Master's Thesis 要旨

Hardness Estimation of the Generalized Learning with Errors Problem

Dept. of Mathematical Informatics 48176229 Weiyao Wang

Supervisor Prof. Tsuyoshi Takagi

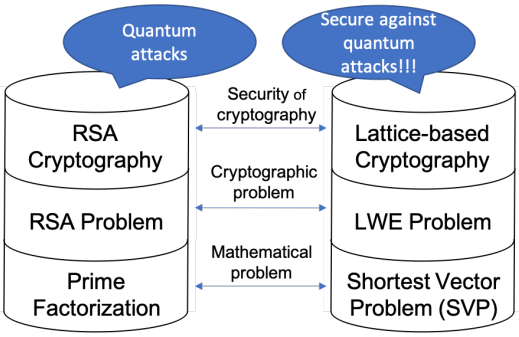

Fig. 1. Three-layer structures of cryptography.

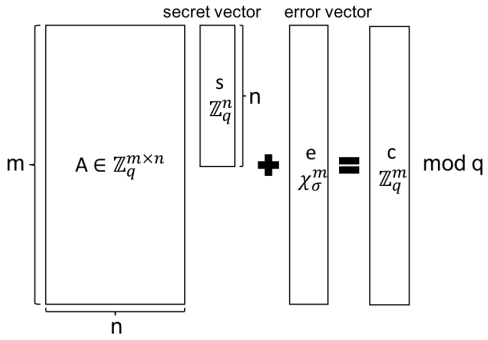

Fig. 2. Learning with Errors (LWE) Problem.

1 Introduction

After Shor proposed a quantum algorithm for computing prime factorization and discrete logarithm in polynomial time, quantum computers are believed to have the potential to attack public key cryptosystems based on these mathematical problems, such as RSA cryptography and elliptic-curve cryptography.

In last few years, with the rapid development of quantum computers, the National Institute of Standards and Technology (NIST) started a project to standardize the next-generation cryptography called the **post-quantum cryptography** (PQC).

Currently, **lattice-based cryptographic** schemes become one of the most promising candidates for the PQC, and has received a remarkable amount of attention. The security of lattice-based cryptography is mainly based on the difficulty of **learning with errors (LWE) problem** proposed by Regev [Reg05], and is eventually based on the hardness of shortest vector problem (SVP). Figure 1 shows the security structures of RSA cryptography and lattice-based cryptography. Since the SVP is in NP-class [Ajt97], the lattice-based cryptography is believed to be secure against quantum attacks.

Therefore, for the purpose of analyzing the security of lattice-based cryptography, **estimating the computational cost of the LWE problem and its related problems** becomes an indispensable topic.

2 Preliminary

2.1 LWE Problem

The LWE problem is defined under the number of samples m, the dimension n, the standard deviation σ and the modulus q.

Let $\mathbb{Z}_q$ denote the ring of integers modulo q and let χ_σ denote a distribution on $\mathbb{Z}_q$ with mean 0 and standard deviation σ. As Figure 2 shows, an LWE problem will keep the secret vector $\mathbf{s}$ and the error vector $\mathbf{e}$ as secrets, and asks us to recover the secret vector $\mathbf{s}$ from a random matrix $\mathbf{A}$ and a vector $\mathbf{c}$ defined as $\mathbf{c} := \mathbf{As} + \mathbf{e} \mod q$.

We call the problem with secret vectors sampled from $\mathbb{Z}_q^n$ the standard LWE problem. Recently, for efficient implementations, several lattice-based schemes with special distributions of secret vectors. Unlike the standard LWE problem, the binary LWE problem samples the secret vectors from $\{0,1\}^n$.

2.2 Solving LWE Problem

Embedding techniques, which reduce the LWE problem to a unique shortest vector problem (uSVP), are believed to be efficient methods to solve the LWE problem.

Kannan's [Kan87] and Bai-Galbraith's [BG14] embedding techniques are usually applied for solving the standard LWE problem and the binary LWE problem, respectively. The uSVP in the lattice with basis constructed by embedding techniques can be solved using the BKZ-β algorithm [Sch87], where β is a parameter positively correlated with its complexity. In this paper, we mainly study the reduction step.

3 Our Motivation and Contribution

As we claim, several lattice-based schemes are based on the LWE problem with special distributions instead of standard and binary LWE problems. However, for the LWE problem, the previous studies have not been generalized to consider all cases. Another fact is that some LWE-based cryptographic schemes, especially key exchange schemes, is constructed by the LWE problem with limited number of samples. In 2017, Bindel et al. [Bin+17] study this case.

Compared with previous works, our interest is to provide **more general estimation of the hardness of LWE**. For this purpose, we define the generalized LWE problem which extend the definition of LWE problem into two aspects. First, the generalized LWE problem samples secret vectors from arbitrary distributions. This extension includes standard and binary settings. Second, we also consider the restric-

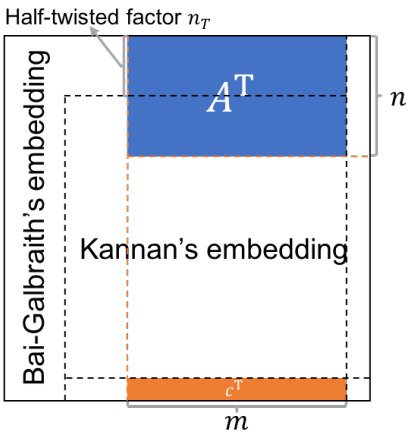

Fig. 3. The lattice basis constructed by half-twisted embedding

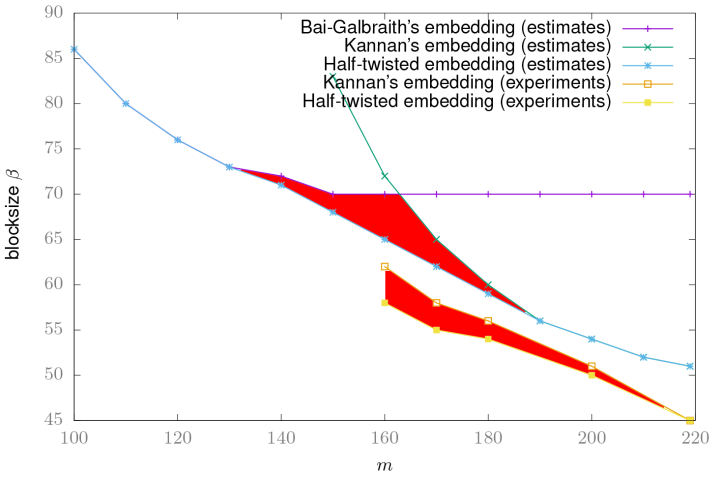

Fig. 4. Experimental result.

tion of the number of LWE samples. Therefore, our work provides a more general estimation of the hardness of LWE.

To solve the generalized LWE problem, we propose the **half-twisted embedding** that combines Kannan's and Bai-Galbraith's embeddings with a half-twisted factor n_T. Figure 3 shows the construction of our half-twisted embedding.

The proposed embedding enable us to analyze the LWE problem in a generic manner by solving the generalized LWE problem. Moreover, it is worth discussing whether the intermediate state of the combined embedding improves the attack. Then, we analyze the half-twisted embedding by using the Alkim et al.'s estimate [Alk+16], and give our hardness estimation of the generalized LWE problem. We also proof that our half-twisted embedding provides an improved reduction under certain parameters.

Finally, we provide sufficient practical results to testify our theoretical study. These results are shown in Figure 4. The horizontal and vertical axes represent the number of samples and the best blocksize β to choose, respectively. We write "estimates" for parameters estimated by Alkim et al.' estimate, and "experiments" for parameters found by experiments. The red area represents benefits from the half-twisted embedding. Although there exists a small gap between numerical and experimental results, the trend of blocksizes change is consistent to our analysis. These results make our half-twisted embedding an important improvement for estimating the security of LWE-based cryptographic schemes.

4 Conclusion

In this paper, we first give an analysis on the LWE problem in a generic manner by using the generalized LWE problem and our proposed half-twisted embedding technique. We find that the half-twisted embedding provides an improved attack on the LWE problems under some certain parameters, which means the proposed method gives a better security estimate on LWE-based cryptographic schemes.

References

[Ajt97] Miklós Ajtai. "The Shortest Vector Problem in L_2 is NP-hard for Randomized Reductions". In: *Electronic Colloquium on Computational Complexity (ECCC)* 4.47 (1997).

[Alk+16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. "Post-quantum Key Exchange—A New Hope". In: *25th USENIX Security Symposium (USENIX Security 16)*. Austin, TX: USENIX Association, 2016, pp. 327–343. ISBN: 978-1-931971-32-4.

[BG14] Shi Bai and Steven D. Galbraith. "Lattice Decoding Attacks on Binary LWE". In: *Information Security and Privacy - 19th Australasian Conference, ACISP 2014*. Vol. 8544. Lecture Notes in Computer Science. Springer, 2014, pp. 322–337.

[Bin+17] Nina Bindel, Johannes A. Buchmann, Florian Göpfert, and Markus Schmidt. "Estimation of the Hardness of the Learning with Errors Problem with a Restricted Number of Samples". In: *IACR Cryptology ePrint Archive, Report 2017/140* (2017).

[Kan87] Ravi Kannan. "Minkowski's Convex Body Theorem and Integer Programming". In: *Math. Oper. Res.* 12.3 (1987), pp. 415–440.

[Reg05] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, STOC 2005*. ACM, 2005, pp. 84–93.

[Sch87] Claus-Peter Schnorr. "A Hierarchy of Polynomial Time Lattice Basis Reduction Algorithms". In: *Theor. Comput. Sci.* 53 (1987), pp. 201–224.