Classification of Lattice-based Fully Homomorphic Encryption from Noisy Polly Cracker*

Rakyong Choi† , Kwangjo Kim‡
Dept. of Computer Science, KAIST

Abstract

Lattices have been used to construct many cryptographic primitives after Ajtai's seminal paper in 1996. The goal of this paper is to design novel cryptographic primitives using lattices, which are still found to be no polynomial time attack by quantum computers. For achieving this, we survey the known lattice-based cryptography and lattice-based fully homomorphic encryption schemes as a first step. We focus on the hard problems in lattice and the relationship between known fully homomorphic encryption scheme and noisy polly cracker model.

Keywords: Post quantum cryptography, Lattice-based cryptography, Learning with errors, Fully homomorphic encryption, Noisy polly cracker

I. Introduction

One challenging issue in modern cryptography is to design novel cryptographic primitives which can be still secure against quantum computer (simply called as "post quantum cryptography"). This challenge becomes very important after Shor's seminal algorithm[1] to solve integer factorization problem(IFP) and discrete logarithm problem(DLP) including elliptic curve DLP in polynomial time was published. This makes our secure systems and applications in a great danger since public key cryptosystem like RSA, ElGamal and elliptic curve cryptosystem can be easily broken by very powerful adversaries with quantum computer. This fact encourages us to make quantum-proof cryptosystems which mean even if quantum computer is exploited to attack the cryptosystem, the security is not to be compromised.

Lattice-based cryptography is known to be secure against quantum computer attack. The popular lattice-based cryptosystems are Ajtai-Dwork cryptosystem by Ajtai and Dwork[2], GGH cryptosystem by Goldreich et al.[3] and NTRU cryptosystem by Hoffstein et al.[4]. Lattices become lots of attention applied for various areas in cryptography such as average-case hardness problem to worst-case hardness problem reduction[5], fully homomorphic encryption (FHE) schemes[6] and multilinear maps[7].

Our aim is to classify the lattice-based FHE schemes from noisy polly cracker. The organization of this paper is as follows: In Chapter II, we define the lattice and hard problems in lattice. Then we review the idea of previous lattice-based cryptosystems and their security model. In Chapter III, we define the FHE schemes and the noisy polly cracker model. After that, we classify known lattice-based FHE schemes from noisy polly

* This research was funded by the MSIP(Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2013.
† thepride@kaist.ac.kr
‡ kkj@kaist.ac.kr

cracker model in Chapter IV. Finally, Chapter V gives a brief conclusion and future work.

II. Lattice-based Cryptography

After seminal work by Ajtai[8] which deals with hard instances of lattice problems, lattices become a powerful tool to make secure cryptographic primitives. We define the lattice and some hard problems in lattice, and we review the previous cryptosystems based on lattice problems.

2.1 Definition and Hard Problems

A lattice is defined as a set of points $L = \{a_1 v_1 + \cdots + a_n v_n | a_i's \text{ are integers}\}$ with n linearly independent vectors $v_1, \cdots, v_n$ in $\mathbb{R}^n$ and the set $\{v_1, \cdots, v_n\}$ is called the basis of L. We say that the basis is good if it is relatively orthogonal to each other and the basis is bad in case they are not that orthogonal.

Lattices behave like a group and among them, there are special lattices called ideal lattices which is similar to ideals in some ring R. Cyclic lattices and anti-cyclic lattices are kind of ideal lattices. We then give some well-known hard problems in lattice.

SVP (Shortest Vector Problem) is given a lattice L, we find the non-zero lattice vector in L which is the closest to the origin. And CVP (Closest Vector Problem) is given a lattice L and a vector w, we find the lattice vector v in L which is closest to the vector w.

Both SVP and CVP are considered as a worst-case hardness problem in lattice. Two popular average-case hardness problems in lattice exist which can be reduced to the worst-case hardness problem in lattice. One is called SIS (Short Integer Solution) problem and is used in one way functions, signature schemes and identification schemes and the other is called LWE (Learning With Errors) problem whose decisional version is used for guaranteeing the security of encryption schemes like IBE and FHE schemes. There are also SIS over rings (R-SIS) problem[9] and LWE over rings (R-LWE) problem[10] but we only state decisional version of LWE problem.

Problem. (DLWE: Decisional version of LWE problem) Given a secret $s \leftarrow \mathbb{Z}_q^n$, polynomially many $a_i \leftarrow \mathbb{Z}_q^n$ and its corresponding noise $n_i \leftarrow \chi$, distinguish $\{A_{s,\chi}\}_i = \{a_i, < a_i, s > + n_i\}_i$ from uniform extraction $\{a_i, b_i\}_i \xleftarrow{\$} \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Indeed, search version of LWE problem which tries to find s is exactly equivalent to this decisional version of LWE problem by using hybrid argument[5]. DLWE over rings (R-DLWE) problem is stated similarly with slight change of the domain.

2.2 Popular Cryptosystems Based on Lattices

We briefly review the idea of some popular public key cryptosystems using lattices.

The first scheme is suggested by Ajtai and Dwork[2]. The idea follows from the Ajtai's previous seminal work in hash functions[8] and Ajtai-Dwork cryptosystem is based on the worst-case hardness problem called unique-SVP, which is the variant of SVP since we find the unique shortest vector. But, since some lattices have no vector satisfying unique-SVP problem, we should determine suitable lattices in advance and hence, this scheme is really inefficient.

Second is GGH cryptosystem[3]. This scheme uses good and bad basis as its private and public key, respectively. The idea is adding a noise vector r to a bad basis for encryption. Then, decryption process is to find the lattice point closest to the ciphertext. But, lattice point should be properly chosen for decryption and the key size should be inefficiently large to prevent the attack using the lattice reduction algorithm.

NTRU cryptosystem[4] remains still secure and practical these days. Its original construction is based on ring structure, but it is later shown that this can be described using lattices with special structure. It is most practical lattice-based cryptography by now. Recently, Stehlé and Steinfold[12] succeeded to give strong security guarantee to NTRU cryptosystem by showing the reduction to standard worst-case problems in ideal lattice.

After Regev's encryption scheme based on LWE problem in 2005[5] was published, the mainstream of lattice-based public key cryptography becomes based on LWE problem or ring version of LWE problem.

III. Fully Homomorphic Encryption and Noisy Polly Cracker

After Gentry's paper in 2009[6], there are huge progress in fully homomorphic encryption area. All previous FHE schemes can be classified as the follow-up research of these schemes - Gentry's original scheme based on ideal lattices[6], van Dijk et al.'s scheme (vDGHV scheme) over the integers[13] and Brakerski and Vaikuntanathan's scheme (BV scheme) based on the LWE problem[14] and Ring-LWE problems[15].

Study on fully homomorphic encryption scheme is very useful in various areas. For example, it can improve the security of clouding system since it delegates processing of user's data without giving away access to user's original data. We explain homomorphic encryption more precisely.

A homomorphic encryption scheme, HE is a scheme whose operation on ciphertexts becomes ciphertext of operation on its corresponding plaintexts. For example, RSA is one well-known homomorphic encryption under multiplication.

And we say an encryption scheme FHE is fully homomorphic if it is a homomorphic encryption for all operations.

For almost all fully homomorphic encryption schemes published, somewhat homomorphic encryption scheme is first constructed with so-called evaluation algorithm and then they use bootstrapping theorem in Gentry's paper to make a fully homomorphic encryption scheme[6]. So, we focus on classifying somewhat homomorphic encryption schemes. But as Gentry did in his thesis, we describe the noisy polly cracker model.

3.1 Polly Cracker[16]

The idea is to take the encryption of zero as polynomials f_i's that evaluate to 0 at the secret key s during the key generation. Encryption is done by summing the plaintext m and the subset sum of such polynomials f_i's and decryption is done by putting the secret key s to the ciphertext c. But this model is very weak since this can be broken by Gaussian elimination. So we need to add the noise into this model.

3.2 Noisy Polly Cracker

In this model, decryption should properly work after adding a noise. The idea is to take the encryption of zero as polynomials f_i's that evaluate to something small and

even or zero at the secret key during the key generation. We assume that messages are with binary forms. Then, encryption process is the same as the polly cracker model but during the decryption process, we must divide it by 2 after putting the secret key into the ciphertext. Since this model cannot be broken by Gaussian elimination or any known attacks in polly cracker model, noisy polly cracker model is more secure than polly cracker model.

IV. Classification of FHE Schemes

We observe three somewhat homomorphic encryption schemes of FHE schemes (vDGHV scheme, BV scheme, GSW scheme) from noisy polly cracker model. Then, we compare those schemes in Table 1 with their special features.

[Table 1] Comparison of three somewhat homomorphic encryption schemes

	vDGHV [13]	BV [14]	GSW [16]
base	integer	lattice	lattice/ideal lattice
security	approximate-GCD	LWE	LWE/Ring-LWE
concept	simple	complex	simple
batch ciphertext	O	O	X
efficiency	Very Low	Very Low	Low
special feature	Add an additional even noise during the encryption	linear ciphertext re-linearization	eigenvector/eigenvalue applicable for making ID-based and Attribute-based encryption

As we can see in Table 1, BV and GSW schemes are based on lattices but vDGHV schemes are based on the integer problem. Normally, since integer is conceptually simpler than lattice, vDGHV scheme is simpler than BV scheme. But GSW scheme becomes simpler by adopting the concept of eigenvalues. On the other hand, GSW scheme does not show the possibility of batch ciphertext, which can be decrypted to many plaintexts. Although all schemes are still not so efficient, GSW scheme is better than other schemes since it can be applied to the problems on ideal lattices as well. Hence, GSW scheme may be the best among FHE schemes from noisy polly cracker model.

V. Conclusion

So far, we review previous lattice-based cryptosystems and several lattice-based FHE schemes. Also, we understand that noisy polly cracker model becomes a great tool to construct new FHE schemes as Gentry did.

For future work, we discuss how to create the batch version of GSW scheme which is the weakness of GSW scheme in Table 1 and we try to find new FHE schemes from other assumptions. Also, we consider how much known FHE schemes are resilient to the key leakage. But to complete this mission, we should discuss more papers about leakage resilient cryptography like the paper by Akavia et al.[18].

[참고문헌]

[1] Peter W Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” *Foundations of Computer Science, 1994 Proceedings, 35th Annual Symposium on,* pp. 124-134. 1994.

[2] Miklós Ajtai and Cynthia Dwork, “A public-key cryptosystem with worst-case/

average-case equivalence", *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pp. 284-293, 1997.

[3] Oded Goldreich, Shafi Goldwasser, and Shai Halevi, "Public-key cryptosystems from lattice reduction problems", *Advances in Cryptology: CRYPTO'97*, pp. 112-131, 1997.

[4] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman, "Ntru: A ring-based public key cryptosystem", *Algorithmic number theory*, pp. 267-288, 1998.

[5] Oded Regev, "On lattices, learning with errors, random linear codes, and cryptography", *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pp. 84-93, 2005.

[6] Craig Gentry, "A fully homomorphic encryption scheme", *Ph. D. thesis*, Stanford University, 2009.

[7] Sanjam Garg, Craig Gentry, and Shai Halevi, "Candidate multilinear maps from ideal lattices", *Advances in Cryptology: EUROCRYPT 2013*, pp. 1-17, 2013.

[8] Miklós Ajtai, "Generating hard instances of lattice problems", *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp 99-108, 1996.

[9] Daniele Micciancio, "Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions", *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pp. 356-365, 2002

[10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev, "On ideal lattices and learning with errors over rings", *Advances in Cryptology: EUROCRYPT 2010*, pp. 1-23, 2010.

[11] Daniele Micciancio and Oded Regev, "Lattice-based cryptography", *Post Quantum Cryptography*, pp. 147-191, 2009.

[12] Damien Stehlé and Ron Steinfeld, "Making NTRU as secure as worst-case problems over ideal lattices", *Advances in Cryptology: EUROCRYPT 2011*, pp. 27-47, 2011.

[13] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan, "Fully homomorphic encryption over the integers", *Advances in Cryptology: EUROCRYPT 2010*, pp. 24-43, 2010.

[14] Zvika Brakerski and Vinod Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) lwe", *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science,* pp. 97-106, 2011.

[15] Zvika Brakerski and Vinod Vaikuntanathan, "Fully homomorphic encryption from ring-lwe and security for key dependent messages", *Advances in Cryptology: CRYPTO 2011*, pp. 505-524, 2011.

[16] Michael Fellows and Neal Koblitz, "Combinatorial cryptosystems galore!", *Contemporary Mathematics 168*, pp. 51-61, 1993

[17] Craig Gentry, Amit Sahai, and Brent Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based", *Advances in Cryptology: CRYPTO 2013*, pp. 75-92, 2013.

[18] Adi Akavia, Sha Goldwasser, and Vinod Vaikuntanathan, "Simultaneous hardcore bits and cryptography against memory attacks", *Theory of Cryptography*, pp. 474-495, 2009.