Improved Hybrid BKZ-MITM Attack on LWE via Noisy-Search*

Sieun Bak[1], Yujeong An[1], and Yongha Son[1]

Sungshin Women's University, Seoul, Korea
{20220182, 20240744, yongha.son}@sungshin.ac.kr

1 Introduction

The Learning with Errors (LWE) problem, a mathematical hardness assumption fundamental to lattice-based cryptography within post-quantum cryptography, is characterized as a system of linear equations perturbed by a small noise component [1]. To effectively deploy LWE-based cryptosystem, it is crucial to study practical attack methods for parameter selection. Lattice-based attacks, which typically involve constructing a specific lattice and finding a short vector within it, are generally considered the most efficient methods. Consequently, many research directions have been proposed to enhance these lattice-based attacks, primarily by utilizing combinatorial methods based on counting.

2 Previous Method

The **Learning With Errors (LWE)** problem is defined by a matrix A, a secret vector $s \in \mathbb{Z}_q^n$, a noise vector $e \in \mathbb{Z}_q^m$ composed of small values, and a vector b derived from these components. This formulation satisfies the condition $b_i = \langle a_i, s \rangle + \mod q$ for the i-th row of A, denoted as a_i. The relationship can be expressed by the following equation

$$b = As + e \pmod{q} \tag{1}$$

The attacker's objective is to infer the hidden secret vector $\vec{s}$ from the given pair $(\vec{A}, \vec{b})$. In this situation, the method that can be used to find the secret vector $\vec{s}$ is the **Meet-in-the-Middle (MITM) attack**. By finding the short vector $(\vec{v}, \vec{w})$ through the BKZ algorithm, the MITM attack can be executed more efficiently. The lattice L is defined as:

$$L = \{(\vec{v}, \vec{w}) \in \mathbb{Z}_q^{m+n_2} : \vec{v}A_2 \equiv_q \vec{w}\} \tag{2}$$

The vector $(\vec{v}, \vec{w})$ represents a short vector that has a linear relationship with A_2.

3 Proposed Method

The standard MITM approach involves pre-computing all possible combinations of $A_1 s_1$ and searching for $b - A_2 s_2$. However, this is not perfectly satisfied because of the noise vector. To address this, a Noisy-Search phase is used with a hash function to store the effect of noise in bin format. The existing hash function is as follows:

$$\mathrm{sgn}(x) = \begin{cases} 0 & (\text{if } x \in [0, \frac{q}{2})) \\ 1 & \text{otherwise} \end{cases} \tag{3}$$

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-70, December 16-18, 2025, Sapporo, Japan.

However, this method requires a solution to mitigate the high probability of failure caused by the effect of the noise vector.

So, our proposed method is a hybrid attack that improves the matching function used in the MITM attack. Following the existing method, we transform the original LWE instance $(\mathbf{A}, \mathbf{b})$ to produce a new equivalent problem $(\mathbf{A}', \mathbf{b}')$, where $\mathbf{b}' = \mathbf{A}'\mathbf{s} + \mathbf{e}'$. The key advantage of this transformation is that it makes the problem more susceptible to a search attack. Then, we apply our improved function to the equation $\mathbf{b}' - \mathbf{A}'_1\mathbf{s}_1 = \mathbf{A}'_2\mathbf{s}_2 + \mathbf{e}'$. Since the noise $\mathbf{e}'$ prevents an exact match, we use a function to find solutions where the Euclidean distance between the two sides is within a small threshold. The final attack complexity combines the costs of both phases, divided by the success probability of the search. Theoretically, this performs a more effective attack than existing methods.

4 Comparison with Existing

To evaluate the effectiveness of our proposed hybrid attack, we compared its final attack complexity with that of existing models using the official SMAUG parameters. These parameters are included in the K_PQC standard candidate list [2], representing realistic post-quantum security levels. The results, presented in Figure 1, show that our model achieves a significantly lower attack complexity for all SMAUG parameter sets. This reduction demonstrates that our approach provides a more efficient attack strategy.

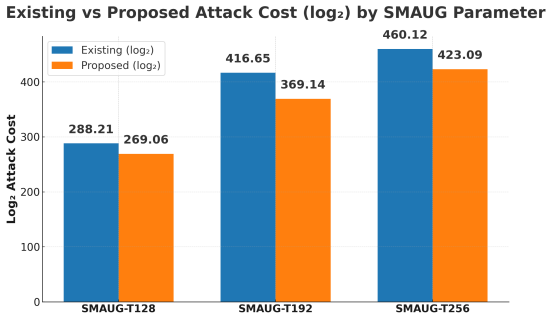

Figure 1: Existing vs Proposed Attack Cost ($\log_2$) by SMAUG Parameter.

5 Conclusion

Our hybrid attack model uses BKZ to transform the LWE problem and a Noisy-Search technique to manage noise. This approach achieves a significantly lower attack complexity on SMAUG parameters than existing methods. For future work, we plan to apply this technique to homomorphic encryption schemes, refine the sign-matching parameters, and develop a more precise probabilistic success model to further validate its practical impact.

References

[1] C. Peikert, A Decade of Lattice Cryptography, Foundations and Trends in Theoretical Computer Science, vol. 10, no. 4, pp. 283–424, 2016.

[2] Jeonchan Ho, Donghoe Heo, Myeonghoon Lee, Changwon Lee, Younglok Choi, Byeongho Chen, and Suhri Kim. Quantum Analysis Techniques for Lattice-Based Post-Quantum Cryptography. In *Journal of The Korea Institute of Information Security and Cryptology*, Vol. 33, No. 1, pp. 26, 2023.