WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Algorithm and Cube-Lattice-Based Cryptography

Michael N. John[1], *Udoaka O. G.*[2]

[1]Department of Mathematics, Akwa Ibom State University. Storm4help1@gmail.com
[2]Department of Mathematics, Akwa Ibom State University. otobongawasi@aksu.edu.ng.

DOI: https://doi.org/10.55248/gengpi.4.1023.102842

ABSTRACT

Cube-lattice-based cryptography stands as a pivotal development in the intersection of mathematics and cybersecurity. Its quantum resistance, versatility, and cryptographic capabilities position it as a crucial component in the ongoing efforts to secure data communication and protect privacy in an increasingly digital world. This paper seeks to advance our understanding of these fundamental principles and their practical applications in real-world security challenges using lattices.

KEYWORDS: Lattice, Lattice based, Cube, Hasse diagram, Encryption, Decryption

1. INTRODUCTION

[9] defines cryptography as the science of securing information through encryption and decryption techniques. Cryptography has played a pivotal role throughout history in safeguarding sensitive data and ensuring privacy. From the ancient Caesar cipher to the modern-day cryptographic protocols that underpin secure internet communication, cryptography has evolved in response to the increasing need for privacy and security in an interconnected world. [10] studied finite semigroup modulo and its applications to symmetric cryptography, the study shows manual Algorithm for the generation of mutually orthogonal Latin squares from a finite semi-group modulo. The concepts of this generators and its relations is seen in [11]. [1] has studied cryptography within the realm of post-quantum cryptography. Lattice-based cryptography has gained prominence due to its potential to withstand quantum attacks. Lattices, complex mathematical structures, serve as the foundation for cryptographic schemes resilient to quantum threats.

Lattice-based cryptography is a burgeoning field that has attracted extensive research and development due to its post-quantum security properties. Here, we highlight key findings, challenges, and the latest advancements:

1. Post-Quantum Security:

Lattice-based cryptography has gained prominence as a promising solution to the threat of quantum computing. Quantum algorithms like Shor's algorithm cannot efficiently break lattice-based encryption schemes. "Lattice-based cryptography as a Post-Quantum candidate" by Alagiannis et al. [1] provides insights into the post-quantum security of lattice-based schemes.

2. Versatile Encryption Schemes:

Lattice-based cryptography offers a wide range of encryption and cryptographic protocols, including Fully Homomorphic Encryption (FHE), Partially Homomorphic Encryption (PHE), and digital signatures. These schemes have applications in secure data processing, privacy-preserving computations, and secure communications. "Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages" by Brakerski and Vaikuntanathan [2] explores practical FHE implementations.

3. Lattice Problems and Assumptions:

The security of lattice-based schemes relies on the hardness of lattice problems, such as the Shortest Vector Problem (SVP) and Learning with Errors (LWE). "On the (In)security of SNOW 2.0 against Differential Cryptanalysis" by Ducas and Laarhoven [3] discusses lattice-based cryptanalysis.

4. Applications:

Lattice-based cryptography is used in various real-world applications, including secure communication (e.g., NewHope for secure key exchange), privacy-preserving data analysis (e.g., Secure Multi-Party Computation), and secure outsourcing of computations. "The SEAL Homomorphic Encryption Library" by Microsoft Research [4] introduces SEAL, a homomorphic encryption library used in secure data processing.

5. Challenges and Advancements:

Optimized algorithms for lattice reduction, such as the LLL algorithm and its variants, are crucial for practical lattice-based cryptography implementations.

"On the concrete hardness of Learning with Errors" by Lyubashevsky [5] discusses the concrete hardness of LWE, a fundamental lattice problem.

6. Post-Quantum Standardization:

The NIST Post-Quantum Cryptography Standardization project includes lattice-based candidates, reflecting the cryptographic community's recognition of their security. "NIST Post-Quantum Cryptography Standardization" [6] provides an overview of the NIST project and the lattice-based proposals.

7. Ring-LWE and Advancements:

Ring-LWE is an extension of lattice-based cryptography that uses polynomial rings. It extends the security assumptions and offers new opportunities.

"LWE and LWR with Binary Secrets: Ring-LWE, Prefix-LWE, and Overrings" by Ducas et al. [7] explores LWE and Ring-LWE variants.

8. Open Problems:

Despite significant progress, lattice-based cryptography is an active area of research with open problems in areas like lattice reduction, parameter selection, and performance optimization. Ongoing research and developments continuously address these challenges.

2. FUNDAMENTAL DEFINATIONS AND CONCEPT

In Discrete Mathematics, a partially ordered set (A, ≼) is called a lattice if every pair of elements a and b in L has both a least upper bound (*LUB*) and a greatest lower bound (*GLB*).

The least upper bound is also called the join of a and b, denoted by $a \vee b$. The greatest lower bound is also called the meet of a and b, and is denoted by $a \wedge b$.

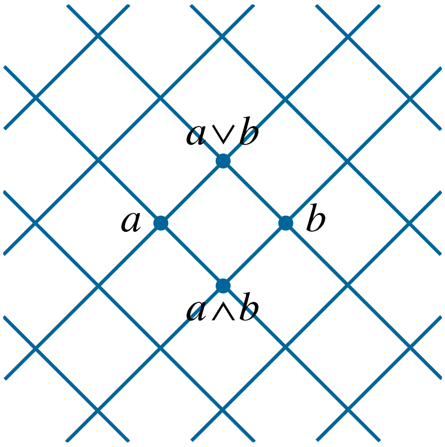

Figure 1.

[2] has worked and illustrated on lattices in cryptography using discrete Mathematics to achieve a highly safe data transfer.

If we consider a partially ordered set (Ω(L{1,2,3}), ⊆). The poset consisting of all subset of A = {1,2,3} under the relation ⊆ forms a lattices in figure 2 below.

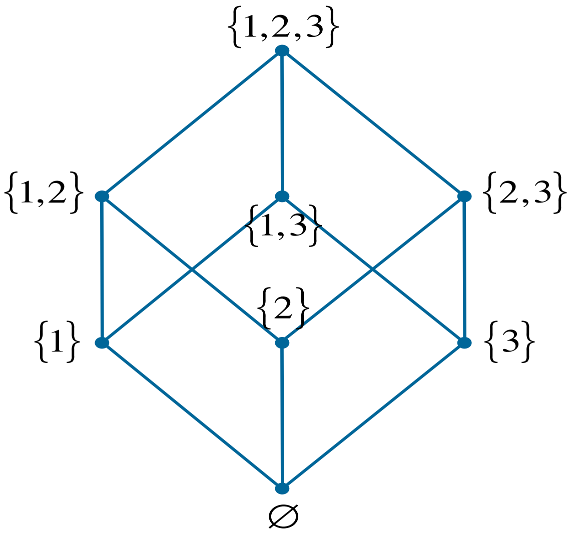

Figure 2.

Every pair of elements in $\Omega(A)$ has a join and a meet. The join of two subsets is defined as their union, and the meet is defined as the intersection of the subsets. For example,

Joint = $\{1\} \vee \{2\} = \{1\} \cup \{2\} = \{1,2\}$

Meet = $\{1\} \wedge \{2\} = \{1\} \cap \{2\} = \emptyset$

This result can be generalized to any set of n elements. So the power set $\Omega(A)$ of any set A under the subset ordering $\subseteq$ forms a lattice.

3. MAIN RESULT

This computational code using Python provides a simplified representation of Cube-Lattice-Cryptography for this paper. In a practical implementation, we advice you use more advanced lattice basis reduction techniques and take additional security measures

3.1 Python Codes

```
import numpy as np

# Define lattice parameters

n = 5  # Dimension

q = 19  # Modulus

# Key generation

private_key = np.random.randint(0, 2, size=(n, n))  # Random binary private key matrix

# Simulate lattice basis reduction (LLL) to get the public key

# In practice, you would use a specialized library for lattice basis reduction.

public_key = private_key  # Placeholder for the public key

# Encryption

plaintext = np.random.randint(0, 2, size=(n, 1))  # Random binary plaintext vector

noise = np.random.randint(0, 2, size=(n, 1))  # Random binary noise vector

ciphertext = (private_key @ plaintext + noise) % 2  # Encryption using binary matrices

# Decryption

recovered_plaintext = (public_key.T @ ciphertext) % 2  # Decryption using the public key

# Print results
```

```
print("Original plaintext:")

print(plaintext)

print("\nCiphertext:")

print(ciphertext)

print("\nDecrypted plaintext:")

print(recovered_plaintext)
```

3.2 Detailed explanation of the code:

We start by defining the lattice parameters, including the dimension (n) and modulus (q).

Key Generation: This will generate a random binary matrix for the private key. Each element is either 0 or 1.

Simulate Lattice Basis Reduction (LLL): In practice, you would use a specialized library for lattice basis reduction. In this paper, we simply copy the private key to the public key, which isn't difficult but serves as a placeholder.

Encryption: The code will create a random binary plaintext vector and a random binary noise vector. The ciphertext is calculated as the product of the private key and the plaintext, with added noise. The result is taken modulo 2, ensuring it remains binary.

Decryption: The ciphertext is decrypted using the public key, which is transposed, and the result is taken modulo 2 to recover the plaintext.

Finally, the code prints the original plaintext, ciphertext, and the decrypted plaintext.

4. CONCLUSION

Cube-Lattice-based cryptography represents a promising solution to the threat of quantum computing and offers versatile encryption schemes with real-world applications. The field continues to evolve, presenting both challenges and opportunities for researchers in the domain of cryptography and cybersecurity.

REFERENCES

1. Alagiannis, I., et al. "Lattice-based cryptography as a Post-Quantum candidate." Journal of Cryptographic Engineering (2014).

2. Auparajita, K. "Lattices in Crytograpy" Aryabhalla Journal of Mathematics & Informatics Vol.14. No.1, Jan-June

3. Brakerski, Z., & Vaikuntanathan, V. "Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages." CRYPTO (2013).

4. Ducas, L., & Laarhoven, T. "On the (In)security of SNOW 2.0 against Differential Cryptanalysis." EUROCRYPT (2019).

5. Microsoft Research. "The SEAL Homomorphic Encryption Library." Link

6. Lyubashevsky, V. "On the concrete hardness of Learning with Errors." ASIACRYPT (2010).

7. NIST Post-Quantum Cryptography Standardization. Link

8. Ducas, L., et al. "LWE and LWR with Binary Secrets: Ring-LWE, Prefix-LWE, and Overrings." EUROCRYPT (2018).

9. Kharchenko N. (2020) (Ph.D thesis), Lattice algorithms and lattice-based cryptography, Ecole doctorate informatique, Telecommunications etElectronique (Paris) (France)

10. Udoaka O. G. & Frank E. A. (2022). Finite Semi-group Modulo and Its Application to Symmetric Cryptography, International Journal of Pure Mathematics DOI: 10.46300/91019.2022.9.13.

11. Udoaka, O. G. (2022). Generators and inner automorphism. THE COLLOQUIUM -A Multi-disciplinary Thematc Policy Journal www.ccsonlinejournals.com. Volume 10, Number 1 , Pages 102 -111 CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632.