IEEE Wirel. Commun. 18 (2) (2011) 66–74.

[14] J.M. Hamamreh, H.M. Furqan, H. Arslan, Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey, IEEE Commun. Surv. Tutor. 21 (2) (2019) 1773–1828.

[15] Y. Liu, H.-H. Chen, L. Wang, Physical layer security for next generation wireless networks: Theories, technologies, and challenges, IEEE Commun. Surv. Tutor. 19 (1) (2017) 347–376.

[16] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R.-A. Stoica, G. Abreu, H. Haas, Physical-Layer Security in 6G Networks, IEEE Open J. Commun. Soc. 2 (2021) 1901–1914.

[17] M. Mitev, A. Chorti, H.V. Poor, G.P. Fettweis, What Physical Layer Security Can Do for 6G Security, IEEE Open J. Veh. Technol. 4 (2023) 375–388.

[18] A. Mukherjee, S.A.A. Fakoorian, J. Huang, A.L. Swindlehurst, Principles of physical layer security in multiuser wireless networks: A survey, IEEE Commun. Surv. Tutor. 16 (3) (2014) 1550–1573.

[19] Y. Zou, J. Zhu, X. Wang, L. Hanzo, A survey on wireless security: Technical challenges, recent advances, and future trends, Proc. IEEE 104 (9) (2016) 1727–1765.

[20] X. Duan, X. Wang, Authentication handover and privacy protection in 5G hetnets using software-defined networking, IEEE Commun. Mag. 53 (4) (2015) 28–35.

[21] Q. Xu, R. Zheng, W. Saad, Z. Han, Device fingerprinting in wireless networks: Challenges and opportunities, IEEE Commun. Surv. Tutor. 18 (1) (2016) 94–104.

[22] K. Zeng, K. Govindan, P. Mohapatra, Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks], IEEE Wirel. Commun. 17 (5) (2010) 56–62.

[23] D. Kapetanovic, G. Zheng, F. Rusek, Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks, IEEE Commun. Mag. 53 (6) (2015) 21–27.

[24] M. Bloch, M. Hayashi, A. Thangaraj, Error-control coding for physical-layer secrecy, Proc. IEEE 103 (10) (2015) 1725–1746.

[25] A. Hyadi, Z. Rezki, M.-S. Alouini, An overview of physical layer security in wireless communication systems with CSIT uncertainty, IEEE Access 4 (2016) 6121–6132.

[26] X. Wang, P. Hao, L. Hanzo, Physical-layer authentication for wireless security enhancement: current challenges and future developments, IEEE Commun. Mag. 54 (6) (2016) 152–158.

[27] L. Samara, A.O. Alabbasi, A. Gouissem, R. Hamila, N. Al-Dhahir, A Novel OFDM Waveform With Enhanced Physical Layer Security, IEEE Commun. Lett. 25 (2) (2021) 387–391.

[28] H.A. Shah, I. Koo, A Novel Physical Layer Security Scheme in OFDM-Based Cognitive Radio Networks, IEEE Access 6 (2018) 29486–29498.

[29] J. Liu, Q. Hu, R. Suny, X. Du, M. Guizani, A Physical Layer Security Scheme with Compressed Sensing in OFDM-based IoT Systems, in: Proceedings of ICC 2020 - 2020 IEEE International Conference on Communications, ICC, 2020, pp. 1–6.

[30] R. Yamaguchi, H. Ochiai, J. Shikata, A Physical-Layer Security Based on Wireless Steganography Through OFDM and DFT-Precoded OFDM Signals, in: Proceedings of 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), 2020, pp. 1–5.

[31] H.M. Furqan, J.M. Hamamreh, H. Arslan, Enhancing physical layer security of OFDM systems using channel shortening, in: Proceedings of 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, PIMRC, 2017, pp. 1–5.

[32] S.E. Zegrar, H.M. Furqan, H. Arslan, Flexible Physical Layer Security for Joint Data and Pilots in Future Wireless Networks, IEEE Trans. Commun. 70 (4) (2022) 2635–2647.

[33] A.K. Yerrapragada, T. Eisman, B. Kelley, Physical Layer Security for Beyond 5G: Ultra Secure Low Latency Communications, IEEE Open J. Commun. Soc. 2 (2021) 2232–2242.

[34] J. Wu, R. Hou, X. Lv, K.-S. Lui, H. Li, B. Sun, Physical Layer Security of OFDM Communication Using Artificial Pilot Noise, in: Proceedings of 2019 IEEE Global Communications Conference, GLOBECOM, 2019, pp. 1–6.

[35] A. Aladi, E. Alsusa, Physical-Layer-Security-based OFDM Transmission with Phase Error Insertion, in: Proceedings of 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall), 2022, pp. 1–7.

[36] J.J. Sadique, S.E. Ullah, M.R. Islam, R. Raad, A.Z. Kouzani, M.A.P. Mahmud, Transceiver Design for Full-Duplex UAV Based Zero-Padded OFDM System With Physical Layer Security, IEEE Access 9 (2021) 59432–59445.

[37] H.S. Gill, S.S. Gill, K.S. Bhatia, A novel approach for physical layer security in future-generation passive optical networks, Photonic Netw. Commun. 35 (2) (2018) 141–150.

[38] M. Jacovic, K. Juretus, I. Savidis, K.R. Dandekar, Physical Layer Encryption for Wireless OFDM Communication Systems, J. Hardw. Syst. Secur. 4 (3) (2020) 230–245.

[39] N. Ishikawa, J.M. Hamamreh, E. Okamoto, C. Xu, L. Xiao, Artificially Time-Varying Differential MIMO for Achieving Practical Physical Layer Security, IEEE Open J. Commun. Soc. 2 (2021) 2180–2194.

[40] M.M. Hasan, M. Cheffena, S. Petrovic, Physical-Layer Security Improvement in MIMO OFDM Systems Using Multilevel Chaotic Encryption, IEEE Access 11 (2023) 64468–64475.

[41] D.H. Hameed, F.S. Hasan, Physical layer security using time-reversal pre-coding based OFDM-DCSK communication system with artificial noise injection, J. Commun. Softw. Syst. 19 (4) (2023) 289–298.

[42] Y.M. Al-Moliki, M.T. Alresheedi, Y. Al-Harthi, Physical-Layer Security Against Known/Chosen Plaintext Attacks for OFDM-Based VLC System, IEEE Commun. Lett. 21 (12) (2017) 2606–2609.

[43] W. Abdallah, D. Krichen, N. Boudriga, An optical backhaul solution for LiFi-based access networks, Opt. Commun. 454 (2020) 124473, URL https://www.sciencedirect.com/science/article/pii/S0030401819307709.

[44] J.-R. Shih, Y. Hu, M.-C. Hsiao, M.-S. Chen, W.-C. Shen, B.-Y. Yang, A.-Y. Wu, C.-M. Cheng, Securing M2M With Post-Quantum Public-Key Cryptography, IEEE J. Emerg. Sel. Top. Circuits Syst. 3 (1) (2013) 106–116.

[45] A. Khalid, S. McCarthy, M. O Neill, W. Liu, Lattice-based Cryptography for IoT in A Quantum World: Are We Ready? in: 2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces, IWASI, 2019, pp. 194–199.

[46] R. Asif, Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms, IoT 2 (1) (2021) 71–91, URL https://www.mdpi.com/2624-831X/2/1/5.

[47] D.-e.-S. Kundi, Y. Zhang, C. Wang, A. Khalid, M. O Neill, W. Liu, Ultra High-Speed Polynomial Multiplications for Lattice-Based Cryptography on FPGAs, IEEE Trans. Emerg. Top. Comput. 10 (4) (2022) 1993–2005.

[48] W. Abdallah, M. Hamdi, N. Boudriga, A public key algorithm for optical communication based on lattice cryptography, in: 2009 IEEE Symposium on Computers and Communications, 2009, pp. 200–205.

[49] N. Boudriga, W. Abdallah, M. Hamdi, Physical layer cryptography in optical networks: A lattice-based approach, in: 2010 12th International Conference on Transparent Optical Networks, 2010, pp. 1–7.

[50] O. Goldreich, S. Goldwasser, S. Halevi, Public-key cryptosystems from lattice reduction problems, in: B.S. Kaliski (Ed.), Advances in Cryptology — CRYPTO ’97, Springer, Berlin, Heidelberg, 1997, pp. 112–131.

[51] J. Hoffstein, J. Pipher, J.H. Silverman, NTRU: A ring-based public key cryptosystem, in: J.P. Buhler (Ed.), Algorithmic Number Theory, Springer, Berlin, Heidelberg, 1998, pp. 267–288.

[52] O. Regev, New lattice-based cryptographic constructions, J. ACM 51 (6) (2004) 899–942.

[53] M. Ajtai, C. Dwork, A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence, in: Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing, STOC ’97, Association for Computing Machinery, New York, NY, USA, 1997, pp. 284–293.

[54] J.H. Silverman, J. Pipher, J. Hoffstein, An Introduction to Mathematical Cryptography, 1, Springer, 2008.

[55] L. Babai, On Lovász lattice reduction and the nearest lattice point problem, Combinatorica 6 (1) (1986) 1–13.

[56] P.Q. Nguyen, Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto ’97, in: Poceedings of Advances in Cryptology - CRYPTO ’99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings, in: Lecture Notes in Computer Science, vol. 1666, Springer, 1999, pp. 288–304.

[57] P.Q. Nguyen, O. Regev, Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures, in: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006, Springer, Berlin, Heidelberg, 2006, pp. 271–288.

[58] A. Mariano, T. Laarhoven, F. Correia, M. Rodrigues, G. Falcão, A Practical View of the State-of-the-Art of Lattice-Based Cryptanalysis, IEEE Access 5 (2017) 24184–24202.

[59] S. Kamel, M. Sarkiss, G.R.-B. Othman, Improving GGH cryptosystem using generalized low density lattices, in: Proceedings of 2016 International Conference on Advanced Communication Systems and Information Security, ACOSIS, 2016, pp. 1–6.

[60] K. Bagheri, M.-R. Sadeghi, T. Eghlidos, An Efficient Public Key Encryption Scheme Based on QC-MDPC Lattices, IEEE Access 5 (2017) 25527–25541.

[61] O. Regev, On Lattices, Learning with Errors, Random Linear Codes, and Cryptography, J. ACM 56 (6) (2009).