IoT

MDPI

Review

Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms

Rameez Asif [1,2]

[1] Power Networks Demonstration Center (PNDC), University of Strathclyde, Glasgow G68 0EF, UK; rameez.asif@strath.ac.uk
[2] Department of Electronics and Electrical Engineering, University of Strathclyde, Glasgow G1 1XQ, UK

Abstract: The latest quantum computers have the ability to solve incredibly complex classical cryptography equations particularly to decode the secret encrypted keys and making the network vulnerable to hacking. They can solve complex mathematical problems almost instantaneously compared to the billions of years of computation needed by traditional computing machines. Researchers advocate the development of novel strategies to include data encryption in the post-quantum era. Lattices have been widely used in cryptography, somewhat peculiarly, and these algorithms have been used in both; (a) cryptoanalysis by using lattice approximation to break cryptosystems; and (b) cryptography by using computationally hard lattice problems (non-deterministic polynomial time hardness) to construct stable cryptographic functions. Most of the dominant features of lattice-based cryptography (LBC), which holds it ahead in the post-quantum league, include resistance to quantum attack vectors, high concurrent performance, parallelism, security under worst-case intractability assumptions, and solutions to long-standing open problems in cryptography. While these methods offer possible security for classical cryptosytems in theory and experimentation, their implementation in energy-restricted Internet-of-Things (IoT) devices requires careful study of regular lattice-based implantation and its simplification in lightweight lattice-based cryptography (LW-LBC). This streamlined post-quantum algorithm is ideal for levelled IoT device security. The key aim of this survey was to provide the scientific community with comprehensive information on elementary mathematical facts, as well as to address real-time implementation, hardware architecture, open problems, attack vectors, and the significance for the IoT networks.

Keywords: Internet-of-Things; cybersecurity; cryptography; quantum processing; encryption; communication systems

Citation: Asif, R. Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms. *IoT* **2021**, *2*, 71–91. http://doi.org/10.3390/iot2010005

Received: 3 December 2020
Accepted: 29 January 2021
Published: 5 February 2021

1. State-of-the-Art

Due to recent developments in the field of quantum computers, the search to build and apply quantum-resistant cryptographic algorithms brings classical cryptography to the next level [1]. Using those machines, many of today's most popular cryptosystems can be cracked by the Shor Algorithm [2]. This is an algorithm that uses quantum computation to equate the prime number phases expressed as sine waves to factor large integers, effectively solving the discreet logarithm problem that many current cryptographic algorithms are focused on [3–5]. Quantum computation is still in its infancy and is limited to a handful of mathematical operations that can be reliably determined by Reference [6]. We do need to build sufficient logical qubits (a logical cubit is stable over time and can be made up of hundreds or thousands of today's physical qubits) that can be used to fully break cryptographic codes [7]. In addition to all previous and continuing advances, quantum-resistant cryptography algorithms need to be rigorously checked using old and current data formats or sources to make them compatible with all platforms [8].

Predominantly, state-of-the-art public key algorithms are based on related problems, three of which are at the top of the list [9]. These three types of problems are known as

the discrete algorithm problem, the entire factoring problem, and the new pre-eminent elliptical curve discrete algorithm problem [10]. These three groups will be broken by Shor's quantum PC approximation. This is undoubtedly concerning, considering that these equations are commonly used to ensure the protected sharing of confidential information across the Internet, the development of digital signatures and the securing of other links over unsafe networks [11].

In view of the inherited shortcomings and major disadvantages involved in the implementation of an effective and smooth Quantum Key Distribution (QKD) [12], the quest for a classic, non-quantum cryptography algorithm that will operate in current real-time infrastructures is an increasingly growing field of study. These quantum robust algorithms are called Post-Quantum Cryptography (PQC) algorithms and are assumed to remain stable after the availability of functional large-scale quantum computing machines [13], as depicted in Figure 1. Every modern cryptography must be combined with existing protocols, such as transport layer security. The latest cryptosystem has to weigh:

- The size of the encryption keys and the signature.
- Time taken to encrypt and decrypt at either end of a contact line, or to sign messages and validate signature.
- For each proposed alternative, the amount of traffic sent over the wire needed to complete encryption or decryption or to transmit a signature.

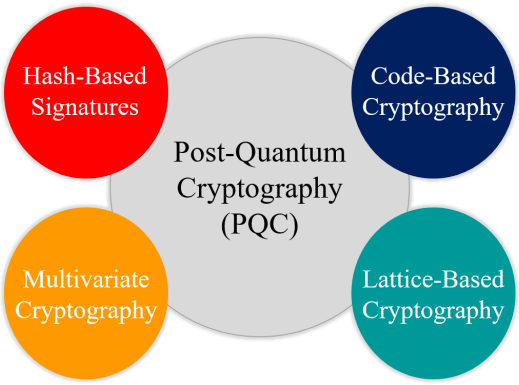

Figure 1. Basic types of Post-Quantum Cryptography (PQC).

Many NIST (National Institute of Standards and Technology) proposal submissions are also under review. Others have been broken or excluded from the process; some are more conservative or demonstrate how far it would be possible to advance classical cryptography so that it could not be cracked by a quantum computer at a fair expense [14]. But it is possible to categorize most cryptographic structures into these families: lattice-based, multivariate, hash-based (signatures only), and code-based. These categories are discussed in Section 2. For certain algorithms, though, there is a concern that they might be too inconvenient to use in the Internet-of-Things (IoT) networks [1]. With current protocols, such as Secure Shell (SSH) or Transport Layer Security (TLS), we must also be able to integrate new cryptographic schemes. Designers of post quantum cryptosystems need to take these attributes into account for IoT use-cases in order to do so:

- Latency induced by encryption and decryption at both ends of the communication line, assuming a number of devices to slow and memory limited IoT devices from large and fast servers.
- For ultra low latency, limit the size of public keys and signatures.
- Clear network architecture that facilitates crypt-analysis and the detection of vulnerabilities that could be exploited in a dense IoT network.
- Seamless integration with the existing infrastructure.

Post-Quantum protocols include a rich collection of primitives that can be used to solve the problems presented by implementation across different computing platforms

(e.g., cloud versus IoT ecosystems) and for various use cases [15–17]. This involves the ability to compute encrypted data by having resilient (somewhat widely described than ever before) protocols against powerful attackers based on asymmetric key cryptography (using quantum machines and algorithms) and to provide security beyond the context of classical cryptography [18]. Indeed, PQ cryptosystems are committed to strengthening the protection [19] of mission-critical infrastructures, especially in energy, medical, surveillance, space exploration, etc. Due to the flexibility and scalability of PQ cryptosystems, these algorithms are also implemented in next generation 5G/NB-IoT networks, as well as for secure communications, for electric vehicle charging infrastructure [20–22].

This survey has the following contributions. In Section 1, we discuss the state-of-the-art of Lattice-Based Cryptography (LBC), including the review papers to date. Section 2 elaborates the wider implementation of post-quantum cryptography (PQC), including Hash-Based Signatures, Code-Based Signatures, Multivariate Cryptography, and Lattice-Based Cryptography. In Section 3, we look at the fundamental mathematics and security-proofs of LBC. Moreover, it discusses the Ajtai-Dwork, Learning with Errors (LWE), and N-th degree Truncated polynomial Ring Units (NTRU) cryptosystems in detail. The extended security proofs of LBC against quantum attacks are discussed in Section 4, whereas Section 5 deals with the implementation challenges of LBC, both at software and hardware domain for authentication, key sharing, and digital signatures. In addition, the studies are applied to the application of LBC for power-restricted IoT applications, i.e., Lightweight Lattice Cryptography (LW-LBC). To conclude the survey, we review the implementation of LBC at FPGA level for the real-time experimentation of post-quantum cryptography. The key motivation of this survey was to provide comprehensive information on the future issues of quantum robust cryptography for IoT devices through LW-LBC.

2. Introduction to Post-Quantum Cryptography (PQC)

The PQC algorithms, as summarized in Figure 2, are mainly implemented by either Hash-Based Signature Algorithms, Code-Based Cryptography, Multivariate Cryptography Protocols, or by Lattice-Based Cryptography. In the following section, we shall discuss the PQC algorithms briefly.

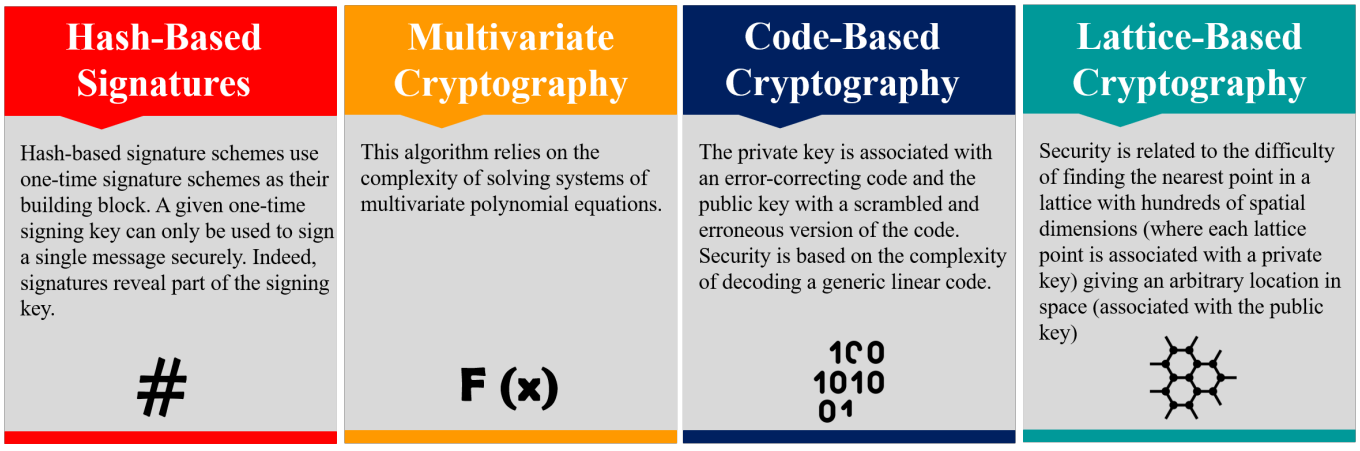

Figure 2. Implementation methods of four basic quantum secure algorithms.

2.1. Hash-Based Signatures

A hash-based signature scheme initializes from a one-time signature (OTS), i.e., a signature scheme where each key pair only needs to be used to sign a message with [23]. If an OTS key pair signs two different notes, this cab threatens the network, and a hacker will easily fake signatures that expose the customer's personal details. Merkle used the scheme of Lamport [24] and its variations. Merkle [25,26] recommended that a binary hash tree later named Merkle tree be used to create a many-time signature scheme. The leaves

are the hash values of OTS public keys in a Merkle tree. Each inner node is measured as the hash of its two child nodes concatenating. If a collision tolerant hash function is used, this ensures that all leaf nodes, i.e., all OTS public keys [27], can be authenticated using the root node.

The root node of the Merkle tree turns into a public key in a Merkle signature scheme (MSS) and the set of all OTS hidden keys becomes the secret key. Random bit strings are the hidden keys for hash-based OTS. Therefore, one can store a short seed and (re)generate the OTS secret keys using a cryptographically protected pseudo-random generator instead of storing all OTS secret keys [28]. To prevent reuse of OTS key pairs, they are used according to the order of the leaves, starting with the leftmost leaf [29]. To do this, the scheme keeps as an internal state the index of the last used OTS key pair. They are used according to the order of the leaves, starting with the leftmost node, to stop reuse of OTS key pairs [29]. In order to do this, the scheme holds the index of the last used OTS key pair as an internal condition.

2.2. Code-Based Signatures

Code-based cryptography is an upcoming contender for the diversification of today's [30] public-key cryptosystems, most of which rely on the complexities of either the factorization or the discrete logarithm problem [31]. Code-based cryptography, unlike public-key algorithms, is based on the problem of decoding unknown error-correcting codes, considered to be *NP*-hard [32]. There are two simple Code-based cryptography systems named after Robert McEliece [33] and Harald Niederreiter [34], their inventors. Compared to traditional cryptosystems, such as RSA [35], both share the issue of having massive key lengths, which renders their implementation impossible on embedded devices with very limited resources.

The input message is converted into a code-word for plain text encryption by either adding random errors to the message or encoding a message in the error sequence [36]. By deleting the errors or retrieving the original input message from the errors, decryption restores plain-text. It is, therefore, important to conceal the algebraic structure of the text, essentially cloaking it as an anonymous generic code [37]. An adversary understanding the particular code used will be able to decipher the message.

2.3. Multivariate Cryptography

The challenge of solving non-linear equation structures over finite fields is the foundation of Multivariate Cryptography schemes [38]. Generally speaking, seeking a solution for such structures is called a *NP*-complete/-hard problem [39]. Patarin's Secret Fields [40] is one of the fascinating cases, generalizing a suggestion by Matsumoto and Imai [41].

The same basic architecture is used for all Multivariate Public-Key Cryptosystems (MPKC), as they all depend on the use of multivariate polynomials over a finite field. The polynomial equations are of degree two in most cases, resulting in multivariate quadratic polynomials, which are still credited with being solved as NP-hard [42]. The MQPKC can not be solved more easily with Shor's algorithm than using a classical computer, since it does not depend on any of the hard problems that Shor's algorithms can solve, as compared to many other forms of PKC (public-key cryptography). It is also a potential candidate group for, a quantum resistant encryption scheme [42].

2.4. Lattice-Based Cryptography

Miklos Ajtai [43] first demonstrated Lattice-based algorithms, with the suggestion of designing stable cryptographic algorithms based on the hard lattice problem (*NP*) [44]. A lattice-based public-key encryption scheme was adopted [44], but a scheme that was sufficiently robust and proven stable was not presented until 2005, when Oded Regev proposed his scheme. This method uses both lattices and a generalization of the problem of parity learning [44]. A lattice, given in n-dimensional vector space, is a particular arrangement of points with an periodic structure and is used in a variety of fields. Lattice-based

cryptographic algorithms are mostly based on either the problem with the nearest vector (CVP) or the problem with the shortest vector (SVP). In most lattice-based cryptographic algorithms, the cryptographic builders used are very time-efficient and simple, while still providing security proofs based on the worst-case hardness [45]. A number of the simple problems used in this type of cryptographic algorithms often tend to be quantum resistant, since they are not based on any of the complicated problems solved by the algorithm of Shor [46]. This results in one of a few types of algorithms that are believed to carry promise as potential candidates for post-quantum cryptography is lattice-based cryptography.

For everyday Internet communications, generic cryptographic protocols, such as TLS and HTTPs [47], ensure that the communication between the two parties (sender and receiver) are authentic and private. Certain encryption algorithms that underpin these protocols, such as RSA [48,49], Diffie-Hellman [50,51], and elliptic curve [52–54], all are based on hard-to-solve mathematical problems and are categorized as asymmetric cryptographic primitives [55]. The time and resources needed to address these issues are prohibitive, which ensures that data encrypted using current encryption algorithms is considered secure. Due to the fact that the quantum computers [56,57] using Shor's factorization quantum algorithm [58] can quickly solve current asymmetric cryptographic primitives. Table 1 summarizes the impact of Shor's [59] and Grover's algorithms processing on typical classical data sets or cryptosystems [60]. The table summarizes public-key cryptography and similar algorithms being demolished by the development of quantum computers, leaving only symmetric cryptography (with greater key sizes) still usable and applicable but also on a small scale [61].

Table 1. Summary of the widely deployed classical cryptographic systems and their security levels against the best pre-quantum and post-quantum attacks known [61].

Name	Function	Pre-Quantum Security Level	Post-Quantum Security Level
Symmetric Cryptography (Private Key)			
AES-128 [62]	Block Cipher	128	64 (Grover)
AES-256 [62]	Block Cipher	256	128 (Grover)
SALSA-20 [63]	Stream Cipher	256	128 (Grover)
GMAC [64]	MAC	128	128 (no impact)
POLY-1305 [65]	MAC	128	128 (no impact)
SHA-256 [66]	Hash Function	256	128 (Grover)
SHA-3 [67]	Hash Function	256	128 (Grover)
Asymmetric Cryptography (Public Key)			
RSA-3072 [68]	Encryption	128	Broken (Shor)
RSA-3072 [68]	Signature	128	Broken (Shor)
DH-3072 [69]	Key Exchange	128	Broken (Shor)
DSA-3072 [70]	Signaure	128	Broken (Shor)
256-bit ECDH [71]	Key Exchange	128	Broken (Shor)
256-bit ECDSA [72]	Signature	128	Broken (Shor)

Several security specialists and scholars agree that the lattice-based cryptography algorithm is the path forward to deliver quantum-resistant encryption and, opposed to the other post-quantum cryptography strategies, is vigorous, as in Table 2. Lattice-based cryptography uses two-dimensional algebraic constructs known as lattices [73,74], which are not easily defeated with quantum computing schemes. A lattice is an infinite arrangement of dots, and the most vital lattice-based computational problem is the Shortest-Vector Problem (SVP) [75,76], which requires finding the point in the grid that is closet to a fixed central point in the space, called the origin. This is easy to solve in a two-dimensional

grid, but, as the number of dimensions increases, even a quantum machine cannot solve the problem effectively. The fact that lattice-based cryptography provides fast, quantum-safe, fundamental primitives, and enables the construction of primitives previously thought impossible, makes it the front runner candidate for IoT applications [77].

Table 2. Comparison among different techniques for post-quantum cryptography [78].

	Hash-Based	Code-Based	Multivariate-Based	Lattice-Based
Schemes	Signature	Signature Encryption Hash	Signature Encryption	Signature Encryption Hash Oblivious Transfer Identity-Based Encryption Homomorphic Encryption
Security Reduction	Collision Resistance	Code Invertibility	Solving Multivariate Equation System	Finding good basis for a lattice Solving lattice problems in special multidimensional lattices
Theoratical Speeds	Dependent on Hash function used	Good for Hardware	Good for Hardware	Good for Software
Practical Speeds	Extremely Fast	Good	Under Test	Under Test
Advantages	Extreme Fast and Modular	Mature and Secure	Fast and Small Keysizes	Excellent Security Robust Flexible
Disadvantages	Large Footprint Only Signature	Extensive Memory Requirements Variants Proven Insecure	Low Security	Not Fully Tested

3. Foundations of Lattice-Based Cryptography

High dimensional geometric structures are implemented by lattice cryptography, as seen in Figure 3, to conceal or mask the original details, generating a complexity that is deemed difficult to overcome even with available fault-tolerant quantum computers without the existence of the original key. A lattice is an infinite grid of dots, often arranged in a 2-dimensional setting.

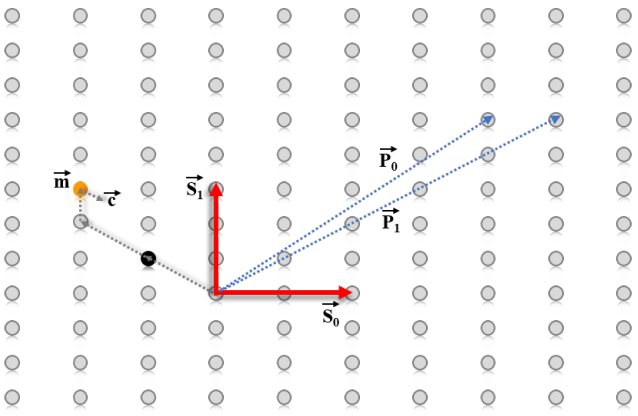

Figure 3. Example for lattice-based encryption (LBC) in a 2-dimensional structure: The secret, symmetrical base is $[\vec{S}_0, \vec{S}_1]$; the public, asymmetrical base is $[\vec{P}_0, \vec{P}_1]$. The sender utilizes $[\vec{P}_0, \vec{P}_1]$ to outline the message to a lattice point m and adds an error vector to obtain the resultant point $[\vec{C}]$. The point $[\vec{C}]$ is adjacent to the $[\vec{m}]$ than to any of the other lattice points. Therefore, the receiver can utilize the well formed secret-base $[\vec{S}_0, \vec{S}_1]$ to easily retrieve $[\vec{m}]$ (dotted vectors); this is a hard computation for an attacker who only has the scrambled base $[\vec{P}_0, \vec{P}_1]$. For a quantum-secure scheme, the n-dimension of the lattice must be much higher than 2 as in this example (source: http://publica.fraunhofer.de/dokumente/N-481797.html (accessed on 3 February 2021)).

LBC's security statement gives much greater faith in the long-lasting transfer of stable data in post-quantum cryptosystems that are directly based on hard lattice problems for two reasons. First of all, certain lattice-theory questions are validated to be *NP*-Hard [79]. *NP*-Hard is the non-deterministic polynomial-time hardness in computational theory that characterizes the property of a class of problems that are informally analogous to the most difficult problems in the NP solution [80]. Secondly, there is a worst-case to average-case simplification of the security of many lattice problems. This reduces the security proof requirement of a cryptosystem to a series of proof of an average-case hardness due to adaptation of the worst-case to average-case. In designing the cryptosystems to help satisfy the requirements of the [43] case, this provides greater flexibility and stability.

3.1. A Simple Lattice Model

A full-rank lattice basis B, as in Equation (1), is defined as a set of n linearly independent vectors in a vector-space of dimension n.

$$B = \{b_1, ..., b_n\}, b_k \in \mathbb{R}^n. \tag{1}$$

A lattice $\mathcal{L}_B$ is characterized as the set of all the integral combinations of the basis B of linearly independent vectors across a vector space of dimensions n [78]. We need a succinct way to represent lattices, as in Equation (2), if we are going to use them in cryptography. For this, we use what is called a 'basis of a lattice'. A basis is a small collection of vectors that can be used to reproduce any point in grid that forms the lattice [81]. An analytically good basis are those vectors in which a given problem is easy to solve without complexities, and it is termed bad basis for those in which it is generally not easier than a random basis to solve a particular lattice problem, i.e., *NP*-Hard.

$$\mathcal{L}_B = \mathbb{Z}b_1 + ... + \mathbb{Z}b_n, \mathbb{R}^n. \tag{2}$$

3.2. Computational Complexities in Lattice

As discussed previously, the evidence for cryptosystems to be secure can be provided by assuming the hardness of the certain lattice problems in the worst-case. The most well known computational problems on lattices [82] are as follows:

Shortest Vector Problem (SVP): Given an irrational basis B of a lattice $\mathcal{L} = \mathcal{L}(B)$, find a shortest non-zero lattice vector in the given set, i.e., $v \in \mathcal{L}$ such that $\|v\| = \lambda(\mathcal{L})$ [83].

Closest Vector Problem (CVP): Given a lattice basis B and a target vector t (not necessarily in the lattice grid or vector set), we have to find the lattice point $v \in \mathcal{L}(B)$ closest to t in the vector space [84].

Shortest Independent Vectors Problem (SIVP): Given the lattice basis $B \in \mathbb{Z}^{n*n}$, find n via linearly independent lattice vectors $S = [S_1, ..., S_n]$, where $S_i \in \mathcal{L}(B)$ for all the values of i, hence minimizing the quantity $S = max_i\|s_i\|$ [75].

Bounded Distance Decoding Problem (BDDP): Given basis B of an n-dimensional lattice $\mathcal{L} = \mathcal{L}(B)$ and a target point $t \in \mathbb{R}^n$ with the affirmation that $\text{dist}(t, \mathcal{L}) < d\Lambda_1(\mathcal{L})/2\gamma(n)$, calculate the distinctive lattice vector $v \in \mathcal{L}$ such that $\|t - v\| > d$ [85].

3.3. Lattice-Based Cryptosystems

In the following section, we will address in depth the all-important lattice cryptosystems, examine their security and application of their realistic real-time problems. It has been shown that the post-quantum stable cryptosystem can be generated via the hidden hyper-plane problem (HHP) with its security proof depending on the worst case of the one-way trapdoor function [86]. Although HHP accepted the worst-case/average-case reduction, large key-sizes are involved for an acceptable security standard [87] due to the colossal cipher-text expansion. Therefore, this cryptosystem was not ever meant to replace the current cryptosystems in an optimal and realistic way. We shall outline the basics of Ajtai-Dwork cryptosystem [88], Learning with Errors (LWE) cryptosystem [89], and N-th

degree Truncated (NTRU) [90]. As a first step, enlist the summary of the key generation, encryption, and decryption.

Key Generation

- Create a good basis $\mathbb{R}$.
- Transform the good basis $\mathbb{R}$ into the bad basis $\mathbb{Q}$ through a uni-modular transformation.
- Publish the bad basis $\mathbb{Q}$ as public basis and keep the good basis $\mathbb{R}$ as private basis.

Encryption

- Choose any lattice vector w using the public basis $\mathbb{Q}$ and add a customized plain-text vector p to it.
- Send this new vector $c = w + p$ as the cipher-text.

Decryption

- Using the private basis, compute the closest lattice vector w to the cipher-text c.
- Subtract this lattice vector w from the cipher-text to give the plain-text $p = c - w$.

Security Evaluation

Lattice-based cryptography offers a great deal of promise for the most realistic, stable post-quantum cryptosystem, with the worst-case/average-case minimization as seen by Ajtai and Dwork [91], along with certain lattice concerns that are shown to be NP-Hard [92]. While several lattice-based cryptosystems improve simplicity, scalability, and robustness, the computational complexity is much too high compared to the algorithms of classical cryptosystems and multivariate cryptosystems. Indeed, it would almost seem as if cryptographic research based on lattices is a race towards quantum-unbreakable security and performance, whereas cryptographic research based on multivariates is a race towards security. With the implementation of advanced q-ary lattices and the ideal lattice classes, this efficiency versus security gap is closing rapidly.

3.3.1. Ajtai-Dwork Cryptosystem

In the following section, we define the state-of-the-art Ajtai-Dwork cryposystem (Algorithm 1), examine its security, and, at the end of the section, we shall discuss its practical real-time implementation [93].

Algorithm 1 Ajtai-Dwork Cryptosystems

- Parameters: Integers n,m;
- Private Key: $s \in \mathbb{R}^n$;
- Public Key: a set of m random points $\{y_i\}_{i=1}^m$, $y_i \in \mathbb{R}^n \forall_i$ such that:$\langle s, y_i \rangle \approx 0 \bmod 1$, i.e., s is a solution of HHP with data $\{y_i\}_{i=1}^m$;
- Encryption: to encrypt the data that is represented by 0 generate a random point y in lattice vector $\mathbb{R}^n$. Similarly, To encrypt 1, consider $y = \sum_{l \in y} y_1$ with $J = \subset [m]$ arbitrary and, finally, send y;
- Decryption: the receiver evaluates $\langle s, y_i \rangle$. By linearity $r \approx 0$, he de-crypts the cipher-text as 1, otherwise as 0.

Security Evaluation

Ajtai and Dwork evaluated the security proof of this cryptosystem through two independent methods and results [91]:

- whoever can determine between the encryption of 0 and 1 can also master the art of solving the HHP with the same data. This means that breaking the semantic security of their cryptosystem is at least as hard as solving HHP (search-to-decision reduction).
- starting from any algorithm that solves HHP, it is possible to implement one that efficiently solves $uSVP_\gamma$, in the worst case, for some $\gamma = poly(n)$.

Combining these results together, Ajtai and Dwork got a worst-case to average-case reduction, which means that breaking the cryptosystem is at least as hard as solving $uSVP_\gamma$ [94].

Complexity and Implementation

This initial version of the cryptosystem is very inefficient when actually applied, i.e., hard boundaries, as stated in the previous sections, despite being a groundbreaking outcome from a theoretical point of view. In 1998, a heuristic attack was demonstrated by Nguyen and Stern [95], which works efficiently for limited parameters and to recover the private key provided that the classical one is known. In this way, the researchers showed that in order to prevent crypt-analytic attacks, the n dimension in vector space should be of several hundred, concluding that Ajtai-Dwork cryptosystem is only of theoretical value without significant improvements. Ajtai proposed a more powerful implementation of the cryptosystem characterized by public keys and cipher-text sizes of $O\ (n^2)$ and $O\ (n)$ respectively in his subsequent work [Ajt05]. However, to date, no average-case to worst-case reduction is known, and, although being very similar to lattice-based protocol, it is based on a Dirichlet issue that does not seem to be connected to any known Dirichlet lattice issues [96].

3.3.2. Learning-With Errors Cryptosystem

In this paragraph, we define the actual LWE cryposystem (Algorithm 2) and examine its security and eventually discuss its practical real-time implementation [97,98].

Algorithm 2 Learning-with Errors (LWE) Cryptosyste

- Parameters: n, q, m positive integers, $\alpha \in \mathbb{R}$ such that $0 < \alpha < 1$ and $\chi = D_z$, discrete distribution over $\mathbb{Z}$;
- Private Key: $s \in \mathbb{Z}_q^n$ uniformly at random;
- Public Key: select m vectors $a_1, ..., a_m \in \sum \mathbb{Z}_q^n$ independently according to the uniform distribution. In addition, draw $e_1, ..., e_m \in \mathbb{Z}$ from χ and get the public key $\{a_i, b_i\}_{i=1}^m$, with $b = \langle a_i, s\rangle + e_i \bmod q$;
- Encryption: Let $\mu \in \{0, 1\}$ be the bit to encode, choose a random set $S \subset [m]$, then to encrypt μ one sends $(a, b) = (\sum_{i\in S} a_i \sum_{i\in S} b_i + \mu\frac{q}{2})$;
- Decryption: If $b - \langle a, s\rangle$ is close to 0 than to $\frac{q}{2}$ mod q output 0, otherwise decrypt as 1.

Security Evaluation

By analyzing encryption and decryption of LWE cryptography, we may notice that the choice of parameters is responsible for the correctness of the crytpographic protocols. For example, if $\mu = 0$, we need χ and q to be such that $b - \langle a, s\rangle = \sum_{i\in S} e_i < \frac{q}{4}$; otherwise, the bit would be decrypted as 1. This condition can be obtained by requiring q significantly larger than the error distribution χ and m. The following set of parameters will guarantee both in order to make this cryptosystem protected and accurate at the same time [98]: q prime between $2n$ and $2n^2$ with n in the order of hundreds. In addition, $m = (1+ \in)(n + 1) \log q$ for an arbitrary $\in > 0$, and, finally, $\chi = D_{\mathbb{Z},\alpha n}$ for $\alpha(n) = \frac{1}{\sqrt{n}log^2}n$.

Complexity and Implementation

The choice of the parameters is the prime priority for the implementation of LWE. The secret and the public key sizes are respectively $O(n)$ and $O(mn)logq = O(n^2)$. Furthermore, it is possible to reduce the public key size by exploiting the set of vectors $a_1, ..., a_m$ can be shared by all users and distributed as part of the encryption and decryption software, thus leading to the public key $b_1, ..., b_m$.

3.3.3. NTRU Encryption Scheme

The first protocol based on polynomial rings, especially on f-ideal lattices [99], is this cryptosystem. As far as output is concerned, both in terms of run times and key size, the NTRU is basically effective. Combined with the presumed protection from quantum attacks, these characteristics are the reasons why NTRU is commonly used as an alternative to RSA and ECC. In the following (Algorithm 3), we describe the original cryptosystem as it was presented and, later on, we briefly discuss subsequent works highlighting an evident trade-off between performance and security.

Algorithm 3 NTRU Encryption Scheme

- Parameters: n power of 2, $f(X) = X^n + 1$ and q odd sufficiently large, we define $R = \mathbb{Z}[X]/f(X)$ and $R_q = \frac{R}{qR}$;
- Private Key: $s, g \in R$ short polynomial, (i.e., with small coefficients) such that s is inevertible mod q and mod 2;
- Public Key: $h = 2g.s^1 \in R_q$ with $g \in R$ short polynomial;
- Encryption: choose a short $e \in R$ such that e mod 2 encodes the desired bit, choose $r \in R_q$ randomly and compute the cipher-text $c = h.r + e \in R_q$ accordingly
- Decryption: multiply the cipher-text with the secret key to get $cs = 2gr + es \in R_q$, lift it in R as $2gr + es$ (possible if the following variables, i.e., g, r, e, s are short enough compared to q) and reduce it $\mid 2 \mid$ obtaining $es \mid 2 \mid$ and, therefore, the initial bit.

Security Evaluation

As already interpreted, neither implementation of the NTRU provided either an average-case reduction to the worst-case reduction or a more general safety proof. Unfortunately, the real-time implementation is less effective than the original scheme to get an acceptable degree of security, and this depicts the trade-off between the security level and the efficiency appraisal, which unfortunately appears to stop the rapid development of lattice-based cryptography.

Complexity and Implementation

Today, the 'NTRUEncypt' is a standard public key cryptosystem (IEEE Std. 1363.1) successfully commercialized and available under a free open source license initiative. Meanwhile, we may notice that both private and secret keys require $O(nlogq)$ bits to be encoded to get the level of security from PQC perspective.

3.4. Lattice Reduction Algorithms

The strategies outlined in the previous section for applying the problems of LWE and NTRU, substantially based on the concepts of lattice reduction, are the strategy of creating a sufficiently orthogonal basis given the definition of a lattice. Slide decrease [100] is the lattice reduction algorithm that achieves the successful theoretical performance. However, we tend to consider the best operating algorithm experimentally, BKZ (Block Korkine Zolotarev) [101]. Given the basis for one of the lattices in vector space as described above, we need to select the block size required to retrieve the shortest vector when running BKZ (i.e., the block size is the smallest size of operating data on a computing device or memory can have). This is done following the analysis introduced in Reference [102] for the LWE and NTRU primal attacks, and the analysis done in Reference [103] for the LWE dual attack.

In exchange, BKZ uses a smaller lattice oracle to solve the Shortest Vector Problem (or SVP oracle). Several SVP algorithms can be used to instantiate this oracle, with current generations of Reference [104] filters or [105] enumeration being the two most powerful. Because we consider security in post-quantum cryptography, we also need to consider quantum algorithms, which mostly implies considering possible Grover [106] speed-ups for the algorithms as of writing [107].

4. Lattice Cryptography Against Quantum Attacks

In this section, we will summarize the fact thet LWC algorithm is secure against the known quantum attacks, i.e., SVP is NP-hard [108,109]. We shall show that the problems of approximating the shortest and closest vector in a lattice to within a factor of $\sqrt{n}$ lies in the NP intersect $coNP$ [110]. Different information is available in the literature to test the security standard of LWC post-quantum cryptographic primitives [110–112]. Consider factoring the NP-Hard and the language to describe factoring is C=$\{(n, c)$, where n has a factor $\leq C$. Now, $C \in P$ and the factoring is highly dependent on P [113], since $\mathbb{N} - C = \mathbb{P} \cup \{1\}$, so that there would be a polynomial time algorithm for deciding whether a string is $s = \mathbb{P}$ or not [114]. If, under some applied conditions, we assume that C is NP complete, but, in cryptography theory, to date, there is no proof available for $P = NP$, it stays $P \neq NP$ [115,116].

Extended Security Proof

The lattices have have been investigated extensively in mathematics, and many different problems can be explored exclusively related to lattices, such as integer programming [117], factoring polynomials with rational co-efficients [118], integer relation finding [119], integer factoring, and diophantine approximation [120,121]. Latest research on the study of lattices gained a lot of attention in the computer science community due to the fact that lattice problems were shown by Ajtai [43] to possess a particularly desirable property for cryptography: worst-case to average-case reducibility. As discussed previously in Section 2, the two problems Shortest Vector Problem (SVP) and Closest Vector Problem (CVP) have been widely studied [122–124]. The most important parameter of interest here is the factor of approximation β in the given basis $v_1, ..., v_n$ of a lattice to find the shortest non-zero lattice point in the Euclidean norm in the case of SVP, whereas, given the basis $v_1, ..., v_n$ of a lattice and a target vector $v \in \mathbb{R}^n$, find the closest lattice point to v in the Euclidean norm for CVP. The problem $GapSVP_\beta$ constitutes of distinguishing between the instances of SVP in which the length of the shortest vector is maximum 1 or larger than β, where β can be a constant or a fixed function of the dimension of the lattice n, whereas, for $GapCVP_\beta$, basis and the extra vector $v \in \mathbb{R}^n$ decodes whether the distance of v from the lattice is at most 1 or larger than β. The un-likelihood of the NP-hardness of approximating SVP and CVP within polynomial factors has also been evaluated in [125]. Here, we formulate the approximation problems associated with the shortest vector problem and the closest vector problem in terms of the following supposition or a promise problem (i.e., a generalization of a decision problem where the input is promised to belong to a particular subset of all the possible inputs of a system):

Definition 1. ***(approximate SVP)****: The promise problem $GapSVP_\gamma$ (where $\gamma \geq 1$) is a function of the dimension that is defined as follows. Instances are pairs (B, d), where $B \in \mathbb{Z}^{nxk}$ is a lattice basis, and d is a positive number and can be expressed as:*

- *(B, d) is a YES instance if $\lambda(B) \leq d$, i.e., $\|Bz\| \leq d$ for some $Z \in \mathbb{Z}^n \setminus \{0\}$,*
- *(B, d) is a NO instance if $\lambda(B) > \gamma.d$, i.e., $\|Bz\| > \gamma.d$ for all $Z \in \mathbb{Z}^n \setminus \{0\}$.*

Definition 2. ***(approximate CVP)****: The promise problem $GapCVP_\gamma$ (where $\gamma \geq 1$) is a function of the dimension that is defined as follows. Instances are triples (B, y, d), where $B \in \mathbb{Z}^{nxk}$ is a lattice basis, $y \in \mathbb{Z}^n$ a vector, and d is a positive number and can be expressed as:*

- *(B, y, d) is a YES instance if $dist(y(\mathcal{L}B)) \geq d$, i.e., $\|Bz - y\| \leq d$ for some $z \in \mathbb{Z}^n$,*
- *(B, y, d) is a NO instance if $dist(y(\mathcal{L}B)) > \gamma d$, i.e., $\|Bz - y\| > \gamma d$ for some $z \in \mathbb{Z}^n$.*

Definition 3. ***(approximate CVP')****: The promise problem $GapCVP'_\gamma$ (where $\gamma \geq 1$) is a function of the dimension that is defined as follows. Instances are triples (B, y, d), where $B \in \mathbb{Z}^{nxk}$ is a full rank matrix, $y \in \mathbb{Z}^n$ a vector, and d is a positive number and can be expressed as:*

- *(B, y, d) is a YES instance if $\|Bz - y\| \leq d$ for some $z \in \{0, 1\}^n$,*

- (B, y, d) *is a NO instance* $\|Bz - wy\| > \gamma d$ *for all* $z \in \mathbb{Z}^n$ *and all* $w \in \mathbb{Z} \setminus \{0\}$.

Therefore, it can be characterized that [125] $GapSVP$, $GapCVP$, and $GapCVP'$ are NP-hard for any constant factor $\gamma \geq 1$. For LWC on the implementation of cryptographic primitives, it is well documented that the security level relies on the hardness of the above mentioned lattice problems [83,126]. For example, in cryptographic constructions based on factoring, the assumption is that it is hard to factor numbers chosen from a certain distribution, which is why it is considered as quantum-secured algorithm.

5. Lightweight Lattice-Based Cryptography for IoT Devices

The emergence of new edge computing platforms, such as cloud computing, software-defined networks, and the Internet-of-Things (IoT), calls for the adoption of an increasing number of security frameworks, which in turn require the introduction of a variety of primitive cryptographic elements, but the security is just one vector in the IoT world [127]. It is also necessary to implement those secure frameworks that consume less on-board processing, memory and power resources [128]. This presents enormous difficulties in the design and execution of new cryptographic principles in a single embodiment, as diverging priorities and restrictions are accurate for the computing platforms. This involves the development of programmable IoT hardware capable of effectively executing not only individual cryptographic algorithms [129], but complete protocols, with the subsequent task of agility design, e.g., developing computer devices that achieve the performance of Application-Specific Integrated Circuits (ASICs), while keeping some programmability level [130,131].

Recently, many researchers are investigating Lightweight Lattice-Based Cryptography (LW-LBC) [128,132], where performance evaluation is fairly measured and benchmarked in terms of low-power footprint, narrow area, lightweight bandwidth requirements and good performance. The main characteristics of post-quantum LBC that makes them well suited for IoT world are: (a) these schemes offer security proofs based on NP-hard problems with average-case to worst-case hardness; (b) secondly, the LBC implementations are noteworthy for their efficiency in addition to being quantum-age stable, largely due to their inherent linear algebra-based matrix/vector operations on integers; and, (c) third, for specialized security, LBC buildings offer expanded features, in addition to the simple classical cryptographic primitives (encryption, signatures, key exchange solutions required in a quantum era, services, such as identity-based encryption (IBE) [133], attribute-based encryption (ABE) [11], and fully homomorphic encryption (FHE)) [134].

Figure 4 depicts the communication bandwidth by calculating the data bytes of various LBC algorithms with sk, pk, and signature variants, as comprehensively analyzed in Reference [128], while the number manifested at the end of each algorithm is the level of security achieved according to the NIST standards. These security levels can be defined as: (a) Level 1: at least as hard to break as AES-128 (exhaustive key search), (b) Level 2: at least as hard to break as SHA-256 (collision search), (c) Level 3: at least as hard to break as AES-192 (exhaustive key search), (d) Level 4: at least as hard to break as SHA-384 (collision search), and (e) Level 5: at least as hard to break as AES-256 (exhaustive key search). It is also worth mentioning that this security matrix is highly dependent on the hardware/computational resources of IoT-Edge nodes in the network. It can be seen from the analysis that Dilithium algorithms have consumed high bandwidth but are unable to achieve a high level of security, whereas the Falcon algorithms have consumed less bandwidth for achieving high level of security. These algorithms are ideal for lightweight implementation of LBC in the IoT devices.

Figure 5 depicts the communication bandwidths of LBC algorithms implemented with public key encryption (PKE) or with Key encapsulation mechanisms (KEM) schemes [128,135,136]. It can be seen from the results that Saber and ThreeBears variants both consume less bandwidth at diverse NIST security levels and can be considered as the suitable candidates for lightweight implementation of LBC in the IoT networks.

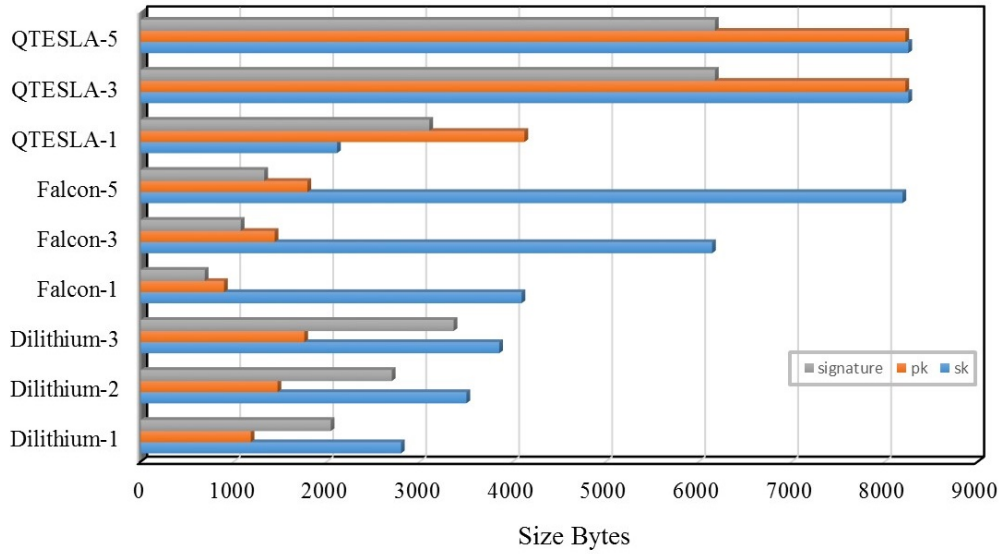

Figure 4. Comparison of Internet-of-Things (IoT) communication bandwidth for lattice-based cryptography (LBC) algorithms with secret key (sk), public key (pk), and signature variants [128].

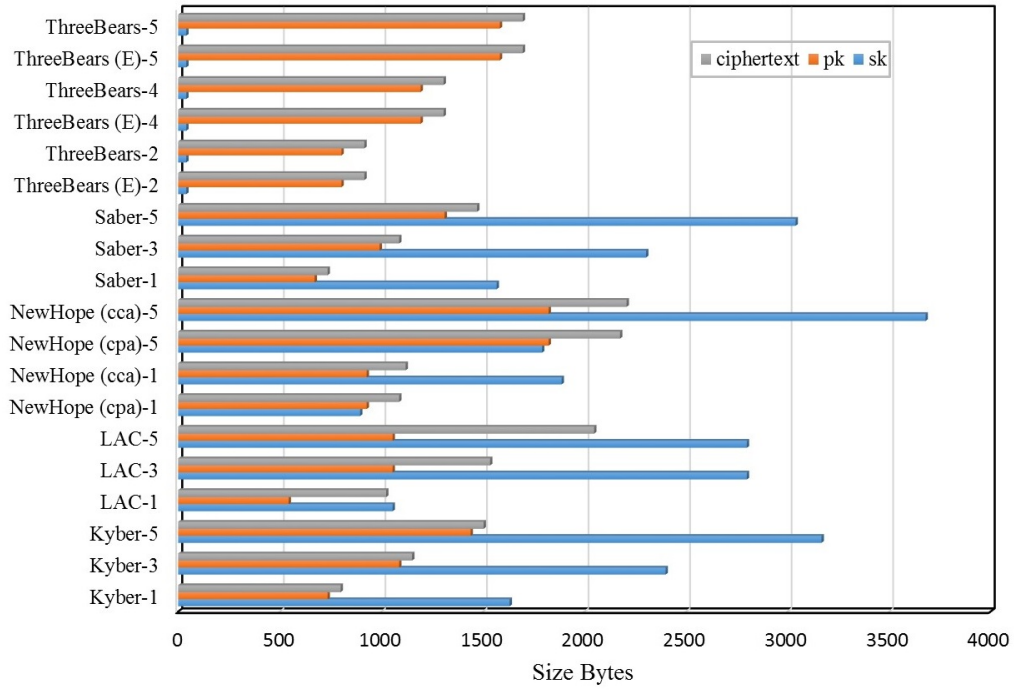

Figure 5. Comparison of IoT communication bandwidth for LBC algorithms implemented via public key encryption (PKE)/KVM schemes with secret key (sk), public key (pk), and signature variants [128].

6. Hardware Implementation of Lightweight Lattice-Based Cryptography

In this section, we have discussed the hardware implementation of LW-LBC on different computational platforms [137]. Many lattice systems originally require large matrices to be stored over integer rings and are very inefficient in both run-time and storage space. The principle of replacing matrices with polynomials in integer rings over ideals enables both to be minimized. Therefore, in very effective structures, the substitution of lattices with perfect lattices occurs [136,137]. It is recommended that, for IoT devices (based on communication technologies, such as IEEE 802.11ah, 802.15.4, low-power Wi-Fi, BLE, LoRawan, Sigfox, NB-IoT, etc.), that inherently have reduced computational resources, limited on-board memory, and small form-factor battery banks (based on hardware platforms,

such as Raspberry Pi, Beaglebones, etc.), instead of storing huge matrices of space $O(n^2)$, where n is larger than 128, it is sufficient to store just $O(n\ log\ n)$ elements. In addition, the Fast Fourier Transform can be used effectively to multiply the elements of ideal lattices (FFT w.r.t time $O(n\ log\ n)$ for serial architecture and $O(log\ n)$ for a parallel architecture rather than complex $O(n^2)$ computation. This way, the hardware resources available can be utilized to implement LW-LBC in a cost-effective way in an IoT network.

The fundamental modules of lattice-based cryptosystem that guides the actual hardware implementation are the multipliers and samplers. The primary performance bottlenecks are polynomial multiplication for perfect lattices, and matrix multiplication for regular lattices, whereas the discrete Gaussian sampling is used to sample noise and cover hidden information. In the literature, there are different algorithms for the sampler and multiplier, providing the researchers with a particular end-user application [138]. For the lightweight arithmetic implementation of LBC, matrix multiplication algorithms are adopted for regular LWE schemes, while number theoretical transform (NTT) is a safer alternative in Ring-LWE for polynomial multiplication [139]. On the other hand the dynamics of large scale implementation of IoT hardware is different. Standard LWE-based systems display a comparatively high memory foot-print when deployed due to the large key scale (hundreds of kilobytes per public key), which makes it impossible to quickly deploy standard LWE-based systems [140]. The adoption of unique ring architectures, such as Ring-LWE, provides a crucial size reduction by a factor of n compared to regular LWE, rendering Ring-LWE an outstanding candidate for resource-restricted IoT devices.

As we can see in more depth in the coming paragraph, high-performance Intel/AMD processors, which are famously equipped with Advanced Vector Extensions (AVX) and ARM/AVR micro-controllers are common software execution platforms [140]. Recently, practical software implementations of standard lattices, encryption schemes and key exchanges have been reported [141]. Other hardware platforms, such as field programmable gate arrays (FPGA) and application-specific integrated circuits (ASICs), have also been used to implement LBC. FPGAs provide flexibility and customization but not agility [142], whereas ASCIs are less power hungry, while offering compactness and design flexibility.

In this section, we summarize the practical hardware implementation of LBC by comparing the memory usage (bytes), computational time (ms) and clock cycle counts on an ARM CORTEX-M AT 168 MHz platform [128]. Table 3 depicts the hardware complexity of implementing LBC based on KEMs [143]. The statistics show that, for a limited memory footprint, Saber stands out both in terms of its resource-constrained existence but also in terms of throughput performance, while it also achieves the level-5 security according to the NIST guidelines. Therefore, it is recommended that Saber can be used as a lightweight LBC algorithm well suited of post-quantum IoT networks.

Table 3. Hardware implementation and complexity of LBC based on Key encapsulation mechanisms (KEMs).

Scheme	Operation	Cycles	Time (ms)	Stack (Bytes)
Saber-5	Key Generation	1147000	7	13883
	Encryption	1444000	9	16667
	Decryption	1543000	9	17763
Kyber-5	Key Generation	1771729	11	15664
	Encryption	2142912	13	19352
	Decryption	2188917	13	20864
NewHopeCCA-5	Key Generation	1243729	7	11152
	Encryption	1963184	12	17448
	Decryption	1978982	12	19648
FrodoKEM-AES-3	Key Generation	101273066	603	35484
	Encryption	106933956	637	63484
	Decryption	107393295	639	63628

Table 4 depicts the hardware complexity of implementing LBC via signature scheme [144,145]. The data analyzed by Reference [128] depicts that signature-based schemes are computationally exhaustive as compared to KEMs schemes. Nevertheless, Dilithium performs well as compared to Falcon and qTesla. We can conclude that, for signature implementation, Dilithium can be used in post-quantum IoT networks where level-5 security is not the prime focus but the acceptable range of security is in between 1 and 3.

A perfect post-quantum cryptosystem, such as pseudorandom generators, pseudorandom functions, and digital signatures, enables to identify the best parameters. As, discussed in this section the performance of diverse PQ algorithms is based on the level of acceptable security levels. The compromise on the security level can lead to side-channel attacks in the IoT networks. The computational cycles, time, and stack (bytes) are the key parameters researchers have to take into account while designing the dense IoT networks. In lattice schemes, the problem of storage (memory) occurs when immense operations of matrices are used in an integer ring. It is, therefore, appropriate to use polynomials for the matrix multiplication of elements using Fast Fourier transformation (FFT). Although the computational time of LW-LBC is much faster than classical LBC algorithms, these algorithms still need extensive research in machine-to-machine (M2M) and industrial IoT environments with dense sensor devices in the operational technology.

Table 4. Hardware implementation and complexity of LBC based on signatures.

Scheme	Operation	Cycles	Time (ms)	Stack (Bytes)
Falcon-1	Key Generation	114516135	682	63652
	Encryption	80503242	479	63653
	Decryption	530900	3	63654
Falcon-5	Key Generation	365950978	2178	120596
	Encryption	165800855	987	120597
	Decryption	1046700	6	120598
Dilithium-3	Key Generation	2320362	14	50488
	Encryption	8348349	50	86568
	Decryption	2342191	14	54800
qTesla-3	Key Generation	30720411	183	43992
	Encryption	11987079	71	58112
	Decryption	2225296	13	45712

7. Conclusions

In this survey, we discussed the practicality of post-quantum cryptography in resource constrained devices, such as Internet-of-Things. We compared the performance of diversified post-quantum key exchange schemes by analyzing the memory usage, computational time and clock cycle counts on hardware platforms. The potential arrival of quantum computation pushes for the realization and implementation of cryptographic algorithms that are quantum-resistant, among which a very promising alternative for IoT networks seems to be lattice-based cryptography (LBC). The versatile processors, i.e., FPGAs, ASICs, and Raspberry Pi, enable low-power edge devices to perform the hardest quantum encryption systems today. For lightweight implementation of LBC, the researchers are adapting advanced hardware designs based on number theoretical transformation (NTT) for post-quantum realization. The updated NTT separates data from vectors and allocates portions through allocated memory with smaller foot-prints ensuring reduced energy consumption, while maintaining the desired throughput and level of security. The scalability and flexibility that can be used to optimize efficiency and security for the implementation of lightweight LBC make lattice cryptography the leading candidate for post-quantum IoT security.

Funding: This research received no external funding.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: The data presented in this study are available on request from the author.

Acknowledgments: The author would like to thank Prof. Alan Woodward from University of Surrey, UK for the valuable discussions and lectures on post-quantum cryptography.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cheng, C.; Lu, R.; Petzoldt, A.; Takagi, T. Securing the Internet of Things in a quantum world. *IEEE Commun. Mag.* **2017**, *55*, 116–120. [CrossRef]
2. Monz, T.; Nigg, D.; Martinez, E.A.; Brandl, M.F.; Schindler, P.; Rines, R.; Wang, S.X.; Chuang, I.L.; Blatt, R. Realization of a scalable Shor algorithm. *Science* **2016**, *351*, 1068–1070. [CrossRef]
3. Nam, Y.; Blümel, R. Performance scaling of Shor's algorithm with a banded quantum Fourier transform. *Phys. Rev. A* **2012**, *86*, 044303. [CrossRef]
4. Nam, Y.; Blümel, R. Streamlining Shor's algorithm for potential hardware savings. *Phys. Rev. A* **2013**, *87*, 060304. [CrossRef]
5. Montanaro, A. Quantum algorithms: An overview. *NPJ Quantum Inf.* **2016**, *2*, 15023. [CrossRef]
6. Hirvensalo, M. *Quantum Computing*; Springer: Berlin/Heidelberg, Germany, 2013.
7. Gibney, E. Physics: Quantum computer quest. *Nat. News* **2014**, *516*, 24. [CrossRef]
8. Jones, N.C.; Van Meter, R.; Fowler, A.G.; McMahon, P.L.; Kim, J.; Ladd, T.D.; Yamamoto, Y. Layered architecture for quantum computing. *Phys. Rev. X* **2012**, *2*, 031007. [CrossRef]
9. Schneier, B. Key-Exchange Algorithms. *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C*; Wiley: Hoboken, NJ, USA, 2015; pp. 513–525.
10. Galbraith, S.D.; Gaudry, P. Recent progress on the elliptic curve discrete logarithm problem. *Des. Codes Cryptogr.* **2016**, *78*, 51–72. [CrossRef]
11. Howe, J.; Pöppelmann, T.; O'neill, M.; O'sullivan, E.; Güneysu, T. Practical lattice-based digital signature schemes. *ACM Trans. Embed. Comput. Syst.* **2015**, *14*, 41. [CrossRef]
12. Asif, R.; Buchanan, W.J. Quantum-to-the-Home: Achieving Gbits/s Secure Key Rates via Commercial Off-the-Shelf Telecommunication Equipment. *Secur. Commun. Netw.* **2017**, *2017*, 7616847. [CrossRef]
13. Maitra, A.; Samuel, J.; Sinha, S. Likelihood Theory in a Quantum World: Tests with Quantum coins and computers. *arXiv* **2019**, arXiv:1901.10704.
14. Bernstein, D.J.; Lange, T. Post-quantum cryptography. *Nature* **2017**, *549*, 188–194. [CrossRef] [PubMed]
15. Nejatollahi, H.; Dutt, N.; Ray, S.; Regazzoni, F.; Banerjee, I.; Cammarota, R. Post-Quantum Lattice-Based Cryptography Implementations: A Survey. *ACM Comput. Surv.* **2019**, *51*, doi:10.1145/3292548. [CrossRef]
16. Fernández-Caramés, T.M. From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 6457–6480. [CrossRef]
17. Malina, L.; Popelova, L.; Dzurenda, P.; Hajny, J.; Martinasek, Z. On Feasibility of Post-Quantum Cryptography on Small Devices. *IFAC-PapersOnLine* **2018**, *51*, 462–467. 15th IFAC Conference on Programmable Devices and Embedded Systems PDeS 2018.
18. Banerjee, U.; Pathak, A.; Chandrakasan, A.P. An Energy-Efficient Configurable Lattice Cryptography Processor for the Quantum-Secure Internet of Things. In Proceedings of the 2019 IEEE International Solid-State Circuits Conference (ISSCC), San Francisco, CA, USA, 17–21 February 2019; pp. 46–48.
19. Fritzmann, T.; Sepúlveda, J. Efficient and Flexible Low-Power NTT for Lattice-Based Cryptography. In Proceedings of the 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA, 5–10 May 2019; pp. 141–150.
20. Gupta, D.S.; Islam, S.H.; Obaidat, M.S.; Karati, A.; Sadoun, B. LAAC: Lightweight Lattice-Based Authentication and Access Control Protocol for E-Health Systems in IoT Environments. *IEEE Syst. J.* **2020**, doi:10.1109/JSYST.2020.3016065. [CrossRef]
21. Kumar, G.; Saha, R.; Rai, M.K.; Buchanan, W.J.; Thomas, R.; Geetha, G.; Hoon-Kim, T.; Rodrigues, J.J.P.C. A Privacy-Preserving Secure Framework for Electric Vehicles in IoT Using Matching Market and Signcryption. *IEEE Trans. Veh. Technol.* **2020**, *69*, 7707–7722. [CrossRef]
22. Cao, J.; Yu, P.; Xiang, X.; Ma, M.; Li, H. Anti-Quantum Fast Authentication and Data Transmission Scheme for Massive Devices in 5G NB-IoT System. *IEEE Internet Things J.* **2019**, *6*, 9794–9805. [CrossRef]
23. Bernstein, D.J.; Hopwood, D.; Hülsing, A.; Lange, T.; Niederhagen, R.; Papachristodoulou, L.; Schneider, M.; Schwabe, P.; Wilcox-O'Hearn, Z. SPHINCS: Practical stateless hash-based signatures. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, 17–21 October 2015; pp. 368–397.
24. Lamport, L. *Constructing Digital Signatures from a One-Way Function*; Technical Report, Technical Report CSL-98; SRI International: Palo Alto, CA, USA, 1979.
25. Hofheinz, D.; Jager, T. Tightly secure signatures and public-key encryption. *Des. Codes Cryptogr.* **2016**, *80*, 29–61. [CrossRef]

26. Merkle, R.C. A certified digital signature. In Proceedings of the Conference on the Theory and Application of Cryptology, Houthalen, Belgium, 10–13 April 1989; pp. 218–238.
27. Pereira, G.C.; Puodzius, C.; Barreto, P.S. Shorter hash-based signatures. *J. Syst. Softw.* **2016**, *116*, 95–100. [CrossRef]
28. McGrew, D.; Kampanakis, P.; Fluhrer, S.; Gazdag, S.L.; Butin, D.; Buchmann, J. State management for hash-based signatures. In Proceedings of the International Conference on Research in Security Standardisation, Gaithersburg, MD, USA, 5–6 December 2016; pp. 244–260.
29. Huelsing, A.; Butin, D.; Gazdag, S.; Rijneveld, J.; Mohaisen, A. *Xmss: Extended Merkle Signature Scheme*; Technical Report; Internet Research Task Force: Wilmington, DE, USA, 2018.
30. Overbeck, R.; Sendrier, N. Code-based cryptography. In *Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 95–145.
31. Bernstein, D.J. Introduction to post-quantum cryptography. In *Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 1–14.
32. Wieschebrink, C. Two NP-complete problems in coding theory with an application in code based cryptography. In Proceedings of the 2006 IEEE International Symposium on Information Theory, Seattle, WA, USA, 9–14 July 2006; pp. 1733–1737.
33. McEliece, R.J. A public-key cryptosystem based on algebraic. *Coding Thv.* **1978**, *4244*, 114–116.
34. Niederreiter, H.; Xing, C. *Algebraic Geometry in Coding Theory and Cryptography*; Princeton University Press: Princeton, NJ, USA, 2009.
35. Yakymenko, I.; Kasianchuk, M.; Ivasiev, S.; Melnyk, A.; Nykolaichuk, Y.M. Realization of Rsa cryptographic algorithm based on vector-module method of modular exponention. In Proceedings of the 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 20–24 February 2018; pp. 550–554.
36. Wang, Z.; Karpovsky, M. Algebraic manipulation detection codes and their applications for design of secure cryptographic devices. In Proceedings of the 2011 IEEE 17th International On-Line Testing Symposium, Athens, Greece, 13–15 July 2011; pp. 234–239.
37. Finiasz, M.; Sendrier, N. Security bounds for the design of code-based cryptosystems. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, 6–10 December 2009; pp. 88–105.
38. Ding, J.; Yang, B.Y. Multivariate public key cryptography. In *Post-Quantum Cryptography*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 193–241.
39. Ding, J.; Petzoldt, A. Current state of multivariate cryptography. *IEEE Secur. Priv.* **2017**, *15*, 28–36. [CrossRef]
40. Patarin, J. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Saragossa, Spain, 12–16 May 1996; pp. 33–48.
41. Patarin, J. Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'98. *Des. Codes Cryptogr.* **2000**, *20*, 175–209. [CrossRef]
42. Goubin, L.; Patarin, J.; Yang, B.Y. Multivariate cryptography. In *Encyclopedia of Cryptography and Security*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2011; pp. 824–828.
43. Ajtai, M. Generating hard instances of lattice problems. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; pp. 99–108.
44. Ajtai, M. Representing hard lattices with O (n log n) bits. In Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, 22–24 May 2005; pp. 94–103.
45. Peikert, C. A decade of lattice cryptography. *Found. Trends Theor. Comput. Sci.* **2016**, *10*, 283–424. [CrossRef]
46. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332. [CrossRef]
47. Clark, J.; Van Oorschot, P.C. SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 19–22 May 2013; pp. 511–525.
48. Bellare, M.; Rogaway, P. Optimal asymmetric encryption. In *Workshop on the Theory and Application of of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1994; pp. 92–111.
49. Jonsson, J.; Kaliski, B.S. On the Security of RSA Encryption in TLS. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2002; pp. 127–142.
50. Krawczyk, H. HMQV: A high-performance secure Diffie-Hellman protocol. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2005; pp. 546–566.
51. Boneh, D. The decision diffie-hellman problem. In *International Algorithmic Number Theory Symposium*; Springer: Berlin/Heidelberg, Germany, 1998; pp. 48–63.
52. Koblitz, N. Elliptic curve cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
53. Hankerson, D.; Menezes, A. *Elliptic Curve Cryptography*; Springer: Berlin/Heidelberg, Germany, 2011.
54. Liu, Z.; Seo, H.; Großschädl, J.; Kim, H. Efficient implementation of NIST-compliant elliptic curve cryptography for 8-bit AVR-based sensor nodes. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1385–1397. [CrossRef]
55. Biryukov, A.; Perrin, L. Symmetrically and Asymmetrically Hard Cryptography. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Hong Kong, China, 3–7 December 2017; pp. 417–445.

56. Preskill, J. Quantum Computing in the NISQ era and beyond. *Quantum* **2018**, *2*, 79. [CrossRef]
57. Ghosh, D.; Agarwal, P.; Pandey, P.; Behera, B.K.; Panigrahi, P.K. Automated error correction in IBM quantum computer and explicit generalization. *Quantum Inf. Process.* **2018**, *17*, 153. [CrossRef]
58. Bocharov, A.; Roetteler, M.; Svore, K.M. Factoring with qutrits: Shor's algorithm on ternary and metaplectic quantum architectures. *Phys. Rev. A* **2017**, *96*, 012306. [CrossRef]
59. Martín-López, E.; Laing, A.; Lawson, T.; Alvarez, R.; Zhou, X.Q.; O'brien, J.L. Experimental realization of Shor's quantum factoring algorithm using qubit recycling. *Nat. Photonics* **2012**, *6*, 773. [CrossRef]
60. Kwiat, P.; Mitchell, J.; Schwindt, P.; White, A. Grover's search algorithm: An optical approach. *J. Mod. Opt.* **2000**, *47*, 257–266. [CrossRef]
61. Bernstein, D.J.; Lange, T. Post-quantum cryptography—Dealing with the fallout of physics success. In *Cryptology ePrint Archive*; Report 2017/314; IACR(The International Association for Cryptologic Research): Lyon, France, 2017.
62. Daemen, J.; Rijmen, V. *The Design of Rijndael: AES—The Advanced Encryption Standard*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2013.
63. Robshaw, M.; Billet, O. *New Stream Cipher Designs: The eSTREAM Finalists*; Springer: Berlin/Heidelberg, Germany, 2008; Volume 4986.
64. Bellare, M.; Kohno, T.; Namprempre, C. Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm. *ACM Trans. Inf. Syst. Secur.* **2004**, *7*, 206–241. [CrossRef]
65. Bernstein, D.J. The Poly1305-AES message-authentication code. In *International Workshop on Fast Software Encryption*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 32–49.
66. Appel, A.W. Verification of a cryptographic primitive: SHA-256. *ACM Trans. Program. Lang. Syst.* **2015**, *37*, 7. [CrossRef]
67. Gilbert, H.; Handschuh, H. Security analysis of SHA-256 and sisters. In *International Workshop on Selected Areas in Cryptography*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 175–193.
68. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
69. Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
70. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* **1985**, *31*, 469–472. [CrossRef]
71. Durlanik, A.; Sogukpinar, I. SIP authentication scheme using ECDH. *World Enformatika Soc. Trans. Eng. Comput. Technol.* **2005**, *8*, 350–353.
72. Gueron, S.; Krasnov, V. Fast prime field elliptic-curve cryptography with 256-bit primes. *J. Cryptogr. Eng.* **2015**, *5*, 141–151. [CrossRef]
73. Olive, D.I.; Turok, N. Algebraic structure of Toda systems. *Nucl. Phys. B* **1983**, *220*, 491–507. [CrossRef]
74. Bayer-Fluckiger, E.; Oggier, F.; Viterbo, E. New algebraic constructions of rotated Z/sup n/-lattice constellations for the Rayleigh fading channel. *IEEE Trans. Inf. Theory* **2004**, *50*, 702–714. [CrossRef]
75. Peikert, C. Public-key cryptosystems from the worst-case shortest vector problem. In Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, Bethesda, Maryland, 31 May–2 June 2009; pp. 333–342.
76. Ajtai, M.; Kumar, R.; Sivakumar, D. A sieve algorithm for the shortest lattice vector problem. In Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing, Crete, Greece, 6–8 July 2001; pp. 601–610.
77. Hoffstein, J.; Howgrave-Graham, N.; Pipher, J.; Whyte, W. Practical lattice-based cryptography: NTRUEncrypt and NTRUSign. In *The LLL Algorithm*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 349–390.
78. Rose, M. Lattice-Based Cryptography: A Practical Implementation. Master's Thesis, School of Computer Science and Software Engineering Faculty of Informatics, University of Wollongong, Wollongong, Australia, 2011.
79. Du, J.; Leung, J.Y.T. Minimizing total tardiness on one machine is NP-hard. *Math. Oper. Res.* **1990**, *15*, 483–495. [CrossRef]
80. Dagum, P.; Luby, M. Approximating probabilistic inference in Bayesian belief networks is NP-hard. *Artif. Intell.* **1993**, *60*, 141–153. [CrossRef]
81. Zheng, T. Incrementally and inductively constructing basis of multiplicative dependence lattice of non-zero algebraic numbers. *arXiv* **2018**, arXiv:1808.02712.
82. Micciancio, D. Lattice-based cryptography. In *Encyclopedia of Cryptography and Security*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 713–715.
83. Khot, S. Hardness of approximating the shortest vector problem in lattices. *J. ACM* **2005**, *52*, 789–808. [CrossRef]
84. Goldreich, O.; Micciancio, D.; Safra, S.; Seifert, J.P. Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. *Inf. Process. Lett.* **1999**, *71*, 55–61. [CrossRef]
85. Lyubashevsky, V.; Micciancio, D. On bounded distance decoding, unique shortest vectors, and the minimum distance problem. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2009; pp. 577–594.
86. Attoh-Okine, N.O.; Cooger, K.; Mensah, S. Multivariate adaptive regression (MARS) and hinged hyperplanes (HHP) for doweled pavement performance modeling. *Constr. Build. Mater.* **2009**, *23*, 3020–3023. [CrossRef]
87. Guo, Q.; Johansson, T.; Stankovski, P. A key recovery attack on MDPC with CCA security using decoding errors. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, 4–8 December 2016; pp. 789–815.

88. Hartmann, M.; Rosenthal, J. *The Ajtai-Dwork Cryptosystem and Other Cryptosystems Based on Lattices*; Universite de Zurich: Zurich, Switzerland, 2015.
89. Brakerski, Z.; Vaikuntanathan, V. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2011; pp. 505–524.
90. Hoffstein, J.; Pipher, J.; Silverman, J.H. NTRU: A ring-based public key cryptosystem. In *International Algorithmic Number Theory Symposium*; Springer: Berlin/Heidelberg, Germany, 1998; pp. 267–288.
91. Nguyen, P.; Stern, J. Cryptanalysis of the Ajtai-Dwork cryptosystem. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 23–27 August 1998; pp. 223–242.
92. Woeginger, G.J. Exact algorithms for NP-hard problems: A survey. In *Combinatorial Optimization—Eureka, You Shrink!* Springer: Berlin/Heidelberg, Germany, 2003; pp. 185–207.
93. Goldreich, O.; Goldwasser, S.; Halevi, S. Eliminating decryption errors in the Ajtai-Dwork cryptosystem. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 1997; pp. 105–111.
94. Wunderer, T. On the Security of Lattice-Based Cryptography Against Lattice Reduction and Hybrid Attacks. Ph.D. Thesis, Technische Universität, Berlin, Germany, 2018.
95. Nguyen, P.; Stern, J. The hardness of the hidden subset sum problem and its cryptographic implications. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 1999; pp. 31–46.
96. Hafner, J.L. New omega theorems for two classical lattice point problems. *Invent. Math.* **1981**, *63*, 181–186. [CrossRef]
97. Brakerski, Z.; Gentry, C.; Halevi, S. Packed ciphertexts in LWE-based homomorphic encryption. In *International Workshop on Public Key Cryptography*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 1–13.
98. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM* **2009**, *56*, 34. [CrossRef]
99. Pöppelmann, T.; Güneysu, T. Towards efficient arithmetic for lattice-based cryptography on reconfigurable hardware. In Proceedings of the International Conference on Cryptology and Information Security in Latin America, Santiago, Chile, 7–10 October 2012; pp. 139–158.
100. Gama, N.; Nguyen, P.Q. Finding short lattice vectors within mordell's inequality. In Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing, Victoria, BC, Canada, 17–18 May 2008; pp. 207–216.
101. Schnorr, C.P.; Euchner, M. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Math. Program.* **1994**, *66*, 181–199. [CrossRef]
102. Alkim, E.; Ducas, L.; Pöppelmann, T.; Schwabe, P. Post-quantum key exchange—A new hope. In Proceedings of the 25th {USENIX} Security Symposium ({USENIX} Security 16), Austin, TX, USA, 10–12 August 2016; pp. 327–343.
103. Albrecht, M.R. On dual lattice attacks against small-secret LWE and parameter choices in HElib and SEAL. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, 30 April–4 May 2017; pp. 103–129.
104. Becker, A.; Ducas, L.; Gama, N.; Laarhoven, T. New directions in nearest neighbor searching with applications to lattice sieving. In Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, Arlington, VA, USA, 10–12 January 2016; pp. 10–24.
105. Micciancio, D.; Walter, M. Fast lattice point enumeration with minimal overhead. In Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, Portland, OR, USA, 5–7 January 2014; pp. 276–294.
106. Grover, L.K. A fast quantum mechanical algorithm for database search. *arXiv* **1996**, arXiv:quant-ph/9605043.
107. Laarhoven, T.; Mosca, M.; Van De Pol, J. Finding shortest lattice vectors faster using quantum search. *Des. Codes Cryptogr.* **2015**, *77*, 375–400. [CrossRef]
108. Cai, J.Y.; Nerurkar, A. Approximating the SVP to within a factor (1-1/dim/sup/spl epsiv//) is NP-hard under randomized conditions. In Proceedings of the Thirteenth Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference) (Cat. No. 98CB36247), Buffalo, NY, USA, 15–18 June 1998; pp. 46–55.
109. Dinur, I. Approximating SVP to within almost-polynomial factors is NP-hard. *Theor. Comput. Sci.* **2002**, *285*, 55–71. [CrossRef]
110. Aharonov, D.; Regev, O. Lattice problems in NP coNP. *J. ACM* **2005**, *52*, 749–765. [CrossRef]
111. Banaszczyk, W. New bounds in some transference theorems in the geometry of numbers. *Math. Ann.* **1993**, *296*, 625–635. [CrossRef]
112. Goldreich, O.; Goldwasser, S. On the limits of nonapproximability of lattice problems. *J. Comput. Syst. Sci.* **2000**, *60*, 540–563. [CrossRef]
113. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.
114. Johnson, D.S. The NP-completeness column. *ACM Trans. Algorithms* **2005**, *1*, 160–176. [CrossRef]
115. Fortnow, L. The status of the P versus NP problem. *Commun. ACM* **2009**, *52*, 78–86. [CrossRef]
116. Baker, T.; Gill, J.; Solovay, R. Relativizations of the P=?NP question. *SIAM J. Comput.* **1975**, *4*, 431–442. [CrossRef]
117. Kannan, R. Improved algorithms for integer programming and related lattice problems. In Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing, Boston, MA, USA, 25–27 April 1983; pp. 193–206.
118. Lenstra, A.K.; Lenstra, H.W.; Lovász, L. Factoring polynomials with rational coefficients. *Math. Ann.* **1982**, *261*, 515–534. [CrossRef]

119. Hastad, J.; Just, B.; Lagarias, J.C.; Schnorr, C.P. Polynomial time algorithms for finding integer relations among real numbers. *SIAM J. Comput.* **1989**, *18*, 859–881. [CrossRef]
120. Schnorr, C.P. Factoring Integers and Computing Discrete Logarithms via Diophantine Approximation. In *Advances in Computational Complexity Theory*; Springer: LNCS Eurocrypt, Aarhus, Denmark, 1990; pp. 171–182.
121. Davis, M. The decision problem for exponential diophantine equations. *Collect. Work. Julia Robinson* **1996**, *6*, 77. [CrossRef]
122. Dinur, I.; Kindler, G.; Safra, S. Approximating-CVP to within almost-polynomial factors is NP-hard. In Proceedings of the 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280), Palo Alto, CA, USA, 8–11 November 1998; pp. 99–109.
123. Dinur, I. Approximating SVP to within almost-polynomial factors is NP-Hard. In Proceedings of the Italian Conference on Algorithms and Complexity, Rome, Italy, 1–3 March 2000; pp. 263–276.
124. Hu, G.; Pan, Y. Improvements on Reductions among Different Variants of SVP and CVP. In *International Workshop on Information Security Applications*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 39–51.
125. Lagarias, J.C.; Lenstra, H.W.; Schnorr, C.P. Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatorica* **1990**, *10*, 333–348. [CrossRef]
126. Nguyen, P. Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from crypto'97. In Proceedings of the Annual International Cryptology Conference, Barbara, CA, USA, 15–19 August 1999; pp. 288–304.
127. Suomalainen, J.; Kotelba, A.; Kreku, J.; Lehtonen, S. Evaluating the Efficiency of Physical and Cryptographic Security Solutions for Quantum Immune IoT. *Cryptography* **2018**, *2*, 5. [CrossRef]
128. Khalid, A.; McCarthy, S.; O'Neill, M.; Liu, W. Lattice-based Cryptography for IoT in A Quantum World: Are We Ready? In Proceedings of the 2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI), Otranto, Italy, 13–14 June 2019; pp. 194–199.
129. Wang, W.; Han, J.; Xie, Z.; Huang, S.; Zeng, X. Cryptographie coprocessor design for IoT sensor nodes. In Proceedings of the 2016 International SoC Design Conference (ISOCC), Jeju, Korea, 23–26 October 2016; pp. 37–38.
130. Zhao, C.; Yan, Y.; Li, W. An efficient ASIC Implementation of QARMA Lightweight Algorithm. In Proceedings of the 2019 IEEE 13th International Conference on ASIC (ASICON), Chongqing, China, 29 October–1 November 2019; pp. 1–4.
131. Asif, R.; Ghanem, K.; Irvine, J. Proof-of-PUF Enabled Blockchain: Concurrent Data and Device Security for Internet-of-Energy. *Sensors* **2021**, *21*, 28. [CrossRef]
132. Abdulkader, O.; Bamhdi, A.M.; Thayananthan, V.; Elbouraey, F.; Al-Ghamdi, B. A Lightweight Blockchain Based Cybersecurity for IoT environments. In Proceedings of the 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Paris, France, 21–23 June 2019; pp. 139–144.
133. Güneysu, T.; Oder, T. Towards lightweight Identity-Based Encryption for the post-quantum-secure Internet of Things. In Proceedings of the 2017 18th International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, USA, 14–15 March 2017; pp. 319–324.
134. Pöppelmann, T.; Naehrig, M.; Putnam, A.; Macias, A. Accelerating Homomorphic Evaluation on Reconfigurable Hardware. In *Cryptographic Hardware and Embedded Systems—CHES 2015*; Güneysu, T., Handschuh, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2015; pp. 143–163.
135. Imran, M.; Abideen, Z.U.; Pagliarini, S. An Experimental Study of Building Blocks of Lattice-Based NIST Post-Quantum Cryptographic Algorithms. *Electronics* **2020**, *9*, 1953. [CrossRef]
136. Ping, Y.; Wang, B.; Tian, S.; Zhou, J.; Ma, H. PKCHD: Towards A Probabilistic Knapsack Public-Key Cryptosystem with High Density. *Information* **2019**, *10*, 75. [CrossRef]
137. Yuan, Y.; Xiao, J.; Fukushima, K.; Kiyomoto, S.; Takagi, T. Portable Implementation of Postquantum Encryption Schemes and Key Exchange Protocols on JavaScript-Enabled Platforms. *Secur. Commun. Netw.* **2018**, *2018*, 9846168. [CrossRef]
138. Nejatollahi, H.; Dutt, N.; Cammarota, R. Special session: Trends, challenges and needs for lattice-based cryptography implementations. In Proceedings of the 2017 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), Seoul, Korea, 15–20 October 2017; pp. 1–3.
139. Ebrahimi, S.; Bayat-Sarmadi, S. Lightweight and Fault-Resilient Implementations of Binary Ring-LWE for IoT Devices. *IEEE Internet Things J.* **2020**, *7*, 6970–6978. [CrossRef]
140. Howe, J.; Moore, C.; O'Neill, M.; Regazzoni, F.; Güneysu, T.; Beeden, K. Lattice-Based Encryption Over Standard Lattices in Hardware. In Proceedings of the 53rd Annual Design Automation Conference (DAC '16), Austin, TX, USA, 5–9 June 2016; Association for Computing Machinery: New York, NY, USA, 2016.
141. Bos, J.; Costello, C.; Ducas, L.; Mironov, I.; Naehrig, M.; Nikolaenko, V.; Raghunathan, A.; Stebila, D. Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16), Vienna, Austria, 24–28 October 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 1006–1018.
142. Oder, T.; Güneysu, T.; Valencia, F.; Khalid, A.; O'Neill, M.; Regazzoni, F. Lattice-based cryptography: From reconfigurable hardware to ASIC. In Proceedings of the 2016 International Symposium on Integrated Circuits (ISIC), Singapore, 12–14 December 2016; pp. 1–4.

143. Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schanck, J.M.; Schwabe, P.; Seiler, G.; Stehle, D. CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS P), London, UK, 24–26 April 2018; pp. 353–367.
144. Nejatollahi, H.; Shahhosseini, S.; Cammarota, R.; Dutt, N. Exploring Energy Efficient Quantum-resistant Signal Processing Using Array Processors. In Proceedings of the ICASSP 2020—2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 4–8 May 2020; pp. 1539–1543.
145. Chaudhary, R.; Aujla, G.S.; Kumar, N.; Zeadally, S. Lattice-Based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions. *IEEE Internet Things J.* **2019**, *6*, 4897–4909. [CrossRef]