An Improved R-LWE Homomorphic Masking Scheme Postprint

Authors: Li Zichen, Sun Yafei, Yang Yatao, Liang Lan, Cao Guangcan

Date: 2018-05-20T00:00:00+00:00

Abstract

Regarding differential power analysis attacks on lattice-based encryption schemes, Reparaz et al. proposed an additively homomorphic R-LWE masking scheme at PQC 2016. While this scheme can effectively resist differential power analysis attacks, the homomorphic addition of ciphertexts leads to increased noise size in the ciphertext, thereby reducing the decryption correctness rate. To address this issue, we propose an improved R-LWE homomorphic masking scheme. By introducing modulus switching technology, we perform modulus reduction on ciphertexts after homomorphic encryption, which reduces the noise size in the ciphertext while preserving the plaintext-ciphertext correspondence, thereby improving the decryption correctness rate of the scheme. To protect the sub-keys, we introduce random matrices to mask the sub-keys and provide correctness analysis and security proofs. Analysis demonstrates that the new scheme achieves significant improvements in both security and efficiency compared to the original scheme.

Full Text

An Improved R-LWE Homomorphic Masking Scheme

Li Zichen[1],[2], Sun Yafei[1], Yang Yatao[1],[3], Liang Lan[1], Cao Guangcan[3]
[1]College of Communication Engineering, Xidian University, Xi'an 710071, China [2]Beijing Institute of Graphic Communication, Beijing 102600, China [3]Beijing Electronic Science & Technology Institute, Beijing 100070, China

Abstract: To address differential power analysis attacks on lattice-based encryption schemes, Reparaz et al. proposed an additively homomorphic R-LWE masking scheme at PQC 2016. This scheme effectively resists differential power analysis, but homomorphic addition of ciphertexts increases the noise magnitude, reducing decryption correctness. To solve this problem, we propose an improved R-LWE homomorphic masking scheme. By introducing modular

switching technology, we perform modulus reduction on ciphertexts after homomorphic operations, which decreases noise magnitude while preserving the plaintext-ciphertext correspondence, thereby improving decryption correctness. To protect subkeys, we introduce a random matrix to mask the subkeys, and provide correctness analysis and security proofs. Analysis shows that the new scheme offers significant improvements in both security and efficiency compared to the original.

Keywords: lattice cryptography; R-LWE; side-channel attack defense; mask matrix; modular switching; homomorphic

0 Introduction

On May 17, 2017, IBM announced the successful development of a 17-qubit quantum processor, marking an increasingly severe challenge for traditional cryptography. Lattice-based public-key cryptography is one of the quantum-resistant cryptographic systems, attracting significant attention from cryptographers. In 2005, Regev combined lattice theory with learning theory to propose a new hard problem on lattices—Learning With Errors (LWE) [1]. In 2010, Lyubashevsky et al. proposed a variant of LWE called Ring-LWE (R-LWE) [2] at Eurocrypt, and simultaneously presented an R-LWE-based public-key encryption scheme. However, existing post-quantum cryptographic schemes based on lattice cryptography also face the risk of side-channel attacks [3].

Reference [4] designed a masking scheme for R-LWE by splitting polynomials, which can effectively resist side-channel attacks but requires a specific decoder. Reference [5] improved upon [4] by analyzing the additive homomorphic property of R-LWE and introducing homomorphic concepts into the decryption process, thereby changing the decryption flow and improving scheme efficiency. This scheme decrypts based on homomorphic properties without requiring a specific decoder, but the decryption correctness rate decreases. Reference [6] conducted side-channel attacks on Gaussian sampling implementations and attacked sliding window defense measures. Reference [7], presented at CHES, used cache attacks to recover some outputs of the Gaussian sampling algorithm, forming the first side-channel attack scheme against lattice-based signature schemes. Reference [8] designed an 8-bit processor for R-LWE cryptographic algorithm implementation, enabling more efficient encryption and decryption. Reference [9] described a new algebraic coding technique, proposed a simple random blinding technique to resist timing and power attacks, and introduced a split-precomputation technique for Gaussian sampling algorithms to resist side-channel attacks.

This paper provides an in-depth analysis of the scheme in [5], identifying two main problems: (a) low decryption correctness rate; (b) lack of masking protection for subkeys. Building upon the original scheme, we introduce random matrix masking and modular switching technology to protect subkeys and reduce

noise magnitude in ciphertexts through masking matrices, thereby improving decryption correctness.

1.1 Preliminaries

Definition 1 (Lattice). Let $v_1, v_2, ..., v_m$ be m linearly independent vectors in $\mathbb{R}^n$. A full-rank lattice L of dimension m is defined as the set of all integer linear combinations of these vectors, i.e., $L = \{\sum_{i=1}^{m} c_i v_i \mid c_i \in \mathbb{Z}\}$. The vectors $v_1, v_2, ..., v_m$ are called a basis of lattice L.

Definition 2 (Learning With Errors). The Learning With Errors (LWE) problem is defined as follows: Given a matrix $A \in \mathbb{Z}_q^{n \times m}$, a vector $s \in \mathbb{Z}_q^n$, and an error vector $e \in \mathbb{Z}_q^m$ sampled from probability distribution χ over $\mathbb{Z}_q$:

(1) **LWE Decision Problem:** Distinguish $(A, As + e)$ from uniformly random $(A, u) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m$. This problem has been proven to reduce to the approximate shortest vector problem in polynomial ideal lattices.

(2) **LWE Search Problem:** Find vector s such that $v = As + e$.

Lemma 1 (Modular Switching). Let $q > p$ be odd integers, $s \in \mathbb{Z}^n$ be an integer vector, and e be a vector close to s with $||e|| < q/(2p)$. For any $c \in \mathbb{Z}_q^n$, we have $\lfloor c \mod q \rceil_p = \lfloor (\lfloor c \rceil_q) \mod p \rceil$. This lemma shows that ciphertexts can be switched from a larger modulus to a smaller modulus without knowing the secret key, requiring only knowledge of a bound on the key length, while still allowing correct decryption.

1.2 Review of Original Scheme

An R-LWE-based cryptosystem involves three main algorithms: key generation, encryption, and decryption.

Parameter Generation: Let $f(x)$ be a globally known polynomial of degree n, where n is the dimension of the polynomial ring, q is the modulus, σ is the standard deviation of the discrete Gaussian distribution, and error vectors are sampled from the discrete Gaussian distribution χ.

Key Generation Algorithm: Sample two polynomials $s, e \leftarrow \chi$ from the discrete Gaussian distribution. The secret key is $sk = s$, and the public key is $pk = (a, b = a \cdot s + e) \in R_q^2$.

Encryption Algorithm: First, encode the message by multiplying each bit by $\lfloor q/2 \rfloor$ to convert the bit input data into a ring element $m \in R_q$. Then compute ciphertext $c = (c_1, c_2) = (a \cdot r + e_1, b \cdot r + e_2 + m \cdot \lfloor q/2 \rfloor)$, where $r, e_1, e_2 \leftarrow \chi$. Output ciphertext c.

Decryption Algorithm: The receiver obtains ciphertext $c = (c_1, c_2)$ corresponding to plaintext m, locally generates a random message m' and encrypts it to produce ciphertext $c' = (c_1', c_2')$. Then performs homomorphic addition on the two ciphertexts: $c'' = c + c' = (c_1 + c_1', c_2 + c_2')$. Next, decrypts ciphertext

c'' to obtain $m'' = c_2'' - s \cdot c_1''$. Finally, using the locally known message m', recovers the original message as $m = m'' \oplus m'$. The specific decryption process is shown in Figure 1 [Figure 1: see original paper].

1.3 Scheme Analysis

First, this additive homomorphic decryption strategy can be viewed as a blinding process for ciphertexts. Randomly splitting the key into two parts mixes the key with ciphertext, altering the original data relationship and eliminating data dependencies. Intuitively, this method can effectively resist first-order differential power attacks. However, in software implementation, subkeys need to be loaded into registers for computation, making unprotected subkeys a potential attack point—attackers could recover subkeys to obtain the final key.

Second, algebraic addition between ciphertexts causes algebraic addition of noise components in the ciphertexts. When the noise magnitude becomes too large and exceeds the decryption threshold, decryption failures occur. Research results in [5] show that ciphertext addition increases the decryption failure rate from 5.3×10^{-6} to 3.3×10^{-4}, representing an expansion of nearly one hundred times.

To address the problem of reduced decryption correctness, we introduce modular switching technology. After performing additive operations on ciphertexts, modular switching reduces the modulus from the original modulus q to a smaller modulus p, which decreases the noise size in ciphertexts while ensuring correct decryption under the same key, thereby improving decryption correctness.

To protect subkeys, we introduce a random masking matrix to mask the subkeys, keeping them in a protected state and effectively preventing differential power attacks.

2 Improved R-LWE Scheme

Chapter 1 analyzed the original scheme and identified several security vulnerabilities. This chapter improves upon these deficiencies to enhance decryption correctness while protecting subkey security. The key generation and encryption algorithms remain identical to the original scheme. This paper only improves the decryption process, with the improved decryption procedure shown in Figure 3 [Figure 3: see original paper].

a) The decryptor receives ciphertext $c = (c_1, c_2)$ corresponding to plaintext m, locally generates random message m' and encrypts it to obtain ciphertext $c' = (c_1', c_2')$. After homomorphic addition of the two ciphertexts, modular reduction is applied to reduce noise, yielding final ciphertext $c'' = (c_1'', c_2'')$. The computation process is shown in Figure 2 [Figure 2: see original paper].

b) The user generates a random matrix M for masking subkeys. Assuming

the generated random matrix is M, compute $M \oplus s$ (where $\oplus$ denotes the masking operation).

c) In each branch, perform decryption computation on ciphertext using masked subkeys: compute $\alpha_1 = \text{INTT}(c_1'' \oplus (s_1 \cdot M))$ and $\alpha_2 = \text{INTT}(c_2'' \oplus (s_2 \cdot M))$.

d) Perform decryption according to the rule $m'' = \alpha_1 \oplus \alpha_2$, then obtain the final original message $m = m'' \oplus m'$.

3.1 Correctness Analysis

Correctness Proof: To prove the correctness of this scheme, we first verify the decryption correctness of homomorphic addition, then demonstrate that modular switching maintains correctness while reducing noise.

Theorem 1. When matrix M and random message m' are independently uniformly distributed over $\mathbb{Z}_p$, the intermediate variables in the decryption algorithm are independently distributed from sensitive information s, m.

Proof. To prove the theorem, we analyze the distribution of variables at each line and demonstrate that all intermediate values are independent of sensitive information s, m.

Lines 1, 5: Matrix M is a random variable that masks intermediate values through XOR operations. The masked variables follow their original distribution without leaking any sensitive information.

Lines 2, 3, 6: In $\mathbb{Z}_p$, the values follow a distribution independent of s, and the results of each statement cannot be used to recover any information about s. Since b depends on key s, but under the R-LWE assumption, attackers cannot obtain any information about s by observing b. Meanwhile, c_2 is part of the ciphertext containing the encryption of random message m', making c_2 independent of both key s and plaintext message m.

Lines 4, 7: Variables that are mutually independent remain independent after INTT conversion.

Line 8: The sum of two independent variables remains an independent variable that leaks no sensitive information.

Line 9: The input is masked data, so the decryption result reveals no information.

Line 10: Message m' is generated locally and saved; the final message m is obtained through XOR operation.

In summary: All intermediate variables in the decryption algorithm are distributed independently of sensitive information s, m. Therefore, attackers cannot effectively perform differential power analysis on this algorithm.

3.2 Security Analysis

3.2.1 Resistance to Timing Attacks

Timing attacks exploit differences in execution time for different bits during cryptographic operations. In our improved scheme, key processing does not iterate through original key bits; instead, keys are randomly split, with each subkey processed independently. Since the splitting is random, attackers cannot determine the specific splitting method and thus cannot identify the starting point of each subkey' s execution through timing information, preventing key recovery via timing attacks.

3.2.2 Resistance to Simple Power Analysis

Simple power analysis directly analyzes power consumption curves collected during cryptographic algorithm execution. Our scheme randomly splits keys, altering the original computation order. Attackers cannot determine the starting point of each subkey' s computation, preventing them from intuitively guessing keys based on power consumption curves, thus effectively preventing simple power analysis.

3.2.3 Resistance to Differential Power Analysis

Differential power analysis primarily exploits data dependencies between intermediate values. Proving that no correlation exists between data—that the probability distribution is independent of the key—effectively resists differential power analysis.

This section implements the R-LWE decryption algorithm and proves its effectiveness against differential power analysis. The R-LWE decryption implementation is as follows:

[Algorithm description with INTT operations]

The proposed masking scheme improves the R-LWE algorithm by eliminating dependencies between data and keys through key splitting technology and homomorphic decryption strategies, effectively resisting timing attacks, simple power analysis, first-order differential power analysis, and higher-order differential power analysis.

3.3 Efficiency Analysis

Decryption Correctness Analysis: Reference [5] notes that homomorphic addition between ciphertexts causes noise magnitude growth, leading to decryption failures when noise exceeds the threshold. To avoid decryption failures, we introduce modular switching technology. By switching the modulus to a smaller value, we ensure correct decryption under the same key while reducing noise magnitude, thereby improving decryption correctness.

Reference [13] proves in Theorem 1 that through modular switching, without knowing the secret key value and requiring only knowledge of a bound on the key, ciphertexts can be converted to a new ciphertext with modulus reduced from the original modulus q to a smaller modulus p, while the corresponding plaintext message remains unchanged. This technology reduces noise size from $||e||$ to $||e|| \cdot (p/q)$, thereby improving decryption correctness.

Comparative Analysis: Power balancing techniques [11] consume significant energy and typically require circuit redesign; power randomization techniques [12] reduce some energy consumption compared to power balancing but usually require extensive data processing, affecting overall performance. Boolean masking requires building lookup tables to store all possible values, increasing storage space. In contrast, our homomorphic decryption changes the algorithm execution process, requires no significant energy overhead, and needs only a register for storing random messages.

3.4 Comparative Analysis

Through analysis and comparison, the proposed scheme is more secure than [4] and [5] by adding subkey protection. In terms of efficiency, modular reduction decreases noise magnitude in ciphertexts, improving decryption correctness to match the original scheme' s success rate. The comparative analysis results are shown in Table 1 .

Table 1. Comparative Analysis of Different Schemes

Scheme	Side-Channel Resistance	Decryption Correctness	Security	Easy to Implement
[4]				
[5]				
Ours				

4 Conclusion

Based on Reparaz et al.'s additively homomorphic R-LWE masking scheme, this paper introduces modular switching technology to change ciphertext processing methods, reducing noise magnitude and improving decryption correctness. By generating random masking matrices to protect subkeys, the scheme enhances side-channel defense capabilities.

References

[1] Regev O. On lattice, learning with errors, random linear codes, and cryptography [C]// Proc of STOC. 2005: 113-127.

[2] Lyubashevshy V, Peikert C, Regev O. On ideal latice and learning with errors over rings [C]// Proc of Eurocrypt 2010. [S. l.]: Spring-Verlag, 2010.

[3] Kocher P, Jaffe J, Jun B. Differential power analysis [C]// Proc of International Cryptology Conference on Advances in Cryptology. [S. l.]: Springer-Verlag, 1999: 388-397.

[4] Reparaz O, Roy S S, Vercauteren F, et al. A masked ring-LWE implementation [C]// Proc of Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2015.

[5] Reparaz O, Clercq R D, Roy S S, et al. Additively homomorphic ring-LWE masking [C]// Proc of Post-Quantum Cryptography. [S. l.]: Springer International Publishing, 2016.

[6] Pessl P. Analyzing the shuffling side-channel countermeasure for lattice-based signatures [C]// Proc of Progress in Cryptology-INDOCRYPT 2016. [S. l.]: Springer International Publishing, 2016.

[7] Bruinderink L G, Hülsing A, Lange T, et al. Flush, Gauss, and reload: a cache attack on the BLISS lattice-based signature scheme [C]// Proc of Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2016.

[8] Liu Z, Seo H, Roy S S, et al. Efficient ring-LWE encryption on 8-bit AVR processors [C]// Proc of Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2015: 663-682.

[9] Saarinen M J O. Arithmetic coding and blinding countermeasures for lattice signatures [J/OL]. Journal of Cryptographic Engineering (2017): 1-14. https://link.springer.com/article/10.1007/s13389-017-0149-6.

[10] Tong Y, Wang Z, Dai K, et al. A DPA and HO-DPA resistant implementation of AES [J]. Journal of Computer Research & Development, 2009, 46(3).

[11] Burns F, Bystrov A, Koelmans A, et al. Design and security evaluation of balanced 1-of-n circuits [J]. Iet Computers & Digital Techniques, 2012, 6(2): 125-135.

[12] Liu P C, Chang H C, Lee C Y. A low overhead DPA countermeasure circuit based on ring oscillators [J]. IEEE Trans on Circuits & Systems II Express Briefs, 2010, 57(7): 546-550.

[13] 汤殿华, 祝世雄, 王林, 等. 基于 RLWE 的全同态加密方案 [J]. 通信学报, 2014, 35(1): 173-182.

Note: Figure translations are in progress. See original paper for figures.