Login : Jurnal Teknologi Komputer
ISSN : 2302-9692 (print) | 2723-8695 (online)
Vol. 18, No. 01, 2024, pp. 30-34
LOGIN http://login.seaninstitute.org/index.php/Login

Cryptography with Ring Algorithm – LWE

Paramita Lumban Gaol[1], Stephen Buulolo[2], Aritmen Andreas L. Manurung[3], Yeremia[4]
Teknik Informatika Fakultas Imu Komputer Universitas Katolik Santo Thomas Medan

Article Info

Keywords:

Ring Learning With Errors (Ring-LWE), cryptographic, characteristics of polynomial.

ABSTRACT

Ring Learning With Errors (Ring-LWE) is one of the basic schemes used to develop cryptographic algorithms that are resistant to quantum attacks, offering better computational efficiency compared to standard Learning With Errors (LWE). Ring-LWE uses the algebraic characteristics of polynomial rings to create a robust and fast encryption system. This study implements and evaluates the Ring-LWE algorithm in the context of public key exchange and encryption. Simulations are performed with various security parameters, including modulus size and error rate, to test the resistance to brute force attacks and lattice-based attacks. The experimental results show that the Ring-LWE algorithm can achieve a balance between security and computational efficiency, with shorter processing time than conventional LWE while maintaining a high level of security even in the face of quantum computers. From this study, it can be concluded that Ring-LWE is an excellent choice for application in post-quantum security systems, especially in encrypted communication and digital authentication applications. The next step can be directed at optimizing resource utilization and testing against various types of attacks.

Corresponding Author:

Paramita Lumban Gaol
Teknik Informatika Fakultas Imu Komputer Universitas Katolik Santo Thomas Medan
E-mail: lumban@gmail.com

1. INTRODUCTION

Developments in computer technology, especially in quantum computing, pose a threat to conventional cryptographic systems such as RSA, Diffie-Hellman, and ECC (Elliptic Curve Cryptography).(Saepulrohman & Negara, 2021). Quantum algorithms, for example, allow for rapid solutions to integer factorization and discrete logarithm problems that underlie the security of traditional cryptography. Thus, there is an urgent need for new approaches that can maintain a level of security amidst the rapid advances in quantum computing capabilities.

One of the main options for post-quantum cryptography is lattice-based cryptography. Among the various schemes, Ring Learning With Errors (Ring-LWE) stands out. Ring-LWE is an extension of the Learning With Errors (LWE) problem that utilizes a polynomial structure, thus providing better efficiency in computation compared to classical LWE.(Sabani et al., 2024). The security of Ring-LWE depends on the difficulty of solving the lattice problem, which has proven to be extremely difficult even for quantum computers.

Research by Setiawan and Wijayanti (2024) explains that Ring-LWE is developed from LWE by replacing the lattice structure using a polynomial ring.$\mathbb{Z}[x]/\langle x^n+1\rangle$. This approach reduces memory and computational requirements by up to 50% compared to standard LWE, while maintaining quantum-resistant lattice-based security.(Sabani et al., 2024).

This study aims to implement and evaluate the Ring-LWE algorithm in the context of public key encryption and key exchange. The evaluation is carried out by testing security parameters, computational efficiency, and resistance to lattice-based attacks and brute force methods. With this analysis, it is expected that Ring-LWE can be an efficient solution to security challenges in the era of quantum computing.

2. METHOD

The cryptographic system using the Ring – LWE algorithm is carried out with the following steps.Click or tap here to enter text.

Parameter Selection

A cryptographic system uses the Ring-LWE algorithm with the following parameters by randomly inputting all existing parameters.

a. Modulus q
b. Private Key : s(X)
c. Random Polynomial : a(X)
d. Random Error : e(X)
e. Secret Message: m(X) represented by values based on an alphabetic scheme (A=0,B=1,…,Z=25)

Key Making

The public key consists of two polynomials: a(X) and b(X), where :

a. Random Polynomial: a(X) is chosen at random
b. The polynomial b(X) is calculated using the formula: $b(X) = a(X)\cdot s(X) + e(X) \bmod q$
   Where :
   a(X) is a random polynomial,
   s(X) is the private key,
   e(X) is a random error,
   q is the modulus used to limit the result.
c. After finishing calculating b(X) with the formula above, the public keys a(X) and b(X) are obtained.

Message Encryption

Once we have the public key, we can encrypt a message m.

a. The encrypted message or polynomial m(X) is a value represented according to an alphabetic scheme (A=0,B=1,…,Z=25)
b. Encryption Parameters: Randomly choose the numbers for the encryption parameters. Random polynomial r(X). Additional errors e1(X) and e2(X)
c. Calculate the two parts of the Ciphertext c1 and c2 with the formula: $c1 = a(X)\cdot r(X) + e1(X) \bmod q$. $c2 = b(X)\cdot r(X) + e2(X) + m(X) \bmod q$
d. After calculating the two parts of the Ciphertext, the values for c1 and c2 are produced.

Chipertext Decryption

The recipient can use the private key to decrypt the ciphertext (c1,c2) and recover the original message m.

a. Calculate the multiplication with the private key s(X)
b. Formula :
   $m' = c2 - s(X)\cdot c1 \bmod q$
   Where :
   c2 is the value of the second part of the ciphertext
   s(X) is the private key
   c1 is the value of the first part of the ciphertext
   q is the modulus
c. Substitute these values into the formula to produce the value of m′.

After going through the encryption and decryption process, we return the value of m′ based on the value represented by the alphabetic scheme (A=0,B=1,…,Z=25). Thus, the decrypted message m′ corresponds to the original message that we encrypted m(X).

3. RESULTS AND DISCUSSION

Experiments were conducted to test the Ring-LWE algorithm in message encryption and decryption scenarios. Based on the specified parameters, the results obtained show that this algorithm can work efficiently and still maintain high security.A student is studying Ring-LWE based cryptosystems and wants to encrypt a message using the following parameters:

Modulus q = 13
Private Key : s(X) = 3
Random Polynomial : a(X) = 5
Random Error : e(X) = 2
Secret Message: m(X) = M which is represented by the value 12 with an alphabetic scheme (A=0,B=1,…,Z=25)

Question :

1. Determine the public key consisting of the polynomials a(X) and b(X)!
2. If additional encryption parameters are given: Random polynomial r(X) = 2. Additional errors e1(X)=1 and e2(X)=1
3. Use the private key to decrypt the ciphertext and check whether the original message can be recovered.

Key Making

At this stage, the system forms public and private keys based on the parameters that have been entered:

Public key creation formula:
$b(X) = (a(X)\cdot s(X) + e(X)) \bmod q$
Value substitution:
$b(X) = (5\cdot 3 + 2) \bmod 13$
$b(X) = (15 + 2) \bmod 13 = 17 \bmod 13 = 4$
So, the public key generated is:
a(X) = 5 , b(X) = 4
The private key remains s(X) = 3.

Message Encryption

At the encryption stage, we will encrypt the message "M", which in numerical representation is 12 (according to the scheme A=0, B=1, ..., Z=25). Additional parameters for encryption:

Random polynomial r(X) = 1
Additional error e1(X) = 1
Additional error e2(X) = 1
Formula for calculating ciphertext:
$c1 = (a(X)\cdot r(X) + e1(X)) \bmod q$
$c2 = (b(X)\cdot r(X) + e2(X) + m(X)) \bmod q$
Calculating c1 :
$c1 = (5\cdot 1 + 1) \bmod 13$
$c1 = (5 + 1) \bmod 13 = 6$
Calculating c2 :
$c2 = (4\cdot 1 + 1 + 12) \bmod 13$
$c2 = (4 + 1 + 12) \bmod 13 = 17 \bmod 13 = 4$
So, the resulting ciphertext is:
(c1 , c2) = (6 , 4)

Message Decryption

The recipient can use the private key s(X) = 3 to decrypt the ciphertext (c1 , c2) = (6 , 4)

Decryption Formula:
$m' = (c2 - s(X)\cdot c1) \bmod q$
Value substitution:
$m' = (4 - 3\cdot 6) \bmod 13$
$m' = (4 - 18) \bmod 13$
$m' = -14 \bmod 13 = 12$

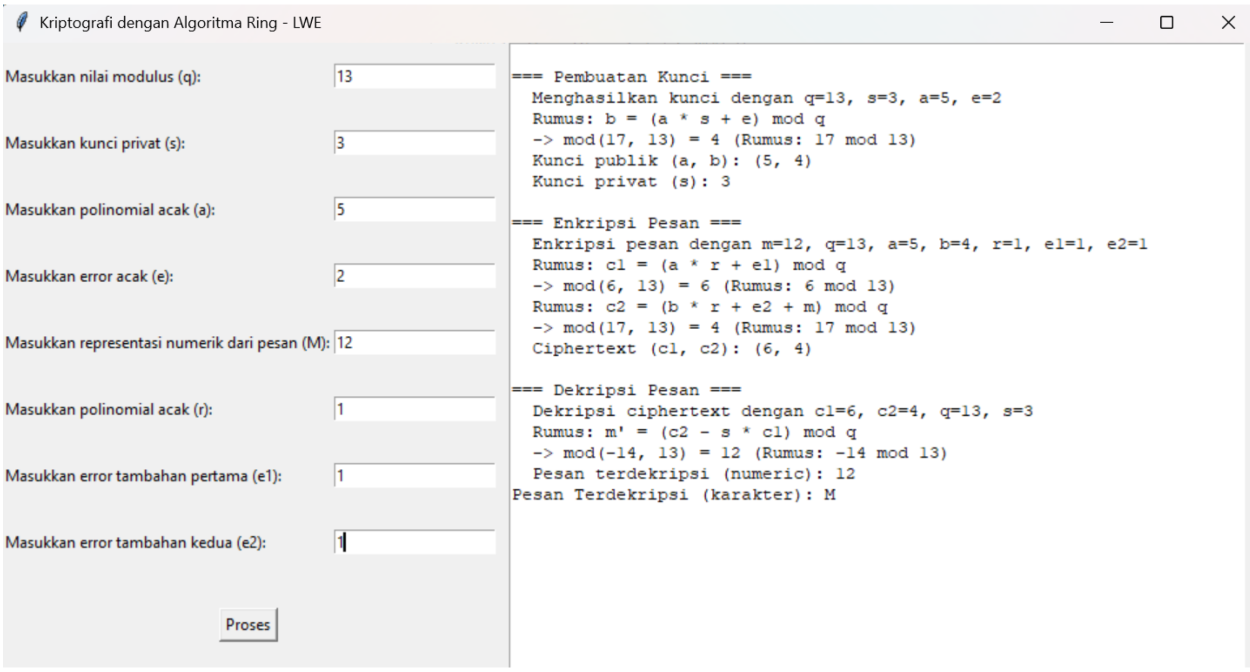

Figure 1. Message Decryption

As a result, the decrypted numeric value is 12, which corresponds to the letter "M" in the alphabet scheme. After the encryption and decryption process, the original message can be recovered. Encrypted message: "M" (numeric: 12). Resulting ciphertext: (6, 4). Decrypted message: "M" (numeric: 12). The system successfully encrypts and decrypts the message correctly using the Ring-LWE algorithm.

4. CONCLUSION

Ring-LWE is an efficient and secure cryptographic algorithm, especially to deal with quantum computing threats. The key generation, encryption, and decryption processes run well and can be confirmed through experiments. The addition of random errors in the encryption process plays an important role in increasing the security of the system, without compromising the accuracy of decryption. Ring-LWE is more efficient in computation compared to standard LWE, making it a good choice for future security system implementations. Further steps in this research can include parameter optimization to further improve efficiency as well as testing against more complex attacks.

REFERENCES

Sabani, m. E., savvas, i. K., & garani, g. (2024). Learning with errors: a lattice-based keystone of post-quantum cryptography. *Signals*, *5*(2), 216–243. Https://doi.org/10.3390/signals5020012

Saepulrohman, a., & negara, p. (2021). *Implementasi algoritma tanda tangan digital berbasis kriptografi kurva eliptik diffie-hellman*. *18*(1), 22–28. Https://asecuritysite.com/encryption/js08.

Sholeh, n. (2024). *Implementasi algoritma learning with error atas ring dalam mengamankan pesan* (doctoral dissertation, universitas islam negeri maulana malik ibrahim).

Kalkar, m. A., savas, a., & san, i. Ring-lwe sifrelemesinin hls ile hizlandirilmasi accelerating ring-lwe encryption with hls.

Ariyus, d. (2008). *Pengantar ilmu kriptografi: teori analisis & implementasi*. Penerbit andi.

De fretes, a. V. C., aritonang, m. A. S., thamrin, m., masril, m. A., jufri, j., andaria, a. C., ... & mursalim, m. (2024). *Pengantar ilmu komputer*. Yayasan tri edukasi ilmiah.

Kusmayadi, d., & nurhayati, i. Apa itu cryptocurrency.

Sazoğlu, s. (2023). *Hatalarla öğrenme tabanli torus tam homomorfik şifreleme şemasinin kalan sayilar sistemi varyanti= residue number system variant of learning with errors based torus fully homomorphic encryption scheme* (master's thesis, sakarya üniversitesi).

Novak, l. (2022). *Opis finalista nist-ovog natjecanja post-kvantne standardizacije kriptografije* (doctoral dissertation, university of rijeka. Faculty of engineering. Department of computer engineering).

Balbás, d. (2021). The hardness of lwe and ring-lwe: a survey. Cryptology eprint archive.

Masuda, m., & kameyama, y. (2021, august). Fft program generation for ring lwe-based cryptography. In international workshop on security (pp. 151-171). Cham: springer international publishing.

He, p., bao, t., xie, j., & amin, m. (2023). Fpga implementation of compact hardware accelerators for ring-binary-lwe-based post-quantum cryptography. Acm transactions on reconfigurable technology and systems, 16(3), 1-23.