IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

An Analysis of Lattice Methods in Quantum-Resilient Cryptographic Designs

Gauswami Rohitgiri Mahendragiri[1] and Dr. Rajeev Kumar [2]
Research Scholar, Department of Math[1]
Associate Professor, Department of Math[2]
Sunrise University, Alwar, Rajasthan, India

Abstract: *A secure encryption technique can be produced by applying mathematics to cryptography. In the realm of cryptography, lattices have become a potent mathematical tool with a wide range of uses, from safe multi-party computing to encryption. This study offers a thorough analysis of lattices' function in cryptography, encompassing both its theoretical underpinnings and real-world applications. The fundamental ideas of lattices and their application to cryptographic protocols are covered in the first section of the study. It then examines important cryptographic primitives based on lattice issues, including digital signatures, completely homomorphic encryption, and lattice-based encryption algorithms. A novel lattice-based cryptography technique is also suggested in the study*

Keywords: Lattice-Based Cryptography, Shortest Vector Problem, Learning With Errors, Post-Quantum Cryptography, Quantum Resistance, Cryptographic Primitives, Public Key Encryption, Digital Signatures, Lattice Reduction, Homomorphic Encryption, Security Proofs, Quantum Computing Threats, Cryptanalysis, Code-based Cryptography, Lattices, group theory

I. INTRODUCTION

Discrete collections of points in n-dimensional space that create a periodic pattern are called lattices, and they are the mathematical building blocks of lattice-based encryption. For in-depth knowledge and comprehension of lattices and their use in cryptography, see and. Understanding the characteristics and uses of these lattices is essential to the mathematical underpinnings of lattice-based encryption. In mathematics, a lattice is a discrete collection of points organized in n-dimensional space in a periodic, grid-like pattern. Numerous areas of mathematics, such as algebra, number theory, and cryptography, are based on this idea.

Definition:

A lattice is a discrete set of points in n-dimensional space that exhibits periodicity and is generated by integer linear combinations of linearly independent basis vectors. Mathematically, a lattice Λ can be defined as:

$$\Lambda = \{V = a_1 + b_1 + \cdots + a_n b_n | a_i \epsilon\ Z$$

where b_1 , b_2 , … , bn are linearly independent basis vectors and ai are integers.

Proof of Periodicity:

Let $v \in \Lambda$, then v can be expressed as $a_1 + b_1 + \cdots + an\ bn$. Now, consider v + t, where t is any vector in the lattice. The new point v + t can be expressed as:

$$v + t = (a_1 + t_1)b_1 + (a_2 + t_2)b_2 + \cdots + (a_n + t_n)b_n$$

Since ai and ti are integers, $v + t$ is also a lattice point. This demonstrates the periodicity of the lattice.

Properties: 1.

Translation Invariance: Let $v \in \Lambda$. Now, consider v + t for any $t\epsilon\Lambda$:

$$v + t = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n + t$$

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

This expression, as shown earlier, is a lattice point, confirming translation invariance. **Example:** Consider a 2D lattice with basis vectors b1= [1, 0] and b2= [0,1]. The lattice points are all integer combinations of these vectors. Translation invariance implies that if v= [a, b] is a lattice point, then v+ [c, d] is also a lattice point.

Basis and Dimension:

Linear independence of basis vectors is a fundamental property of lattices. If b_1, b_2, $bn$are linearly independent, they span an n-dimensional space.

Example: In a 3D lattice, the basis vectors b1=[1,0,0], b2=[0,1,0], and b3=[0,0,1] form a basis. The lattice points are all combinations of integers multiplied by these vectors.

Lattice Points: Every point on a lattice is a consequence of integer linear combinations of basis vectors, as stated clearly in the definition of a lattice. For instance: Examine the basis vectors b1= [1, 0] and b2= [0, 1] in a 2D lattice. The integer pairs (a, b) that make up the lattice points are all such that v=ab1+bb2. Exploring the uses of lattices in many mathematical and cryptographic contexts requires an understanding of these qualities.

Fundamental Lattice Problems

The security of lattice-based cryptography is based on lattice issues. The Shortest Vector Problem (SVP) and Learning with Errors (LWE) are two basic issues in lattice theory. We'll examine these issues with examples and offer succinct justifications for their importance.

Shortest Vector Problem (SVP)

The shortest non-zero vector in a lattice Λ is found by SVP, which means that v ∈ Λ such that ||v|| is minimized. Let b1= [2,1] and b2= [−1,3] be basis vectors on a 2D lattice. Finding the shortest non-zero vector is the SVP for this lattice. Lattice-based cryptographic systems are based on the SVP, which is computationally challenging in generic lattices. It guarantees that determining a lattice's shortest vector is a difficult task, which is crucial for lattice-based encryption security.

Learning with Errors (LWE)

LWE determines the secret vectors that are utilized to build a set of noisy linear equations. This entails determining s∈Z n given samples of the form ai, < ai, s > +ei in the setting of lattices, where ai is a lattice vector,⟩ is the dot product, and ei is a little mistake. Assume that a1= [3,4], a2= [1,2] are lattice vectors and that s = [2,−1] is the secret vector. $a1$, < $a1$, s > +$e1$ and $a2$, < $a2$, s > +$e2$ would be the samples. For lattice-based cryptography, the LWE problem's difficulty is essential. Security assurances are offered by LWE-based systems, particularly when building cryptographic primitives like digital signatures and encryption. To appreciate the security underpinnings of lattice-based cryptography systems, one must comprehend the computational difficulty and importance of these basic lattice challenges. These issues help make these systems more resistant to certain types of cryptographic assaults.

Hardness Assumptions In Lattice Cryptography

The presumptive difficulty of particular lattice issues is the foundation of lattice-based encryption. The difficulty of the Learning with Errors issue and the Shortest Vector issue are two important presumptions. We'll examine these presumptions using instances; for evidence of their importance, see.

Assumption: Hardness of Shortest Vector Problem (SVP)

The presumption that it is computationally difficult to determine the shortest non-zero vector in a lattice. Let b1= [3, 1] and b2= [−2,4] be basis vectors on a 2D lattice. The shortest non-zero vector in this lattice must be found for the SVP. Lattice-based cryptographic systems are kept safe by the SVP's difficulty. If there were an effective method for solving SVP, lattice-based encryption's security may be jeopardized.

Assumption: Hardness of Learning with Errors (LWE)

It is assumed that it is computationally difficult to extract a secret vector s from noisy linear ai, < ai, s > +ei. Assume that a1= [3, 4], a_2= [1,2] are lattice vectors and that s= [2,−1] is the secret vector. Finding s given samples ai, < ai, s > +ei is part of the LWE. A key component of lattice-based encryption is the hardness of LWE. It is thought that cryptographic primitives built on LWE assumptions, such as digital signatures and encryption, are safe against both conventional and quantum assaults. The security of lattice-based cryptography systems depends on these hardness assumptions. Their importance is demonstrated by the assumed computational impossibility of effectively resolving certain lattice issues, which guarantees the security of cryptographic techniques based on them.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

II. PROPOSED IDEA

When strong adversaries, especially those with quantum capabilities, are present, lattice-based encryption systems use the difficulty of lattice issues to enable secure communication. Together with mathematical formulations and security proofs, we provide a lattice-based encryption system based on the Learning with Errors (LWE) issue. Read thoroughly and view the work of.

Lattice-Based Encryption Scheme Proposal

Key Generation:

1. Parameters Setup:

Choose security parameters n and q and define a lattice $\Lambda \subset Zq\ n$ generated by a basis matrix A. Select a noise distribution D over Z with small support. See for his security setup.

2. Generate Public Key:

Choose a random matrix, say $S\ R\ Zq\ n{\times}m$ and compute the matrix $E\ R\ D\ n{\times}m$. The public key is A=S + E mod q.

3. Generate Secret Key:

The secret key is the matrix S.

Encryption:

1. Choose Message and Encode:

Choose a message m and encode it into a vector u using a suitable encoding function.

2. Generate Noise and Encrypt:

Choose a random vector $r\ R\ Zq\ m$ and a noise vector $e\ R$. The ciphertext is computed as c=Ar + e + Encode (u) mod q.

Decryption:

1. Compute Inner Product:

Compute the inner product ⟨c, S⟩ mod q to obtain an approximation of Encode (u).

2. Decode and Recover Message:

Verify Equality:

Check to see whether c, A⟩ mod q equals the original message m's hash. If equality is maintained, accept the signature; if not, reject it. To get the original message m, decode the approximation that was obtained. This lattice-based encryption method's security depends on how difficult the Learning with Errors (LWE) issue is thought to be. In particular, the security proof shows that an adversary cannot effectively differentiate between encryptions of distinct communications, even if they have access to the cipher text and public key. In the security sketch, the encryption scheme breaking challenge is reduced to the LWE problem. Assume that an effective adversary A has a non-negligible advantage in breaking the encryption system. We can create algorithm B that effectively solves the LWE problem by utilizing A. Given the assumption of difficulty in solving LWE, it follows that the lattice-based encryption method is likewise difficult to crack.

Computation

Complex mathematical procedures and cryptographic protocols are required to implement a complete lattice-based cryptography method. For further information on computational algebra, see. Nonetheless, we have shown a simple illustration of lattice-based encryption using Python's Learning with Errors (LWE) issue. Keep in mind that this is a simplified example and does not encompass all of the subtleties of a cryptographic system in the real world. Their algorithms may be found in and. Please be aware that this example is simplified for Python and should not be used for real security. Implementations of lattice-based encryption in the real world require more complex methods, parameter selections, and security concerns. The procedure is the same for Java, but the syntax is different. Here is an example of a Java implementation of matrix operations using the Apache Commons Math library:

III. CONCLUSION

The hardness of the Ring-LWE issue is increased by this suggested cryptographic technique, which provides a safe and effective solution for digital signatures and public key encryption. The scheme's resistance to different cryptographic assaults is firmly shown by the security proofs. To confirm the viability and effectiveness of the suggested plan, more research and application are advised. The suggested lattice-based encryption method shows how secure communication

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

may be accomplished by utilizing the difficulty of lattice issues, especially the LWE problem. A viable contender for post-quantum safe cryptography, the scheme's security stems on the projected difficulties of solving LWE.

REFERENCES

[1] Regev, O. (2006, August). Lattice-based cryptography. In Annual International Cryptology Conference (pp. 131-141). Springer, Berlin, Heidelberg.
[2] Dadheech, A. (2018, September). Preventing Information Leakage from Encoded Data in Lattice Based Cryptography. In 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1952-1955). IEEE.
[3] Shor, P. W. (1994, November). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). Ieee.
[4] Ajtai, M. (1996, July). Generating hard instances of lattice problems. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 99-108). ACM.
[5] Nejatollahi, H., Dutt, N., & Cammarota, R. (2017, October). Special session: trends, challenges and needs for lattice-based cryptography implementations. In 2017 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS) (pp. 1-3). IEEE.
[6] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2), 303- 332.
[7] Nguyen, P. Q., & Stern, J. (2001, March). The two faces of lattices in cryptology. In International Cryptography and Lattices Conference (pp. 146- 180). Springer, Berlin, Heidelberg.
[8] Michael N. John & Udoaka O. G (2023). Algorithm and Cube-Lattice-Based Cryptography. International journal of Research Publication and reviews, Vol 4, no 10, pp 3312-3315 October 2023.
[9] Micciancio, D. (2011). Lattice-based cryptography. Encyclopedia of Cryptography and Security , 713-715.
[10] Nyang, D., & Song, J. (1998). Method for hiding information in lattice. Electronics Letters, 34(23), 2226-2228.
[11] Schaller, R. R. (1997). Moore's law: past, present and future. I EEE spectrum, 34(6), 52-59.
[12] Micciancio, D. (2001). Improving lattice based cryptosystems using the Hermite normal form. In Cryptography and lattices(pp. 126-145). Springer, Berlin, Heidelberg.
[13] Michael N. John, Udoaka O. G., "Computational GroupTheory and Quantum-Era Cryptography",International Journal of Scientific Research in Science,Engineering and Technology (IJSRSET), Online ISSN :2394- 4099, Print ISSN : 2395-1990, Volume 10 Issue 6,pp. 01-10, NovemberDecember 2023. Available at doi :https://doi.org/10.32628/IJSRSET2310556.