Proceedings of the 3rd International Conference on Mechatronics and Smart Systems
DOI: 10.54254/2755-2721/135/2025.21190

A Survey of Lattice Cryptography

Yuchong Wei[1,a,*]

[1]*FedUni Information Engineering Institute, Hebei University of Science and Technology, Yuxiang Street, Shijiazhuang, China*
a. 2401603108@stu.hebust.edu.cn
**corresponding author*

Abstract: Lattice cryptography has become one of the focal points in the era of quantum computing development. RSA and ECC, traditional public key cryptosystems, may become insecure in the face of quantum computers. In contrast, lattice cryptography is considered a potential solution for cryptographic security in the quantum computing age due to its inherent mathematical problems that require the use of quantum computers to solve. Moreover, lattice cryptographic algorithms can achieve efficient encryption and decryption processes and support a variety of cryptographic constructions, including encryption, signatures, and fully homomorphic encryption (FHE). With its high efficiency, multifunctionality, and high security, lattice cryptography has applications in various fields such as finance, e-commerce, government agencies, military, and network communications. It has also become one of the top contenders for the post-quantum cryptographic algorithm standards that have been recognized by the National Institute of Standards and Technology (NIST). This paper discusses the main contributions of lattice cryptography to society and its potential future development directions, as well as the challenges it may face and potential solutions. This thesis elaborates on lattice-based cryptography and comprehensively discusses the key technologies of lattice cryptography, its applications, security analysis, performance evaluation, and the latest progress.

Keywords: Lattice Cryptography, Lattice Cryptographic Security, Lattice Cryptographic Performance.

1. Introduction

Modern cryptography originated during World War II, playing a significant role in the war. The famous Turing decryption team and Germany's Enigma machine were born in this special period. Subsequently, Claude Shannon's theory of confidential communication and his various works provided the theoretical foundation for modern cryptography [1]. In 1976, Whitfield Diffie and Martin Hellman first publicly proposed the concept of public key cryptography [2]. It achieved the independence of encryption and decryption keys and further solved the problem of both parties having to share a key in symmetric cryptographic systems, a concept of epoch-making significance. They also proposed the Diffie-Hellman key exchange protocol [2], a method that allows for the secure sharing of keys over an insecure channel, laying the foundation for the development of public key cryptography. In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman proposed the RSA public key cryptosystem [3]. This was the first successful public key cryptosystem, providing security based on

DOI: 10.54254/2755-2721/135/2025.21190

the difficulty of factoring large integers. Due to the limitations of algorithms and computational power at the time, it became one of the most widely used public key cryptosystems. The emergence of public key cryptography opened up a new direction for the development of modern cryptography, bringing about the second leap in cryptography. It not only allowed cryptographic algorithms themselves to be directly public, but even the encryption keys could be made public. Any user sending encrypted information to another user could directly look up the recipient's publicly available encryption key in this "key book" and use it for encryption. The recipient would then use their unique decryption key to obtain the plaintext. In this process, any third party, without the decryption key, could not obtain the plaintext, successfully protecting the content through encryption. In the 21st century, with the success of quantum computing, the security of traditional cryptographic algorithms is facing an unprecedented threat. Quantum computing algorithms reduce the protection time of traditional keys. For example, Shor's algorithm can solve problems related to discrete logarithms and prime factorization in polynomial time [4], while Grover's algorithm accelerates search problems [5]. The former threatens the security of widely used RSA and ECC public key cryptography, while the latter threatens the security of symmetric encryption and hash functions. The development of post-quantum cryptography was prompted by quantum computing. Current research hotspots include code-based cryptography, multivariate-based cryptography, lattice-based cryptography and hash-based digital signatures.

2. Key Technologies of Lattice Cryptography

2.1. Mainstream algorithms

There are two main algorithms: the Lenstra-Lenstra-Lovász algorithm (LLL algorithm)and its improved version, the Block Korkine-Zolotarev algorithm (BKZ algorithm).

2.1.1. LLL Algorithm

The LLL algorithm's significant application in cryptography is primarily in attacking encryption systems. As a classic lattice basis reduction algorithm, it uses Gram-Schmidt orthogonalization and size reduction steps to ensure that the basis vectors meet specific conditions. The goal of the algorithm is to find an LLL-reduced basis, which satisfies the Lovász condition (the length relationship between each vector and its orthogonalized vector meets a certain inequality). The LLL algorithm continuously performs size reduction and checks the Lovász condition until all vectors meet the criteria, then outputs the LLL-reduced basis. Therefore, if the parameters of a cryptographic system are not chosen properly, the LLL algorithm can effectively find weaknesses in the cryptographic system.

2.1.2. BKZ Algorithm

The BKZ algorithm is used in cryptography to crack certain lattice-based encryption schemes, such as NTRU and LWE. The BKZ algorithm first performs LLL preprocessing on the input lattice basis, then processes each local basis in blocks, ensuring that the first vector in the local basis is the shortest in the projected lattice. It enumerates in the local projected lattice to find vectors that meet specific conditions. If a found vector is better than the first vector of the current block, it is inserted before the block, and LLL reduction is performed again. This process is repeated several times until all blocks have been processed, and the output basis is usually better than the LLL-reduced basis, thereby successfully extracting the low-dimensional form of high-dimensional data.

DOI: 10.54254/2755-2721/135/2025.21190

2.2. Coding Theory in Lattice Cryptography

Error-correcting codes in coding theory can be used to enhance the reliability of data transmission.

In lattice cryptography, this error-correcting capability is used to enhance the security of encrypted data, so that even if errors occur during data transmission, the recipient can correctly decrypt the information. The novel public key cryptosystem constructed based on lattice problems has faster operation speeds than existing schemes and can resist quantum attacks. As a linear structure, most operations on lattices are linear, thus the novel public key cryptosystem constructed based on lattice problems has potential advantages in terms of quantum resistance.

3. Applications of Lattice Cryptography

3.1. Post-Quantum Cryptography

The security of lattice-based cryptographic systems is based on some problems that are considered difficult in lattice theory, such as the Shortest Vector Problem (SVP), the Closest Vector Problem (CVP), the Learning With Errors (LWE) problem, and the Short Integer Solution (SIS) problem. These problems do not have known efficient solutions even on quantum computers, giving lattice-based encryption a significant advantage in the quantum computing era.

3.2. Cloud Computing and Data Security

The application of lattice cryptography in cloud computing and data security mainly involves the encryption, decryption, and signing of data to ensure the confidentiality and integrity of transaction information. Due to the linear characteristics of lattice cryptographic systems, they have faster implementation efficiency than classic public key cryptosystems like RSA. Moreover, their security is based on NP-Hard or NP-Complete problems, making lattice cryptographic systems one of the core research areas in quantum-resistant cryptographic systems. Additionally, because lattice operations have homomorphic properties, designing lattice homomorphic encryption cryptographic systems has potential application value in solving problems such as secure cloud computing environments, ciphertext retrieval, and encrypted data processing.

3.3. Blockchain and Cryptocurrencies

In the blockchain field, lattice cryptography can be used to protect the privacy of transaction addresses, oracles, and smart contracts. Combined with homomorphic encryption, lattice cryptography can establish post-quantum secure commitment schemes with additive homomorphism to protect data privacy. Furthermore, lattice-based algorithms can speed up blockchain user transactions. The computational complexity of key generation and signing is relatively low, allowing for efficient and secure execution of blockchain privacy data computations in the post-quantum era.

3.4. Internet of Things (IoT) Security

The security and privacy of data in the Internet of Things (IoT) are crucial. Lattice cryptography, as a highly secure cryptographic system, can effectively protect the security and privacy of data in IoT. In IoT devices, lattice-based cryptography can provide a solution that is both secure and efficient, and these solutions remain effective even in the presence of quantum computing.

DOI: 10.54254/2755-2721/135/2025.21190

4. Security Analysis of Lattice Cryptography

4.1. Security Proofs

4.1.1. Security Models of Lattice Cryptographic Schemes

The security models of lattice cryptographic schemes are usually based on computational complexity theory, particularly on difficult problems in lattices, such as the Shortest Vector Problem (SVP) and the Learning With Errors (LWE) problem. These models assume that these problems are difficult to solve in polynomial time, thereby ensuring the security of the cryptographic scheme.

4.1.2. Methods of Security Proofs

These typically include reduction proofs and simulation proofs. Reduction proofs demonstrate that if there is an attack method that can crack the cryptographic system, then the same method can also be used to solve a known difficult problem, thereby proving the security of the cryptographic system. Simulation proofs, on the other hand, simulate the behavior of attackers to demonstrate the theoretical security of the system.

4.2. Attack Methods

4.2.1. Key Mismatch Attacks

Attacks targeting the establishment of shared keys in lattice cryptographic algorithms. If one party reuses a key during communication, the other party may attempt to recover the reused key. Defense strategies include designing secure key management and update mechanisms.

4.2.2. Side-Channel Attacks

Side-channel attacks obtain key information by analyzing the physical implementation of cryptographic systems (such as power consumption, electromagnetic leakage, etc.). Defense strategies include adopting side-channel attack protection technologies, such as masking techniques and randomization techniques.

Any new quantum algorithms or technological advancements may impact the security of lattice cryptography. Therefore, continuous research and improvement are crucial to ensuring the secure and reliable operation of lattice cryptography in the future quantum era.

5. Performance Evaluation of Lattice Cryptography

5.1. Computational Efficiency

In the performance evaluation of cryptography, computational efficiency is an important consideration. To improve the operational efficiency of lattice cryptography in practical applications, Ma Yuan et al. proposed an optimized implementation technique for polynomial multiplication in lattice cryptography in *Hardware Implementation Optimization and Evaluation of Key Operation Modules in Lattice Cryptography* [6]. This technique uses a ping-pong structure to store polynomial coefficients to enhance access bandwidth, eliminates prescaling operations, reduces modular multiplication operations and storage space usage, and effectively reduces the occupation of logical resources. The evaluation results show that the optimized butterfly operation module can reach maximum working frequencies of over 150, 250, and 350 MHz, respectively. Compared with existing implementation techniques, the optimized hardware implementation of polynomial multiplication can achieve higher working frequencies with a smaller circuit area, increasing circuit efficiency by 22.8%.

DOI: 10.54254/2755-2721/135/2025.21190

5.2. Storage and Bandwidth Requirements

Regarding storage and bandwidth requirements, the hardware implementation of NTT (Number Theoretic Transform) polynomial multiplication proposed by Ma Yuan et al. has attracted widespread attention in the academic community. The design challenge lies in the complex access scheduling of polynomial coefficients in memory and the high bandwidth requirements. NTT requires the use of specific moduli in cryptographic algorithms to increase operation speed. NTT polynomial multiplication requires prescaling and postscaling operation steps, causing certain operation delays. Moreover, the in-place operation implementation of NTT requires a large data access bandwidth, which general dual-port RAMs cannot directly meet.

5.3. Challenges in Practical Deployment

Challenges in practical deployment include the optimization of hardware resources and the timing requirements of algorithms. The NTT polynomial multiplication optimization methods and hardware architectures proposed by Ma Yuan et al. can meet the timing requirements of different cryptographic hardware systems. The optimization techniques can achieve higher working frequencies with a smaller circuit area, providing certain reference value for the implementation of lattice-based post-quantum cryptography. Experimental results show that, compared with existing hardware implementation methods, the polynomial multiplication hardware optimization techniques can achieve an efficiency improvement of 22.8%.

6. Latest Developments in Lattice Cryptography

6.1. New Lattice Cryptographic Schemes

6.1.1. CRYSTALS-Kyber and CRYSTALS-Dilithium

The National Institute of Standards and Technology (NIST) is standardizing post-quantum cryptographic algorithms, including the lattice-based key encapsulation mechanism standard CRYSTALS-Kyber and the digital signature standard CRYSTALS-Dilithium.

CRYSTALS-Kyber first generates public and private keys, uses the public key to encrypt information, generates ciphertext, and then uses the private key to decrypt the ciphertext to restore the original information. The CRYSTALS-Kyber algorithm is a post-quantum key encapsulation mechanism (KEM) that facilitates secure key exchange. It comprises three steps: Key Generation, where a public key (pk) and a private key (sk) are created based on the Ring-LWE problem; Encapsulation, where a sender uses the public key to generate a ciphertext and a shared secret; and Decapsulation, where the recipient uses the private key to extract the shared secret from the ciphertext. Kyber is designed to resist quantum attacks and is under consideration for standardization by NIST.As an algebraic lattice cryptography, it uses the Moore lattice and polynomial rings to construct, thus the generated key pairs have high randomness and are difficult to crack. If it needs to flexibly switch between different security levels, only a few parameters need to be changed. Therefore, it is widely used in scenarios such as the Internet of Things, smart homes, and mobile communications [7]. CRYSTALS-Dilithium provides security based on difficult lattice problems, especially the Learning With Errors (LWE) problem and the Short Integer Solution (SIS) problem. It uses a lattice-based Fiat-Shamir scheme with rejection sampling based on NTRU. Moreover, among any lattice-based signature schemes that only use uniform sampling, it has the smallest public key + signature size. In addition, CRYSTALS-Dilithium is particularly suitable for resisting chosen-message attacks [8].

DOI: 10.54254/2755-2721/135/2025.21190

6.1.2. Aigis-enc, Aigis-sig, LAC.PKE

Domestic cryptographic algorithm design competition winning algorithms, they are also lattice-based cryptographic schemes.

Aigis-enc and Aigis-sig are post-quantum cryptographic algorithms designed by Professor Yu Yu's PQMagic team from the Computer Science Department of Shanghai Jiao Tong University. These two algorithms are based on asymmetric (M)LWE and (M)SIS problems and provide key encapsulation and digital signature functions, respectively. Aigis-enc, as a post-quantum public key encryption algorithm, utilizes asymmetric lattice difficult problems to provide encryption functions. While ensuring security, it achieves shorter public key, private key, and ciphertext lengths. Aigis-sig is a post-quantum digital signature algorithm based on asymmetric lattice difficult problems. Aigis-sig, under the premise of unchanged or slightly stronger security, achieves shorter public key, private key, and signature lengths by changing parameter selection[9].

LAC.PKE is a public key encryption scheme based on the ring LWE problem. It is a specific implementation of a ring LWE scheme, and its main feature at the algorithm level is that plaintext messages are encoded as large block error-correcting codes. Its main deviation lies in the use of large block error-correcting codes to encode plaintext messages. This design allows LAC.PKE to provide higher efficiency and practicality while maintaining security[10].

6.2. Performance Optimization Techniques

6.2.1. Polynomial Multiplication Optimization

Ma Yuan et al. proposed an optimized implementation of polynomial multiplication in lattice cryptography in "Hardware Implementation Optimization and Evaluation of Key Operation Modules in Lattice Cryptography." This technique uses a ping-pong structure to store polynomial coefficients to enhance access bandwidth, eliminates prescaling operations, reduces modular multiplication operations and storage space usage, and effectively reduces the occupation of logical resources. The optimized butterfly operation module can reach maximum working frequencies of over 150, 250, and 350 MHz, respectively. Compared with existing implementing techniques, the optimized hardware implementation of polynomial multiplication can achieve higher working frequencies with a smaller circuit area, increasing circuit efficiency by 22.8%.

6.2.2. NTT Polynomial Multiplication Optimization

For the hardware implementation of NTT polynomial multiplication, optimized methods and hardware architectures have been proposed, which satisfies the timing demands of various cryptographic hardware systems. The optimization techniques can achieve higher working frequencies with a smaller circuit area, providing certain reference value for the implementation of lattice-based post-quantum cryptography.

6.3. Standardization Progress

6.3.1. NIST Post-Quantum Cryptography Standard Draft

The National Institute of Standards and Technology (NIST) has officially announced three post-quantum cryptography (PQC) algorithm standard drafts, which are expected to be put into use in 2024. These three standards include the lattice-based key encapsulation mechanism standard FIPS 203, the lattice-based digital signature standard FIPS 204, and the stateless digital signature standard based on hash algorithms FIPS 205. The draft of the fourth algorithm standard will also be released to the public in 2024.

DOI: 10.54254/2755-2721/135/2025.21190

6.3.2. Development Trends of Lattice Cryptographic Systems

Lattice cryptographic systems will gradually become standardized and normalized to facilitate implementation and application in various scenarios.

7. Conclusion

This paper reviews the development of lattice cryptography and reveals the recent developments and challenges.

The computational efficiency of lattice cryptography is currently still at a relatively low level. Lattice cryptography should further develop in the direction of increasing access bandwidth and eliminating prescaling operations to speed up the operation of lattice cryptography and enhance defense capabilities. This will also help to further implement the previous research results of lattice cryptography.

Lattice cryptography devices currently still need to enhance defense against side-channel attacks to maintain the normal operation of lattice cryptography. At the same time, they should pursue a smaller circuit area while achieving higher computational efficiency.

These developments show the active development trend of lattice cryptography in new scheme development, performance optimization, and standardization. They provide direction and opportunities for the development of lattice cryptography.

References

[1] *Gallager, R. G. (2001). Claude Shannon: a retrospective on his life, work, and impact IEEE Transactions on Information Theory, VOL. 47, NO. 7.*

[2] *Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.*

[3] *Rivest, R. L., Shamir, A., & Adleman, L. M. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.*

[4] *Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (pp. 124-134). IEEE.*

[5] *Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing (pp. 212-219). Philadelphia, Pennsylvania, USA.*

[6] *Chen, Z., Ma, Y., & Jing, J. (2021). Hardware implementation optimization and evaluation of key operation modules in lattice cryptography. Peking University Journal (Natural Science Edition), 57(4), 595-604.*

[7] *Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., & Stehlé, D. (2017). CRYSTALS -- Kyber: a CCA-secure module-lattice-based KEM. IACR Cryptology ePrint Archive, 2017, 634.*

[8] *Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2017). CRYSTALS -- Dilithium: Digital Signatures from Module Lattices. IACR Cryptology ePrint Archive, 633.*

[9] *Zhao, X. F., & Fu, Y. (2022). A new threshold digital signature protocol for Aigis-sig. Journal of Cryptologic Research, 9(5), 872-882.*

[10] *Lu, X., Liu, Y., Zhang, Z., Jia, D., Xue, H., He, J., Li, B., & Wang, K. (2018). LAC: Practical Ring-LWE Based Public-Key Encryption with Byte-Level Modulus. IACR Cryptology ePrint Archive, 2018, 1009.*