IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Overview of Lattice-Based Cryptography for Communication Networks

Chandrashekhar Diwakar[1], **Nasheem Khan**[2]*

[1]Assistant Professor, Department of Mathematics, Govt. Degree College, Mant, Mathura (U. P.) - 281202

[2]Assistant Professor, Department of Mathematics, Babu Shivnath Agrawal College, Mathura (U. P.) - 281004

[1, 2)]Dr. Bhimrao Ambedkar University, Agra (U. P.) - 282004, India

Abstract. Due to recent advancements in technology, our computer systems, the data stored on computer systems, and our daily communications through mobile devices and other electronic devices are not entirely safe. The emergence of quantum computers has attracted the attention of researchers and computer scientists. Because, the security of our data and daily communications depends on cryptographic primitives based on discrete logarithmic problems and integer factorization problems, which are not safe in the current quantum computing era. So, there is a need for cryptographic systems that are safe in a quantum computing environment. Researchers have found that cryptographic algorithms based on lattices are secure against quantum computing attacks. Lattice-Based Cryptography (LBC) is considered an alternative to classical cryptosystems based on discrete logarithmic problems and integer factorization problems in a quantum computing environment. This paper aims to provide an overview of LBC, its significance, and its fields of interest.

Index Terms: Lattice-based cryptography, NTRU, RLWE, Security, Privacy.

I. INTRODUCTION

In the past few years, the advancements in technology have increased rapidly. Our computers and communication systems have been advanced with the latest technologies. In our daily life, we store most of our data on computers and mobiles. We use electronic devices for different types of communication including talking, gaming, streaming, chatting, and money transfer, etc. There are various cryptographic systems that are used to secure our computer systems and communication systems. The security of these cryptosystems is based on discrete logarithmic problems and integer factorization problems. Some of them are ECC, RSA, Diffie-Hellman, etc. The standard public-key cryptographic protocols like RSA, Diffie-Hellman, ECC, etc., yield mathematical problems that are difficult to solve, or one can say that their solution is likely to be impossible. But in recent times, these cryptosystems are not secure because of the emergence of quantum computers. These cryptosystems can be broken on a quantum computer by Shor's [1] algorithm, given by Peter Shor in 1994. In the absence of quantum computers, these algorithms are only a theoretical concern but they have a long-standing reputation. However, in recent years, the growth in the field of quantum computers stipulates the requirement of quantum-resistant cryptographic primitives that could be a feasible replacement for standard public-key cryptographic primitives. Lattice-based public-key cryptographic algorithms are possible replacements.

There are two faces of lattices [2] in cryptography:

(i) Lattices have been used mostly as an algorithmic tool to break cryptographic systems.
(ii) Lattices can be used to form cryptographic algorithms that could be hard to break even on quantum computers.

In the early 80s, since the development of Lenstra, Lenstra, and Lovasz's [3] basis reduction algorithm, lattices have been used to attack a wide range of public-key cryptosystems. In the late 90s, the computational complexity of lattice problems attracted renewed attention, stimulated by Ajtai's surprising discovery [4] of a connection between the worst-case and average-case complexity of certain lattice approximation problems. He suggested a totally different way of using lattices in cryptography by showing how to use computational lattice problems to build cryptographic primitives that are impossible to break. Namely, design cryptographic functions that are as difficult to crack as it is to solve a computationally hard lattice problem. Cryptography requires problems that are hard to solve on average, so when a cryptographic key is chosen at random, the corresponding function is hard to break with high probability. Post-quantum cryptography pertains to cryptographic primitives that are considered to be safe against quantum computing attacks. So LBC is also known as a part of post-quantum cryptography.

1.1 MOTIVATION

The classical public-key cryptosystems are not safe in quantum computing environments. Lattice-based cryptosystems are based on the hardness of some lattice problems, and these cryptosystems are hard to break even on quantum computers. Also, the less running time and lower computational cost of lattice-based cryptosystems compared to standard public-key cryptosystems are important to attract researchers and computer scientists.

1.2 ROADMAP OF THIS PAPER

In the next section, we discuss related work. Section III covers primary information on lattices, some special types of lattices, and some important problems related to lattices. Section IV covers a concise discussion of some generally used lattice-based cryptosystems. Section V covers the significance of LBC. Section VI covers fields of interest. In the last section, we have given an obligatory conclusion.

II. RELATED WORK

M. Ajtai [4] generated hard instances of lattice problems. D. Cash et al. [5] told about bonsai trees or how to delegate a lattice basis. N. Gama et al. [6] gave the lattice enumeration technique using extreme pruning. C. Gentry [7] proposed a fully homomorphic encryption scheme using ideal lattices. C. Gentry et al. [8] gave Trapdoors for hard lattices and some new cryptographic constructions. O. Goldreich et al. [9] gave a Collision-free hashing technique using lattice Problems. O. Goldreich et al. [10] made some public key cryptosystems from lattice reduction problems. O. Goldreich et al. [11] explained that approximating shortest lattice vectors is not harder than approximating closest lattice vectors. J. Hoffstein et al. [12] gave a ring-based public key cryptosystem (NTRU). V. Lyubashevsky et al. [13] explained asymptotically efficient lattice-based digital signatures. V. Lyubashevsky et al. [14] told about ideal lattices and the ring learning with errors problem. A. May et al. [15] gave some methods of dimension reduction for convolution modular lattices. D. Micciancio et al. [16] gave information about Generalized Compact Knapsacks, Cyclic Lattices, Computational Complexity of lattices, and Efficient One-Way Functions. D. Micciancio et al. [17] gave a survey on Lattice-based cryptography. P. Nguyen and J. Stern [2] explained how lattices work with two faces in cryptology. C. Peikert et al. [18] gave a framework for efficient and composable oblivious transfer. O. Regev [19] explained how lattices with learning with error to generate random linear codes in cryptography. P. W. Schor [20] gave Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. D. Stehle et al. [21] gave an Efficient public key encryption technique using ideal lattices.

III. PRIMARY INFORMATION OF LATTICES

3.1 Lattices and their mathematical background

A lattice is a set of objects (or points) structured consistently in a space. Arrangement of atoms in a crystal is an example of a lattice (Fig. 1). The points are connected through straight lines to form a geometric pattern or structure. In LBC, this geometric pattern scrambles and unscrambles messages. Because of the structure of a lattice, it is difficult to break lattice-based cryptosystems (as some patterns extend infinitely).

Mathematically, a set L defined by $L = \{\sum_{i=1}^{n} a_i X_i : a_i \; is \; an \; integer \; for \; all \; i\}$ is said to be a lattice. The set $B = \{X_1, X_2, \dots \dots \dots, X_n\}$ of n linearly independent vectors is said to be a basis of the lattice L. A lattice can have multiple bases, some of which are nearly orthogonal, and these bases are known as good bases (Fig. 2). The fact that a lattice can have multiple bases is the heart of various applications of lattices in cryptography. Another example of a lattice is the set of all n-vectors whose components are integers. Let σ be the minimum distance of a lattice L. Then σ is defined as $\sigma = \{\|X - Y\| : X, Y \in L \; and \; X \neq Y\} = min\{\|X\| : X \in L \; and \; X \neq 0\}$, where the function $\|.\|$ is defined as $\|a\| = \sqrt{X_1^2 + X_2^2 + \cdots + X_n^2}$, $a = (X_1, X_2, \dots, X_n) \in R^n$.

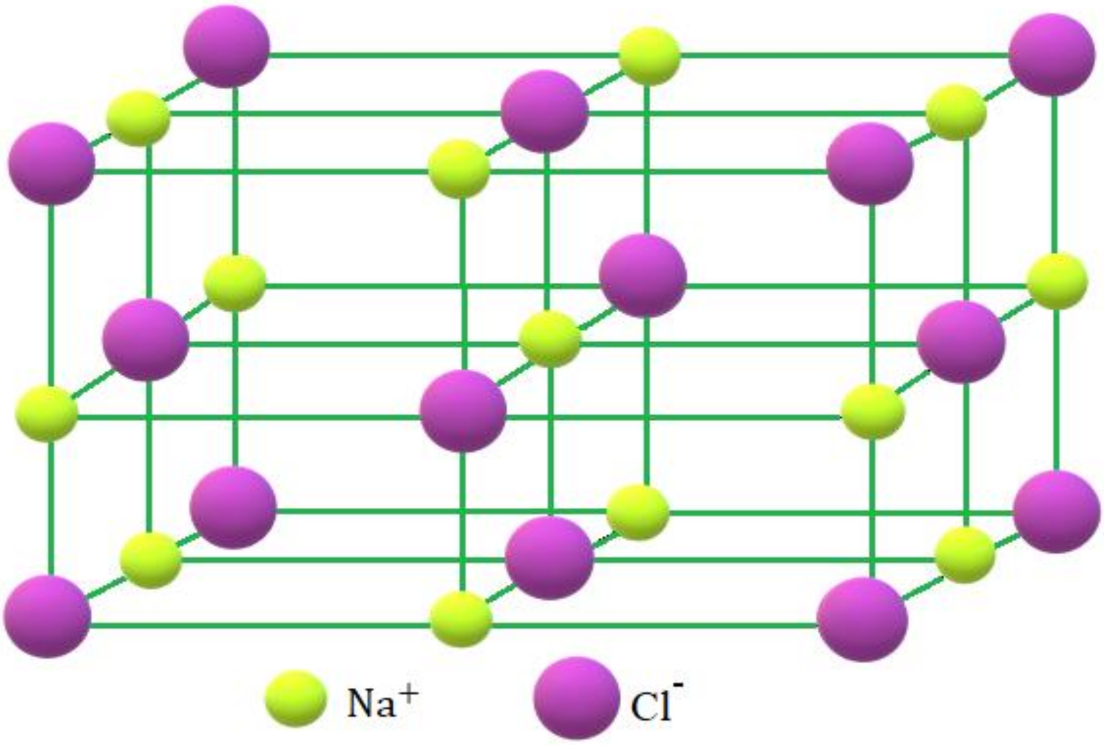

figure 1. Crystal of Sodium Chloride

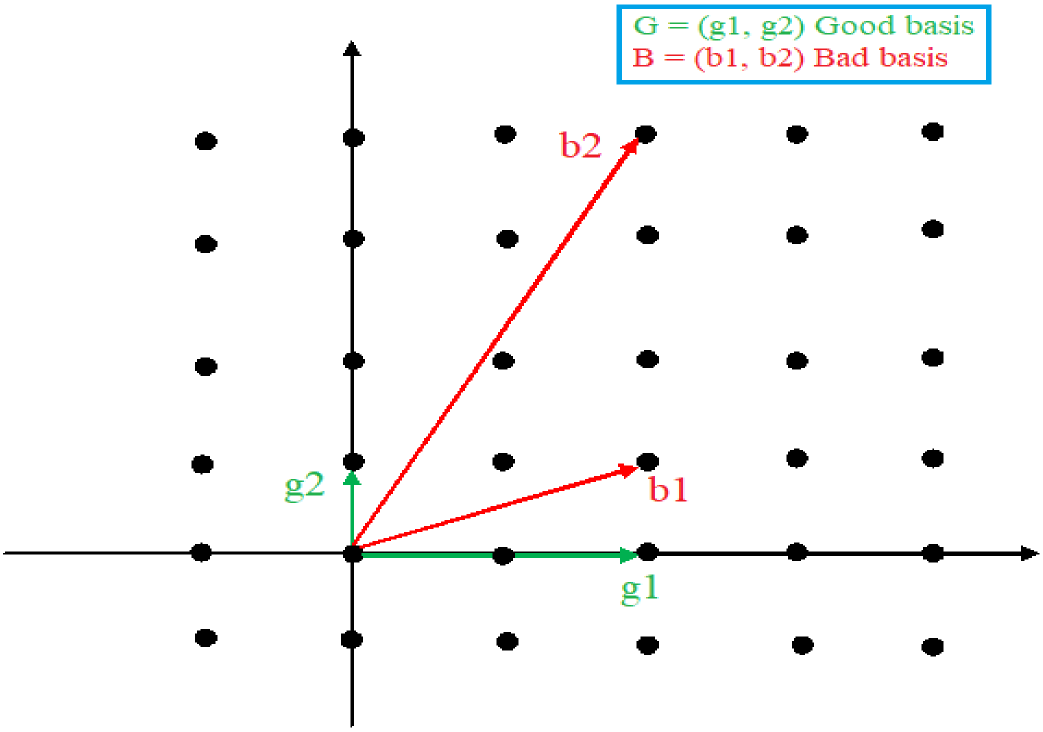

figure 2. Representation of good basis and bad basis

Definition 3.1 The rotation or cyclic rotation of a vector $a = (X_1, X_2, \ldots, X_n) \in R^n$ is defined by $rot(a) = (X_n, X_1, \ldots, X_{n-1}) \in R^n$. The lattice L is called a cyclic lattice if $a \in L \Rightarrow rot(a) \in L(B)$.

Definition 3.2 Let g be an irreducible polynomial of degree n with unity as the coefficient of the highest degree term. Consider a lattice $L(B) \subseteq Z^n$ such that $L(B) = \{h\, mod(g) : h \in I \; and \; I \subseteq \frac{Z(x)}{g} \; is \; an \; ideal\}$. The lattice L is called an ideal lattice, which means that $(c_0, c_1, \ldots, c_{n-1}) \in L$ if and only if $c_0 + c_1 X + \cdots + c_{n-1} X^{n-1} \in I$.

Definition 3.3 A lattice defined by $L_s = \{c * s \equiv d \; mod \; m\}$ is known as a $2N$-dimensional convolution modular lattice associated with the vector s and modulus m.

3.2 Some important lattice problems used to construct lattice-based cryptographic primitives:

(i) **Shortest vector problem (SVP):** For all non-zero vectors Y in a lattice L, one has to find a non-zero vector X in L such that $||X|| \leq ||Y||$.

(ii) **Closest vector problem (CVP):** For any given vector $0 \neq X \notin L$ and all $Z \in L$, one has to find a vector $Y \in L$ such that $||Y - X|| \leq ||Z - X||$.

(iii) **Shortest independent vector problem ($SIVP$):** Consider a lattice L with the basis $B = \{Y_1, Y_2, \ldots, Y_n\}$. Then in SIVP one has to find n linearly independent vectors $X_1, X_2, \ldots, X_n$ in L such that $max||X_i|| \leq max_B||Y_i||$.

(iv) **Approximate Shortest Vector Problem (SVP_α):** Let X be the shortest non-zero vector in a lattice L. Then, in approximate shortest vector problem, one has to find a non-zero vector Y such that $||Y|| \leq \alpha||X||$.

(v) **Approximate Closest Vector Problem (CVP_α):** Let Y be the closest vector to a given vector X of a lattice L. Then in approximate closest vector problem, one has to find a vector Y^* in L such that $||Y^* - X|| \leq \alpha||Y - X||$.

(vi) **Bounded Distance Decoding (BDD) Problem:** In a lattice L the aim of the BDD problem is to find the closest lattice point to a given target vector while the target vector lies within a finite distance of the lattice. This distance is usually defined relative to the minimum distance of the lattice.

(vii) **Shortest Integer Solution (SIS) Problem:** Consider a matrix A with entries from Z_p, the integer modulo p, and a bound δ. The SIS problem aims to find a non-zero vector X such that $AX = 0 \; (mod \; p)$ and $||X|| \leq \delta$.

(viii) **Learning with Errors (LWE) Problem:** Consider $m \geq 1, q \geq 2$, and φ be an “error” probability distribution on Z_q. Let $u \in Z_q$ be a vector with m coefficients. Choose $a \in Z_q$ identically at random and choose $e \in Z_q$ according to φ. Consider the output $\{a, \{a, u\} + e\}$ where additions are as defined in Z_q. Then, we get the probability distribution $B_{u,\varphi}$ on $Z_q^m \times Z_q$. It is said that an algorithm can solve the LWE problem with modulus q and error distribution φ if for any $u \in Z_q^m$ given enough samples from $B_{u,\varphi}$ it outputs u with strong probability.

(ix) **Ring Learning with Errors ($RLWE$) Problem:** Let $K = Q$ be a number field and $R = Z$ be the ring of integers. Let $q \geq 2$ be an integer modulus and $J_q = J/qJ = Z/qZ$ (taking $J = Z$) be a fractional ideal in K. Let $U = K_R/R^V$, where R^V is the dual of R. Consider the secret $s \in (R^V)_q$ and an error distribution φ over K_R. Then a number $r \in R_q$ can be mapped onto the same number in K_R by using the simple embedding f of R_q. A sample of $B_{s,f}$ on $K_R \times U$ is created by taking a from R_q uniformly at random, taking e from φ, which are between 0 and $q-1$, and calculate $(a, c = (a \times s)/q + e \, mod \, R^V)$. Then we say that the Ring-LWE can be solved by an algorithm if given enough samples from $B_{s,f}$ it can retrieve s with strong probability.

The hardness of the above problems is based on the dimension n of the lattice L. As the dimension n of the lattice L increases to a large number, the above problems tend to become difficult. The results after solving the above problems have surprisingly many applications in various fields. The CVP is known to be NP-hard, and the SVP is NP-hard if we use the l^∞ norm. The researchers found that the reduced CVP to an SVP is relatively more difficult than an SVP, as it is used in [11]. Ajtai suggested an entirely different way of using lattices in cryptography. He has shown how to use computational problems like SVP, CVP, SIVP, etc., to build cryptographic primitives that are likely to be impossible to break. That is, design functions in cryptography such that they are as difficult to break as it is to find the solution of a mathematically difficult lattice problem. In cryptography, there is a requirement of problems that are difficult to solve on average. So, when an attacker chooses a key randomly, the corresponding cryptographic function is difficult to break.

LBC is the generic term to construct cryptographic algorithms that include lattices, either in the creation itself or the security proof. In recent time, lattice-based cryptosystems are the prime candidates for post-quantum cryptography. The classical public-key cryptosystems, such as the Diffie-Hellman, RSA, and ECC, could likely be defeated using Shor's algorithm [20] on quantum computers [22]. Lattice-based cryptosystems can resist attacks by standard and quantum computers.

IV. SOME LATTICE-BASED CRYPTOSYSTEMS

Various cryptosystems based on lattices are introduced. Some of them are described below:

Ajtai-Dwork: Ajtai and Dwork proposed the cryptosystem. They asserted that the system is surely safe unless a worst-case lattice problem could be solved in polynomial time. This cryptosystem is not easy to practice because of the large key size. It has been shown that an efficient implementation of the system is not secure [2].

GGH: This is an asymmetric lattice-based cryptosystem proposed by Goldreich, Goldwasser, and Halevi in 1997 [10]. There is also a GGH signature scheme. This cryptosystem works under the assumption that the CVP problem can be hard. This system uses a one-way trapdoor function that relies on the hardness of lattice reduction. Phong Q. Nguyen [11] cryptanalyzed (broken) the GGH encryption scheme in 1999. The related GGH signature scheme was broken or cryptanalyzed by Nguyen and Oded Regev in 2006.

Bonsai Tree: A new lattice-based cryptosystem was introduced in 2010, known as Bonsai Tree [5]. This cryptosystem has applications for some important lattice problems in LBC. Two of them are as follows:

(i) An effective "hash-and-sign" signature scheme in the standard model without using the random oracle problem, which is important because the random oracle problem is very problematic in cryptography.

(ii) The HIBE (hierarchical identity-based encryption) scheme, which does not depend on bilinear pairings, with the basic problem, for instance, the Learning with Errors problem.

Number Theory Research Unit (NTRU): NTRU is the most well-known lattice-based cryptosystem proposed by J. Hoffstein, J. Pipher, and J. H. Silverman in 1996.

It contains two algorithms:

(i) NTRUEncrypt: NTRUEncrypt is used for encryption

(ii) NTRUSign: NTRUSign is used for digital signatures

The American agency, National Institute of Standards and Technology (NIST), recognized this cryptosystem as the most useful lattice-based cryptosystem, which is secure against quantum computing attacks. The security of the cryptosystem is based on SVP. So, the searching for short vectors is a way to attack the cryptosystem, which becomes practically impossible if the dimension of the lattice is very large.

The LLL algorithm also takes too long time to find the smallest vector, so that the smallest vector is not too much smaller than the expected length of the smallest vector [12]. J. Hoffstien et al. have shown some approximate breaking timings of the NTRU cryptosystem [23]. For a better variant of the LLL algorithm running on a 400MHz Celeron machine, approximate breaking times of the NTRU system are shown in [23], which is around 5200 years for the modest security level.

LWE Cryptosystem: The LWE-based cryptosystem was developed by O. Regev in 2005 [19]. This cryptosystem is secure, but the main downside of this system is that it is not convenient due to the magnification of information or data while converting it from plaintext to ciphertext. During the process of converting the message or information from plaintext to ciphertext, the content of the information gets magnified by n. So, if n is large, it is very unsuitable to send large messages, because if the encryption scheme works on 1-bit, then the part of information obtained after encryption is an n-vector.

RLWE Cryptosystem: Stephen Harrigan proposed this cryptosystem in 2017 [24]. The keys of the RLWE-based cryptosystems are generally the square root of the keys of the LWE-based cryptosystems. This is the main supremacy of RLWE-based cryptosystems over LWE-based cryptosystems. An RLWE-based cryptosystem uses a public-key of around 7000 bits [25] to get a 128-bit security level, while for the same level of security, the LWE-based cryptosystem would require a key of 49 million bits. Rather, the key sizes of RLWE-based cryptosystems are greater than the key sizes used in standard public-key cryptosystems. For instance, ECC, Diffie-Hellman, and RSA require keys of 256 bits and 3072 bits respectively, for the security level of 128-bit [25].

V. SIGNIFICANCE OF LBC

A detailed significance of LBC is given below:

Post-Quantum Security: Classical cryptosystems like RSA, ECC, and Diffie-Hallmen, etc., are based on integer factorization and discrete logarithmic problems which are solvable on a quantum computer by Shor's algorithm [1]. On the other hand, Lattice-based cryptosystems are based on hard lattice problems, like SVP, SIVP, LWE, and RLWE etc., that are trusted to be unsolvable on a quantum computer. So, LBC is trusted to resist quantum computing attacks.

Efficiency and Scalability: Lattice-based cryptosystems are efficient and computationally faster than classical cryptosystems since Lattice-based cryptographic primitives are based on mathematical operations (like linear algebra) that are easier than a large number of exponentiations used in classical cryptosystems.

Strong Security Proofs: Lattice-based cryptographic primitives have strong security proofs because they are based on hard lattice problems that stipulate the difficulty of solving various lattice problems.

Versatility: Lattice-based cryptography comprises the construction of several cryptographic algorithms, like Authentication, Key Exchange Mechanisms, Encryption, and Digital Signatures etc. The versatility of LBC makes it an important candidate for various applications on a broad scale.

NIST Standardization: In 2016, Lattice-based cryptography was approved by the National Institute of Standards and Technology (NIST) as an important candidate that is secure against quantum computing attacks. Thus, LBC is important for secure communications in the future.

Potential Applications: There are different sectors like government, military, commercial industries, etc., which are important for a country to be secured. LBC is believed to protect these sectors and ensure data protection and the security of communications in the current quantum computing era.

Thus, LBC provides a track to secure our future from quantum computing attacks, where existing cryptosystems are not secure.

VI. FIELDS OF INTEREST

Digital Money: This is the money that we transfer through a UPI, internet banking, and ATM, etc. This money is also known as electronic money. During the transaction, the level of security is most important. The security of the transaction depends on the encryption method. Thus, the method of encryption decides the security of our digital money. The most secure encryption technique will secure our transactions from hacking, and a little imperfection will take us to an enormous loss. Suppose, if possible, an anonymous user enters the database using some flaw in encryption and adds three or more digits to the end of his account balance. From this, he can get a huge amount of money than his account balance. Thus, you can think about what he can do from a small imperfection or a small flaw in encryption.

Anonymous Remailers: Re-mailing is a practice in which people resend an email to other people who did not open the first message. In this method, only the first remailer can have the identity of the sender, and instead of trusting the operator, it uses many anonymous remailers to rely the message before sending it to the recipient. Thus, in this process, it is not possible from the endpoint to get the identity of the original sender, and only the remailer who received the mail at first can recognize the original sender. Since all users want anonymity for their information, they use such types of methods whose encryption depends on lattices.

Hardware Implementations: Presently, the research focuses on expanding effective hardware designs for lattice-based cryptographic operations, specifically polynomial multiplication using the Number Theoretic Transform (NTT).

Cryptographic Protocols: LBC is accustomed to constructing cryptographic protocols such as public-key encryption, identity-based encryption, hash-based encryption, attribute-based encryption, lattice-based encryption, key exchange, and digital signatures.

Real-World Applications: Some real-world applications are given below:

(i) **Secure communications**: Government and military, e-commerce, IoT devices, General encrypted communication.

(ii) **Privacy-preserving protocols:** Anonymous remailers, Secure multi-party computation, Homomorphic encryption.

(iii) **Post-quantum cryptography:** Replacement for RSA and ECC, Future-proofing security.

Other real-world applications are embedded devices, machine learning, and digital signatures. In essence, LBC offers a versatile and robust approach to secure our digital world against future threats, particularly those posed by quantum computers. So LBC is also known as post-quantum cryptography.

VII. CONCLUSION

The emergence of quantum computers has disturbed the security of standard public-key cryptosystems and compelled us to turn to new cryptosystems that are safe in this quantum computing era. There are different types of cryptosystems, like public-key, identity-based, hash-based, attribute-based, code-based, and lattice-based, that can replace the classical public-key cryptosystems. Small devices that have confined storage are not adequate to use lattice-based cryptosystems since the key sizes of these cryptosystems are greater than that of the standard public-key cryptosystems. Lattice-based cryptosystems are notably more difficult to understand compared to classical public-key cryptosystems. Since the lattices are more complicated than integers so the encryption and decryption techniques in LBC are also more complicated than standard public-key cryptosystems. Thus, researchers who have no mathematical background are not able to understand these cryptosystems. But, if we can make these cryptosystems slightly accessible to researchers, then these cryptosystems can be appropriate for cryptographic systems that are secure against quantum computing attacks. Lattice-based cryptosystems are speedy, have less computational cost, and are powerful against quantum computing attacks. So, in the present era, lattice-based cryptographic techniques are the most useful techniques to secure our data and network communications.

REFERENCES

1. P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring”, Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124–134, 1994.
2. P. Nguyen, J. Stern, “The two faces of lattices in cryptology”, In J. Silverman, editor, Cryptography and lattices conference CaLC 2001, volume 2146 of Lecture Notes in Computer Science, Springer, pp. 146−180, 2001.
3. A. K. Lenstra, H. W. Lenstra, L. Lovasz, “Factoring polynomials with rational coefficients”, Math. Ann., 261(4), pp. 515−534, 1982.
4. M. Ajtai, “Generating hard instances of lattice problems”, Proc. of 28th ACM Symp. on Theory of Computing, pp. 99−108, 1996.
5. D. Cash, D. Hofheinz, E. Klitz, C. Peikert, “Bonsai trees, or how to delegate a lattice basis”, EUROCRYPT 2010.
6. A. N. Gama, P. Q. Nguyen, O. Regev, “Lattice enumeration using extreme pruning”, EUROCRYPT 2010.
7. C. Gentry, “Fully homomorphic encryption using ideal lattices”, In: STOC, pp. 169−178, 2009.
8. C. Gentry, C. Peikert, V. Vaikuntanathan, “Trapdoors for hard lattices and new cryptographic constructions”, Proc. 40th ACM Symp. on Theory of Computing (STOC), pp. 197−206, 2008.
9. O. Goldreich, S. Goldwasser, S. Halevi, “Collision-free hashing from lattice problems”, Electronic Colloquium on Computational Complexity (ECCC) 3(42), 1996.
10. O. Goldreich, S. Goldwasser, S. Halevi, “Public-key cryptosystems from lattice reduction problems”, In Advances in cryptology, volume 1294 of Lecture Notes in Comput. Sci., Springer, pp. 112−131, 1997.

11. O. Goldreich, D. Micciancio, S. Safra, J.P. Seifert, “Approximating shortest lattice vectors is not harder than approximating closest lattice vectors”, In Inform. Process. Lett. 71(2), pp. 55−61, 1999.
12. J. Hoffstein, J. Pipher, J. H. Silverman, “NTRU: A Ring-based public key cryptosystem”, 1998.
13. V. Lyubashevsky, D.Micciancio, “Asymptotically efficient lattice-based digital signatures”, Canetti, R. (ed.) TCC 2008, vol. 4948, Springer, 2008, pp. 37−54.
14. V. Lyubashevsky, C. Peikert, O. Regev, “On ideal lattices and learning with errors over rings”, Advances in Cryptology, EUROCRYPT 2010, Lecture Notes in Computer Science, Volume 6110/2010, pp. 1−23, 2010.
15. A. May, J. H. Silverman, “Dimension reduction methods for convolution modular lattices”, In J. Silverman, editor, Cryptography and lattices conference−CaLC 2001, volume 2146 of Lecture Notes in Computer Science, Providence, RI, USA, Springer, pp. 110−125, Mar. 2001.
16. D. Micciancio, “Generalized compact knapsacks, cyclic lattices, and efficient one-way functions”, Computational Complexity, Volume 16, Number 4, Springer, pp. 365−411, 2007.
17. D. Micciancio, O. Regev, “Lattice-based cryptography, Book chapter in Post-quantum Cryptography”, D. J. Bernstein and J. Buchmann (eds.), Springer, 2008.
18. C. Peikert, V. Vaikuntanathan, B. Waters, “A framework for efficient and composable oblivious transfer”, In Advances in Cryptology (CRYPTO), LNCS. Springer, 2008.
19. O. Regev, “On lattices, learning with errors, random linear codes and cryptography”, In Proc. 37th ACM Symp. on Theory of Computing, pp. 84−93, 2005.
20. P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, SIAM J. on Computing 26(5), pp. 1484−1509, 1997.
21. D. Stehle, R. Steinfeld, K. Tanaka, K. Xagawa, “Efficient public key encryption based on ideal lattices”, In ASIACRYPT, pp. 617−635, 2009.
22. Hidary, Jack, “Quantum computing: An applied approach”, Cham: Springer, p. 3. ISBN 978-3-030-23922- 0 OCLC 1117464128, 2019.
23. J. Hoffstein, J. Pipher, J. H. Silverman, “NTRU: A Public key cryptosystem” 1999.
24. S. Harrigan, “Lattice-based cryptography and the Learning with Errors Problem” 2017.
25. Verbauwhede, R. D. Clercq, S. S. Roy, F. Vercauteren Ingrid, "Efficient Software Implementation of Ring-LWE Encryption", Cryptology ePrint Archive 2014.