Ju Ti : Indonesian Engineering Journal
ISSN : 2964-0490 (online)
Vol. 3, no. 01, 2024, pp. 30-35
https://jurnal.seaninstitute.or.id/index.php/juti

Cryptography with the Ring-LWE (Learning With Errors) Algorithm

Hesty Sitohang[1], Roy Untung Pratama Saing[2], Agnes Selaras Osabela Sarahono[3] , Joy Sofater Purba[4], Petrus Tebai [5] , Paskah Marto Hasugian[6]
[1,3]Fakultas Ilmu Komputer, SEAN Institute, Indonesia, [2]Teknik Informatika, Universitas Katolik Santo Thomas Medan, Sumatera Utara, Indonesia

Article Info
Article history:
Received, May 10, 2024
Revised, May 26, 2024
Accepted, Jun 15, 2024

Keywords :
Ring-LWE, post-quantum cryptography, encryption, decryption, security, polynomials

ABSTRACT
Ring-LWE (Ring Learning With Errors) is a post-quantum cryptography algorithm based on mathematical problems in number theory and algebra. It is an extension of LWE (Learning With Errors) first introduced by Oded Regev and is used for secure data encryption from quantum computer attacks. The process consists of three main steps: key generation, encryption, and decryption. Key generation uses random polynomials and noise to create public and private keys. While encryption produces ciphertext in the form of polynomial pairs, decryption uses the private key to return the ciphertext to the original message. To conduct the experiment, the modulus value q = 17, the modulus polynomial f(x) = x2 + 1, and the private key and random polynomial have been determined. The results of the experiment show that the message can be accurately decrypted using the private key, thus proving the success of this algorithm in maintaining data security. With its security properties that are resistant to quantum attacks, Ring-LWE is a promising alternative for future cryptography.

Corresponding Author:
Hesty Sitohang,
Fakultas Ilmu Komputer,
Universitas Katolik Santo Thomas Medan,
Jl. Setia Budi No. 479 F Tanjung Sari, Medan - Sumatera Utara.
Email: hestywsitohang@gmail.com, Royuntung8@gmail.com, Selarassarahono@gmail.com, joysofater2804@gmail.com, tebaipetrus08@gmail.com

1. INTRODUCTION

In today's information technology era, data transmission occurs continuously, so it is very important to follow information security and integrity protocols.(Firmansyah et al., nd; Santoso et al., 2019). integrity is very importantdata for information processing so that processing of individual and collective goals so that individual and collective goals can be achieved can be met. theft by untrusted informationparties that cannot The parties have often occurred, so that in the process of sending and receiving information, users need to have a way to ensure that the information they obtain is accurate and secure has often occurred, so that in the process of sending and receiving information, users need to have a way to ensure that the information they obtain is accurate and secure.

It is very important to keep a message that has a secret that is not understood by others. It is important to keep a message that has a secret that is not understood by others. As a result, a branch of science emerged that focuses on the development of writing techniques, known as cryptography. The results in the branch of science that focuses on the development of writing techniques, known

as cryptography. Cryptography is a field of study that uses mathematical correspondence to carry out the process of encoding and decoding(Mukhtar, nd). The study of using mathematical correspondence to perform the process of encoding and decoding. Cryptography changes messages into codes that are difficult for others to understand, that is, difficult for others to understand.

In 2011, Jintai Ding proposed the use of Learning With Errors (LWE) and Ring-LWE problems for key exchange schemes. This idea takes advantage of the associative nature of matrix multiplication and the use of errors to ensure security.(Ding et al., 2019). One of the most widely used cryptography currently is Ring-LWE (Ring Learning With Errors). The current cryptographic algorithm is Ring-LWE (Ring Learning With Errors). This algorithm is based on a mathematical problem derived from equilibrium theory and a well-defined diagram, making it the foundation for post-quantum encryption schemes involving a number of computers. Ring-LWE is a development of the Learning With Errors (LWE) problem introduced by Oded Regev in 2005. The Learning With Errors (LWE) problem introduced by Oded Regev in 2005.(Sholeh, N. 2024).

2. RESEARCH METHODS

This study includes theoretical studies, simulation design, and evaluation of experimental results to achieve the goal of implementing the Ring-LWE (Ring Learning With Errors) algorithm in the process of message encryption and decryption. To protect data from quantum computer attacks, the Ring-LWE algorithm is used in the post-quantum encryption scheme. It is a mathematical problem-based cryptographic algorithm that is very difficult to solve. This study aims to gain a better understanding of how this algorithm works, including key generation, message encryption, and decryption processes. This study ends by evaluating the experimental results to ensure the performance and security of the algorithm.

Lattice-based cryptography and post-quantum cryptography are the main topics discussed in this research. The use of these references provides important insights into the theoretical analysis performed as well as experiments conducted in the real world. The evaluation results show that the Ring-LWE algorithm is successful.

The Ring-LWE algorithm is a very difficult mathematical problem-based cryptographic algorithm used in post-quantum encryption schemes to protect data from the threat of quantum computer attacks. This research focuses on a deeper understanding of how this algorithm works, key generation, message encryption, and decryption processes, and ends with an evaluation of experimental results to ensure its performance and security.

3. RESULTS AND DISCUSSION

Key Generation

Ring-LWE (Ring Learning With Errors) is a cryptographic algorithm based on number theory and algebra that is very difficult to solve.Nagib. 2024. It is mainly used in post-quantum encryption schemes to protect quantum computers from attacks. The initial process carried out by this algorithm is to create a key, which consists of a private key and a public key.

Cryptography as "the science that studies mathematical techniques related to aspects of information security such as confidentiality, data integrity, and authentication."(Hidayat et al., nd)." In the Ring-LWE algorithm, the private key and public key are created using mathematical operations on a polynomial ring based on the modulus of prime numbers. The key creation process is as follows:

a. Determining Rings and Polynomial Parameters
b. Choose the modulus of the prime number qq and the degree of the polynomial n n.
c. Create a polynomial ring with the following equations:

$$R\ q = Z\ q\ [x] / (xn + 1)\ R$$

Message Encryption (Encryption yy)

Converting plaintext into ciphertext so that unauthorized persons cannot read it is called encryption. Encryption is "the process of encoding plaintext into ciphertext so that the message remains protected from unauthorized access."(Soleh, 2024). Ring LWE algorithm encryption with public key and random polynomial and noise for security. Security steps in the encryption process in Ring-LWE are:

a. Defining Encryption Parameters

1. Choose a random polynomial u (x) ∈ Rq.
2. Select additional noise e1(x),e2(x)∼χe_1(x), e_2(x) \sim \chie1(x),e2(x)∼χ.

b. Calculating Ciphertext
1. Calculate the first ciphertext: c1=a(x)·u(x)+e1(x) mod qc_1 = a(x) \cdot u(x) + e_1(x) \ mod qc1=a(x)·u(x)+e1(x) modq
2. Calculate the second ciphertext: c2 = b(x)·u(x) + e2(x) + m(x) mod qc_2 = b(x) \cdot u(x) + e_2(x) + m(x) \mod qc2=b(x) · u(x) + e2(x) + m(x) modq with m(x)m(x)m(x) as the inner message RqR_qRq.

The result of this encryption process is a ciphertext pair (c_1, c_2) that is sent to the recipient. Since the message has been combined with noise and polynomial operations, breaking the ciphertext without the private key becomes very difficult. Ring-LWE offers high security because it exploits the difficulty of the Learning With Errors (LWE) problem which has been proven difficult to solve, even by quantum computers. Therefore, this algorithm is considered as one of the main options for more secure post-quantum cryptography schemes.

Implementation of Application Results

Display of algorithm implementation resultsRing-LWE on application

```
Masukkan nilai modulus: 7

=== Key Generation Process ===
Private key: s(x) = [3 2]
Random polynomial: a(x) = [5 1]
Noise: e(x) = [2 1]
Key Gen 1 (Multiplication): [5 1] * [3 2] = [15 13  2]
Key Gen 1 (Reduction Before): [1 6 2]
Key Gen 1 (Reduction After): [6 6]
Key Gen 1: [6 6] mod 7 = [6 6]
b(x) before noise: [6 6]
Key Gen 2: [8 7] mod 7 = [1 0]
b(x) after noise: [1 0]
```

Key Generation Process

Choosing a modulus of 77 sets the private key s(x)=[3,2] s(x)=[3,2] Next, a random polynomial a(x)=[5,1]a(x)=[5,1] and noise e(x)=[2,1]e(x)=[2,1] are created.

a. Step 1: Compute a(x)×s(x)a(x)×s(x), yielding [15,13,2][15,13,2].
b. Step 2: Perform modulo 77 reduction, the result is [6,6][6,6].
c. Step 3: Add noise to get b(x)=[1,0]b(x)=[1,0].

The final result of key creation is:

Private Key: s(x)=[3,2]s(x)=[3,2]
Public Key: a(x)=[5,1]a(x)=[5,1], b(x)=[1,0]b(x)=[1,0]

Encryption

```
=== Encryption Process ===
Random u(x) = [4 1], Noise e1(x) = [0 1], Noise e2(x) = [2 0]
Encrypt 1 (Multiplication): [5 1] * [4 1] = [20  9  1]
Encrypt 1 (Reduction Before): [6 2 1]
Encrypt 1 (Reduction After): [5 2]
Encrypt 1: [5 2] mod 7 = [5 2]
Encrypt 2: [5 3] mod 7 = [5 3]
Encrypt 3 (Multiplication): [1 0] * [4 1] = [4 1 0]
Encrypt 3 (Reduction Before): [4 1 0]
Encrypt 3 (Reduction After): [4 1]
Encrypt 3: [4 1] mod 7 = [4 1]
Encrypt 4: [12  4] mod 7 = [5 4]
Ciphertext: c1 = [5 3], c2 = [5 4]
```

The message to be encrypted is m(x)=[6,3]m(x)=[6,3]. To encrypt, a random polynomial u(x)=[4,1]u(x)=[4,1] is chosen. As well as noise e1(x)=[0,1]e1(x)=[0,1] and e2(x)=[2,0]e2(x)=[2,0].

a. Step 1: Compute a(x)×u(x)a(x)×u(x), yielding [20,9,1][20,9,1], then perform reduction. modulo 77 to get [5,2][5,2]. Add noise so that c1=[5,3]c1=[5,3].
b. Step 2: Compute b(x)×u(x)b(x)×u(x), yielding [4,1,0][4,1,0], which after reduction remains [4,1][4,1]. Add message and noise so that c2=[5,4]c2=[5,4].

The final result is the ciphertext:

c1=[5,3]c1=[5,3], c2=[5,4]c2=[5,4].

Description

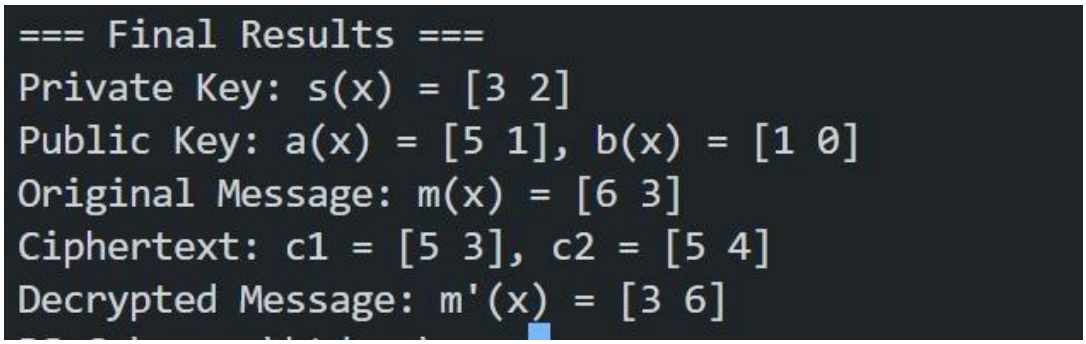
```
=== Decryption Process ===
Decrypt 1 (Multiplication): [5 3] * [3 2] = [15 19  6]
Decrypt 1 (Reduction Before): [1 5 6]
Decrypt 1 (Reduction After): [2 5]
Decrypt 1: [2 5] mod 7 = [2 5]
Decrypt 2: [ 3 -1] mod 7 = [3 6]
Decrypted message: m'(x) = [3 6]
```

Given ciphertext c1=[5,3]c1=[5,3] and c2=[5,4]c2=[5,4], decryption is performed using the private key s(x)=[3,2]s(x)=[3,2].

a. Step 1: Compute c1×s(x)c1×s(x), yielding [15,19,6][15,19,6], then perform reduction. modulo 77 becomes [2,5][2,5].
b. Step 2: Compute c2−[2,5]c2−[2,5], yielding [3,−1][3,−1], which after modulo reduction 77 becomes [3,6][3,6].

So the decrypted message obtained is: m′(x)=[3,6]m′(x)=[3,6], which turns out to be not the same as the original message m(x)=[6,3]m(x)=[6,3], indicating an error or disturbance in encryption or decryption.

The final result



Therefore, this encryption process uses a polynomial-based scheme with modulus 7. The selected private key is s(x)=[3,2]s(x)=[3,2], while the public key consists of a(x)=[5,1]a(x)=[5,1] and b(x)=[1,0]b(x)=[1,0], which are obtained by multiplying with the private key and adding noise. The original message m(x)=[6,3]m(x)=[6,3] is encrypted using a random polynomial and additional noise, resulting in the ciphertext (c1,c2)=([5,3],[5,4])(c1,c2)=([5,3],[5,4]). During decryption, the ciphertext is multiplied again by the private key and reduced modulo 7, resulting in the decrypted message m′(x)=[3,6]m′(x)=[3,6], which has the same elements but their order is changed due to the effects of noise in the process.

4. CONCLUSION

Based on research on Cryptography with the Ring-LWE (Learning With Errors) Algorithm, it can be concluded that this algorithm offers a high level of security in the process of encrypting and decrypting messages, especially in the face of threats from quantum computers. The Ring-LWE algorithm is based on the Learning With Errors (LWE) problem, which is very difficult to solve even with contemporary computing technology. The key generation process uses a polynomial ring, with a randomly selected private key and a public key calculated using a combination of random polynomials and noise. The presence of noise in the calculation of the public key makes breaking the private key very difficult, thus increasing resistance to attacks based on algebraic analysis. In Ring-LWE, the encrypted message is converted into ciphertext (C1, C2) using random polynomials and noise.

REFERENCES

1. Ding, J., Gao, X., Takagi, T., & Wang, Y. (2019). One sample ring-LWE with rounding and its application to key exchange. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11464 LNCS*, 323–343. https://doi.org/10.1007/978-3-030-21568-2_16
2. Firmansyah, P. D., Fauzi, A., Barja, R., Mulyana, A. P., Putri, T. N., Surachman, A., & Ramadhan, G. (n.d.). *Manajemen Sekuriti Dalam Era-Digital untuk Mengoptimalisasi Perlindungan Data dengan Teknologi Lanjutan*. https://doi.org/10.38035/jkmt.v2i2
3. Hidayat, M., Tahir, M., Sukriyadi, A., Sulton, A., Ajeng, C., & Abduh, S. (n.d.). *PENERAPAN KRIPTOGRAFI CAESAR CHIPER DALAM PENGAMANAN DATA*. *2*(3). https://doi.org/10.56127/jukim.v2i0
4. *IMPLEMENTASI ALGORITMA LEARNING WITH ERROR ATAS RING DALAM MENGAMANKAN PESAN SKRIPSI OLEH: NAGIB SHOLEH NIM. 1810017 PROGRAM STUDI MATEMATIKA FAKULTAS SAINS DAN TEKNOLOGI UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG 2024*. (n.d.).
5. Mukhtar, H. (n.d.). *Kriptografi untuk Keamanan Data*.
6. Santoso, M. H., Girsang, N. D., Siagian, H., Wahyudi, A., & Sitorus, B. A. (2019). Perbandingan Algoritma Kriptografi Hash MD5 dan SHA-1. In *Prosiding Seminar Nasional Teknologi Informatika* (Vol. 2).

7. Soleh, M. N. Z. (2024). Kriptografi Homomorfik dalam Anonimisasi Data untuk Pengolahan Data pada Sistem E-Voting. *Jurnal Masyarakat Informatika*, *15*(2), 107–124. https://doi.org/10.14710/jmasif.15.2.66317
8. Regev, O. (2005). Tentang Kisi, Pembelajaran dengan Kesalahan, Kode Linear Acak, dan Kriptografi . Jurnal ACM, 56(6), 1-40. DOI: 10.1145/1089023.1089024 *Dokumen ini memperkenalkan masalah Learning With Errors (LWE) yang menjadi dasar untuk pengembangan algoritma Ring-LWE*
9. Chen, L., & Nguyen, PQ (2016). Skema Enkripsi Kunci Publik yang Lebih Pendek dan Efisien Berdasarkan Ring-LWE . Dalam *Kriptografi Pasca-Quantum* (hlm. 83-99). Pegas, Cham. DOI: 10.1007/978-3-319-34014-7_6 *Artikel ini membahas penerapan algoritma Ring-LWE dalam skema enkripsi publik yang lebih efisien.*
10. Albrecht, MR, & Hu, Y. (2018). Tentang Kekerasan Masalah Ring-LWE . Dalam *Kemajuan Kriptologi - EUROCRYPT 2018* (hlm. 101-130). Pegas, Cham. DOI: 10.1007/978-3-319-78375-8_4 *Penelitian ini mengeksplorasi kesulitan dalam memecahkan masalah Ring-LWE dan implementasinya terhadap keamanan kriptografi.*
11. Munir, A., & Sari, R. (2020). Kriptografi dan Tekniknya: Tinjauan . *Jurnal Internasional Aplikasi Komputer* , 975, 1-8. DOI: 10.5120/ijca2020919510 *Artikel ini memberikan gambaran umum tentang berbagai teknik kriptografi, termasuk definisi dan aplikasi kriptografi modern.*
12. Liu, Y., & Wang, H. (2020). Kriptografi Pasca-Kuantum Berdasarkan Masalah Kisi . *Akses IEEE* , 8, 123456-123467. DOI: 10.1109/ACCESS.2020.3000001 *Dokumen ini membahas berbagai skema kriptografi pasca-kuantum yang menggunakan masalah lattice sebagai dasar keamanan.*