이학 박사 학위논문

Efficient Instantiation of LWE-based Public-Key Encryption and Commitment Schemes

(LWE 문제 기반 공개키 암호 및 commitment 스킴의 효율적인 인스턴스화)

2017년 2월

서울대학교 대학원

수리과학부

김진수

Efficient Instantiation of LWE-based Public-Key Encryption and Commitment Schemes

(LWE 문제 기반 공개키 암호 및 commitment 스킴의 효율적인 인스턴스화)

지도교수 천정희

이 논문을 이학 박사 학위논문으로 제출함

2017년 10월

서울대학교 대학원

수리과학부

김진수

김진수의 이학 박사 학위논문을 인준함

2017년 12월

위 원 장	김 명 환	(인)
부 위 원 장	천 정 희	(인)
위 원	김 영 훈	(인)
위 원	현 동 훈	(인)
위 원	서 재 홍	(인)

Efficient Instantiation of LWE-based Public-Key Encryption and Commitment Schemes

A dissertation
submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
to the faculty of the Graduate School of
Seoul National University

by

Jinsu Kim

Dissertation Director : Professor Jung Hee Cheon

Department of Mathematical Sciences
Seoul National University

February 2017

Abstract

Efficient Instantiation of LWE-based Public-Key Encryption and Commitment Schemes with application to Threshold Cryptosystems

Jinsu Kim

Department of Mathematical Sciences

The Graduate School

Seoul National University

The Learning with Errors (LWE) problem has been used as a underlying problem of a variety of cryptographic schemes. It makes possible constructing advanced solutions like fully homomorphic encryption, multi linear map as well as basic primitives like key-exchange, public-key encryption, signature. Recently, developments in quantum computing have triggered interest in constructing practical cryptographic schemes. In this thesis, we propose efficient post-quantum public-key encryption and commitment schemes based on a variant LWE, named as spLWE. We also suggest related zero-knowledge proofs and LWE-based threshold cryptosystems as an application of the proposed schemes. In order to achieve these results, it is essential investigating the hardness about the variant LWE problem, spLWE. We describe its theoretical, and concrete hardness from a careful analysis.

Key words: lattice, learning with errors, LWE, sparse, public-key encryption, commitment, threshold cryptosystems

Student Number: 2014-30074

Contents

Abstract **i**

1 Introduction **1**

2 Preliminaries **5**

2.1 Notations 5

2.2 Cryptographic notions 5

2.2.1 Key Encapsulation Mechanism 5

2.2.2 Commitment Scheme 6

2.2.3 Zero-Knowledge Proofs and Σ-Protocols 7

2.3 Lattices 9

2.4 Discrete Gaussian Distribution 11

2.5 Computational Problems 12

2.5.1 SVP 12

2.5.2 LWE and Its Variants 12

2.6 Known Attacks for LWE 13

2.6.1 The Distinguishing Attack 14

2.6.2 The Decoding Attack 15

3 LWE with Sparse Secret, spLWE **16**

3.1 History 16

3.2 Theoratical Hardness 17

3.2.1 A Reduction from LWE to spLWE 18

3.3 Concrete Hardness 21

3.3.1 Dual Attack (distinguish version) 21
3.3.2 Dual Attack (search version) 23
3.3.3 Modified Embedding Attack. 25
3.3.4 Improving Lattice Attacks for spLWE 26

4 LWE-based Public-Key Encryptions 29
4.1 History 29
4.2 spLWE-based Instantiations 31
4.2.1 Our Key Encapsulation Mechanism 31
4.2.2 Our KEM-Based Encryption Scheme 33
4.2.3 Security 35
4.2.4 Correctness 36
4.3 Implementation 37
4.3.1 Parameter Selection 38
4.3.2 Implementation Result 39

5 LWE-based Commitments and Zero-Knowledge Proofs 41
5.1 History 42
5.2 spLWE-based Instantiations 43
5.2.1 Our spLWE-based Commitments 44
5.2.2 Proof for Opening Information 47
5.3 Application to LWE-based Threshold Crytosystems 50
5.3.1 Zero-Knowledge Proofs of Knowledge for Threshold Decryption 50
5.3.2 Actively Secure Threshold Cryptosystems 58

6 Conclusions 63

Abstract (in Korean) 75

Chapter 1

Introduction

With advances in quantum computing, many people in various fields are working on making their information security systems resistant to quantum computing. For example, the National Security Agency (NSA) has announced a plan to change its Suite B guidance [NSA15], and the National Institute of Standards and Technology (NIST) is preparing a standardization of post-quantum crypto for the transition into quantum-resistant cryptography [NIS15]. There have been also substantial support for post-quantum cryptography project from national funding agencies including the PQCRYPTO projects [DL+15] in Europe.

In that sense, lattice-based cryptography is a promising field to conduct practical quantum-resistant research. This is due to the seminal work of Ajtai [Ajt96] who proved a reduction from the worst-case to the average-case for some lattice problems. This means that certain problems are hard on average, as long as the related lattice problems are hard in all cases. This enables provably secure constructions of cryptographic schemes unless all instances of related lattice problems are easy to solve. Another remarkable work in lattice-based cryptography is the introduction of Learning with Errors problem (LWE) by Regev in [Reg09]. This work shows that there exists a quantum reduction from some worst-case lattice problems (the shortest independent vectors problem, the shortest vector problem with a gap) to LWE. With a

strong security guarantee, LWE makes versatile cryptographic constructions possible including fully homomorphic encryption, multi-linear map which are not ever constructed with classical problems. For more details, we refer to the recent survey [Pei16].

In order to increase efficiency on lattice-based cryptographic schemes, ring structured problems such as Learning with Errors over the ring (RLWE) and NTRU [LPR10, Joe98] have received much attentions. A major advantage of using a ring structure is that one can get a relatively smaller key size and faster speed. For that reason, a lot of works about cryptographic schemes with practical implementation have been proposed in RLWE and NTRU settings: public-key encryptions ([DCRVV15, RVM+14, LSR+15]), signatures ([EBB13, DDLL13, GLP12]), key-exchanges ([BCNS15, Sin15]). However, additional ring structures may give some advantages to attackers. As an example, some analyses using the ring structure have been proposed recently. In particular, some NTRU-based fully homomorphic encryptions proved valueless [ABD16, CJL16] and some parameters of RLWE are confirmed to be weak [HKK15, HKK16]. Hence, there are growing concerns about the security gap for ring-structured cryptosystems.

On the other hand, it is reported that LWE-based signatures [DDLL13, GLP12, DEBG+14] achieve good performance without the use of RLWE, and studies of practicality of LWE-based key exchange protocols have been recently started in [BCD+16]. However, less attention has been paid to efficient instantiations of LWE-based cryptosystems, commitments and related protocols. In that sense, proposing of efficient LWE-based public-key encryption and commitment schemes would be an interesting topic in lattice-based cryptography. However, constructing of such schemes, which satisfy both high levels of security and efficiency, is a very non-trivial work and would be a hard task. it requires a suitable balance between security and efficiency to constitute a complete proposal, which considers practical usage of them.

This thesis mainly concerns about efficient instantiations of LWE-based public-key encryption and commitment schemes with a variant of LWE with

sparse secret which is known as spLWE in [CHK+16]. This also enables efficient instantiations of LWE-based zero knowledge protocols as well. In particular, a zero knowledge proof of opening information of commitments, and zero knowledge proofs which can prove some relations among those commitments are suggested. All of theses allow us to make known LWE-based threshold cryptosystems actively secure. In particular, this thesis suggest a threshold version of LWE-based PKE, [48], which has active security, and IND-CCA security in random oracle model.

On the other hand, the use of sparse secret for efficient instantiation has one drawback. It requires relatively larger dimension than that of LWE to maintain security. This is a significant factor for the performance of LWE-based schemes. A important question then arises: How large dimension is needed to maintain security? Our main observation is that the problem of increase in dimension can be relieved by using a small modulus q. Since the security of LWE is proportional to the size of dimension and error rate, smaller modulus leads to larger error rate. In conclusion, we can choose a relatively small modulus q in spLWE-based encryption and commitment schemes from a thoughtful analysis.

In order to describe the conclusion, we first define the variant problem, spLWE, and provide analysis for it: We show that spLWE can be reduced from LWE, which means that the hardness of spLWE can also be based on the worst-case lattice problems. We also extend all known LWE attacks to investigate concrete hardness of spLWE. These are used to select efficient and secure parameters. A remark is that we exclude the parameters which have provable security from our reduction under the consideration about practicality. Our reduction serves to guarantee the hardness of spLWE, but is not tight enough to be useful in setting concrete parameters for our scheme.

Next, we propose post-quantum public-key encryption and commitment schemes with related zero knowledge protocols based on spLWE. More concretely, we suggest an IND-CPA PKE inspired from [Pei14] and its IND-CCA conversion in the quantum random oracle model by applying the modified

Fujisaki-Okamoto conversion of Unruh [TU15]. In commitment case, we give a variety of versions of commitment schemes which are based on a generalization of the LPN-based commitment scheme in [JKPT12]. We also propose a commitment scheme dedicated for zero-knowledge proofs suggested in this thesis. Finally, as a application, we show how to convert our PKE into a threshold cryptosystem with active security.

List of Papers. This thesis contains results of the following articles:

- 김진수, 천정희: 랜덤선형부호의 복호화 문제와 그의 암호학적 응용. 한국통신학회지 (정보와통신), 제32권 제6호, 30-38, 2015.
- Jung Hee Cheon, Kyoo Hyung Han, Jinsu Kim, Changmin Lee, and Yongha Son. A practical post-quantum public-key cryptosystem based on spLWE. In Information Security and Cryptology–ICISC 2016: 19th International Conference, Seoul, South Korea, November 30–December 2, 2016, Revised Selected Papers, volume 10157, page 51. Springer, 2016.
- Jung Hee Cheon, Jinsu Kim, and Jae Hong Seo. spLWE-based Commitment Scheme and Zero-Knowledge Proofs for Lattice-based Threshold Cryptosystems.(In preparation)

Chapter 2

Preliminaries

2.1 Notations

In this thesis, we use upper-case bold letters to denote matrices, and lower-case bold letters for column vectors. For a distribution $\mathcal{D}$, $a \leftarrow \mathcal{D}$ denotes choosing an element according to the distribution of $\mathcal{D}$ and $\mathbf{a} \leftarrow \mathcal{D}^m$ means that each component of $\mathbf{a}$ is sampled independently from $\mathcal{D}$. For a set $\mathcal{A}$, $\mathcal{U}(\mathcal{A})$ means a uniform distribution on the set $\mathcal{A}$ and $a \leftarrow \mathcal{A}$ denotes choosing an element according to the uniform distribution on $\mathcal{A}$. We denote by $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z} = \{0, 1 \cdots, q-1\}$ and $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ the additive group of real numbers modulo 1, and $\mathbb{T}_q$ the a subgroup of $\mathbb{T}$ having order q, consisting of $\{0, \frac{1}{q}, \cdots, \frac{q-1}{q}\}$. The $\langle\ ,\ \rangle$ means the inner product of two vectors and $[\mathbf{x}]_i$ means the its i-th component.

2.2 Cryptographic notions

In this section, we provide cryptographic notions required in this thesis.

2.2.1 Key Encapsulation Mechanism

A *key encapsulation mechanism* (in short, KEM) is a key exchange algorithm to transmit an ephemeral key to a receiver with the receiver's public

key. It differs from encryption scheme where a sender can choose a message. The sender cannot intend to make a specific ephemeral key. A KEM with ciphertext space $\mathcal{C}$ and key space $\mathcal{K}$ consists of polynomial time algorithms Setup, Keygen, Encap(may be randomized), Decap(should be deterministic):

- Params outputs a public parameters.
- Keygen outputs a public encapsulation key pk and secret decapsulation key sk.
- Encap takes an encapsulation key pk and outputs a ciphertext $c \in \mathcal{C}$ and a key $k \in \mathcal{K}$.
- Decap takes a decapsulation key sk and a ciphertext c, and outputs some $k \in \mathcal{K} \cup \{\perp\}$, where $\perp$ denotes decapsulation failure.

2.2.2 Commitment Scheme

Intuitively, commitment schemes can be regard as a digital version of a secure box. Thus anyone can commit to secret values without revealing about their information. Whenever checking for the committed values is needed, he convinces to a verifier that the value claimed by the committer is indeed the value in the secure box. we give a formal definition of commitment schemes [JKPT12], [BKLP15] A commitment scheme with message space $\mathcal{M}$ consists of PPT(probabilistic polynomial time) algorithms Setup, Com, Ver:

- Setup$(1^k, 1^\kappa)$ The setup algorithm Setup takes as input $1^k, 1^\kappa$ for security parameters k, κ, and outputs a public key pk with public parameters.
- Com(pk, m) The commitment algorithm Com takes as input a public key pk, and a message $m \in \mathcal{M}$. It outputs a commitment c, and a reveal value d.

- $\mathsf{Ver}(pk, c, m, d)$ A verification algorithm Ver takes as input a public key pk, a message m, a commitment c, and a reveal value d. It returns 1 or 0 to accept or reject, respectively.

Our commitment scheme satisfies the following security requirements:

- Correctness : The verification algorithm Ver outputs 1 with overwhelming probability for all $m \in \mathcal{M}$ whenever the inputs were computed honestly, i.e.,

$$Pr\left[\mathsf{Ver}(pk, c, m, d) = 1 : pk \leftarrow \mathsf{setup}(1^k, 1^\kappa), (c, d) \leftarrow \mathsf{Com}(pk, m)\right] = 1 - negl(k).$$

- Computational Hiding : Every commitment computationally hides the committed messages. Formally, for every probabilistic polynomial time (PPT) adversary A there is a negligible function $negl(k)$ such that:

$$Pr\left[b = b' : \begin{array}{c} pk \leftarrow \mathsf{Setup}(1^k, 1^\kappa), (m, m', aux) \leftarrow A(pk) \\ b \leftarrow \{0,1\}, (c, d) = \mathsf{Com}(m_b, pk) \\ b' \leftarrow A(c, aux) \end{array}\right] \leq \frac{1}{2} + negl(k)$$

.

- Perfect Binding : Every commitment cannot be opened to different messages. This means that the following holds with overwhelming probability over the choice of the public key $pk \leftarrow Setup(1^k, 1^\kappa)$:

$$(\mathsf{Ver}(pk, c, m, d) = 1) \wedge (\mathsf{Ver}(pk, c, m', d') = 1) \Rightarrow m = m'$$

2.2.3 Zero-Knowledge Proofs and Σ-Protocols

A zero-knowledge proof of knowledge is a two party, prover and verifier (in short, P and V), protocol. In this protocol, P can convince V that he knows some secret information without revealing anything about the secret apart from what is exposed by the claim itself. (For a formal definition, see Bellare and Goldreich's work [BG92]). Proof of knowledges are usually designed by using Σ-protocols [Cra96, Dam10]. Our Zero-knowledge proofs are instantiations of the following definition, which is a generalization of the standard notion of Σ-protocols, and is introduced by Benhamouda et al.

[BCK+14, BKLP15] in order to achieve negligible soundness error probability of their protocols without parallel repetitions.

Definition 2.2.1. Let (P, V) be a two-party protocol, where V is PPT, and let $L, L' \subseteq \{0,1\}^*$ be languages with witness relations $R \subseteq R' \subseteq \{0,1\}^* \times \{0,1\}^*$. Then (P, V) is called a Σ' -protocol for R, R' with completeness error α, challenge set C, public input c and private input w, if and only if it satisfies the following conditions:

- Three-move form:
  - On input (c, w), P computes a commitment t and sends it to V.
  - On input c, V samples a challenge $d \leftarrow C$ and sends it to P.
  - P sends a response s to the verifier.
  - V accepts or rejects the proof depending on the protocol transcript (t, d, s) with public input c. Here, (t, d, s) is called accepting transcript, if the verifier accepts the protocol run with (t, d, s).
- Completeness: Whenever $(c, w) \in R$, V accepts with probability $1 - \alpha$ for some $0 \leq \alpha \leq 1$.
- Special soundness: There exists a PPT algorithm E (the knowledge extractor) which takes two accepting transcripts $(t, d, s), (t, d', s')$ where $d \neq d'$, and outputs w' such that $(c, w') \in R'$.
- Special honest-verifier computational zero-knowledge: There exists a PPT algorithm S (the simulator) taking $c \in L$ and $d \in C$ as inputs, that outputs triples (t, d, s) whose distribution is computationally indistinguishable from accepting protocol transcripts generated by real protocol runs.

We would like to give intuitive remarks regarding the above definition. First, $\alpha > 0$ means even an honest prover sometimes fails to prove knowledge correctly. This is the case of our zero-knowledge proofs like [BCK+14,

BKLP15, BDOP16], which have rejection sampling procedures in their protocols. Second, special soundness property says that even an dishonest prover, which does not know any w's such that $(c, w) \in R'$ can knows a witness w_0 such that $(c, w_0) \in R'$ from the given two accepting transcripts. Thus, an dishonest prover can answer correctly at most one challenge, i.e. the soundness error is $1/|C|$. ([Dam10]) Finally, the existence of a such simulator in zero-knowledge property means the corresponding real protocol reveals no information about w. Unlike real protocols, a challenge d is determined in advance before fixed a commitment t in the proof. This is possible by rewinding the random tape of a honest-verifier.

2.3 Lattices

A *lattice* $L \subseteq \mathbb{R}^m$ is a set of integer linear combinations of a $\{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$ which is a subset of independent column vectors in $\mathbb{R}^m$,

$$L = \{\sum_{i=1}^{n} a_i \mathbf{b}_i : a_i \in \mathbb{Z}\}$$

The set of vectors $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$, and its matrix form $\mathbf{B}$ are called a basis, and basis matrix of L respectively. Two bases matrices $\mathbf{B}_1$ and $\mathbf{B}_2$ describe the same lattice, if and only if $\mathbf{B}_2 = \mathbf{B}_1\mathbf{U}$, where $\mathbf{U}$ is a unimodular matrix, i.e. $\det(U) = \pm 1$, $U \in \mathbb{Z}^{m \times m}$. Dimension of a lattice is defined as cardinality of a basis, i.e. $n = \dim(L)$. If $n = m$, we call lattice L to a full rank lattice. A sublattice is a subset $L' \subset L$ which is also a lattice. We define determinant (volume) of L by

$$\det(L) := \sqrt{\det(\mathbf{B}^T\mathbf{B})}$$

A length of the shortest vector in a lattice $L(\mathbf{B})$ is denoted by $\lambda_1(L(\mathbf{B}))$. More generally, the *i-th successive minima* $\lambda_i(L)$ is defined as the smallest radius r such that $\dim(\mathrm{span}(L \cap B(r))) \geq i$ where $B(r)$ is a n dimensional ball with radius r. There exist several bounds and estimations for the length of the shortest vector in a lattice.

- Minkowski's first theorem: $\lambda_1(L(\mathbf{B})) \leq \sqrt{n}(\det L(\mathbf{B}))^{1/n}$
- Gaussian heuristic: $\lambda_1(L(\mathbf{B})) \approx \sqrt{\frac{n}{2\pi e}}\det(L(\mathbf{B}))^{1/n}$.

The *dual lattice* of L, denoted $\bar{L}$, is defined to be $\bar{L} = \{\mathbf{x} \in \mathbb{R}^n : \forall \mathbf{v} \in L, \langle \mathbf{x}, \mathbf{v} \rangle \in \mathbb{Z}\}$. In this thesis, we mainly deal with q-ary integer lattices when solving LWE problem. A q-ary lattice is a full-ranked lattice Λ such that $q\mathbb{Z}^m \subseteq \Lambda \subseteq \mathbb{Z}^m$. Such q-ary lattices with a basis matrix $\mathbf{A} \in \mathbb{Z}^{m \times n}$ are denoted by,

$$\Lambda_q(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m | \exists \mathbf{y} \in \mathbb{Z}^n : \mathbf{x} = \mathbf{A}\mathbf{y} \bmod q\}$$

$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m | \mathbf{A}\mathbf{x} = 0 \bmod q\}$$

We would like to note that given a matrix $\mathbf{A} \in \mathbb{Z}^{mn}$, one can find a basis of $\Lambda_q(\mathbf{A})$. With high probability, the determinant of a q-ary lattice is q^{m-n} when m is relatively larger than n.

We recall the Gram-Schmidt orthogonalization that is closely related with lattice basis reduction. The Gram-Schmidt algorithm computes orthogonal vectors $\{\mathbf{b}_1^*, \ldots, \mathbf{b}_m^*\}$ iteratively as follows:

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j<i} \mu_{i,j}\mathbf{b}_j^* \text{ where } \mu_{i,j} = \frac{\mathbf{b}_i \cdot \mathbf{b}_j^*}{\mathbf{b}_j^* \cdot \mathbf{b}_j^*}.$$

The goal of lattice (basis) reduction is to find a good basis for a given lattice. A basis is considered good, when the basis vectors are almost orthogonal and correspond approximately to the successive minima of the lattice. Performance of lattice reduction algorithms is evaluated by the *root Hermite factor* δ_0 defined by

$$\delta_0 = (||\mathbf{v}||/\det(L)^{1/n})^{1/n}$$

where $\mathbf{v}$ is the shortest vector of the reduced output basis.

2.4 Discrete Gaussian Distribution

For given $s > 0$, a *discrete Gaussian distribution* over a lattice $L \subseteq \mathbb{R}^m$ centered at $\mathbf{v} \in \mathbb{R}^m$ is defined as $D_{L,\mathbf{v},s}(\mathbf{x}) = \rho_{\mathbf{v},s}(\mathbf{x})/\rho_{\mathbf{v},s}(L)$ for any $\mathbf{x} \in L$, where

$$\rho_{\mathbf{v},s}(\mathbf{x}) = \exp(-\pi\|\mathbf{x}-\mathbf{v}\|^2/s^2) \text{ and } \rho_s(L) := \sum_{\mathbf{x}\in L} \rho_{\mathbf{v},s}(\mathbf{x}).$$

We note that the standard deviation is $\sigma = s/\sqrt{2\pi}$. Alternatively, we can represent the Gaussian function $\rho_{\mathbf{v},s}(\mathbf{x})$ as $\rho_{\mathbf{v},\sigma}(\mathbf{x})$ then the discrete Gaussian distribution $D_{L,\mathbf{v},s}(\mathbf{x})$ is defined as $D_{L,\mathbf{v},s}(\mathbf{x}) = D_{L,\mathbf{v},\sigma}(\mathbf{x}) = \rho_{\mathbf{v},\sigma}(\mathbf{x})/\rho_{\mathbf{v},\sigma}(L)$ where

$$\rho_{\mathbf{v},\sigma}(\mathbf{x}) = \exp(-\|\mathbf{x}-\mathbf{v}\|^2/2\sigma^2) \text{ and } \rho_{\mathbf{v},\sigma}(L) := \sum_{\mathbf{x}\in L} \rho_{\mathbf{v},\sigma}(\mathbf{x}).$$

When $L = \mathbb{Z}$, $\mathbf{v} = 0$, we omit the subscript L, $\mathbf{v}$ respectively and denote $D_{\mathbb{Z}^m,\mathbf{v},\sigma}(\mathbf{x})$ by $D^m_{\mathbf{v},\sigma}(\mathbf{x})$. We collect some useful lemmas related to a discrete Gaussian distribution.

Lemma 2.4.1 ([Ban95], Lemma 2.4)**.** *For any real $s > 0$ and $T > 0$, and any vector $\boldsymbol{x} \in \mathbb{R}^n$, we have*

$$Pr[|\langle \mathbf{x}, D^n_{\mathbb{Z},s}\rangle| \geq T \cdot s\|\mathbf{x}\|] < 2\exp(-\pi \cdot T^2).$$

Lemma 2.4.2 ([Reg05], Corollary 3.10)**.** *Let L be an n-dimensional lattice, let $\boldsymbol{u}, \boldsymbol{z} \in \mathbb{R}^n$ be arbitrary vectors, and let r, α be positive real numbers. Assume that $(1/r^2 + (\|\boldsymbol{z}/\alpha\|)^2)^{-1/2} \geq \eta_\epsilon(\Lambda)$ for some $\epsilon < 1/2$. Then the distribution of $\langle \boldsymbol{z}, \boldsymbol{v}\rangle + e$ where $\boldsymbol{v} \leftarrow D_{L+\boldsymbol{u},r}$ and $e \leftarrow D_\alpha$ is within statistical distance 4ϵ of D_β for $\beta = \sqrt{(r\|\boldsymbol{z}\|)^2 + \alpha^2}$.*

Lemma 2.4.3 ([GPV08], Lemma 3.1)**.** *For any $\epsilon > 0$ and an n-dimensional lattice Λ with basis matrix $\boldsymbol{B}$, the smoothing parameter $\eta_\epsilon(\Lambda) \leq \|\tilde{\boldsymbol{B}}\| \ln(2n(1+1/\epsilon))/\pi$ where $\|\tilde{\boldsymbol{B}}\|$ denotes the length of the longest column vector of $\tilde{\boldsymbol{B}}$ which*

is the Gram-Schmidt orthogonalization of $\boldsymbol{B}$.

Lemma 2.4.4 ([Lyu12], Lemma 4.4)**.** *Tail Bounds of discrete Gaussians:*

- *For any* $k > 0$, $Pr\left[|z| > k\sigma; z \leftarrow D_\sigma\right] \leq 2\exp(-k^2/2)$.
- *For any* $k > 1$, $Pr\left[\|\mathbf{z}\| > k\sigma\sqrt{m}; \mathbf{z} \leftarrow D_\sigma^m\right] < k^m \exp(m - mk^2/2)$.

2.5 Computational Problems

2.5.1 SVP

The Shortest Vector Problem(SVP) is one of well-known lattice problem. The goal is to find a shortest non-zero lattice vector, given a basis of a lattice Λ. An important variant is the Unique Shortest Vector Problem (uSVP). In this problem, one knows in advance that $\lambda_2(\Lambda) > \alpha\lambda_1(\Lambda)$ for a fixed factor $\alpha > 1$ and is called $\alpha-$uSVP. A detailed analysis with experiments about uSVP is conducted by Albrecht et al. [AFG13]. They claimed that the attack succeeds with high probability if

$$\frac{\lambda_2(\Lambda)}{\lambda_1(\Lambda)} \geq \tau\delta^m$$

where τ is a constant depending on a lattice reduction algorithm used. They also show $\tau \approx 0.4$ for the BKZ case. For random lattices, the attack succeeds if

$$\tau\delta^m \leq \frac{\sqrt{m}\det(\Lambda)^{1/m}}{\sqrt{2\pi e}\lambda_1(\Lambda)}$$

from the Gaussian heuristic.

2.5.2 LWE and Its Variants

For integers $n, q \geq 1$, a vector $\mathbf{s} \in \mathbb{Z}_q^n$, and a distribution ϕ on $\mathbb{R}$, let $A_{q,\mathbf{s},\phi}$ be the distribution of the pairs $(\mathbf{a}, b = \langle \mathbf{a}, \mathbf{s}\rangle + e) \in \mathbb{T}_q^n \times \mathbb{T}$, where $\mathbf{a} \leftarrow \mathbb{T}_q^n$ and $e \leftarrow \phi$.

Definition 2.5.1 (Learning with Errors (LWE))**.** For integers $n, q \geq 1$, an error distribution ϕ over R, and a distribution $\mathcal{D}$ over $\mathbb{Z}_q^n$, $\mathsf{LWE}_{n,q,\phi}(\mathcal{D})$, is to distinguish (given arbitrarily many independent samples) the uniform distribution over $\mathbb{T}_q^n \times \mathbb{T}$ from $A_{q,\mathbf{s},\phi}$ with a fixed sample $\mathbf{s} \leftarrow \mathcal{D}$.

We note that a search variant of LWE is the problem of recovering $\mathbf{s}$ from $(\mathbf{a}, b) = (\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \in \mathbb{T}_q^n \times \mathbb{T}$ sampled according to $A_{q,\mathbf{s},\phi}$, and these are also equivalently defined on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ rather than $\mathbb{T}_q^n \times \mathbb{T}$ for discrete (Gaussian) error distributions over $\mathbb{Z}_q$. Let $\mathsf{LWE}_{n,m,q,\phi}(\mathcal{D})$ denotes the case when the number of samples are bounded by $m \in \mathbb{N}$. We simply denote $\mathsf{LWE}_{n,q,\phi}$ when the secret distribution $\mathcal{D}$ is $\mathcal{U}(\mathbb{Z}_q^n)$. In many cases, ϕ is a (discrete) Gaussian distribution so we simply denote by $\mathsf{LWE}_{n,m,q,s}$ instead of $\mathsf{LWE}_{n,m,q,\phi}$. We remark that in the above definition, $A_{q,\mathbf{s},\phi}$ can be substituted by the distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ for a distribution ϕ on $\mathbb{Z}$ by sampling $\mathbf{a} \leftarrow \mathbb{Z}_q^n$. Clearly these two problems are equivalent.

Let $\mathbf{z} = \mathbf{A}^t\mathbf{s} \bmod q \in \Lambda_q(\mathbf{A})$. The Search-$\mathsf{LWE}$ problem naturally can be considered as a bounded distance decoding problem (BDD) in $\Lambda_q(\mathbf{A})$ with $\mathbf{b} = \mathbf{z} + \mathbf{e} \bmod q$. If one can solve the BDD problem and recover $\mathbf{z}$, then finding $\mathbf{s}$ is easy.

We denote binLWE by the LWE problem whose secret vector is sampled from uniform distribution over $\{0,1\}^n$. For a set $X_{n,\rho,\theta}$ which consists of the vectors $\mathbf{s} \in \mathbb{Z}^n$ whose nonzero components are in $\{\pm 1, \pm 2, \pm 4, \cdots, \pm\rho\}$, and the number of nonzero components is θ, we write $\mathsf{spLWE}_{n,m,q,s,\rho,\theta}$ as the problem $\mathsf{LWE}_{n,m,q,s}(\mathcal{U}(X_{n,\rho,\theta}))$. We also consider a variant of LWE, $\mathsf{LWE}_{n,q,\leq\alpha}$, in which the amount of noise is some unknown $\beta \leq \alpha$ as in [BLP+13]. Similarly, $\mathsf{spLWE}_{n,q,\leq\alpha,\rho,\theta}$ can be defined by the same way.

2.6 Known Attacks for LWE

There are a number of known attacks for LWE. One of those attack was introduced by Arora and Ge [AG11]. This attack is an algebraic attack, which requires a lot of LWE samples to be applied. A combinatorial approach for

solving LWE was introduced in [BKW03]. This attack is a generalization of LPN solving algorithms, and is called BKW attack. It is known that the algorithm also requires too many samples. Thus, commonly these attacks are not considered for parameter selection.

Unlike these attacks, lattice based attacks are usually considered as practical attacks and used for parameter selections. One of a basic lattice based approach is the distinguishing attack. In [LP11], a direct decoding attack is also proposed, and showed that it is more powerful than the distinguishing attack. several variants of the decoding attack, including the enumeration attack are also proposed [LN13]. A embedding approach to reduce LWE to the u-SVP is also investigated in [AFG13, BG14b] as mentioned in section 2.5.1.

2.6.1 The Distinguishing Attack

The goal of this attack is to distinguish whether the vector $\mathbf{b}$ sampled from an LWE distribution or from the uniform distribution over $\mathbb{Z}_q^m$, when $(\mathbf{A}, \mathbf{b})$ is given. The attack first finds a small vector in the dual lattice

$$\Lambda_q(\mathbf{A})^\perp = \{\mathbf{v} \in \mathbb{Z}_m | \mathbf{A}\mathbf{v} = 0 \bmod q\}$$

. Then, it checks whether $|\langle \mathbf{v}, \mathbf{b} \rangle|$ is small or not. If $\mathbf{b}$ was sampled uniformly random, $\langle \mathbf{v}, \mathbf{b} \rangle$ is uniformly random in $\mathbb{Z}_q$, thus the value is not small in general. In case $\mathbf{b}$ comes from an LWE distribution, $\langle v, b \rangle = \langle e, b \rangle$ is small when $\mathbf{v}$ is small enough. A typical setting is that the distinguisher outputs "LWE sample" if the absolute value of the inner product is smaller than $q/4$, and "uniform sample" otherwise. The following lemma says that the distinguishing advantage is bounded by $\exp(-\pi(\|\mathbf{v}\|s/q)^2)$ for any setting.

Lemma 2.6.1 ([LP11])**.** *Given $\mathsf{LWE}_{n,m,q,s}$ samples and a vector $\boldsymbol{v}$ of length $\|\boldsymbol{v}\|$ in the lattice $L = \{\boldsymbol{w} \in \mathbb{Z}_q^m : \boldsymbol{w}^T \boldsymbol{A} \equiv 0 \bmod q\}$, the advantage of distinguishing $\langle \boldsymbol{v}, \boldsymbol{e} \rangle$ from uniform random is close to $\exp(-\pi(\|\boldsymbol{v}\|s/q)^2)$.*

2.6.2 The Decoding Attack

A natural approach for LWE is that one solves a CVP derived from LWE instances. More specifically, since $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$, we get $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} + q\mathbf{x}$ for some integer vector $\mathbf{x} \in \mathbb{Z}^m$. Thus, by solving the CVP problem in the lattice $\Lambda_q(\mathbf{A})$ with target vector $\mathbf{b}$, one can get the vector $\mathbf{A}\mathbf{s} + q\mathbf{x}$, and $\mathbf{s}$.

The known algorithms to solve CVP are the nearest-plane algorithm introduced by Babai [Bab86], its generalizations [LP11] or enumeration [LN13]. The performance of all these algorithms only depends on the error distribution of LWE. Therefore, we expect that there are no improved version of such attacks for sparse secret variants.

Chapter 3

LWE with Sparse Secret, spLWE

In this chapter, we show the theoratical hardness of spLWE via a security reduction. This implies that spLWE is as hard as worst-case lattice problems. For that, we provide a reduction from LWE to spLWE by generalizing the techniques used in [BLP$^+$13]. For concrete hardness, we also present modified attacks for spLWE, which exploit the sparsity of secret vectors from all known existing attacks for LWE and binLWE [BG14, BGPW16].

3.1 History

In 2005, Regev provide a quantum reduction from worst-case lattice problems to the average case problem, LWE in [Reg05]. In 2010, Goldwasser et al. gave a reduction from the standard LWE to LWE with binary secret in [GKPV10]. In 2013, a classical version of reductions for LWE are proved, and the reduction for LWE with binary secret is more refined in [BLP+13]. The worst case results for LWE with uniformly distributed error are also reported in [MP13]. The reduction for LWE with uniformly distributed error requires a restriction on the number of samples. On the other hand, the result for binLWE has no limitation on the number of samples.

The hardness of binLWE was proved to show robustness of the LWE in terms of leakage-resilient cryptography in [GKPV10]. The main idea of the reduction is that they substituted a uniformly random matrix $\mathbf{A}$ in binLWE by many bunches of LWE samples. In other words, the binLWE samples $(\mathbf{A}, \mathbf{As}+\mathbf{e})$ is converted to $(\mathbf{BC}+\mathbf{Z}, \mathbf{BCs}+\mathbf{Zs}+\mathbf{e})$ where $\mathbf{A} \leftarrow \mathbb{Z}_q^{m\times n}, \mathbf{s} \leftarrow \{0,1\}^n, \mathbf{e} \leftarrow D_{\mathbb{Z},\sigma}^m, \mathbf{B} \leftarrow \mathbb{Z}_q^{m\times l}, \mathbf{C} \leftarrow \mathbb{Z}_q^{l\times n}, \mathbf{Z} \leftarrow D_{\mathbb{Z},\beta}^{m\times n}$. The latter component $\mathbf{BCs} + \mathbf{Zs} + \mathbf{e}$ can be viewed as LWE samples from that $\mathbf{Cs}$ is uniform random by the leftover hash lemma, and a small perturbation of the Gaussian distribution $\mathbf{Zs}+\mathbf{e}$ is close to another Gaussian one. Finally, $(\mathbf{BC}+\mathbf{Z}, \mathbf{BCs}+\mathbf{Zs}+\mathbf{e})$ is computationally indistinguishable from uniform random under the standard LWE assumption and by standard hybrid lemma. This reduction was improved in [BLP+13]. In this reduction, the standard deviation β is only bounded by $\sqrt{10n}\sigma$. The refined reduction was introduced to show classical hardness of LWE. That was accomplished by considering the part $\mathbf{Zs}+\mathbf{e}$ in continuous case.

3.2 Theoratical Hardness

As a prior work, we recall some definitions for variants of LWE and some notion, which were introduced in [BLP+13] to show the reduction between binLWE and LWE.

Definition 3.2.1 ("first-is-errorless" LWE)**.** For integers $n, q \geq 1$ and an error distribution ϕ over $\mathbb{R}$, the "first-is-errorless" variant of the LWE problem is to distinguish between the following two scenarios. In the first, the first sample is uniform over $\mathbb{T}_q^n \times \mathbb{T}_q$ and the rest are uniform over $\mathbb{T}_q^n \times \mathbb{T}$. In the second, there is an unknown uniformly distributed $\mathbf{s} \in \{0, \ldots, q-1\}^n$, the first sample we get is from $A_{q,\mathbf{s},\{0\}}$ (where $\{0\}$ denotes the distribution that is deterministically zero) and the rest are from $A_{q,\mathbf{s},\phi}$.

Definition 3.2.2 (extLWE)**.** For integers $n, m, q, t \geq 1$, a set $X \subseteq \mathbb{Z}^m$, and a distribution χ over $\frac{1}{q}\mathbb{Z}^m$, the $\mathsf{extLWE}_{n,m,q,\chi,X}$ is as follows. The algorithm gets to choose $\mathbf{x} \in X$ and then receives a tuple $(\mathbf{A}, (\mathbf{b}_i)_{i\in[t]}, (\langle \mathbf{e}_i, \mathbf{x}\rangle)_{i\in[t]}) \in$

$\mathbb{T}_q^{n\times m} \times (\mathbb{T}_q^m)^t \times (\frac{1}{q}\mathbb{Z})^t$. Its goal is to distinguish between the following two cases. In the first, $A \in \mathbb{T}_q^{n\times m}$ is chosen uniformly, $\mathbf{e}_i \in \frac{1}{q}\mathbb{Z}^m$ are chosen from χ, and $\mathbf{b}_i = \mathbf{A}^T\mathbf{s}_i + \mathbf{e}_i \bmod 1$ where $\mathbf{s}_i \in \{0,\ldots,q-1\}^n$ are chosen uniformly. The second case is identical, except that the $\mathbf{b}_i$ are chosen uniformly in $\mathbb{T}_q^m$ independently of everything else.

Definition 3.2.3 (Quality of a set)**.** A set $X \subset \mathbb{Z}^m$ is said of quality ξ if given any $\mathbf{x} \in X$, we can efficiently find a unimodular matrix $U \in \mathbb{Z}^{m\times m}$ such that if $U' \in \mathbb{Z}^{m\times(m-1)}$ is the matrix obtained from U by removing its leftmost column then all of the columns of U' are orthogonal to $\mathbf{z}$ and its largest singular value is at most ξ. It denoted by $Qual(X)$.

We give a lemma to show a reduction to spLWE from the standard LWE in section 4.1.

Lemma 3.2.1. *The quality of a set $X \subseteq \{0, \pm1, \pm2, \ldots, \pm\rho\}^m$, $\rho = 2^l$ is bounded by $1 + \sqrt{\rho}$.*

Proof. Let $\mathbf{x} \in X$ and without loss of generality, we assume leftmost k components of $\mathbf{x}$ are nonzero, remainings are zero, and $|[\mathbf{x}]_i| \le |[\mathbf{x}]_{i+1}|$ for nonzero components after reordering. We have $[\mathbf{x}]_{i+1} = \pm 2^{t_i}[\mathbf{x}]_i$ for some $t_i \le l$. Now consider the upper bidiagonal matrix $\mathbf{U}$ whose diagonal is all 1 and whose diagonal above the main diagonal is $\mathbf{y} \in \mathbb{Z}^{m-1}$ such that $[\mathbf{x}]_{i+1} - [\mathbf{y}]_j[\mathbf{x}]_i = 0$ for $1 \le j \le k-1$, and rightmost $(m-k)$ components of $\mathbf{y}$ are 0. Since $[\mathbf{x}]_{i+1} = \pm 2^{t_i}[\mathbf{x}]_i$, it follows that $[\mathbf{y}]_j$ is 2^{t_j} or -2^{t_j}. Then $\mathbf{U}$ is clearly unimodular ($\det(\mathbf{U}) = 1$) and all the columns except the first one are orthogonal to $\mathbf{x}$. Moreover, by the triangle inequality, we can bound the norm (the largest singular value) of $\mathbf{U}$ by the sum of that of the diagonal 1 matrix and the off-diagonal matrix of which clearly have norm at most $\sqrt{\rho}$. □

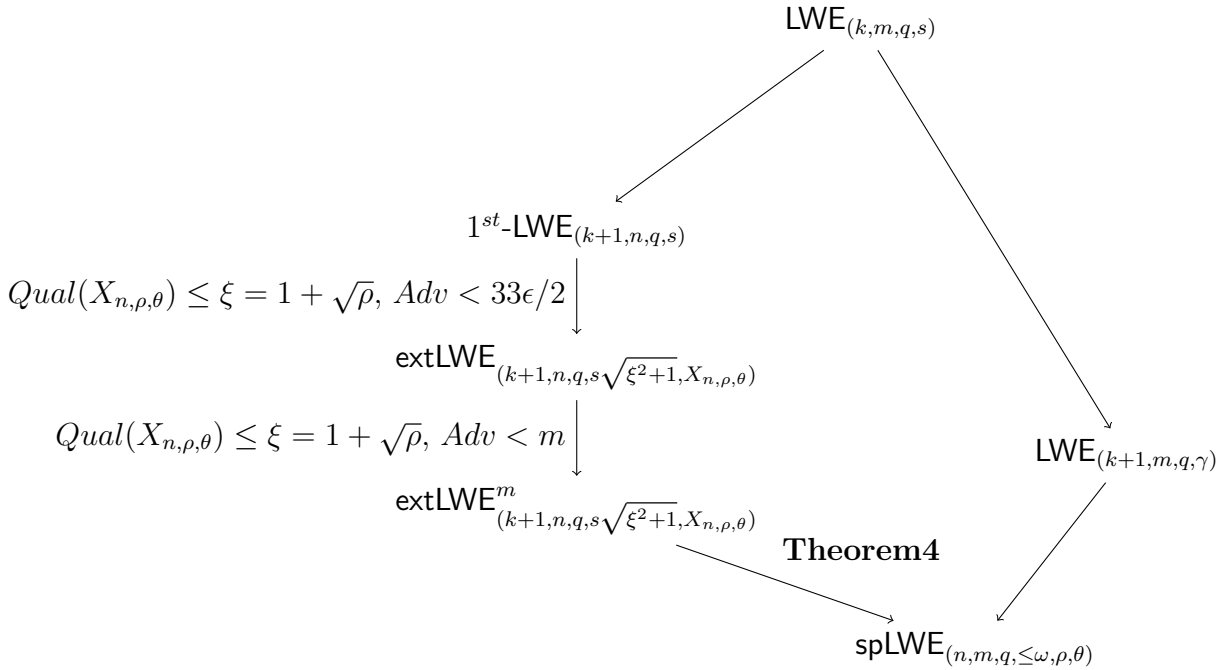
3.2.1 A Reduction from LWE to spLWE

To show our reduction for spLWE, we need extLWE^m problem whose hardness was proved in [BLP+13]. They showed that for a set X of quality ξ,

there exists a reduction from $\mathsf{LWE}_{k,m,q,s}$ to $\mathsf{extLWE}^{m}_{(k+1,n,q,\beta=\sqrt{s^2\xi^2+s^2},X)}$. (Here, $n \leq m$) Based on a reduction from LWE to extLWE in [BLP+13], we prove a reduction of spLWE as shown in the diagram below. Here, ω, γ and s are constant satisfying the following:

$$\omega = s\rho\sqrt{2\theta(2+2\sqrt{\rho}+\rho)},\ \gamma = \rho s\sqrt{\theta(2+2\sqrt{\rho}+\rho)},\ \beta \geq \frac{(\ln(2n(1+1/\epsilon))/\pi)^{1/2}}{q}.$$

Because $\mathsf{Qual}(X_{n,\rho,\theta}) < 1+\sqrt{\rho}$ by lemma 3.2.1, $\mathsf{extLWE}_{k+1,n,q,s\sqrt{(1+\sqrt{\rho})^2+1},X_{n,\rho,\theta}}$ is hard based on the hardness of $\mathsf{LWE}_{k,n,q,s}$. Following theorem shows that $\mathsf{spLWE}_{n,m,q,\leq\omega,\rho,\theta}$ problem can be hard based on the hardness of $\mathsf{LWE}_{k,m,q,\gamma}$ and $\mathsf{extLWE}_{n,m,q,s\sqrt{(1+\sqrt{\rho})^2+1},X_{n,\rho,\theta}}$ for the $\omega, \gamma > 0$ as above. In particular, if $\log\left(\binom{n}{\theta}\cdot(2l+2)^{\theta}\right) \geq k\log q + 2\log(1/\delta)$, there is a reduction from $\mathsf{LWE}_{k,m,q,s}$ to $\mathsf{spLWE}_{n,m,q,\leq\omega,\rho,\theta}$.



Theorem 3.2.1. *Let k, n, m, $\rho = 2^l$, θ, $q \in \mathbb{N}$, $\epsilon \in (0, 1/2)$, and $\delta, \omega, \beta, \gamma > 0$*

such that

$$\beta \geq \sqrt{2\ln(2n(1+1/\epsilon))/\pi}/q \text{ where } \beta = s\sqrt{(1+\sqrt{\rho})^2+1},$$

$$\omega = \rho\beta\sqrt{2\theta},\ \gamma = \rho\beta\sqrt{\theta},\ \log\left(\binom{n}{\theta}\cdot(2l+2)^{\theta}\right) \geq k\log q + 2\log(1/\delta).$$

There exist (two) reductions to $\mathsf{spLWE}_{n,m,q,\leq\omega,\rho,\theta}$ *from* $\mathsf{extLWE}^{m}_{k,n,q,\beta,X_{n,\rho,\theta}}$, $\mathsf{LWE}_{k,m,q,\gamma}$. *An advantage of* $\mathcal{A}$ *for* $\mathsf{spLWE}_{n,m,q,\leq\omega,\rho,\theta}(\mathcal{D})$ *is bounded as follows:*

$$Adv[\mathcal{A}] \leq 2Adv[\mathcal{C}_1] + Adv[\mathcal{C}_2] + 4m\epsilon + \delta$$

for the algorithms (distinguishers) of $\mathsf{extLWE}^{m}_{k,n,q,\beta,X_{n,\rho,\theta}}$, $\mathsf{LWE}_{k,m,q,\gamma}$, $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *respectively.*

Proof. The proof follows by a sequence of distribution to use hybrid argument as stated in [BLP+13]. We take into account the following six distributions:

H_0:= $\{(\mathbf{A}, \mathbf{b} = \mathbf{A}^T\mathbf{x} + \mathbf{e}) \mid \mathbf{A} \leftarrow \mathbb{T}_q^{n\times m}, \mathbf{x} \leftarrow X_{n,\rho,\theta}, \mathbf{e} \leftarrow D^m_{\alpha'}$ for $\alpha' = \sqrt{\beta^2\|\mathbf{x}\|^2+\gamma^2} \leq \rho\beta\sqrt{2\theta} = \omega\}$.

H_1:=$\{(\mathbf{A}, \mathbf{A}^T\mathbf{x} - \mathbf{N}^T\mathbf{x} + \hat{\mathbf{e}} \bmod 1) \mid \mathbf{A} \leftarrow \mathbb{T}_q^{n\times m}, \mathbf{x} \leftarrow X, \mathbf{N} \leftarrow D^{n\times m}_{\frac{1}{q}\mathbb{Z},\beta}, \hat{\mathbf{e}} \leftarrow D^m_\gamma\}$.

H_2:= $\{(q\mathbf{C}^T\mathbf{B} + \mathbf{N}, q\mathbf{B}^T\mathbf{C}\mathbf{x} + \hat{\mathbf{e}}) \mid \mathbf{B} \leftarrow \mathbb{T}_q^{k\times m}, \mathbf{C} \leftarrow \mathbb{T}_q^{k\times n},\ \mathbf{x} \leftarrow X, \mathbf{N} \leftarrow D^{n\times m}_{\frac{1}{q}\mathbb{Z},\beta}, \hat{\mathbf{e}} \leftarrow D^m_\gamma\}$.

H_3:= $\{(q\mathbf{C}^T\mathbf{B} + \mathbf{N}, \mathbf{B}^T\mathbf{s} + \hat{\mathbf{e}}) \mid \mathrm{s} \leftarrow \mathbb{Z}_q^k,\ \mathbf{B} \leftarrow \mathbb{T}_q^{k\times m}, \mathbf{C} \leftarrow \mathbb{T}_q^{k\times n},\ \mathbf{N} \leftarrow D^{n\times m}_{\frac{1}{q}\mathbb{Z},\beta}, \hat{\mathbf{e}} \leftarrow D^m_\gamma\}$.

H_4:= $\{(q\mathbf{C}^T\mathbf{B} + \mathbf{N}, \mathbf{u}) \mid \mathbf{u} \leftarrow \mathbb{T}^m,\ \mathbf{B} \leftarrow \mathbb{T}_q^{k\times m}, \mathbf{C} \leftarrow \mathbb{T}_q^{k\times n},\ \mathbf{N} \leftarrow D^{n\times m}_{\frac{1}{q}\mathbb{Z},\beta}\}$.

H_5:= $\{(\mathbf{A}, \mathbf{u}) \mid \mathbf{A} \leftarrow \mathbb{T}_q^{n\times m}, \mathbf{u} \leftarrow \mathbb{T}^m\}$.

Let $\mathcal{B}_i$ be the distinguisher for the distributions between H_i and H_{i+1} for $0 \leq i \leq 4$. There are some efficient transformations from the distributions $(\mathbf{C}, \mathbf{A}, \mathbf{N}^T\mathbf{z}), (\mathbf{C}, \hat{\mathbf{A}}, \mathbf{N}^T\mathbf{z})$ to H_1, H_2, from $(\mathbf{B}, \mathbf{B}^T\mathbf{s} + \hat{\mathbf{e}}), (\mathbf{B}, \mathbf{u})$ to

H_3, H_4, and from $(\mathbf{C}, \hat{\mathbf{A}}), (\mathbf{C}, \mathbf{A})$ to H_4, H_5. In fact, the samples $(\mathbf{C}, \hat{\mathbf{A}}, \mathbf{N}^T\mathbf{z})$, $(\mathbf{B}, \mathbf{B}^T\mathbf{s}+\hat{\mathbf{e}})$, and $(\mathbf{C}, \hat{\mathbf{A}})$ are $\mathsf{extLWE}^m_{k,n,q,\beta,X}$, $\mathsf{LWE}_{k,m,q,\gamma}$ and $\mathsf{extLWE}^m_{k,n,q,\beta,\{0^n\}}$ samples respectively. The others are uniform distribution samples in the corresponding domain. It follows that $Adv[\mathcal{B}_1]$, $Adv[\mathcal{B}_3]$, $Adv[\mathcal{B}_4]$ are bound by the distinguishing advantages of $\mathsf{extLWE}^m_{k,n,q,\beta,X}$, $\mathsf{LWE}_{k,m,q,\gamma}$, $\mathsf{extLWE}^m_{k,n,q,\beta,\{0^n\}}$ respectively.

Since $\|\mathbf{x}\| \leq \rho\sqrt{\theta}$, and $\beta \geq \sqrt{2\ln(2n(1+1/\epsilon))/\pi}/q \geq \sqrt{2}\eta_\epsilon(\mathbb{Z}^n)/q$ from lemma 2.4.3, it follows that the statistical distance between $-\mathbf{N}^T\mathbf{x} + \hat{\mathbf{e}}$ and $D^m_{\alpha'}$ is at most $4m\epsilon$ by lemma 2.4.2. This gives $Adv[\mathcal{B}_0] \leq 4m\epsilon$. The last $Adv[\mathcal{B}_2]$ is bound by δ from the Leftover hash lemma. To sum up, $Adv[\mathcal{A}] \leq 2Adv[\mathcal{C}_1] + Adv[\mathcal{C}_2] + 4m\epsilon + \delta$ with trivial reduction to $\mathsf{extLWE}^m_{k,n,q,\beta,\{0^n\}}$ from $\mathsf{extLWE}^m_{k,n,q,\beta,X}$. □

3.3 Concrete Hardness

There exist many attacks for LWE including a dual attack and primal attacks ([APS15, DM15]). Here, we exclude a combinatorial BKW algorithm, the Arora and Ge algorithm and their variants, as they are not suitable in our case ([ACF+14, AG11, DTV15, KF15, GJS15]). Since the analysis of traditional dual attack is based on the (discrete) Gaussian error (and secret in the LWE normal form), these traditional attacks are not directly applicable to spLWE. Therefore, we modify those attacks to analyze concrete hardness of spLWE. We also consider random guess on a sparse secret vector $\mathbf{s}$.

3.3.1 Dual Attack (distinguish version)

Assume that we are given $(\mathbf{A}, \mathbf{b}) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$ and want to distinguish whether they are uniform random samples or spLWE samples. For a constant $c \in \mathbb{R}$ with $c \leq q$, consider a lattice $L_c(\mathbf{A})$ defined by

$$L_c(\mathbf{A}) = \left\{(\mathbf{x}, \mathbf{y}/c) \in \mathbb{Z}^m \times (\mathbb{Z}/c)^n : \mathbf{x}^T\mathbf{A} = \mathbf{y} \bmod q\right\}.$$

If the samples $(\mathbf{A}, \mathbf{b})$ came from spLWE, for $(\mathbf{x}, \mathbf{y}) \in L_c(\mathbf{A})$, we have

$$\begin{aligned}\langle \mathbf{x}, \mathbf{b} \rangle &= \langle \mathbf{x}, \mathbf{A}\mathbf{s} + \mathbf{e} \rangle \\ &= \langle \mathbf{x}, \mathbf{A}\mathbf{s} \rangle + \langle \mathbf{x}, \mathbf{e} \rangle \\ &= c\langle \mathbf{y}, \mathbf{s} \rangle + \langle \mathbf{x}, \mathbf{e} \rangle \bmod q\end{aligned}$$

For a sufficiently small vector $(\mathbf{v}, \mathbf{w}) \in L_c(\mathbf{A})$, the value $\langle \mathbf{v}, \mathbf{b} \rangle \bmod q$ becomes small when the samples are spLWE ones, and $\langle \mathbf{v}, \mathbf{b} \rangle \bmod q$ is uniformly distributed when $(\mathbf{A}, \mathbf{b})$ came from the uniform distribution. Hence, one can decide whether the samples came from spLWE distribution or uniform distribution from the size of $\langle \mathbf{v}, \mathbf{b} \rangle \bmod q$ with some success probability. We now determine how small a vector $(\mathbf{v}, \mathbf{w})$ must be found as follows. First, we estimate the length of $(\mathbf{v}, \mathbf{w}) \in L_c(\mathbf{A})$. One can easily check that

$$\left(\begin{array}{c|c} I_m & 0 \\ \hline \frac{1}{c}\mathbf{A}^T & \frac{q}{c} I_n \end{array}\right)$$

is a basis matrix of $L_c(\mathbf{A})$. Hence, we can figure out $\dim(L_c(\mathbf{A})) = m + n$ and $\det(L_c(\mathbf{A})) = (q/c)^n$.

Therefore, a lattice reduction algorithm with a root Hermite factor δ_0 gives $(\mathbf{v}, \mathbf{w}) \in L_c(\mathbf{A})$, such that

$$||(\mathbf{v}, \mathbf{w})|| = \delta_0^{m+n} (q/c)^{\frac{n}{m+n}}, \tag{3.3.1}$$

and the length is minimized when $m = \sqrt{n(\log q - \log c)/\log \delta_0} - n$.

Next, we consider the distribution of $c\langle \mathbf{w}, \mathbf{s} \rangle + \langle \mathbf{v}, \mathbf{e} \rangle \bmod q$. Here, we assume that the coefficients of sparse vector $\mathbf{s}$ are independently sampled by $(b_1 d_1, b_2 d_2, \ldots, b_n d_n)$ where $d_i \leftarrow \mathrm{Ber}(n, \theta/n)$, $b_i \leftarrow \{\pm 1, \pm 2, \pm 4, \ldots, \pm \rho\}$,

and $\rho = 2^l$ for some $l \in \mathbb{Z}_{\geq 0}$. Since $c\langle \mathbf{w}, \mathbf{s} \rangle$ is the sum of many independent random variables, asymptotically it follows a Gaussian distribution with mean 0, and variance $(c||\mathbf{w}||)^2 \cdot \frac{2\theta(4^{l+1}-1)}{3n(2l+2)}$. From that $\langle \mathbf{v}, \mathbf{e} \rangle$ follows a Gaussian distribution with mean 0, variance $(\sigma||\mathbf{v}||)^2$, and lemma 2.6.1, we have distinguishing advantage

$$\exp(-\pi(s'/q)^2) \text{ where } s' = \sqrt{2\pi}\sqrt{\sigma^2||\mathbf{v}||^2 + c^2\frac{2\theta(4^{l+1}-1)}{3n(2l+2)}||\mathbf{w}||^2}. \quad (3.3.2)$$

From above equations 3.3.1, 3.3.2 with distinguishing advantage ϵ, we need to find small δ_0 such that

$$\delta_0 = (c/q)^{\frac{-n}{(m+n)^2}}(\frac{q}{M}\sqrt{\ln(1/\epsilon)/\pi})^{1/(m+n)}$$

where $M = \sqrt{2\pi}\sqrt{\sigma^2\frac{m}{m+n} + c^2\frac{2\theta(4^{l+1}-1)}{3n(2l+2)}\frac{n}{m+n}}$.

3.3.2 Dual Attack (search version)

In this section, we assume the Geometric Series Assumption (GSA) on q-ary lattices, introduced by Schnorr [Sch03], and this will be used to estimate the length of last vector of BKZ 2.0 reduced basis. Let $\mathbf{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$ be a basis for an n-dimensional lattice Λ, which is reduced by the BKZ 2.0 with root Hermite factor δ_0, then the GSA says:

$$\|\mathbf{b}_i^*\| = \beta^{i-1} \cdot \|\mathbf{b}_1^*\| \text{ for some constant } 0 < \beta \leq 1,$$

where $\{\mathbf{b}_1^*, \cdots, \mathbf{b}_n^*\}$ is the Gram-schmidt orthogonalization of $\{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$. From $\|\mathbf{b}_1\| = \delta_0^n \cdot \det(\mathbf{B})^{1/n}$, we have:

$$\det(\mathbf{B}) = \prod_{i=1}^{n} \|\mathbf{b}_i^*\| = \prod_{i=1}^{n} \beta^{i-1} \cdot \|\mathbf{b}_1^*\| = \beta^{\frac{(n-1)n}{2}} \cdot \delta_0^{n^2} \cdot \det(\mathbf{B}).$$

From the equation above, it follows that $\beta = \delta_0^{-2n^2/(n-1)n}$. Since BKZ reduced basis satisfies $\mathbf{b}_i = \mathbf{b}_i^* + \sum_{j=0}^{i-1} \mu_{ij} \cdot \mathbf{b}_j^*$ with $|\mu_{ij}| \leq 1/2$, one can show that,

$$\|\mathbf{b}_i\| \leq ||\mathbf{b}_1|| \cdot \sqrt{\frac{1-\beta^{2i-2}}{4-4\beta^2} + \beta^{2i-2}}.$$

We now describe the dual attack against a small number of LWE instances $(\mathbf{A}, \mathbf{As}+\mathbf{e}) = (\mathbf{A}, \mathbf{b}) \in \mathbb{Z}^{m\times n} \times \mathbb{Z}^m$. For some constant $c \in \mathbb{N}$ with $c \leq q$, we consider a scaled lattice $\Lambda_c(\mathbf{A})$.

$$\Lambda_c(\mathbf{A}) = \{(\mathbf{x}, \mathbf{y}/c) \in \mathbb{Z}^m \times (\mathbb{Z}^n/c) : \mathbf{xA} = \mathbf{y} \bmod q\}.$$

A dimension and determinant of the lattice $\Lambda_c(\mathbf{A})$ is $n+m$ and $(q/c)^n$ respectively. With the assumptions above, we can obtain vectors $\{(\mathbf{v}_i, \mathbf{w}_i)\}_{1\leq i\leq n}$ in $\Lambda_c(\mathbf{A})$ such that,

$$\|(\mathbf{v}_i, \mathbf{w}_i)\| \quad \leq \quad \delta_0^{m+n} \cdot (q/c)^{\frac{n}{m+n}} \cdot \sqrt{\frac{1-\beta^{2i-2}}{4-4\beta^2} + \beta^{2i-2}} \approx \delta_0^{m+n}(q/c)^{\frac{n}{m+n}} \cdot \sqrt{\frac{1}{4-4\beta^2}}.$$

Clearly, the element $(\mathbf{v}_i, \mathbf{w}_i)$ in $\Lambda_c(\mathbf{A})$ satisfies

$$\mathbf{v}_i \cdot \mathbf{b} = \mathbf{v}_i \cdot (A \cdot \mathbf{s} + \mathbf{e}) = \langle c \cdot \mathbf{w}_i, \mathbf{s}\rangle + \langle \mathbf{v}_i, \mathbf{e}\rangle = \langle (\mathbf{v}_i, \mathbf{w}_i), (\mathbf{e}, c \cdot \mathbf{s})\rangle \bmod q.$$

If, for $1 \leq i \leq n$, $(\mathbf{v}_i, \mathbf{w}_i)$ is short enough to satisfy $\|(\mathbf{v}_i, \mathbf{w}_i)\| \cdot \|(\mathbf{e}, c\cdot\mathbf{s})\| < q/2$, the above equation hold over $\mathbb{Z}$. Then we can recover $\mathbf{e}$ and $\mathbf{s}$ by solving the system of linear equations. Since, $\|(\mathbf{e}, c\mathbf{s})\| \approx \sqrt{n \cdot \sigma^2 + c^2 \cdot \|\mathbf{s}\|^2}$, condition for attack is following:

$$\delta_0^{n+m} \cdot (q/c)^{\frac{n}{m+n}} \cdot \sqrt{\frac{n \cdot \sigma^2 + c^2 \cdot \|\mathbf{s}\|^2}{4-4\beta^2}} < \frac{q}{2}$$

for constant $0 < c \leq q$. To find an optimized constant c, we assume $m = n$. In this case, the size is optimized with $c = \sqrt{n \cdot \sigma^2/||s||^2}$. Therefore, final

condition to success attack is following:

$$2\delta_0^{4n} \cdot \sigma \cdot \|\mathbf{s}\| \cdot \sqrt{n} < q(1-\beta^2).$$

3.3.3 Modified Embedding Attack.

One can reduce the LWE problem to unique-SVP problem via Kannan's embedding technique. First, we consider a column lattice

$$\Lambda_q(\mathbf{A}') = \{\mathbf{y} \in \mathbb{Z}^{m+1} : \mathbf{y} = \mathbf{A}'\mathbf{x} \bmod q\} \text{ for } \mathbf{A}' = \begin{pmatrix} 1 & 0 \\ -\mathbf{b} & \mathbf{A} \end{pmatrix}.$$

The vector $(1, \mathbf{e})^T$ is in lattice $\Lambda_q(\mathbf{A}')$ and its size is approximately $\sigma\sqrt{m}$. If this value is sufficiently smaller than $\lambda_2(\Lambda_q(\mathbf{A}'))$ ($\approx \sqrt{\frac{m}{2\pi e}} q^{(m-n)/m}$), one can find the vector $(1, \mathbf{e})^T$ via some lattice reduction algorithms. In particular, the vector $(1, \mathbf{e})^T$ can be found with high probability with the BKZ algorithms in [AFG13], if

$$\frac{\lambda_2(\Lambda_{m+1})}{\lambda_1(\Lambda_{m+1})} = \frac{\lambda_2(\Lambda_q(\mathbf{A}))}{||(1, \mathbf{e})||} \geq \tau \cdot \delta_0^m,$$

where $\tau \approx 0.4$. For spLWE case, we can obtain a much larger gap than that of the ordinary attack for LWE. We now consider a scaled lattice $\Lambda_c(\mathbf{B})$ generated by the following matrix:

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & c\mathbf{I}_n & 0 \\ -\mathbf{b} & \mathbf{A} & q\mathbf{I}_m \end{pmatrix}$$

for a constant $0 < c < 1$. The vector $(1, c\mathbf{s}, \mathbf{e})^T$ is in this lattice and its size is approximately $\sqrt{m \cdot \sigma^2 + c^2\|\mathbf{s}\|^2}$. Define a matrix $\mathbf{B}'$ as following,

$$\mathbf{B}' = \begin{pmatrix} c\mathbf{I}_n & 0 \\ \mathbf{A} & q\mathbf{I}_m \end{pmatrix}.$$

We have

$$\lambda_1(\Lambda_c(\mathbf{B})) = \sqrt{m \cdot \sigma^2 + c^2 \cdot ||\mathbf{s}||^2}$$

and

$$\lambda_1(\Lambda_c(\mathbf{B}')) = \sqrt{\frac{n+m}{2\pi e}} \cdot \det(\Lambda_c(\mathbf{B}'))^{1/(n+m)} = \sqrt{\frac{n+m}{2\pi e}} \cdot (q^m c^n)^{1/n+m}$$

. Therefore, it is necessary to find the root Hermite factor δ_0 such that:

$$\begin{aligned} \sqrt{\frac{n+m}{2\pi e}} \cdot (q^m c^n)^{1/n+m} &\geq 0.4 \cdot \delta_0^{n+m} \cdot \sqrt{m \cdot \sigma^2 + c^2 \|\mathbf{s}\|^2} \\ \Leftrightarrow \sqrt{\frac{n+m}{2\pi e \cdot (m \cdot \sigma^2 + c^2 \|\mathbf{s}\|^2)}} \cdot (q^m c^n)^{1/n+m} &\geq 0.4 \cdot \delta_0^{n+m} \end{aligned}$$

The left part of inequality above is maximized when $c = \sqrt{n\sigma^2}/\|\mathbf{s}\|$, so we have:

$$\sqrt{\frac{1}{2\pi e \cdot \sigma^2}} \left(q^m \cdot \left(\frac{\sigma\sqrt{n}}{\|\mathbf{s}\|} \right)^n \right)^{1/(n+m)} \geq 0.4 \cdot \delta_0^{n+m}$$

3.3.4 Improving Lattice Attacks for spLWE

A time complexity of all attacks suggested in this paper is heavily depend on the dimension of lattices used in the attacks. Therefore, if one can reduce the dimension of lattices, one can obtain a high advantage to solve the LWE problem. In this section, we introduce two techniques to improve lattice-based attacks for spLWE instances. The first thing is a method of ignoring some components of a sparse secret and the other is a method of trading between dimension and modulus, which has been introduced in [BLP+13]. For convenience, we denote $T(m)$ as the expected time of solving m-dimensional LWE.

Ignoring Components on Secret Vectors.

Most entries of a secret vector $\mathbf{s}$ are zero. Therefore, by ignoring some components, one can reduce the dimension of LWE. More precisely, we delete k

entries of secret vector $\mathbf{s}$ and its corresponding column of $\mathbf{A}$. For convenience, we denote it as $\mathbf{s}'$ and $\mathbf{A}'$, respectively. If the deleted components of $\mathbf{s}$ are zero, the following equation also hold:

$$\mathbf{A} \cdot \mathbf{s} + \mathbf{e} = \mathbf{A}' \cdot \mathbf{s}' + \mathbf{e} \bmod q.$$

The probability P_k that the selected k entries are zero is $\binom{n-\theta}{k}/\binom{n}{k}$. It implies that one can reduce the n-dimensional LWE to $(n-k)$-dimensional LWE with probability P_k. In other words, solving $1/P_k$ instances in $(n-k)$-dimensional LWE, one can expect to solve the n dimension LWE. Hence, in order to guarantee λ bits security, it gives:

$$T(n-k)/P_k \geq 2^{\lambda}. \tag{3.3.3}$$

Modulus Dimension Switching.

In [BLP+13], they describe a modulus dimension switching technique for LWE instances. Using the corollary 3.4 in [BLP+13], for n, q, θ, w that divides n and $\epsilon \in (0, 1/2)$, one can reduce a $\mathsf{LWE}_{n,q,\leq\alpha}$ instances to $\mathsf{LWE}_{n/w,q^w,\leq\beta}$ instances, where β is a constant satisfying $\beta^2 \geq \alpha^2 + (4/\pi)\ln(2n(1+1/\epsilon)) \cdot \theta/q^2 \approx \alpha^2$. Along this reduction, a secret vector $\mathbf{s} = (s_1, s_2, \cdots, s_n)$ of $\mathsf{spLWE}_{n,q,\leq\alpha,\rho,\theta}$ is changed to $\mathbf{s}'' = (s_1 + qs_2 + \cdots + q^{w-1}s_w, \cdots, s_{n-w+1} + \cdots + q^{w-1}s_n)$ of $\mathsf{spLWE}_{n/w,q^w,\leq\beta,\rho',\theta'}$. Hence, if one can recover the $\mathbf{s}''$ by solving $\mathsf{LWE}_{n/w,q^w,\leq\beta,\rho',\theta'}$ instances, one can also reveal the vector $\mathbf{s}$. Let t be the number of a set $W = \{s_{wi} | s_{wi} \neq 0, 1 \leq i \leq n/w\}$ and P'_w be the probability of $t = 0$, i.e. P'_w is equal to $\dfrac{\binom{n-\theta}{n/w}}{\binom{n}{n/w}}$. When t is not zero, the expected size of $\|\mathbf{s}''\|$ is $\sqrt{tq^w}$. In that case, applying the attacks in section 4.2, 6.1 and 6.2 to converted n/w-dimensional LWE instances is not a good approach to obtain higher the advantage. Hence, we only consider the case $t = 0$. We can obtain the following conditions to get λ-bit security:

$$T(n/w)/P'_w \geq 2^{\lambda}. \tag{3.3.4}$$

By combining the ignoring k components with modulus dimension switching techniques, we can reach the final condition to obtain the λ-bit security:

$$T((n-k)/w)/(P_k P'_w) \geq 2^{\lambda}. \tag{3.3.5}$$

Chapter 4

LWE-based Public-Key Encryptions

In this chapter, we briefly review the previous LWE-based public key encryptions, which have IND-CPA security. In terms of design principle, all of them are similar. Therefore, we try to give a alteration on the base problem and choose a different construction strategy. In particular, we propose an efficient instantiation of a PKE scheme based on spLWE. We first construct an IND-CPA PKE and convert it to an IND-CCA scheme in the quantum random oracle model by applying a modified Fujisaki-Okamoto conversion of Unruh. Our implementation shows that the 256-bit IND-CCA scheme takes 313 μ seconds and 302 μ seconds respectively for encryption and decryption with the parameters that have 128-bit quantum security.

4.1 History

The LWE-based public-key encryption scheme which is mostly related ours is introduced by Regev [Reg05]. This encryption scheme uses LWE dimension n, modulus q, width s, and number of samples m as parameters and can be described as follows:

- The secret key vector $\mathbf{s} \in \mathbb{Z}_q^n$ is sampled randomly from $\mathbb{Z}_q^n$,and the

public key is m samples of LWE, $(\mathbf{A}, \mathbf{b}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m$ where $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$

- In order to encrypt a bit $\mu \in \{0, 1\}$ using the public key $\mathbf{A}$, one chooses a uniformly random vector $\mathbf{x} \in \{0, 1\}^m$ and outputs the ciphertext as $\mathbf{c} = (\mathbf{c}_1, c_2) = (\mathbf{x}^T\mathbf{A}, \langle \mathbf{x}, \mathbf{b} \rangle + \lfloor q/2 \rfloor \mu)$.

- For decryptions with the secret key $\mathbf{s}$, one computes $c_2 - \langle \mathbf{c}_1, \mathbf{s} \rangle = \lfloor q/2 \rfloor \mu + \langle \mathbf{x}, \mathbf{e} \rangle$, and checks whether it is closer to 0 or to $q/2$.

The above encryption is information-theoretically secure for sufficiently large m by the well-known Left-over Hash lemma, and the decryption is correct as long as the size of decryption error $\langle \mathbf{e}, \mathbf{x} \rangle$ is less than $q/4$. It requires the modulus q to be large enough relative to the magnitude of decryption error. It is known that one can choose parameters $s = \Theta(\sqrt{n})$ and $q = \tilde{O}(n)$, which correspond to the error rate of $\alpha = s/q = 1/\tilde{O}(\sqrt{n})$ and worst-case approximation factors of $\gamma = \tilde{O}(n^{3/2})$ in order to secure under a worst-case assumption.

A dual version of LWE-based encryption scheme was proposed by Gentry, Peikert, and Vaikuntanathan [GPV08]. Unlike the Regev's encryption scheme, the public keys are subset-sum instances and the ciphertexts are LWE instances. Thus, a public keys has many possible secret keys, and this is useful for constructing a variety of more advanced cryptosystems including IBE.

In 2011, a more compact LWE-based encryption scheme was proposed by Lindner and Peikert [LP11] with concrete parameters which are derived from a new decoding attack for LWE. In this encryption scheme, public keys, and ciphertexts are LWE instances. Unlike the encryptions mentioned above, it only relies on computational arguments, the LWE assumption, and does not require the statistical lemma. As a result, the keys and ciphertexts are smaller than those in the above LWE-based schemes by a factor of about log q.

4.2 spLWE-based Instantiations

In this section, we describe a public-key encryption scheme whose security is based on spLWE. One of advatages of our scheme is that the ciphertext size is smaller than those of the previous works [Reg05, LP11]. We also use a noisy subset sum in our encryption algorithm which is proposed in the previous LWE-based encryption scheme [LP11], but our message encoding method is different: we first construct a KEM(key encapsulation mechanism) based on spLWE, and conceal messages as a OTP manner with an ephemeral key shared by the KEM.

We propose two versions of our encryption scheme based on the spLWE-based KEM, where one is IND-CPA secure and the other is an IND-CCA secure under the conversion proposed in [TU15]. We note that these different types of schemes can be applied to various circumstances.

4.2.1 Our Key Encapsulation Mechanism

We use a *reconciliation* technique in [Pei14] which is the main tool to construct our spLWE-based KEM. In our KEM, the sender generates a random number $v \in \mathbb{Z}_{2q}$ for some even integer $q > 0$, and sends $\langle v \rangle_2$ where $\langle v \rangle_2 := [\lfloor \frac{2}{q} \cdot v \rfloor]_2 \in \mathbb{Z}_2$ to share $\lfloor v \rceil_2 := [\lfloor \frac{1}{q} \cdot v \rceil]_2 \in \mathbb{Z}_2$ securely. For all vectors $\mathbf{v} \in \mathbb{Z}_{2q}^k$, $\langle \mathbf{v} \rangle_2$ and $\lfloor \mathbf{v} \rceil_2$ are naturally defined by applying $\langle \rangle_2$ and $\lfloor \rceil_2$ component-wise, respectively. The receiver recovers $\lfloor v \rceil_2$ from $\langle v \rangle_2$ and sk using a special function named *rec*. The reconciliation function *rec* is defined as follows.

Definition 4.2.1. For disjoint intervals $I_0 := \left\{0, 1, \cdots, \left\lfloor \frac{q}{2} \right\rceil - 1\right\}$, $I_1 := \left\{-\left\lfloor \frac{q}{2} \right\rfloor, \cdots, -2, -1\right\}$ and $E = \left[-\frac{q}{4}, \frac{q}{4}\right) \cap \mathbb{Z}$, we define

$$rec : \mathbb{Z}_{2q} \times \mathbb{Z}_2 \to \mathbb{Z}_2 \text{ where } rec(w, b) := \begin{cases} 0 & \text{if } w \in I_b + E \bmod 2q, \\ 1 & \text{otherwise.} \end{cases}$$

It is naturally extended to a vector-input function $\boldsymbol{rec} : \mathbb{Z}_{2q}^k \times \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ by applying *rec* component-wise.

The following lemmas show that $\langle v \rangle_2$ reveals no information about $\lfloor v \rceil_2$, and *rec* decapsulates $\lfloor v \rceil_2$ correctly when it is provided with a proper approximation of v.

Lemma 4.2.1. *If $v \in \mathbb{Z}_{2q}$ is uniformly random, then $\lfloor v \rceil_2$ is uniformly random given $\langle v \rangle_2$.*

Proof. Suppose that $\langle v \rangle_2 = b \in \mathbb{Z}_2$. It implies that v is uniform over $I_b \cup (q + I_b)$. If $v \in I_b$, then $\lfloor v \rceil_2 = 0$, and if $v \in (q + I_b)$, then $\lfloor v \rceil_2 = 1$. Therefore $\lfloor v \rceil_2$ is uniformly random over $\{0, 1\}$ given $\langle v \rangle_2$. □

Lemma 4.2.2. *For $v, w \in \mathbb{Z}_{2q}$, if $|v - w| < q/4$, then $rec(w, \langle v \rangle_2) = \lfloor v \rceil_2$.*

Proof. Let $\langle v \rangle_2 = b \in \mathbb{Z}_2$, then $v \in I_b \cup (q + I_b)$. Then $\lfloor v \rceil_2 = 0$ if and only if $v \in I_b$. Since $(I_b + E) - E = I_b + (-\frac{q}{2}, \frac{q}{2})$ and $(q + I_b)$ are disjoint (mod $2q$), we know that $v \in I_b$ if and only if $w \in I_b + E$. □

The purpose of our KEM is sharing the ephemeral key from $\mathbf{u}^T\mathbf{A}\mathbf{s} + error$ and the reconciliation function between two parties as in [Pei14]. Here, we describe our spLWE-based KEM for k-bit sharing as follows.

- KEM.Params(λ): generate a bit-length of shared key k, a bit-length of seed y and spLWE parameters $n, m, q, s, \rho, \theta, s', \rho', \theta'$ with λ-bit security. Publish all parameters by pp.

- KEM.Keygen(pp): sample $seed_A \leftarrow \{0,1\}^y, \mathbf{A} \leftarrow Gen(seed_A), \mathbf{E} \leftarrow D_{\mathbb{Z},s}^{m \times k}$ and $\mathbf{S} \leftarrow \mathcal{U}(X_{n,\rho,\theta})^k$, and compute $\mathbf{B} = \mathbf{A}\mathbf{S} + \mathbf{E} \in \mathbb{Z}_q^{m \times k}$. For a secret key $\mathsf{sk} = \mathbf{S}$, publish a corresponding public key $\mathsf{pk} = (seed_A, \mathbf{B})$.

- KEM.Encap(pk,pp): sample $\mathbf{u} \leftarrow X_{m,\rho',\theta'}$, $(\mathbf{e}_1, \mathbf{e}_2) \leftarrow D_{\mathbb{Z},s'}^k \times D_{\mathbb{Z},s'}^n$ and $\mathbf{e}_3 \in \{0,1\}^k$. Let $\mathbf{v} = \mathbf{u}^T\mathbf{B} + \mathbf{e}_1 \in \mathbb{Z}_q^k$ and $\bar{\mathbf{v}} = 2\mathbf{v} + \mathbf{e}_3 \in \mathbb{Z}_{2q}^k$. Compute $\mathbf{c_1} = \langle \bar{\mathbf{v}} \rangle_2 \in \mathbb{Z}_2^k$ and $\mathbf{c_2} = \mathbf{u}^T\mathbf{A} + \mathbf{e_2} \in \mathbb{Z}_q^n$ from $\mathbf{A} \leftarrow Gen(seed_A)$. Send a ciphertext $\mathbf{c} = (\mathbf{c_1}, \mathbf{c_2}) \in \mathbb{Z}_2^k \times \mathbb{Z}_q^n$ to the receiver, and store an ephemeral secret key $\mu = \lfloor \bar{\mathbf{v}} \rceil_2 \in \mathbb{Z}_2^k$.

- KEM.Decap($\mathbf{c}$, sk): If q is odd, compute $\mathbf{w} = 2\mathbf{c_2}^T\mathbf{S} \in \mathbb{Z}_q^k$, and ouput $\mu = \boldsymbol{rec}(\mathbf{w}, \mathbf{c_1})$.

We would like to note that if q is even, the *doubling* process in the encapsulation phase, i.e. converting $\mathbf{v} = \mathbf{u}^T\mathbf{B} + \mathbf{e}_1$ to $\bar{\mathbf{v}} = 2\mathbf{v} + \mathbf{e}_3$, is not required.

4.2.2 Our KEM-Based Encryption Scheme

We now construct a public key encryption scheme based on the spLWE-based KEM in the previous section. When the message slot increases by one, the ciphertext spaces of our scheme grow only one or two bits, which is more efficient than the known LWE based encryption schemes [Reg05], [LP11], where the growth is about $\log q$ bits.

$\mathbf{PKE}_1$ (IND-CPA) :

With a key exchange mechanism which shares a ℓ-bit length key, it is well-known that one can convert it into a public key encryption of the ℓ-bit length message having the same security as the key exchange mechanism. This conversion only includes XOR operations after generating an ephemeral key. Note that the ciphertext space is given as $\mathbb{Z}_q^n \times \mathbb{Z}_2^{2\ell}$, which is very efficient than $\mathbb{Z}_q^{n+\ell}$, ciphertext spaces of other LWE-based scehems.

PKE_1 is described as follows.

- PKE_1.Params(λ): let ℓ be a message length, and run KEM.Params(λ) with $k = \ell$. Publish all parameters by pp.
- PKE_1.Keygen(pp): output a key pair (pk, sk)$\leftarrow$ KEM.Keygen(pp).
- PKE_1.Enc(pk, $\mathbf{m}$, pp): for $\mathbf{c}, \mu \leftarrow$ KEM.Encap(pk,pp), let $\mathbf{c}' = \mathbf{m} \oplus \mu$ and output a ciphertext $(\mathbf{c}, \mathbf{c}')$.
- PKE_1.Dec($(\mathbf{c}, \mathbf{c}')$, sk): for $\mu =$ KEM.Decap($\mathbf{c}$, sk), output $\mathbf{m} = \mathbf{c}' \oplus \mu$.

PKE_2 (IND-CCA) :

We can apply the transformation suggested in [TU15], which can improve security of the existing public key encryption schemes. As a trade-off of security, this scheme requires a more complex construction than PKE_1, but note that this also use light operations such as XOR or hashing, which are not serious tasks for implementation.

We specially denote the encryption phase of PKE_1 by $\mathrm{PKE}_1.\mathsf{Enc}(\mathsf{pk}, \mathbf{m}, \mathsf{pp}; \mathbf{r})$ to emphasize that a random bit-string $\mathbf{r}$ is used for random sampling. Here, $\mathrm{PKE}_1.\mathsf{Enc}(\mathsf{pk}, \mathbf{m}, \mathsf{pp}; \mathbf{r})$ becomes deterministic.

It also requires quantumly secure hash functions $G : \{0,1\}^{k_1+\ell} \to \{0,1\}^*$, $H : \{0,1\}^{k_1} \to \{0,1\}^{k_2}$ and $H' : \{0,1\}^{k_1} \to \{0,1\}^{k_3}$, where k_i will be determined later. With these parameters, our scheme has a ciphertext space $\mathbb{Z}_q^n \times \mathbb{Z}_2^{k_1+k_2+k_3+\ell}$, which also gradually increases with the growth of message slot.

PKE_2 is described as follows.

- $\mathrm{PKE}_2.\mathsf{Params}(\lambda)$: let ℓ be a message length and $k_i > 0$ be integers such that hash functions $G : \{0,1\}^{k_1+\ell} \to \{0,1\}^*$, $H : \{0,1\}^{k_1} \to \{0,1\}^{k_2}$ and $H' : \{0,1\}^{k_1} \to \{0,1\}^{k_3}$ have λ-bit security. Let pp be an output of $\mathsf{KEM.Params}(\lambda)$ with $k = k_1$. Publish ℓ, pp and k_i.

- $\mathrm{PKE}_2.\mathsf{Keygen}(\mathsf{pp})$: output a key pair $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KEM.Keygen}(k_1)$.

- $\mathrm{PKE}_2.\mathsf{Enc}(\mathsf{pk}, \mathbf{m}, \mathsf{pp}, k_i)$: randomly choose $\omega \leftarrow \{0,1\}^{k_1}$, and let $\mathbf{c_m} = H(\omega) \oplus \mathbf{m}$. Compute $\mathbf{c}_h = H'(\omega)$ and $(\mathbf{c}, \mathbf{c}') \leftarrow \mathrm{PKE}_1.\mathsf{Enc}(\mathsf{pk}, \omega; G(\omega || \mathbf{c_m}))$. Output a ciphertext $(\mathbf{c}, \mathbf{c}', \mathbf{c}_h, \mathbf{c_m})$.

- $\mathrm{PKE}_2.\mathsf{Dec}((\mathbf{c}, \mathbf{c}', \mathbf{c}_h, \mathbf{c_m}), \mathsf{sk}, \mathsf{pp}, k_i)$: compute $\omega = \mathrm{PKE}_1.\mathsf{Dec}((\mathbf{c}, \mathbf{c}'), \mathsf{sk})$ and $\mathbf{m} = H(\omega) \oplus \mathbf{c_m}$. Check whether $(\mathbf{c}, \mathbf{c}') = \mathrm{PKE}_1.\mathsf{Enc}(\mathsf{pk}, \omega; G(\mathbf{w} || \mathbf{c_m}))$ and $\mathbf{c}_h = H'(\omega)$. If so, output $\mathbf{m}$, otherwise output $\perp$.

4.2.3 Security

In this section, we show (IND-CPA, IND-CCA) security of our encryption scheme (PKE_1, PKE_2). Security of our encryption scheme is reduced to security of KEM and security of KEM comes from hardness of spLWE. Consequently, under the hardness of spLWE, PKE_1 can reach to IND-CPA security and PKE_2 achieves further quantumly IND-CCA security with the random oracle assumption. Here is a statement for security of KEM.

Theorem 4.2.1. *Under the* $\mathsf{spLWE}_{n,m,q,s,\rho,\theta}$, *and* $\mathsf{spLWE}_{n,m,q,s',\rho',\theta'}$ *assumption, our KEM is IND-CPA secure.*

Proof. (Sketch) By Lemma 3, one cannot extract any information about $\mu = \lfloor \mathbf{v} \rceil_2$ with $\mathbf{c_1}$. Moreover, even if one can know some information of $\mathbf{v}$, the distribution of $(\mathbf{c_2}, \mathbf{v})$ can be regarded as LWE instances as :

$$(\mathbf{c_2}, \mathbf{v}) = (\mathbf{u}^T \cdot \mathbf{A} + \mathbf{e_2}, \mathbf{u}^T \cdot \mathbf{B} + \mathbf{e_1}) = (\mathbf{C}, \mathbf{C} \cdot \mathbf{S} + \mathbf{e}')$$

for $\mathbf{C} = \mathbf{u^T} \cdot \mathbf{A} + \mathbf{e_2}$ and for some $\mathbf{e}'$. Thus, hardness of spLWE insures that the distribution of $(\mathbf{c_2}, \mathbf{v})$ is indistinguishable from the uniform distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q^k$. □

We refer [Pei14] for the detailed IND-CPA game-based proof, where the only difference is that we assume the hardness of spLWE, not RLWE.

It is well-known in many cryptographic texts that PKE_1 has the same security level with KEM. Hence, security of PKE_1 has been demonstrated from the previous theorem. Moreover, the transformation of [TU15] gives quantumly IND-CCA security for PKE_2, when it is converted from an IND-CPA secure PKE with random oracle modeled hashes. When the aforementioned statements are put together, we can establish the following security theorem.

Theorem 4.2.2. *Assuming the hardness of* $\mathsf{spLWE}_{n,m,q,s,\rho,\theta}$, $\mathsf{spLWE}_{n,m,q,s',\rho',\theta'}$, *$\mathrm{PKE}_1$ is IND-CPA secure, and PKE_2 is quantumly IND-CCA secure with further assumption that the function G, H and H' are modeled as random oracles.*

Proof. (Sketch) We only need to show that PKE_2 is IND-CCA secure. The transformation of [TU15] actually make an IND-CCA secure public key encryption from a public key encryption which is *well-spread* and *one-way*, and we briefly explain why (IND-CPA) PKE_1 is well-spread and one-way.

- Well-spreadness: Note that a ciphertext of PKE_1 is of the form

$$(\mathbf{c}_1, \mathbf{c}_2) = \left(\langle \mathbf{2}(\mathbf{u}^T B + \mathbf{e}_1) + \mathbf{e}_3 \rangle_2, \mathbf{u}^T A + \mathbf{e}_2\right),$$

  where $\mathbf{u} \leftarrow X_{m,\rho',\theta'}, (\mathbf{e}_1, \mathbf{e}_2) \leftarrow D^k_{\mathbb{Z},s'} \times D^n_{\mathbb{Z},s'}$. From hardness of spLWE, distributions of $\mathbf{u}^T B + \mathbf{e}_1 \in \mathbb{Z}_q^k$ and $\mathbf{u}^T A + \mathbf{e}_2 \in \mathbb{Z}_q^n$ are statistically close to uniform distributions over $\mathbb{Z}_q^k$ and $\mathbb{Z}_q^n$, and then PKE_1 is well-spread.

- One-wayness: With an oracle $\mathcal{O}$ finding $\mathbf{m}$ from $\mathrm{PKE}_1.\mathrm{Enc}(\mathsf{pk}, \mathbf{m})$ for any pk with probability ϵ, an adversary equipped with $\mathcal{O}$ wins the IND-CPA game for PKE_1 with bigger advantage than $\frac{\epsilon}{2}$: After given $\mathrm{PKE}_1.\mathrm{Enc}(\mathsf{pk}, \mathbf{m}_b)$, the adversary outputs the answer of $\mathcal{O}$. It can be easily shown that the advantage is bigger than $\frac{\epsilon}{2}$.

□

4.2.4 Correctness

Similar to the security case, correctness of our (IND-CPA, IND-CCA) encryption scheme is dependent on that of our spLWE-based KEM. We remark that generally, one can obtain some correctness condition for all LWE variants by examining a bound of error term in the proof below. Here, we assume $s = s', \rho = \rho'$ and $\theta = \theta'$, which is used for our parameter instantiation.

Theorem 4.2.3. *Let $n, m, \sigma, \rho, \theta$ be parameters in $\mathsf{spLWE}_{n,m,q,\sigma,\rho,\theta}$, and ℓ be the shared key length in KEM. For a per-symbol error probability γ, the KEM decapsulates correctly if*

$$q \geq 8s\rho\sqrt{\frac{2\theta}{\pi}\ln(2/\gamma)}.$$

Proof. As shown in the description of KEM.Decap, the ephemeral key is decapsulated correctly if $|\bar{\mathbf{v}} - \mathbf{w}| < q/4$ by lemma 4.2.2. Since $\bar{\mathbf{v}} = 2\mathbf{u}^T\mathbf{AS} + 2\mathbf{u}^T\mathbf{E} + 2\mathbf{e}_1 + \mathbf{e}_3$, and $\mathbf{w} = 2\mathbf{u}^T\mathbf{AS} + 2\mathbf{e}_2\mathbf{S}$, it is rephrased by

$$|2\mathbf{u}^T \cdot \mathbf{E} - 2\mathbf{e_1} \cdot \mathbf{S} + 2\mathbf{e_2} + \mathbf{e_3}| < q/4,$$

which is equivalent to

$$|2\langle \mathbf{u}, [\mathbf{E}]^j \rangle + 2\langle -\mathbf{e_1}, [\mathbf{S}]^j \rangle + 2[\mathbf{e_2}]_j + [\mathbf{e_3}]_j| < q/4, 1 \leq j \leq \ell$$

where $\mathbf{u} \leftarrow X_{m,\rho',\theta'}, [\mathbf{S}]^j \leftarrow X_{n,\rho,\theta}, [\mathbf{E}]^j \leftarrow D^m_{\mathbb{Z},s}, \mathbf{e}_1 \leftarrow D^n_{\mathbb{Z},s'}, [\mathbf{e_2}]_j \leftarrow D_{\mathbb{Z},s'}, [\mathbf{e_3}]_j \leftarrow \{0,1\}$. For simplicity, we ignore the small term $2[\mathbf{e_2}]_j + [\mathbf{e_3}]_j$. (This is compensated in our final choice of parameters.) By applying lemma 5.3.1 to a $(m+n)$ dimensional vector $\mathbf{x} = (\mathbf{u}, [\mathbf{S}]^j)$ and the bound $Ts\|\mathbf{x}\| = q/8$, we came to have per-symbol error probability γ,

$$\gamma = 2\exp(-\pi(\frac{q}{8s\rho\sqrt{(2\theta)}})^2)$$

from $T = \frac{q}{8s\rho\sqrt{2\theta}}$. From the equation above, we get the bound on q as the statement. □

4.3 Implementation

We have suggested concrete parameters for both classical and quantum security, implementation results of our scheme and a comparison table with the previous LWE-based PKE [LP11] and RLWE-based PKE [LPR10]. In 128-quantum bit security, the IND-CPA version of our encryption took about $314\mu s$ and the IND-CCA version of our encryption takes $313\mu s$ for 256-bit messages on Macbook Pro with CPU 2.6GHz Intel Core i5 without parallelization.

4.3.1 Parameter Selection

In order to deduce appropriate parameters, we assume that the best known classical and quantum sieving algorithm in dimension k runs in time $2^{0.292k}$ and $2^{0.265k}$ respectively [BDGL16, Laa15]. The BKZ 2.0 lattice basis reduction algorithm gives the root Hermite factor $\delta_0 \approx (\frac{k}{2\pi e}(\pi k)^{1/k})^{1/2(k-1)}$ for block size k [Che13], and the iteration number of exact SVP solver is $\frac{n^3}{k^2}\log n$ [HPS11].

We also consider a direct CVP attack by sieving [Laa16], modified dual (distinguish) and embedding attack. Moreover, since our secret key is a sparse vector, our attack can be improved if one can guess some components of secret to be zero. After that, we can apply the attack to a smaller dimensional spLWE instances. We denote the probability of the correct guessing t components from n components by $p_{n,t,\theta}$. It can be computed as $\binom{n-\theta}{t}/\binom{n}{t}$.

To sum up, the parameters must satisfy the followings for the classical and quantum security:

- $n\log q \cdot (2l+1)^\theta \cdot \binom{n}{\theta} > 2^{2\lambda}$ from bruteforce attack (grover algorithm), where $\binom{n}{\theta} = \frac{n!}{(\theta!)(n-\theta!)}$ (For classical security, 2λ becomes λ)

- Let $T(n,q,\theta,s,l)$ be a BKZ 2.0 running time to get root Hermite factor δ_0, which satisfies the following equation:

$$\delta_0 = \max_{1<c<q, 1\le m\le n}\left\{(c/q)^{\frac{-n}{(m+n)^2}}(\frac{q}{M}\sqrt{\ln(1/\epsilon)/\pi})^{1/(m+n)}\right\}$$

  where

$$M = \sqrt{2\pi}\cdot\sqrt{\sigma^2\frac{m}{m+n} + c^2\frac{2\theta(4^{l+1}-1)}{3n(2l+2)}\frac{n}{m+n}}.$$

  Taking into the probability $p_{n,t,\theta}$, our parameters should satisfy the following:

$$\min_t\left\{\frac{1}{p_{n,t,\theta}}\cdot T(n-t,q,\theta,s,l)\right\} > 2^\lambda \text{ where } p_{n,t,\theta} = \binom{n-\theta}{t}/\binom{n}{t}$$

  .

- To prevent the direct CVP attack, n and θ should satisfy the following equation:
$$\min_t \left\{ \frac{1}{p_{n,t,\theta}} \cdot 2^{0.265(n-t)} \right\} > 2^{\lambda}$$
For classical security, 0.265 becomes 0.292.

- For the correctness, $q \geq 8s\rho\sqrt{\frac{2\theta}{\pi}\ln(2/\gamma)}$ by the Lemma 4.2.2.

- The parameters k_1 and k_2 are a symmetric key length of XOR operations, and k_3 is a length of hash value. For λ-bit security, it is known that k_1 and k_2 should be λ (2λ) and k_3 should be 2λ (3λ) in classical (quantum) security model.

4.3.2 Implementation Result

We use C++ on a Linux-based system, with GCC compiler and apply the Eigen library (www.eigen.tuxfamily.org), which makes vector and matrix operations fast. To sample $\mathbf{u}$ efficiently in our encryption algorithm, we assume that there are only one non-zero element in each n/θ-size block. To follow the previous reduction and security proof, we need a sampling of discrete Gaussian distribution when we generate error vectors in key generation and encryption algorithm. We use *box-muller transformation* to generate discretized Gaussian distribution. In the case below, message space length is 32-byte and secret key is ternary vector. We used PC (Macbook Pro) with CPU 2.6GHz Intel Core i5 without parallelization.

Parameters					IND-CPA				IND-CCA		
λ	n	q	s	θ	Setup(ms)	Enc(μs)	Dec(μs)	Cptx(byte)	Enc(μs)	Dec(μs)	Cptx(byte)
72	300	382	5	27	9.8	96	41	401	116	130	435
96	400	441	5	36	16.3	167	62	513	181	182	548
128	565	477	5	42	29.3	273	102	700	291	282	733

Table 4.1: Implementation result in classical hardness with 256 bit message

Parameters					IND-CPA				IND-CCA		
λ	n	q	s	θ	Setup(ms)	Enc(μs)	Dec(μs)	Cptx(byte)	Enc(μs)	Dec(μs)	Cptx(byte)
72	300	410	5	31	9.8	96	41	401	108	130	435
96	400	477	5	42	16.0	163	56	514	186	191	548
128	565	520	5	50	129.5	314	106	770	313	302	804

Table 4.2: Implementation result in quantum hardness with 256 bit message

We also compare our implemetation with software implementation in [GFS+12], which implements LWE-based PKE [LP11] and Ring version PKE [LPR10, LPR13]. Their implementation is executed on an Intel Core 2 Duo CPU running at 3.00 GHz PC. Parameters in each rows are secure in same security parameters.

Our scheme			[GFS+12]	LWE		RLWE	
(n, q, s, θ)	Enc	Dec	(n, q, s)	Enc	Dec	Enc	Dec
(150, 285, 5.0, 15)	0.027	0.011	(128, 2053, 6.77)	3.01	1.24	0.76	0.28
(300, 396, 5.0, 29)	0.063	0.019	(256, 4093, 8.87)	11.01	2.37	1.52	0.57
(400, 545, 5.0, 55)	0.109	0.026	(384, 4093, 8.35)	23.41	3.41	2.51	0.98
(560, 570, 5.0, 60)	0.223	0.04	(512, 4093, 8.0)	46.05	4.52	3.06	1.18

Table 4.3: Our scheme vs. LWE vs. RLWE: Time in milliseconds for encryption and decryption for a 16-byte plaintext.

The table above shows that our PKE scheme is about 20 times faster than RLWE-based PKE scheme in [LPR10, LPR13]. The sparsity of secret vector make modulus size q smaller and complexity in encryption/decryption algorithm lower.

Chapter 5

LWE-based Commitments and Zero-Knowledge Proofs

In this chapter, we propose a new post-quantum commitment scheme which can commit to arbitrary vectors over $\mathbb{Z}_q$. Our scheme satisfies computational hiding and perfect binding properties under spLWE-assumption. To the best of our knowledge, our scheme is the first LWE-based commitment scheme where the message space does not restricted to any subspace. We show that our commitment scheme is efficient when used as a subblock of zero-knowledge proof of opening information of commitments. We also construct zero-knowledge proofs which can prove some relations among those commitments. All of theses allow us to make known LWE-based threshold cryptosystems actively secure. In particular, we suggest a efficient threshold version of LWE-based PKE, [CHK$^+$16], which achieves active security in random oracle model. To the best of our knowledge, this is the first actively secure LWE-based threshold cryptosystem which has no additional assumption like DL, RLWE problem, and has no restriction on threshold conditions.

5.1 History

Commitment schemes [Blu82] are basic building blocks in designs of cryptographic protocols and have a lot of applications including a classical application, coin flipping over telephone. Intuitively, they can be described as a electronic version of lockable box. When used to commit to some value in zero-knowledge proofs, they can enforce regular behavior of corrupted parties. As a result, it is possible to make protocols secure against active attackers. Prime examples of these are threshold signatures and threshold decryption. In threshold decryption, the decryption key of a original public-key encryption scheme is split to N shares and then distributed to N servers, so that any t servers can decrypt collaborately. By giving suitable proofs for partial decryption via some NIZKs, malicious behaviors of partial decryption servers can be detected. This prevents outputing of unusual decryption results. In other words, it guarantees robustness property.

In context of lattice based cryptography, the first LWE-based threshold cryptosystem, a threshold version of Regev's PKE [Reg09], was given in [BD10]. After then threshold versions of PKE and FHE's were proposed for various purpose including Multi-Party Computation (MPC), electronic votes [MSS11, XXZ11, AJLA+12, MW16]. (See [BGGK17] for more details) A limitation of these threshold PKE's, and FHE's is that they only achieve passive or semi-honest security.(c.f. One can achieve active security without additional tools by adjusting the threshold with Shamir's secret sharing as in [BD10]). In this background, we construct LWE-based NIZKs in order to enforce robustness on LWE-based cryptosystems as well as homomorphic cryptosystems. For efficiency reason, we construct them in random oracle model by transforming interactive zero-knowledge proofs via the well-known technique 'Fiat-Shamir Heuristic' [FS86].

In order to construct zero-knowledge proofs that checks each server performs decryption correctly, it is essential to consider commitment schemes which can commit arbitrary vectors over $\mathbb{Z}_q$. There are several related works in lattice-based cryptography: A commitment scheme based on SIS problem

was introduced in [KTX08], and an ring variant of the scheme was suggested in [Xag10]. However, the message space is restricted to a binary space. The LWE-based commitment scheme [ZTH10] is also the case. Thereafter, Jain et al. also proposed a bit commitment scheme whose security is based on the Learning Parity with Noise (LPN) problem, and zero-knowledge proofs to prove general relations. A RLWE version of the scheme in [JKPT12] was introduced in [XXW13, BCK+14]. The soundness error of all related zero-knowledge proofs achieve a non-negligible soundness error. This cause many parallel repetitions in order to get negligible soundness error. However, an improved RLWE-based commitment scheme which is perfectly binding and computationally hiding, and corresponding zero-knowledge protocols were proposed in [BKLP15]. The message space is a vector space over $\mathbb{Z}_q$, and they gave zero-knowledge proofs with negligible soundness error. On the other hand, Ring-SIS-based commitment and related zero knowledge protocols were suggested in [BDOP16].

Therefore, in post-quantum sense, we can only exploit RLWE or Ring-SIS based commitments and the related zero-knowledge proofs for actively secure threshold cryptosystems. This enforces assuming the hardness of ring variant problems even the underlying cryptosystems are based on hard problems over generic lattices, not ideal lattices like LWE, SIS. In this thesis, we suggest commitment schemes and zero-knowledge proofs based on LWE for actively secure LWE-based threshold cryptosystems. In particular, we use spLWE that is a variant of LWE with sparse secret vectors in order to improve their efficiency.

5.2 spLWE-based Instantiations

We first consider a LWE-based commitment scheme which is analogous to the one in [JKPT12]. Informally, for dimension n, the number of samples m, and modulus q, the commitment with message space $\mathbb{Z}_q^l$ is in the form $\mathbf{Am}+\mathbf{Br}+\mathbf{e} \bmod q$, where $(\mathbf{A}, \mathbf{B}) \in \mathbb{Z}_q^{m\times l} \times \mathbb{Z}_q^{m\times n}$ is a public random matrix,

$\mathbf{r} \in \mathbb{Z}_q^n$ is a uniformly random vector, and $\mathbf{e} \in \mathbb{Z}_q^m$ is a short error vector. This commitment scheme is computationally hiding under LWE assumption. In particular, the distribution of $\mathbf{Br} + \mathbf{e} \bmod q$ is statistically close to the uniform, and random distribution. Thus, it can hide message information. The scheme is perfect binding. This property follows from that $\mathbf{A}(\mathbf{m}-\mathbf{m}')+\mathbf{B}(\mathbf{r}-\mathbf{r}') = \mathbf{e}-\mathbf{e}' \bmod q$ does not hold overwhelmingly for sufficiently large q and m, since $\|\mathbf{e}-\mathbf{e}'\|$ is small. Here, the probability that the above equation holds only depends on the cardinalities of message and randomness domains under the consideration of union bounds. Thus, using of relatively small dimensions l, n and small vectors $\mathbf{r}$'s rather than arbitrary vectors over $\mathbb{Z}_q^n$ leads to more efficient instantiations of the LWE-based commitment scheme. In this background, spLWE is a suitable hard problem for efficient instantiations.

5.2.1 Our spLWE-based Commitments

In this section, we propose a new spLWE-based commitment scheme, which is closely related to zero-knowledge proofs. The setup algorithm chooses a spLWE dimension n, the number of sample m, a weight θ, a bound of non-zero coefficient ρ, a prime modulus q, a message space rank l, and a bound of elements in a challenge set β, and set width parameters s_1, s_2, s_3, and rejection sampling parameters α_1, α_2. The commitment algorithm computes the commitment vector $\mathbf{c}$ with public random matrices $\mathbf{A}, \mathbf{B}$ and randomness vectors $\mathbf{r}, \mathbf{e}$. The verification algorithm checks if the commitment computed from opening informations $(\mathbf{m}', \mathbf{r}', \mathbf{e}', f')$ is indeed the commitment $\mathbf{c}$, and the norm of randomness vector used in the commitment $\mathbf{c}$ is sufficiently small. Finally our commitment scheme is described as follows:

- Setup$(1^\kappa, 1^k)$: Set parameters $n, m, q, l, \theta, \rho, \beta \in \mathbb{N}$ and $s_1, s_2, s_3 \in \mathbb{R}$ with $2^\kappa, 2^k$-bit security where $s_2 = \alpha_2\beta\rho\sqrt{2\pi\theta}$, $s_3 = 2\alpha_3 s_1 \beta\sqrt{m}$ for some $\alpha_1, \alpha_2 \in \mathbb{R}_{\geq 1}$ and q is prime. Sample $seed_A \leftarrow \{0,1\}^{y_1}, seed_B \leftarrow \{0,1\}^{y_2}$. The public commitment key pk is $(seed_A, seed_B)$.

- $\mathrm{Com}(\mathbf{m} \in \mathbb{Z}_q^n)$: Generate random matrices $\mathbf{A} \leftarrow Gen(seed_A), \mathbf{B} \leftarrow Gen(seed_B)$ where $(\mathbf{A}, \mathbf{B}) \in \mathbb{Z}_q^{m \times l} \times \mathbb{Z}_q^{m \times n}$ and sample $\mathbf{r} \leftarrow X_{n,\rho,\theta}$, $\mathbf{e} \leftarrow D_{\mathbb{Z},s_1}^m$, compute

$$\mathbf{c} = Com(\mathbf{m}, \mathbf{r}, \mathbf{e}) = \mathbf{Am} + \mathbf{Br} + \mathbf{e} \bmod q$$

.

- $\mathrm{Ver}(\mathbf{c}, (\mathbf{m}', \mathbf{r}', \mathbf{e}', f'))$: Given a commitment $\mathbf{c}$ with a opening infomation $(\mathbf{m}, \mathbf{r}, \mathbf{e}, f)$, the verifier accepts if and only if $\mathbf{Am}' + \mathbf{B}(f'^{-1}\mathbf{r}') + f'^{-1}\mathbf{e}' = \mathbf{c}$, $\|\mathbf{r}'\|_\infty \leq 24s_2/\sqrt{2\pi}$, $\|\mathbf{e}'\|_\infty \leq 24s_3/\sqrt{2\pi}$, $|f'| \leq \beta$.

We would like note that honest committer can open his commitment by setting as $f' = 1$, $\mathbf{r}' = \mathbf{r}$, $\mathbf{e}' = \mathbf{e}$. Here, we also relax the verification condition in order to prove soundness property of our related zero-knowledge protocols. The distribution of $\mathbf{e}$, $D_{\mathbb{Z},s_1}^m$, is not bounded, but we set that the norm of $\mathbf{e}$ is bounded with overwhelming probability. This leads to correctness of our scheme. As mentioned above, our commitment scheme satisfies computational hiding property under spLWE assumption. The following theorem shows that the commitment scheme satisfies statistical binding property.

Theorem 5.2.1. *Let $m = kn$ with $k > 2$, $l = n$ and $\beta \leq 2^{\frac{n}{4}-1} - \frac{1}{2}$. Assuming the hardness of $\mathsf{spLWE}_{n,m,q,s_1,\rho,\theta}$ with the following condition*

$$\log q \geq \frac{2}{k-1} \log(24\sigma_2 + 1) + \frac{2k}{k-1} \log(24\sigma_3 + 1) + 1,$$

the above commitment scheme is correct and satisfies the computational hiding and statistical binding properties.

Proof. We prove correctness, computational hiding and statistical binding properties in this order.
Correctness: This is obvious since $\|\mathbf{r}\|_\infty \leq \rho < s_2 < 24s_2/\sqrt{2\pi}$ for $\mathbf{r} \leftarrow X_{n,\rho,\theta}$, $\|\mathbf{e}\|_\infty \leq 12s_1/\sqrt{2\pi}$ with probability $1 - 2^{-100}$ for $\mathbf{e} \leftarrow D_{\mathbb{Z},s_1}^m$, which is strictly

less than $24s_3/\sqrt{2\pi}$ and $f' = 1 \leq \beta$.

Computational hiding: Under the $\mathsf{spLWE}_{n,m,q,s_1,\rho,\theta}$-assumption, $\mathbf{Br}+\mathbf{e} \bmod q$ is pseudo-random, thus $\mathbf{Am}+\mathbf{Br}+\mathbf{e} \bmod q$ is also pseudo-random.

Statistical binding: Let $\mathbf{c}$ be a commitment with two opening infomations $(\mathbf{m}, \mathbf{r}, \mathbf{e}, f)$, $(\mathbf{m}', \mathbf{r}', \mathbf{e}', f')$ where $\mathbf{m} \neq \mathbf{m}'$. Then

$$\mathbf{Am} + \mathbf{B}(f^{-1}\mathbf{r}) + f^{-1}\mathbf{e} = \mathbf{c} = \mathbf{Am}' + \mathbf{B}(f'^{-1}\mathbf{r}') + f'^{-1}\mathbf{e}' \bmod q$$

and so

$$\mathbf{A}(\mathbf{m}-\mathbf{m}') + \mathbf{B}(f^{-1}\mathbf{r} - f'^{-1}\mathbf{r}') = f'^{-1}\mathbf{e}' - f^{-1}\mathbf{e} \bmod q.$$

Let $\mathbf{m}'' = \mathbf{m} - \mathbf{m}' \neq 0$. Now, we have that

$$Pr[\mathbf{Am}''+\mathbf{B}(f^{-1}\mathbf{r}-f'^{-1}\mathbf{r}') = (f'^{-1}\mathbf{e}'-f^{-1}\mathbf{e}) \bmod q : \mathbf{A} \leftarrow \mathbb{Z}_q^{m\times l}, \mathbf{B} \leftarrow \mathbb{Z}_q^{m\times n}] = \frac{1}{q^m}.$$

By taking union bound over all $\mathbf{m}'', \mathbf{r}, \mathbf{r}', \mathbf{e}, \mathbf{e}', f, f'$, we have the overall probability that there exist $\mathbf{m}'' \neq 0$ satisfying the above eqation is at most

$$\frac{q^l(24\sigma_2+1)^{2n}(24\sigma_3+1)^{2m}(2\beta+1)^2}{q^m}$$

This probability is negligible in n if

$$\frac{q^{l/n}(24\sigma_2+1)^2(24\sigma_3+1)^{2m/n}(2\beta+1)^{2/n}}{q^{m/n}} \leq \frac{1}{c}$$

for some constant $1 < c \leq 2$ or equivalently,

$$\log c + 2\log(24\sigma_2+1) + \frac{2m}{n}\log(24\sigma_3+1) + \frac{2}{n}\log(2\beta+1) \leq \frac{m-l}{n}\log q,$$

and $\log c + \frac{2}{n}\log(2\beta+1) \leq 1$ under the conditions in the Theorem. Therefore, the overall probability is c^{-n}, which is negligible in n. □

5.2.2 Proof for Opening Information

In order to prove zero-knowledgeness of protocols, it is essential that one can construct a simulator that statistically simulates the accepting transcripts. The following lemmas will be exploited for these purposes.

Lemma 5.2.1 ([Lyu12] Theorem 4.9, Rejection Sampling)**.** *Let $n, T \in \mathbb{N}$ be natural numbers and $U \subseteq \mathbb{Z}^n$, such that all elements in U have norm less than T. Let further $D : U \to \mathbb{R}$ be a probability distribution and $\sigma \in \omega(T\sqrt{\log n})$. Then there exists a constant $M \in O(1)$ such that the output distributions of the algorithms A_1, A_2 where*

- *A_1 : draw $\mathbf{v} \leftarrow D, \mathbf{z} \leftarrow D_\sigma^n$ and output $(\mathbf{z}, \mathbf{v})$ with probability $\frac{D_\sigma^n(\mathbf{z})}{MD_{\mathbf{v},\sigma}^n(\mathbf{z})}$.*
- *$A2$: draw $\mathbf{v} \leftarrow D, \mathbf{z} \leftarrow D_\sigma^n$ and output $(\mathbf{z}, \mathbf{v})$ with probability $\frac{1}{M}$.*

have at most statistical distance $2 - \omega(\log n)/M$. In particular A_1 outputs something with probability at least $1 - 2^{-\omega(\log n)}/M$. For a concrete instantiation $\sigma = \alpha T$ for $\alpha \in \mathbb{R}_{>0}$, we have $M = \exp(12/\alpha + 1/(2\alpha^2))$ and the outputs of A_1 and A_2 are within statistical distance $2^{-100}/M$.

Intuitively, the rejection sampling lemma says that some small translation of a discrete Gaussian distribution with sufficiently large standard deviation can be hidden by rejecting the sampling with a certain policy.

We now describe our zero-knowledge proofs. Let $\mathbf{c} = \mathbf{Am} + \mathbf{Br} + \mathbf{e} \bmod q$ be a commitment that is published by the prover. The prover can prove that he knows a valid opening information of $\mathbf{c}$ from the following protocol without revealing secret information. The public input is $\mathbf{c}$ and the private input is $(\mathbf{m}, \mathbf{r}, \mathbf{e})$:

- P computes $\mathbf{t} = \mathbf{A}\mu + \mathbf{B}\rho + \eta$ where $\mu \leftarrow \mathbb{Z}_q^l, \rho \leftarrow D_{\sigma_2}^n, \eta \leftarrow D_{\sigma_3}^m$, and sends $\mathbf{t}$ to V.
- V sends a random integer $d \in [-\beta, \beta] \cap \mathbb{Z}$.

- P checks $d \in [-\beta, \beta] \cap \mathbb{Z}$, and computes $\mathbf{s}_m = \mu + d\mathbf{m} \bmod q, \mathbf{s}_r = \rho + d\mathbf{r} \bmod q, \mathbf{s}_e = \eta + d\mathbf{e} \bmod q$. If $d = 0$, P sends $\mathbf{s}_m, \mathbf{s}_r, \mathbf{s}_e$ to V. Otherwise, P sends $\mathbf{s}_m, \mathbf{s}_r, \mathbf{s}_e$ to V with probability $p = D^n_{\sigma_2}(\rho)/M_2 D^n_{d\mathbf{r},\sigma_2}(\rho) \times D^n_{\sigma_3}(\eta)/M_3 D^n_{d\mathbf{e},\sigma_3}(\eta)$, and $\perp$ with probability $1 - p$.

- V accepts iff $\mathbf{t} + d\mathbf{c} = \mathbf{A}\mathbf{s}_m + \mathbf{B}\mathbf{s}_r + \mathbf{s}_e \bmod q$, $\|\mathbf{s}_r\|_\infty \leq 12\sigma_2$, and $\|\mathbf{s}_e\|_\infty \leq 12\sigma_3$.

We now prove that the above protocol is indeed a zero-knowledge proof.

Theorem 5.2.2. *The protocol is a Σ'-protocol with completeness error close to $\frac{1}{\beta} + \frac{\beta-1}{\beta M_2 M_3}$ overwhelmingly for the relations:*

Proof. We prove the protocol satisfies the following properties:

- Completeness: The verifier accepts with overwhelming probability if the protocol is not aborted by the prover, and the accepting probability is close to $\frac{1}{2\beta+1} + \frac{2\beta}{(2\beta+1)M_2M_3}$ overwhelmingly.

- Special Soundness: Given a commitment $\mathbf{c}$ and a pair of accepting transcripts $(\mathbf{t}, d, (\mathbf{s}_m, \mathbf{s}_r, \mathbf{s}_e))$, $(\mathbf{t}, d, (\mathbf{s}'_m, \mathbf{s}'_r, \mathbf{s}'_e))$ where $d \neq d'$, we can extract a vaild opening information of $\mathbf{c}$.

- Honest-Verifier Zero-Knowledge: Transcripts of the protocol with an honest verifier can be simulated with computationally indistinguishable distribution.

Completeness: When $d = 0$, P sends $\mathbf{s}_m = \mu, \mathbf{s}_r = \rho, \mathbf{s}_e = \eta$ to V. Thus $\mathbf{t} + d\mathbf{c} = \mathbf{t} = \mathbf{A}\mu + \mathbf{B}\rho + \eta = \mathbf{A}\mathbf{s}_m + \mathbf{B}\mathbf{s}_r + \mathbf{s}_e \bmod q$. Since $\rho \leftarrow D^n_{\sigma_2}, \eta \leftarrow D^m_{\sigma_3}$, $\|\mathbf{s}_r\|_\infty = \|\rho\|_\infty \leq 12\sigma_2$, and $\|\mathbf{s}_e\|_\infty = \|\eta\|_\infty \leq 12\sigma_3$ with overwhelming probability by lemma 5.3.1.

In the case $d \neq 0$, P sends $\mathbf{s}_m = \mu + d\mathbf{m}, \mathbf{s}_r = \rho + d\mathbf{r}, \mathbf{s}_e = \eta + d\mathbf{e}$ to V with probability close to $\frac{1}{M_2 M_3}$ overwhelmingly by the rejection sampling lemma. Thus $\mathbf{A}\mathbf{s}_m + \mathbf{B}\mathbf{s}_r + \mathbf{s}_e = \mathbf{A}\mu + \mathbf{B}\rho + \eta + d(\mathbf{A}\mathbf{m} + \mathbf{B}\mathbf{r} + \mathbf{e}) = \mathbf{t} + d\mathbf{c}$. Note that the distribution of $\mathbf{s}_r = \rho + d\mathbf{r}, \mathbf{s}_e = \eta + d\mathbf{e}$ are statistically close to $D^n_{\sigma_2}, D^m_{\sigma_3}$

respectively by the rejection sampling lemma. Hence, $\|\mathbf{s}_r\|_\infty \leq 12\sigma_2$, and $\|\mathbf{s}_e\|_\infty \leq 12\sigma_3$ with overwhelming probability by lemma 5.3.1. Therefore, V accepts with probability close to $\frac{1}{2\beta+1} + \frac{2\beta}{(2\beta+1)M_2M_3}$ overwhelmingly.

Special Soundness: Suppose two accepting transcripts $(\mathbf{t}, d, (\mathbf{s}_m, \mathbf{s}_r, \mathbf{s}_e))$, $(\mathbf{t}, d, (\mathbf{s}'_m, \mathbf{s}'_r, \mathbf{s}'_e))$ where $d \neq d'$ are given. Then the following equations are hold:

$$\mathbf{t} + d\mathbf{c} = \mathbf{A}\mathbf{s}_m + \mathbf{B}\mathbf{s}_r + \mathbf{s}_e \bmod q$$

$$\mathbf{t} + d'\mathbf{c} = \mathbf{A}\mathbf{s}'_m + \mathbf{B}\mathbf{s}'_r + \mathbf{s}'_e \bmod q$$

By subtracting the above equations, we get:

$$(d - d')\mathbf{c} = \mathbf{A}(\mathbf{s}_m - \mathbf{s}'_m) + \mathbf{B}(\mathbf{s}_r - \mathbf{s}'_r) + (\mathbf{s}_e - \mathbf{s}'_e) \bmod q$$

In other words, we have a witness $((d - d')^{-1}(\mathbf{s}_m - \mathbf{s}'_m), (\mathbf{s}_r - \mathbf{s}'_r), (\mathbf{s}_e - \mathbf{s}'_e), d - d')$ for $(\mathbf{A}, \mathbf{B}, \mathbf{c})$ such that $\|\mathbf{s}_r - \mathbf{s}'_r\|_\infty \leq 24\sigma_2$, and $\|\mathbf{s}_e - \mathbf{s}'_e\|_\infty \leq 24\sigma_3$. Note that the binding property of the commitment scheme implies $(d - d')^{-1}(\mathbf{s}_m - \mathbf{s}'_m) = \mathbf{m}$.

Honest-Verifier Zero-Knowledge: Let $\mathbf{c}$ and challenge d are given as inputs. First, the simulator samples $\mathbf{s}'_m \leftarrow \mathbb{Z}_q^l, \mathbf{s}'_r \leftarrow D_{\sigma_2}^n$, and $\mathbf{s}'_e \leftarrow D_{\sigma_3}^m$, and computes $\mathbf{t} = \mathbf{A}\mathbf{s}'_m + \mathbf{B}\mathbf{s}'_r + \mathbf{s}'_e - d\mathbf{c}$. In the case $d = 0$, the simulator outputs $(\mathbf{t}, 0, (\mathbf{s}'_m, \mathbf{s}'_r, \mathbf{s}'_e))$. This is statistically indistinguishable from accepting transcripts of the real protocol, since the distribution of response $(\mathbf{s}'_m, \mathbf{s}'_r, \mathbf{s}'_e)$ is statistically indistinguishable from the the distribution of real response by the rejection sampling lemma, and $\mathbf{t}$ is uniquely determined by $\mathbf{s}'_m, \mathbf{s}'_r, \mathbf{s}'_e$, and d in the real protocol and in the simulation. When $d \neq 0$, the simulator outputs $(\mathbf{t}, d, (\mathbf{s}'_m, \mathbf{s}'_r, \mathbf{s}'_e))$ with probability $\frac{1}{M_2M_3}$. Otherwise, the simulator outputs $(\mathbf{t}_0, d, \perp)$ where $\mathbf{t}_0 \leftarrow \mathbb{Z}_q^m$. The non-aborting case of this simulation is indistinguishable from the non-aborting case of the real protocol similary. $\mathbf{B}\rho + \eta \bmod q$ in $\mathbf{t} = \mathbf{A}\mu + \mathbf{B}\rho + \eta \bmod q$ in real protocol can be regarded as an instance of $\mathsf{LWE}_{n,m,q,\sigma_3}(D_{\sigma_2}^n)$, which is hard under the condition, $\mathsf{spLWE}_{n,m+n,q,s_1,\rho,\theta}$ is hard. Thus $\mathbf{t}$ is computationally indistinguishable

from $\mathbf{t}_0$, which is sampled from uniform random distribution over $\mathbb{Z}_q^m$. $\square$

5.3 Application to LWE-based Threshold Cytosystems

5.3.1 Zero-Knowledge Proofs of Knowledge for Threshold Decryption

Proof for Committed Messages

Like our zero-knowledge proof of opening information, let $\mathbf{c} = \mathbf{Am} + \mathbf{Br} + \mathbf{e} \bmod q$ be a commitment that is published by the prover. The prover can prove that $\mathbf{c}$ is a commitment of the message $\mathbf{m}$. This can be done by showing that the prover can prove he knows a valid randomness of $\mathbf{c}$ without revealing it. In this case, the public input is $(\mathbf{c}, \mathbf{m})$ and the private input is $(\mathbf{r}, \mathbf{e})$:

- P computes $\mathbf{t} = \mathbf{B}\rho + \eta \bmod q$ where $\rho \leftarrow D_{\sigma_2}^n, \eta \leftarrow D_{\sigma_3}^m$, and sends $\mathbf{t}$ to V.
- V sends a random integer $d \in [-\beta, \beta] \cap \mathbb{Z}$.
- P checks $d \in [-\beta, \beta] \cap \mathbb{Z}$, and computes $\mathbf{s}_r = \rho + d\mathbf{r} \bmod q, \mathbf{s}_e = \eta + d\mathbf{e} \bmod q$. If $d = 0$, P sends $\mathbf{s}_m = 0, \mathbf{s}_r, \mathbf{s}_e$ to V. Otherwise, P sends $\mathbf{s}_m = 0, \mathbf{s}_r, \mathbf{s}_e$ to V with probability $p = D_{\sigma_2}^n(\rho)/M_2 D_{d\mathbf{r},\sigma_2}^n(\rho) \times D_{\sigma_3}^n(\eta)/M_3 D_{d\mathbf{e},\sigma_3}^n(\eta)$, and $\perp$ with probability $1 - p$.
- V accepts iff $\mathbf{s}_m = 0$, $\mathbf{t} + d\mathbf{c} = \mathbf{B}\mathbf{s}_r + \mathbf{s}_e$, $\|\mathbf{s}_r\|_\infty \leq 12\sigma_2$, and $\|\mathbf{s}_e\|_\infty \leq 12\sigma_3$.

We now prove that the above protocol is indeed a zero-knowledge proof.

Theorem 5.3.1. *The protocol is a Σ'-protocol with completeness error close to $\frac{1}{\beta} + \frac{\beta-1}{\beta M_2 M_3}$ overwhelmingly for the relations:*

Proof. We can prove completeness, special soundness, and HVCZK of this protocol as in the previous case. The only difference is $\mathbf{s}_m = 0$. In this case, the simulator set the $\mathbf{s}'_m$ as 0 vector.

- Completeness: The verifier accepts with overwhelming probability if the protocol is not aborted by the prover, and the accepting probability is close to $\frac{1}{2\beta+1} + \frac{2\beta}{(2\beta+1)M_2M_3}$ overwhelmingly.
- Special Soundness: Given a commitment $\mathbf{c}$ and a pair of accepting transcripts $(\mathbf{t}, d, (0, \mathbf{s}_r, \mathbf{s}_e))$, $(\mathbf{t}, d, (0, \mathbf{s}'_r, \mathbf{s}'_e))$ where $d \neq d'$, we can extract a vaild opening information of $\mathbf{c}$.
- Honest-Verifier Zero-Knowledge: Transcripts of the protocol with an honest verifier can be simulated with computationally indistinguishable distribution.

□

Proof of Linear Relation

We now describe our zero-knowledge proof of linear relation. Let $\mathbf{c}_i = \mathbf{A}\mathbf{m}_i + \mathbf{B}\mathbf{r}_i + \mathbf{e}_i \bmod q$ for $i = 1, 2$ be commitments that are published by the prover such that $\mathbf{m}_2 = g(\mathbf{m}_1)$ for a linear function g. The goal of following protocol is to prove the linear relation of commited messages in zero-knowledge fashion. This can be done by modifying the previous zero-knowledge proof of opening information. The public inputs are $\mathbf{c}_i$ and g for $i = 1, 2$, and the private inputs are $(\mathbf{r}_i, \mathbf{e}_i)$ for $i = 1, 2$:

- P computes $\mathbf{t}_i = \mathbf{A}\mu_i + \mathbf{B}\rho_i + \eta_i \bmod q$ for $i = 1, 2$ where $\mu_1 \leftarrow \mathbb{Z}_q^l, \mu_2 = g(\mu_1), \rho_i \leftarrow D_{\sigma_2}^n, \eta_i \leftarrow D_{\sigma_3}^m$ for $i = 1, 2$, and sends $\mathbf{t}_1, \mathbf{t}_2$ to V.
- V sends a random integer $d \in [-\beta, \beta] \cap \mathbb{Z}$.
- P checks $d \in [-\beta, \beta] \cap \mathbb{Z}$, and computes $\mathbf{s}_{m,i} = \mu_i + d\mathbf{m}_i \bmod q, \mathbf{s}_{r,i} = \rho_i + d\mathbf{r}_i \bmod q, \mathbf{s}_{e,i} = \eta_i + d\mathbf{e}_i \bmod q$ for $i = 1, 2$. If $d = 0$, P sends $\mathbf{s}_{m,i}, \mathbf{s}_{r,i}, \mathbf{s}_{e,i}$

for $i = 1, 2$ to V. Otherwise, P sends $\mathbf{s}_{m,i}, \mathbf{s}_{r,i}, \mathbf{s}_{e,i}$ for $i = 1, 2$ to V with probability $p = \prod_{i=1}^{2} D^n_{\sigma_2}(\rho_i)/M_{2,i}D^n_{d\mathbf{r}_i,\sigma_2}(\rho_i) \times D^n_{\sigma_2}(\eta_i)/M_{3,i}D^n_{d\mathbf{e}_i,\sigma_2}(\eta_i)$, and $\perp$ with probability $1 - p$.

- V accepts iff $\mathbf{t}_i + d\mathbf{c}_i = \mathbf{A}\mathbf{s}_{m,i} + \mathbf{B}\mathbf{s}_{r,i} + \mathbf{s}_{e,i} \bmod q$, $\|\mathbf{s}_{r,i}\|_\infty \leq 12\sigma_2$, and $\|\mathbf{s}_{e,i}\|_\infty \leq 12\sigma_3$ for $i = 1, 2$, and $\mathbf{s}_{m,2} = g(\mathbf{s}_{m,1})$.

We now prove that the above protocol is indeed a zero-knowledge proof.

Theorem 5.3.2. *The protocol is a Σ'-protocol with completeness error close to $\frac{1}{2\beta+1} + \frac{2\beta}{(2\beta+1)\prod_{i=1}^{2} M_{2,i}M_{3,i}}$ overwhelmingly for the relations:*

Proof. We prove the protocol satisfies the following properties:

- Completeness: The verifier accepts with overwhelming probability if the protocol is not aborted by the prover, and the accepting probability is close to $\frac{1}{2\beta+1} + \frac{2\beta}{(2\beta+1)\prod_{i=1}^{2} M_{2,i}M_{3,i}}$ overwhelmingly.
- Special Soundness: Given commitments $\mathbf{c}_1, \mathbf{c}_2$ and a pair of accepting transcripts

$$(\mathbf{t}_1, \mathbf{t}_2, d, (\mathbf{s}_{m,1}, \mathbf{s}_{m,2}, \mathbf{s}_{r,1}, \mathbf{s}_{r,2}, \mathbf{s}_{e,1}, \mathbf{s}_{e,2}))$$

$$(\mathbf{t}_1, \mathbf{t}_2, d', (\mathbf{s}'_{m,1}, \mathbf{s}'_{m,2}, \mathbf{s}'_{r,1}, \mathbf{s}'_{r,2}, \mathbf{s}'_{e,1}, \mathbf{s}'_{e,2}))$$

  where $d \neq d'$, we can extract a vaild opening information of $\mathbf{c}_1$, and $\mathbf{c}_2$.

- Honest-Verifier Zero-Knowledge: Transcripts of the protocol with an honest verifier can be simulated with computationally indistinguishable distribution.

We can prove completeness, special soundness, and HVCZK of this protocol as in the previous case. The only difference is $\mathbf{s}_m = 0$. In this case, the simulator set the $\mathbf{s}'_m$ as 0 vector.

Completeness: When $d = 0$, P sends $\mathbf{s}_{m,i} = \mu_i, \mathbf{s}_{r,i} = \rho_i, \mathbf{s}_{e,i} = \eta_i$ to V for $i = 1, 2$. Thus $\mathbf{t}_i + d\mathbf{c}_i = \mathbf{t}_i = \mathbf{A}\mu_i + \mathbf{B}\rho_i + \eta_i = \mathbf{A}\mathbf{s}_{m,i} + \mathbf{B}\mathbf{s}_{r,i} + \mathbf{s}_{e,i} \bmod q$ for $i = 1, 2$. Since $\rho_i \leftarrow D^n_{\sigma_2}, \eta_i \leftarrow D^m_{\sigma_3}$, $\|\mathbf{s}_{r,i}\|_\infty = \|\rho_i\|_\infty \leq 12\sigma_2$, and

$\|\mathbf{s}_{e,i}\|_\infty = \|\eta_i\|_\infty \leq 12\sigma_3$ for $i = 1, 2$ with overwhelming probability by lemma 5.3.1. Note that $\mathbf{s}_{m,2} = \mu_2 = g(\mu_1) = g(\mathbf{s}_{m,1})$

In the case $d \neq 0$, P sends $\mathbf{s}_{m,i} = \mu_i + d\mathbf{m}_i, \mathbf{s}_{r,i} = \rho_i + d\mathbf{r}_i, \mathbf{s}_{e,i} = \eta_i + d\mathbf{e}_i$ to V with probability close to $\frac{1}{\prod_{i=1}^{2} M_{2,i}M_{3,i}}$ overwhelmingly by the rejection sampling lemma. Thus $\mathbf{A}\mathbf{s}_{m,i} + \mathbf{B}\mathbf{s}_{r,i} + \mathbf{s}_{e,i} = \mathbf{A}\mu_i + \mathbf{B}\rho_i + \eta_i + d(\mathbf{A}\mathbf{m}_i + \mathbf{B}\mathbf{r}_i + \mathbf{e}_i) = \mathbf{t}_i + d\mathbf{c}_i$ for $i = 1, 2$. Note that the distributions of $\mathbf{s}_{r,i} = \rho_i + d\mathbf{r}_i, \mathbf{s}_{e,i} = \eta_i + d\mathbf{e}_i$ for $i = 1, 2$ are statistically close to $D^n_{\sigma_2}, D^m_{\sigma_3}$ respectively by the rejection sampling lemma. Hence, $\|\mathbf{s}_{r,i}\|_\infty \leq 12\sigma_2$, and $\|\mathbf{s}_{e,i}\|_\infty \leq 12\sigma_3$ for $i = 1, 2$ with overwhelming probability by lemma 5.3.1, and $\mathbf{s}_{m,2} = \mu_2 + d\mathbf{m}_2 = g(\mu_1) + dg(\mathbf{m}_1) = g(\mathbf{s}_{m,1})$. Therefore, V accepts with probability close to $\frac{1}{2\beta+1} + \frac{2\beta}{(2\beta+1)(\prod_{i=1}^{2} M_{2,i}M_{3,i})}$ overwhelmingly.

Special Soundness: Suppose given two accepting transcripts

$$(\mathbf{t}_1, \mathbf{t}_2, d, (\mathbf{s}_{m,1}, \mathbf{s}_{m,2}, \mathbf{s}_{r,1}, \mathbf{s}_{r,2}, \mathbf{s}_{e,1}, \mathbf{s}_{e,2})),$$

$$(\mathbf{t}_1, \mathbf{t}_2, d', (\mathbf{s}'_{m,1}, \mathbf{s}'_{m,2}, \mathbf{s}'_{r,1}, \mathbf{s}'_{r,2}, \mathbf{s}'_{e,1}, \mathbf{s}'_{e,2}))$$

where $d \neq d'$. Then the following equations are hold:

$$\mathbf{t}_i + d\mathbf{c}_i = \mathbf{A}\mathbf{s}_{m,i} + \mathbf{B}\mathbf{s}_{r,i} + \mathbf{s}_{e,i} \bmod q$$

$$\mathbf{t}_i + d'\mathbf{c}_i = \mathbf{A}\mathbf{s}'_{m,i} + \mathbf{B}\mathbf{s}'_{r,i} + \mathbf{s}'_{e,i} \bmod q$$

By subtracting the above equations, we get:

$$(d - d')\mathbf{c}_i = \mathbf{A}(\mathbf{s}_{m,i} - \mathbf{s}'_{m,i}) + \mathbf{B}(\mathbf{s}_{r,i} - \mathbf{s}'_{r,i}) + (\mathbf{s}_{e,i} - \mathbf{s}'_{e,i}) \bmod q$$

In other words, we have a witness $((d-d')^{-1}(\mathbf{s}_{m,i} - \mathbf{s}'_{m,i}), (\mathbf{s}_{r,i} - \mathbf{s}'_{r,i}), (\mathbf{s}_{e,i} - \mathbf{s}'_{e,i}), d - d')$ for $(\mathbf{A}, \mathbf{B}, \mathbf{c}_i)$ such that $\|\mathbf{s}_{r,i} - \mathbf{s}'_r\|_\infty \leq 24\sigma_2$, and $\|\mathbf{s}_e - \mathbf{s}'_e\|_\infty \leq 24\sigma_3$ for $i = 1, 2$.

Honest-Verifier Zero-Knowledge: Let $\mathbf{c}_1, \mathbf{c}_2$ and challenge d are given as inputs. First, the simulator samples $\mathbf{s}'_{m,1} \leftarrow \mathbb{Z}^l_q, \mathbf{s}'_{r,i} \leftarrow D^n_{\sigma_2}$, $\mathbf{s}'_{e,i} \leftarrow D^m_{\sigma_3}$, and

computes $\mathbf{s}'_{m,2} = g(\mathbf{s}'_{m,1})$, $\mathbf{t}_i = \mathbf{A}\mathbf{s}'_{m,i} + \mathbf{B}\mathbf{s}'_{r,i} + \mathbf{s}'_{e,i} - d\mathbf{c}_i$ for $i = 1, 2$. In the case $d = 0$, the simulator outputs $(\mathbf{t}_1, \mathbf{t}_2, 0, (\mathbf{s}'_{m,1}, \mathbf{s}'_{m,2}, \mathbf{s}'_{r,1}, \mathbf{s}'_{r,2}, \mathbf{s}'_{e,1}, \mathbf{s}'_{e,2}))$. This is statistically indistinguishable from accepting transcripts of the real protocol, since the distribution of response $(\mathbf{s}'_{m,1}, \mathbf{s}'_{m,2}, \mathbf{s}'_{r,1}, \mathbf{s}'_{r,2}, \mathbf{s}'_{e,1}, \mathbf{s}'_{e,2})$ is statistically indistinguishable from the the distribution of real response by the rejection sampling lemma, and $\mathbf{t}_i$ is uniquely determined by $\mathbf{s}'_{m,i}, \mathbf{s}'_{r,i}, \mathbf{s}'_{e,i}$, and d in the real protocol and in the simulation. When $d \neq 0$, the simulator outputs $(\mathbf{t}_1, \mathbf{t}_2, 0, (\mathbf{s}'_{m,1}, \mathbf{s}'_{m,2}, \mathbf{s}'_{r,1}, \mathbf{s}'_{r,2}, \mathbf{s}'_{e,1}, \mathbf{s}'_{e,2}))$ with probability $\prod_{i=1}^{2} M_{2,i} M_{3,i}$. Otherwise, the simulator outputs $(\mathbf{t}_{0,1}, \mathbf{t}_{0,2}, d, \perp)$ where $\mathbf{t}_{0,i} \leftarrow \mathbb{Z}_q^m$ for $i = 1, 2$. The non-aborting case of this simulation is indistinguishable from the non-aborting case of the real protocol simillary. $\mathbf{B}\rho_i + \eta_i \bmod q$ in $\mathbf{t}_i = \mathbf{A}\mu_i + \mathbf{B}\rho_i + \eta_i \bmod q$ in real protocol can be regarded as an instance of $\mathsf{LWE}_{n,m,q,\sigma_3}(D^n_{\sigma_2})$, which is hard under the condition, $\mathsf{spLWE}_{n,m+n,q,s_1,\rho,\theta}$ is hard. Thus $\mathbf{t}_i$ is computationally indistinguishable from $\mathbf{t}_{0,i}$, which is sampled from uniform random distribution over $\mathbb{Z}_q^m$

□

Proof of Sum

We now describe our zero-knowledge proof of sum. Let $\mathbf{c}_i = \mathbf{A}\mathbf{m}_i + \mathbf{B}\mathbf{r}_i + \mathbf{e}_i \bmod q$ for $i = 1, 2, 3$ be commitments that are published by the prover such that $\mathbf{m}_3 = \mathbf{m}_1 + \mathbf{m}_2$. The goal of following protocol is to prove the sum relation of commited messages in zero-knowledge fashion. The idea of the zero-knowledge proof is similar to the previous proof of linear relation. We now describe the zero-knowledge proof of sum as follows. The public inputs are $\mathbf{c}_i$ for $i = 1, 2, 3$, and the private inputs are $(\mathbf{r}_i, \mathbf{e}_i)$ for $i = 1, 2, 3$:

- P computes $\mathbf{t}_i = \mathbf{A}\mu_i + \mathbf{B}\rho_i + \eta_i \bmod q$ for $i = 1, 2, 3$ where $\mu_1, \mu_2 \leftarrow \mathbb{Z}_q^l, \mu_3 = \mu_1 + \mu_2, \rho_i \leftarrow D^n_{\sigma_2}, \eta_i \leftarrow D^m_{\sigma_3}$ for $i = 1, 2, 3$, and sends $\mathbf{t}_1, \mathbf{t}_2, \mathbf{t}_3$ to V.

- V sends a random integer $d \in [-\beta, \beta] \cap \mathbb{Z}$.

- P checks $d \in [-\beta, \beta] \cap \mathbb{Z}$, and computes $\mathbf{s}_{m,i} = \mu_i + d\mathbf{m}_i \bmod q, \mathbf{s}_{r,i} = \rho_i + d\mathbf{r}_i \bmod q, \mathbf{s}_{e,i} = \eta_i + d\mathbf{e}_i \bmod q$ for $i = 1, 2, 3$. If $d = 0$, P sends $\mathbf{s}_{m,i}, \mathbf{s}_{r,i}, \mathbf{s}_{e,i}$ for $i = 1, 2, 3$ to V. Otherwise, P sends $\mathbf{s}_{m,i}, \mathbf{s}_{r,i}, \mathbf{s}_{e,i}$ for $i = 1, 2, 3$ to V with probability $p = \prod_{i=1}^{3} D^n_{\sigma_2}(\rho_i)/M_{2,i}D^n_{d\mathbf{r}_i,\sigma_2}(\rho_i) \times D^n_{\sigma_3}(\eta_i)/M_{3,i}D^n_{d\mathbf{e}_i,\sigma_2}(\eta_i)$, and $\perp$ with probability $1 - p$.

- V accepts iff $\mathbf{t}_i + d\mathbf{c}_i = \mathbf{A}\mathbf{s}_{m,i} + \mathbf{B}\mathbf{s}_{r,i} + \mathbf{s}_{e,i} \bmod q$, $\|\mathbf{s}_{r,i}\|_\infty \leq 12\sigma_2$, and $\|\mathbf{s}_{e,i}\|_\infty \leq 12\sigma_3$ for $i = 1, 2, 3$, and $\mathbf{s}_{m,3} = \mathbf{s}_{m,1} + \mathbf{s}_{m,2}$.

We now prove that the above protocol is indeed a zero-knowledge proof.

Theorem 5.3.3. *The protocol is a Σ'-protocol with completeness error close to $\frac{1}{2\beta+1} + \frac{2\beta}{(2\beta+1)\prod_{i=1}^{3} M_{2,i}M_{3,i}}$ overwhelmingly for the relations:*

Proof. We prove the protocol satisfies the following properties:

- Completeness: The verifier accepts with overwhelming probability if the protocol is not aborted by the prover, and the accepting probability is close to $\frac{1}{2\beta+1} + \frac{2\beta}{(2\beta+1)\prod_{i=1}^{3} M_{2,i}M_{3,i}}$ overwhelmingly.

- Special Soundness: Given commitments $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3$ and a pair of accepting transcripts

$$(\mathbf{t}_1, \mathbf{t}_2, \mathbf{t}_3, d, (\mathbf{s}_{m,1}, \mathbf{s}_{m,2}, \mathbf{s}_{m,3}, \mathbf{s}_{r,1}, \mathbf{s}_{r,2}, \mathbf{s}_{r,3}, \mathbf{s}_{e,1}, \mathbf{s}_{e,2}, \mathbf{s}_{e,3}))$$

$$(\mathbf{t}'_1, \mathbf{t}'_2, \mathbf{t}'_3, d, (\mathbf{s}'_{m,1}, \mathbf{s}'_{m,2}, \mathbf{s}'_{m,3}, \mathbf{s}'_{r,1}, \mathbf{s}'_{r,2}, \mathbf{s}'_{r,3}, \mathbf{s}'_{e,1}, \mathbf{s}'_{e,2}, \mathbf{s}'_{e,3}))$$

  where $d \neq d'$, we can extract a vaild opening information of $\mathbf{c}_1$, $\mathbf{c}_2$ and $\mathbf{c}_3$.

- Honest-Verifier Zero-Knowledge: Transcripts of the protocol with an honest verifier can be simulated with computationally indistinguishable distribution.

We can prove completeness, special soundness, and zero knowledgeness of this protocol as in the previous case, proof of linear relation. The only difference is $\mathbf{s}_m = 0$. In this case, the simulator set the $\mathbf{s}'_m$ as 0 vector. □

Proof of Bound

We now describe our zero-knowledge proof of bound. Let $\mathbf{c} = \mathbf{Am} + \mathbf{Br} + \mathbf{e} \bmod q$ be a commitment that is published by the prover. The goal of the following protocol is to prove the smallness of committed messages in zero-knowledge fashion. The idea of the zero-knowledge proof is to check smallness of a commited message when a short random vector is added. We now describe the zero-knowledge proof of bound as follows. The public inputs is $\mathbf{c}$, and the private inputs is $(\mathbf{m}, \mathbf{r}, \mathbf{e})$:

- P computes $\mathbf{t} = \mathbf{A}\mu + \mathbf{B}\rho + \eta$ where $\mu \leftarrow ([-\beta_m(1+\frac{\gamma m}{2}, \beta_m(1+\frac{\gamma m}{2})] \cap \mathbb{Z})^l, \rho \leftarrow D^n_{\sigma_2}, \eta \leftarrow D^m_{\sigma_3}$, and sends $\mathbf{t}$ to V.
- V sends a random integer $d \leftarrow \{0,1\}$.
- P checks $d \in \{0,1\}$, and computes $\mathbf{s}_m = \mu + d\mathbf{m} \bmod q, \mathbf{s}_r = \rho + d\mathbf{r} \bmod q, \mathbf{s}_e = \eta + d\mathbf{e} \bmod q$. When $d = 0$, if $\|\mathbf{s}_m\|_\infty > \gamma m\beta_m/2$, P sends $\perp$, otherwise sends $\mathbf{s}_m, \mathbf{s}_r, \mathbf{s}_e$ to V. When $d \neq 0$, if $\|\mathbf{s}_m\|_\infty > \gamma m\beta_m/2$, P sends $\perp$, otherwise sends $\mathbf{s}_m, \mathbf{s}_r, \mathbf{s}_e$ to V with probability $p = D^n_{\sigma_2}(\rho)/M_2 D^n_{d\mathbf{r},\sigma_2}(\rho) \times D^n_{\sigma_2}(\eta)/M_3 D^n_{d\mathbf{e},\sigma_2}(\eta)$, and $\perp$ with probability $1-p$.
- V accepts iff $\mathbf{t} + d\mathbf{c} = \mathbf{A}\mathbf{s}_m + \mathbf{B}\mathbf{s}_r + \mathbf{s}_e \bmod q$, $\|\mathbf{s}_m\|_\infty \leq \gamma m\beta_m/2$, $\|\mathbf{s}_r\|_\infty \leq 12\sigma_2$, and $\|\mathbf{s}_e\|_\infty \leq 12\sigma_3$.

We now prove that the above protocol is indeed a zero-knowledge proof.

Theorem 5.3.4. *The protocol is a Σ'-protocol with completeness error close to $\frac{p'}{2} + \frac{p'}{2M_2M_3}$ overwhelmingly for the relations where $p' = (1 - \frac{2\beta_m}{2\beta_m(1+\gamma m/2)+1})^l$:*

Proof. We prove the protocol satisfies the following properties:

- Completeness: The verifier accepts with overwhelming probability if the protocol is not aborted by the prover, and the accepting probability is close to $\frac{p'}{2} + \frac{p'}{2M_2M_3}$ overwhelmingly.

- Special Soundness: Given a commitment $\mathbf{c}$ and a pair of accepting transcripts $(\mathbf{t}, d, (\mathbf{s}_m, \mathbf{s}_r, \mathbf{s}_e))$, $(\mathbf{t}, d, (\mathbf{s}'_m, \mathbf{s}'_r, \mathbf{s}'_e))$ where $d \neq d'$, we can extract a vaild opening information of $\mathbf{c}$ whose infinite norm of message $\mathbf{m}$ is bounded by $\gamma m \beta_m / 2$.

- Honest-Verifier Zero-Knowledge: Transcripts of the protocol with an honest verifier can be simulated with computationally indistinguishable distribution.

Completeness: The probability that a single coefficient of $\mathbf{s}_m$ will cause an abortion of the protocol is $\frac{2\beta_m}{2\beta_m(1+\gamma m/2)+1}$. Thus, the probability that $\mathbf{s}_m$ will cause an abortion of the protocol is $1 - (1 - \frac{2\beta_m}{2\beta_m(1+\gamma m/2)+1})^l = 1 - p'$.

When $d = 0$, and $\|\mathbf{s}_m\|_\infty \leq \gamma m \beta_m / 2$, P sends $\mathbf{s}_m = \mu, \mathbf{s}_r = \rho, \mathbf{s}_e = \eta$ to V. Thus $\mathbf{t} + d\mathbf{c} = \mathbf{t} = \mathbf{A}\mu + \mathbf{B}\rho + \eta = \mathbf{A}\mathbf{s}_m + \mathbf{B}\mathbf{s}_r + \mathbf{s}_e \bmod q$. Since $\rho \leftarrow D^n_{\sigma_2}, \eta \leftarrow D^m_{\sigma_3}$, $\|\mathbf{s}_r\|_\infty = \|\rho\|_\infty \leq 12\sigma_2$, and $\|\mathbf{s}_e\|_\infty = \|\eta\|_\infty \leq 12\sigma_3$ with overwhelming probability by lemma 5.3.1. The probability that this case occurs is $\frac{p'}{2}$

In the case $d = 1$, if $\|\mathbf{s}_m\|_\infty \leq \gamma m \beta_m / 2$, P sends $\mathbf{s}_m = \mu + \mathbf{m}, \mathbf{s}_r = \rho + \mathbf{r}, \mathbf{s}_e = \eta + \mathbf{e}$ to V with probability close to $\frac{1}{M_2 M_3}$ overwhelmingly by the rejection sampling lemma. Thus $\mathbf{A}\mathbf{s}_m + \mathbf{B}\mathbf{s}_r + \mathbf{s}_e = \mathbf{A}\mu + \mathbf{B}\rho + \eta + (\mathbf{A}\mathbf{m} + \mathbf{B}\mathbf{r} + \mathbf{e}) = \mathbf{t} + d\mathbf{c}$. Note that the distribution of $\mathbf{s}_r = \rho + \mathbf{r}, \mathbf{s}_e = \eta + \mathbf{e}$ are statistically close to $D^n_{\sigma_2}, D^m_{\sigma_3}$ respectively by the rejection sampling lemma. Hence, $\|\mathbf{s}_r\|_\infty \leq 12\sigma_2$, and $\|\mathbf{s}_e\|_\infty \leq 12\sigma_3$ with overwhelming probability by lemma 5.3.1. Therefore, V accepts with probability close to $\frac{p'}{2} + \frac{p'}{2M_2 M_3}$ overwhelmingly.

Special Soundness: Suppose two accepting transcripts $(\mathbf{t}, d, (\mathbf{s}_m, \mathbf{s}_r, \mathbf{s}_e))$, $(\mathbf{t}, d, (\mathbf{s}'_m, \mathbf{s}'_r, \mathbf{s}'_e))$ where $d \neq d'$ are given. Then the following equations are hold:

$$\mathbf{t} + d\mathbf{c} = \mathbf{A}\mathbf{s}_m + \mathbf{B}\mathbf{s}_r + \mathbf{s}_e \bmod q$$

$$\mathbf{t} + d'\mathbf{c} = \mathbf{A}\mathbf{s}'_m + \mathbf{B}\mathbf{s}'_r + \mathbf{s}'_e \bmod q$$

By subtracting the above equations, we get:

$$(d-d')\mathbf{c} = \mathbf{A}(\mathbf{s}_m - \mathbf{s}'_m) + \mathbf{B}(\mathbf{s}_r - \mathbf{s}'_r) + (\mathbf{s}_e - \mathbf{s}'_e) \bmod q$$

In other words, we have a witness $((d-d')^{-1}(\mathbf{s}_m - \mathbf{s}'_m), (\mathbf{s}_r - \mathbf{s}'_r), (\mathbf{s}_e - \mathbf{s}'_e), d-d')$ for $(\mathbf{A}, \mathbf{B}, \mathbf{c})$ such that $\|\mathbf{s}_r - \mathbf{s}'_r\|_\infty \leq 24\sigma_2$, and $\|\mathbf{s}_e - \mathbf{s}'_e\|_\infty \leq 24\sigma_3$. Note that $\|(d-d')^{-1}(\mathbf{s}_m - \mathbf{s}'_m)\|_\infty = \|\mathbf{s}_m - \mathbf{s}'_m\|_\infty \leq 2\|\mathbf{s}_m\|_\infty = \gamma m \beta_m$.

Honest-Verifier Zero-Knowledge: Let $\mathbf{c}$ and challenge d are given as inputs. First, the simulator samples $\mathbf{s}'_m \leftarrow \{-\gamma m\beta_m/2, \gamma m\beta_m/2\}^l, \mathbf{s}'_r \leftarrow D^n_{\sigma_2}$, and $\mathbf{s}'_e \leftarrow D^m_{\sigma_3}$, and computes $\mathbf{t} = \mathbf{A}\mathbf{s}'_m + \mathbf{B}\mathbf{s}'_r + \mathbf{s}'_e - d\mathbf{c}$. In the case $d = 0$, the simulator outputs $(\mathbf{t}, 0, (\mathbf{s}'_m, \mathbf{s}'_r, \mathbf{s}'_e))$ with probability p'. This is statistically indistinguishable from accepting transcripts of the real protocol, since the distribution of response $(\mathbf{s}'_m, \mathbf{s}'_r, \mathbf{s}'_e)$ is statistically indistinguishable from the the distribution of real response by the rejection sampling lemma, and $\mathbf{t}$ is uniquely determined by $\mathbf{s}'_m, \mathbf{s}'_r, \mathbf{s}'_e$, and d in the real protocol and in the simulation. When $d = 1$, the simulator outputs $(\mathbf{t}, d, (\mathbf{s}'_m, \mathbf{s}'_r, \mathbf{s}'_e))$ with probability $\frac{p'}{M_2 M_3}$. Otherwise, the simulator outputs $(\mathbf{t}_0, d, \perp)$ where $\mathbf{t}_0 \leftarrow \mathbb{Z}^m_q$. The non-aborting case of this simulation is indistinguishable from the non-aborting case of the real protocol simillary. $\mathbf{B}\rho + \eta \bmod q$ in $\mathbf{t} = \mathbf{A}\mu + \mathbf{B}\rho + \eta \bmod q$ in real protocol can be regarded as an instance of $\mathsf{LWE}_{n,m,q,\sigma_3}(D^n_{\sigma_2})$, which is hard under the condition, $\mathsf{spLWE}_{n,m+n,q,s_1,\rho,\theta}$ is hard. Thus $\mathbf{t}$ is computationally indistinguishable from $\mathbf{t}_0$, which is sampled from uniform random distribution over $\mathbb{Z}^m_q$. □

5.3.2 Actively Secure Threshold Cryptosystems

In this section, we explain how to convert LWE-based cryptosystems into actively secure threshold cryptosystem with the proofs which is introduced in previous section. This conversion can be applied to a broad class of LWE-based PKE's and FHE's such as [Reg09], [LP11], [CHK+16], [GSW13], [BV14], [ZB12] satisfying the following properties. The decryption algorithm consists of two procedures. In the first step, the algorithm takes as input a

secret key $\mathbf{s}k \in \mathbb{Z}_q^{n\times l}$ and a ciphertext $\mathbf{c}t \in \mathbb{Z}_q^l$ and computes a function $f_{\mathbf{c}t}$, which is linear in $\mathbf{s}k$ to output $encode(\mathbf{m}) + \mathbf{e}$ where each $\mathbf{e}_i \in [-B, B]$ is an error term bounded by for some $B \ll q$ and $\mathbf{m} \in \{0,1\}^l$ is the message of the ciphertext $\mathbf{c}t$. In the second step, it properly decodes the output of the first step to recover message $\mathbf{m}$. Since the decryption algorithm performs linear function $f_{\mathbf{c}t}$ with the key $\mathbf{s}k$, one can construct a threshold version of the decryption naively: Simply split the secret key $\mathbf{s}k$ with a linear secret sharing scheme Π with some access structure A on a set of servers $S = \{S_1, \ldots, S_N\}$ into $\mathbf{s}k_1, \ldots, \mathbf{s}k_N$, and transmit the secret key share $\mathbf{s}k_i$ to the server S_i for all i. Then each server compute $f_{\mathbf{c}t}(\mathbf{s}k_i)$ as a partial decryption. For any set $T \in A \subseteq 2^S$, there exist a set of coefficients $\{c_i\}_{i\in T}$ such that $\sum_{i\in T} c_i \mathbf{s}k_i = \mathbf{s}k$ and then by linearity of $f_{\mathbf{c}t}$, the combiner gets $c_i f_{\mathbf{c}t}(\mathbf{s}k_i) = encode(\mathbf{m}) + \mathbf{e}$. To sum up, naive version of threshold decryption can be obtained by applying a linear secret sharing since the decryption algorithm consists of linear operations. However, a sufficient numbers of outputs of partial decryption allows a reconstruction of the secret key share $\mathbf{s}k_i$ by linearty of $f_{\mathbf{c}t}$. In order to adress this problem, a masking is necessary i.e. each server must output the partial decryption as

$$f_{\mathbf{c}t}(\mathbf{s}k_i) + \mathbf{e}_{smudge}$$

where each component of $\mathbf{e}_{smudge}$ is sampled from a uniform distribution over sufficiently large interval. The following lemma tell us how big error bounds are required. This technique is known as "smudging".

Lemma 5.3.1 ([Koh16] , Smudging)**.** *Let k be the security parameter and let $negl : \mathbb{N} \to \mathbb{R}_{>0}$ be a negligible function. Let $b_1(k), b_2(k) \in \mathbb{N}$ be bounds with $b_1(k)/b_2(k) \leq negl(k)$. Let $e(k) \in [-b_1, b_1]$ be an arbitrary integer and $\psi(k)$ be the uniform distributionon $[-b_2, b_2] \cap \mathbb{Z}$. Then the distribution $e + \psi$ obtained by drawing an $\tilde{e} \in \psi$ and returning $e + \tilde{e}$, is statistically indistinguishable to the distribution ψ.*

By applying the above technique, we get a LWE-based threshold cryptosystem that is passively secure, and IND-CCA secure in random oracle

model. One can convert the threshold cryptosystem to a actively secure one by adding some additional proof for decryption procedure. This can be done via non-interactive version of the previous zero-knowledge proofs. One can obtain these proofs by applying the "Fiat-Shamir Heuristic": The challenge c is computed by a prover as $c = H(\mathbf{t})$, where $H : \{0,1\}^* \to \{0,1\}^t$ be a hash function. Let $proof_i = (proof_{bd,i}, proof_{lin,i}, proof_{sum,i}, proof_{mes,i})$ be the non-interactive version of the previous zero-knowledge proofs. Sine one can get negligible soundness error and overwhelming completeness error from parallel repeations, we assume the proof $proof_i$ also achieves that. We first thresholdize the spLWE-based KEM in [CHK+16].

- TKEM.Params(λ): generate a bit-length of seed y and spLWE parameters $n, m, q, s, \rho, \theta, s', \rho', \theta'$ with λ-bit security. Publish all parameters by pp.

- TKEM.Keygen(pp): sample $seed_A \leftarrow \{0,1\}^y, \mathbf{A} \leftarrow Gen(seed_A), \mathbf{e} \leftarrow D^m_{\mathbb{Z},s}$ and $\mathbf{s} \leftarrow \mathcal{U}(X_{n,\rho,\theta})$, and compute $\mathbf{b} = \mathbf{As}+\mathbf{e} \in \mathbb{Z}_q^m$. For a secret key $\mathsf{sk} = \mathbf{s}$, $\mathbf{s}$ is randomly divided into t pieces $\mathsf{sk}_1 = \mathbf{s}_1, \ldots, \mathsf{sk}_t = \mathbf{s}_t$. The verification key vk is the description of the commitment scheme. The verification key share $vk_i = Com(sk_i)$, sk_i is the opening information of vk_i. publish a corresponding public key $\mathsf{pk} = (seed_A, \mathbf{b})$.

- TKEM.Encap(pk,pp): sample $\mathbf{u} \leftarrow X_{m,\rho',\theta'}$, $(e_1, \mathbf{e}_2) \leftarrow D_{\mathbb{Z},s'} \times D^n_{\mathbb{Z},s'}$ and $e_3 \in \{0,1\}$. Let $\mathbf{v} = \mathbf{u}^T\mathbf{b} + \mathbf{e}_1 \in \mathbb{Z}_q$ and $\bar{\mathbf{v}} = 2\mathbf{v} + \mathbf{e}_3 \in \mathbb{Z}_{2q}$. Compute $\mathbf{c_1} = \langle \bar{\mathbf{v}} \rangle_2 \in \mathbb{Z}_2$ and $\mathbf{c_2} = \mathbf{u}^T\mathbf{A} + \mathbf{e_2} \in \mathbb{Z}_q^n$ from $\mathbf{A} \leftarrow Gen(seed_A)$. Send a ciphertext $\mathbf{c} = (\mathbf{c_1}, \mathbf{c_2}) \in \mathbb{Z}_2 \times \mathbb{Z}_q^n$ to the receiver, and store an ephemeral secret key $\mu = \lfloor \bar{\mathbf{v}} \rceil_2 \in \mathbb{Z}_2$.

- TKEM.PartialDecap($\mathbf{c}, \mathsf{sk_i}, vk, vk_i$): Compute $w_i = 2\mathbf{c_2}^T\mathbf{s}_i + e_{sm,i} \in \mathbb{Z}_q$, $Com(e_{sm,i}), Com(\mathbf{c_2}^T\mathbf{s_i}), Com(\mathbf{c_2}^T\mathbf{s_i}+e_{sm,i})$, and send them with $proof_i$.

- TKEM.Combine($\mathbf{c}, \{w_i\}_{i=1}^t, \{vk_i\}_{i=1}^t, (Com(e_{sm,i}), Com(\mathbf{c_2}^T\mathbf{s_i}), Com(\mathbf{c_2}^T\mathbf{s_i}+e_{sm,i})), proof_i$): If one of proofs is invalid, output $\perp$. Otherwise, Compute $\sum w_i = 2\mathbf{c_2}^T\mathbf{s} + \sum e_{sm,i}$, and output $\mu = \boldsymbol{rec}(\sum w_i, c_1)$.

We now construct a (t, t)-threshold public cryptosystem based on the spLWE-based threshold KEM.

- TPKE_1.Params(λ): let ℓ be a message length, and run TKEM.Params(λ) with ℓ. Publish all parameters by pp.(For simple description, we assume that $l = 1$.)

- TPKE_1.Keygen(pp): output a key pair, and secret key shares (pk, sk), $\mathbf{s}_1, \ldots, \mathbf{s}_t$, and verification key vk, its shares vk_i's $\leftarrow$ TKEM.Keygen(pp).

- TPKE_1.Enc(pk, $\mathbf{m}$, pp): for $\mathbf{c}, \mu \leftarrow$ TKEM.Encap(pk,pp), compute $\mathbf{c}' = \mathbf{m} \oplus \mu$ and output a ciphertext $(\mathbf{c}, \mathbf{c}')$.

- TPKE_1.PartialDec($(\mathbf{c}, \mathbf{c}')$, $\mathsf{sk_i}$, vk, vk_i): Output $w_i, Com(e_{sm,i}), Com(\mathbf{c_2}^T\mathbf{s_i})$, $Com(\mathbf{c_2}^T\mathbf{s_i} + e_{sm,i})$, $proof_i \leftarrow$ TKEM.PartialDecap($\mathbf{c}$, $\mathsf{sk_i}$, vk, vk_i)

- TPKE_1.Combine($(\mathbf{c}, \mathbf{c}')$, $\{w_i\}_{i=1}^t$, $(Com(e_{sm,i}), Com(\mathbf{c_2}^T\mathbf{s_i}), Com(\mathbf{c_2}^T\mathbf{s_i} + e_{sm,i})), proof_i$): for $\mu =$ TKEM.Combine($\mathbf{c}$, $\{w_i\}_{i=1}^t$, $(Com(e_{sm,i}), Com(\mathbf{c_2}^T\mathbf{s_i})$, $Com(\mathbf{c_2}^T\mathbf{s_i} + e_{sm,i})), proof_i$), output $\mathbf{m} = \mathbf{c}' \oplus \mu$.

Finally, we have a LWE-based threshold public-key cryptosystem PKE_2 which is actively secure in random oracle model.

- PKE_2.Params(λ): let ℓ be a message length and $k_i > 0$ be integers such that hash functions $G : \{0,1\}^{k_1+\ell} \to \{0,1\}^*$, $H : \{0,1\}^{k_1} \to \{0,1\}^{k_2}$ and $H' : \{0,1\}^{k_1} \to \{0,1\}^{k_3}$ have λ-bit security. Let pp be an output of KEM.Params(λ) with k_1. Publish ℓ, pp and k_i.

- PKE_2.Keygen(pp): output a key pair, and secret key shares (pk, sk), $\mathbf{s}_1, \ldots, \mathbf{s}_t$, and verification key vk, its shares vk_i's $\leftarrow$ TKEM.Keygen(pp).

- PKE_2.Enc(pk, $\mathbf{m}$, pp, k_i): randomly choose $\omega \leftarrow \{0,1\}^{k_1}$, and let $\mathbf{c_m} = H(\omega) \oplus \mathbf{m}$. Compute $\mathbf{c}_h = H'(\omega)$ and $(\mathbf{c}, \mathbf{c}') \leftarrow \mathrm{PKE}_1$.Enc(pk, ω; $G(\omega || \mathbf{c_m})$). Output a ciphertext $(\mathbf{c}, \mathbf{c}', \mathbf{c}_h, \mathbf{c_m})$.

- $\text{PKE}_2.\mathsf{PartialDec}((\mathbf{c}, \mathbf{c}', \mathbf{c}_h, \mathbf{c_m}), \mathsf{sk_i}, vk, vk_i)$: Output $w_i, Com(e_{sm,i}), Com(\mathbf{c_2}^T\mathbf{s_i}), Com(\mathbf{c_2}^T\mathbf{s_i} + e_{sm,i}), proof_i \leftarrow \mathsf{KEM.PartialDecap}(\mathbf{c}, \mathsf{sk_i}, vk, vk_i)$

- $\text{PKE}_2.\mathsf{Combine}((\mathbf{c}, \mathbf{c}', \mathbf{c}_h, \mathbf{c_m}), \{w_i\}_{i=1}^t, \mathsf{pp}, k_i, Com(\mathbf{c_2}^T\mathbf{s_i}), Com(\mathbf{c_2}^T\mathbf{s_i} + e_{sm,i})), proof_i)$: Compute $\omega = \text{PKE}_1.\mathsf{Combine}((\mathbf{c}, \mathbf{c}'), \{w_i\}_{i=1}^t, Com(\mathbf{c_2}^T\mathbf{s_i}), Com(\mathbf{c_2}^T\mathbf{s_i} + e_{sm,i})), proof_i)$ and $\mathbf{m} = H(\omega) \oplus \mathbf{c_m}$. Check whether $(\mathbf{c}, \mathbf{c}') = \text{PKE}_1.\mathsf{Enc}(\mathsf{pk}, \omega; G(\mathbf{w}||\mathbf{c_m}))$ and $\mathbf{c}_h = H'(\omega)$. If so, output $\mathbf{m}$, otherwise output $\perp$.

Chapter 6

Conclusions

In this thesis, we introduced a variant of LWE with a sparse secret, spLWE for more efficient construction of public-key encryption and commitment schemes. First, we define the variant problem, spLWE, and provide analysis for it: We show that spLWE can be reduced from LWE, which means that the hardness of spLWE can also be based on the worst-case lattice problems, gapSVP and SIVP. On the other hand, we exclude the parameters which have provable security from our reduction since it is not tight enough to be useful in parameter setting. We also extend all known LWE attacks in order to estimate concrete hardness of spLWE. These are used to select efficient and secure parameters: It requires relatively larger dimension than that of LWE to maintain security. However, we verify that the problem of increase in dimension can be relieved by using a small modulus q. In conclusion, we can choose more compact parameters in spLWE-based encryption and commitment schemes. Of course, new developments of cryptanalysis for spLWE with a bigger community would be required.

From the analysis of spLWE, we propose efficient post-quantum public-key encryption and commitment schemes with related zero knowledge protocols based on spLWE: We suggest an IND-CPA PKE and its IND-CCA conversion in the quantum random oracle model by applying the modified Fujisaki-Okamoto conversion of Unruh. In commitment case, we give a variety of

versions of commitment schemes which are based on LWE and its variants. In particular, we also propose a commitment scheme dedicated for the zero-knowledge proofs suggested in this thesis. Finally, as a application, we show how to convert our PKE into a threshold cryptosystem which has active security with previous constructions.

Bibliography

[ABD16] Martin Albrecht, Shi Bai, and Léo Ducas. A subfield lattice attack on overstretched ntru assumptions: Cryptanalysis of some fhe and graded encoding schemes. Cryptology ePrint Archive, Report 2016/127, 2016. `http://eprint.iacr.org/2016/127`.

[ACF+14] Martin Albrecht, Carlos Cid, Jean-Charles Faugere, Robert Fitzpatrick, and Ludovic Perret. Algebraic algorithms for lwe problems. 2014.

[AFG13] Martin R Albrecht, Robert Fitzpatrick, and Florian Göpfert. On the efficacy of solving lwe by reduction to unique-svp. In *International Conference on Information Security and Cryptology*, pages 293–310. Springer, 2013.

[AG11] Sanjeev Arora and Rong Ge. New algorithms for learning in presence of errors. In *International Colloquium on Automata, Languages, and Programming*, pages 403–415. Springer, 2011.

[AJLA+12] Gilad Asharov, Abhishek Jain, Adriana López-Alt, Eran Tromer, Vinod Vaikuntanathan, and Daniel Wichs. Multiparty computation with low communication, computation and interaction via threshold fhe. *Advances in Cryptology–EUROCRYPT 2012*, pages 483–501, 2012.

BIBLIOGRAPHY

[Ajt96] Miklós Ajtai. Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 99–108. ACM, 1996.

[APS15] Martin R Albrecht, Rachel Player, and Sam Scott. On the concrete hardness of learning with errors. *Journal of Mathematical Cryptology*, 9(3):169–203, 2015.

[Ban95] Wojciech Banaszczyk. Inequalities for convex bodies and polar reciprocal lattices inr n. *Discrete & Computational Geometry*, 13(2):217–231, 1995.

[BCD+16] Joppe Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from lwe. 2016.

[BCK+14] Fabrice Benhamouda, Jan Camenisch, Stephan Krenn, Vadim Lyubashevsky, and Gregory Neven. Better zero-knowledge proofs for lattice encryption and their application to group signatures. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 551–572. Springer, 2014.

[BCNS15] Joppe W Bos, Craig Costello, Michael Naehrig, and Douglas Stebila. Post-quantum key exchange for the tls protocol from the ring learning with errors problem. In *2015 IEEE Symposium on Security and Privacy*, pages 553–570. IEEE, 2015.

[BD10] Rikke Bendlin and Ivan Damgård. Threshold decryption and zero-knowledge proofs for lattice-based cryptosystems. In *TCC*, volume 5978, pages 201–218. Springer, 2010.

[BDGL16] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications

to lattice sieving. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 10–24. SIAM, 2016.

[BDOP16] Carsten Baum, Ivan Damgård, Sabine Oechsner, and Chris Peikert. Efficient commitments and zero-knowledge protocols from ring-sis with applications to lattice-based threshold cryptosystems. *IACR Cryptology ePrint Archive*, 2016:997, 2016.

[BG92] Mihir Bellare and Oded Goldreich. On defining proofs of knowledge. In *Annual International Cryptology Conference*, pages 390–420. Springer, 1992.

[BG14] Shi Bai and Steven D Galbraith. Lattice decoding attacks on binary lwe. In *Australasian Conference on Information Security and Privacy*, pages 322–337. Springer, 2014.

[BGGK17] Dan Boneh, Rosario Gennaro, Steven Goldfeder, and Sam Kim. A lattice-based universal thresholdizer for cryptographic systems. *IACR Cryptology ePrint Archive*, 2017:251, 2017.

[BGPW16] Johannes Buchmann, Florian Göpfert, Rachel Player, and Thomas Wunderer. On the hardness of lwe with binary error: revisiting the hybrid lattice-reduction and meet-in-the-middle attack. In *International Conference on Cryptology in Africa*, pages 24–43. Springer, 2016.

[BKLP15] Fabrice Benhamouda, Stephan Krenn, Vadim Lyubashevsky, and Krzysztof Pietrzak. Efficient zero-knowledge proofs for commitments from learning with errors over rings. In *European Symposium on Research in Computer Security*, pages 305–325. Springer, 2015.

[BLP+13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with er-

rors. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 575–584. ACM, 2013.

[Blu82] Manuel Blum. Coin flipping by telephone: A protocol for solving impossible problems. *Advances in Cryptology-A Report on CRYPTO'81*, 1982.

[BV14] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) lwe. *SIAM Journal on Computing*, 43(2):831–871, 2014.

[Che13] Yuanmi Chen. *Réduction de réseau et sécurité concrete du chiffrement completement homomorphe*. PhD thesis, ENS-Lyon, France, 2013.

[CHK+16] Jung Hee Cheon, Kyoo Hyung Han, Jinsu Kim, Changmin Lee, and Yongha Son. A practical post-quantum public-key cryptosystem based on splwe. In *Information Security and Cryptology–ICISC 2016: 19th International Conference, Seoul, South Korea, November 30–December 2, 2016, Revised Selected Papers*, volume 10157, page 51. Springer, 2016.

[CJL16] JungHee Cheon, Jinhyuck Jeong, and Changmin Lee. An algorithm for ntru problems and cryptanalysis of the ggh multilinear map without a low level encoding of zero. Cryptology ePrint Archive, Report 2016/139, 2016. `http://eprint.iacr.org/2016/139`.

[Cra96] Ronald Cramer. Modular design of secure yet practical cryptographic protocol. *PhD thesis, University of Amsterdam*, 1996.

[Dam10] Ivan Damgård. On σ-protocols. 2010. `http://www.cs.au.dk/~ivan/Sigma.pdf`.

[DCRVV15] Ruan De Clercq, Sujoy Sinha Roy, Frederik Vercauteren, and Ingrid Verbauwhede. Efficient software implementation of ring-lwe encryption. In *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*, pages 339–344. EDA Consortium, 2015.

[DDLL13] Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal gaussians. In *Advances in Cryptology–CRYPTO 2013*, pages 40–56. Springer, 2013.

[DEBG+14] Özgür Dagdelen, Rachid El Bansarkhani, Florian Göpfert, Tim Güneysu, Tobias Oder, Thomas Pöppelmann, Ana Helena Sánchez, and Peter Schwabe. High-speed signatures from standard lattices. In *International Conference on Cryptology and Information Security in Latin America*, pages 84–103. Springer, 2014.

[DL+15] Augot Daniel, Batina Lejla, et al. Initial recommendations of long-term secure post-quantum systems. Technical report, 2015. `http://pqcrypto.eu.org/docs/initial-recommendations.pdf`.

[DM15] Lauren De Meyer. *Security of LWE-based cryptosystems*. PhD thesis, 2015. `https://www.esat.kuleuven.be/cosic/publications/thesis-267.pdf`.

[DTV15] Alexandre Duc, Florian Tramèr, and Serge Vaudenay. Better algorithms for lwe and lwr. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 173–202. Springer, 2015.

[EBB13] Rachid El Bansarkhani and Johannes Buchmann. Improvement and efficient implementation of a lattice-based signature scheme. In *International Conference on Selected Areas in Cryptography*, pages 48–67. Springer, 2013.

BIBLIOGRAPHY

[FS86] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 186–194. Springer, 1986.

[GFS+12] Norman Göttert, Thomas Feller, Michael Schneider, Johannes Buchmann, and Sorin Huss. On the design of hardware building blocks for modern lattice-based encryption schemes. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 512–529. Springer, 2012.

[GJS15] Qian Guo, Thomas Johansson, and Paul Stankovski. Coded-bkw: solving lwe using lattice codes. In *Annual Cryptology Conference*, pages 23–42. Springer, 2015.

[GKPV10] Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert, and Vinod Vaikuntanathan. Robustness of the learning with errors assumption. 2010.

[GLP12] Tim Güneysu, Vadim Lyubashevsky, and Thomas Pöppelmann. Practical lattice-based cryptography: A signature scheme for embedded systems. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 530–547. Springer, 2012.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206. ACM, 2008.

[GSW13] Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In *Advances in Cryptology–CRYPTO 2013*, pages 75–92. Springer, 2013.

BIBLIOGRAPHY

[HKK15] Chen Hao, Lauter Kristin, and E. Stange Katherine. Attacks on search rlwe. Cryptology ePrint Archive, Report 2015/971, 2015. http://eprint.iacr.org/2015/971.

[HKK16] Chen Hao, Lauter Kristin, and E. Stange Katherine. Vulnerable galois rlwe families and improved attacks. Cryptology ePrint Archive, Report 2016/193, 2016. http://eprint.iacr.org/2016/193.

[HPS11] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé. Analyzing blockwise lattice algorithms using dynamical systems. In *Annual Cryptology Conference*, pages 447–464. Springer, 2011.

[JKPT12] Abhishek Jain, Stephan Krenn, Krzysztof Pietrzak, and Aris Tentes. Commitments and efficient zero-knowledge proofs from learning parity with noise. In *ASIACRYPT*, volume 7658, pages 663–680. Springer, 2012.

[Joe98] Buhler Joe, editor. *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, volume 1423 of *Lecture Notes in Computer Science*. Springer, 1998.

[KF15] Paul Kirchner and Pierre-Alain Fouque. An improved bkw algorithm for lwe with applications to cryptography and lattices. In *Annual Cryptology Conference*, pages 43–62. Springer, 2015.

[Koh16] Lisa Kohl. New tools for multi-party computation. *IACR Cryptology ePrint Archive*, 2016:417, 2016.

[KTX08] Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa. Concurrently secure identification schemes based on the worst-case hardness of lattice problems. In *ASIACRYPT*, volume 5350, pages 372–389. Springer, 2008.

BIBLIOGRAPHY

[Laa15] Thijs Laarhoven. *Search problems in cryptography*. PhD thesis, PhD thesis, Eindhoven University of Technology, 2015. http://www. thijs. com/docs/phd-final. pdf. 8, 2015.

[Laa16] Thijs Laarhoven. Sieving for closest lattice vectors (with preprocessing). *arXiv preprint arXiv:1607.04789*, 2016.

[LP11] Richard Lindner and Chris Peikert. Better key sizes (and attacks) for lwe-based encryption. In Aggelos Kiayias, editor, *CT-RSA*, volume 6558 of *LNCS*, pages 319–339. Springer, 2011.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 1–23. Springer, 2010.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-lwe cryptography. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 35–54. Springer, 2013.

[LSR+15] Zhe Liu, Hwajeong Seo, Sujoy Sinha Roy, Johann Großschädl, Howon Kim, and Ingrid Verbauwhede. Efficient ring-lwe encryption on 8-bit avr processors. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 663–682. Springer, 2015.

[Lyu12] Vadim Lyubashevsky. Lattice signatures without trapdoors. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 738–755. Springer, 2012.

[MSS11] Steven Myers, Mona Sergi, and Abhi Shelat. Threshold fully homomorphic encryption and secure computation. *IACR Cryptology ePrint Archive*, 2011:454, 2011.

BIBLIOGRAPHY

[MW16] Pratyay Mukherjee and Daniel Wichs. Two round multiparty computation via multi-key fhe. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 735–763. Springer, 2016.

[NIS15] NIST. Technical report, http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm, 2015.

[NSA15] NSA. Cryptography today. Technical report, https://www.nsa.gov/ ia/programs/suiteb cryptography/, Also at: https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm, 2015.

[Pei14] Chris Peikert. Lattice cryptography for the internet. In *International Workshop on Post-Quantum Cryptography*, pages 197–219. Springer, 2014.

[Pei16] Chris Peikert. *Decade of Lattice Cryptography*. World Scientific, 2016.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC*, LNCS, pages 84–93, 2005.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):34, 2009.

[RVM+14] Sujoy Sinha Roy, Frederik Vercauteren, Nele Mentens, Donald Donglong Chen, and Ingrid Verbauwhede. Compact ring-lwe cryptoprocessor. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 371–391. Springer, 2014.

[Sch03] Claus Peter Schnorr. Lattice reduction by random sampling and birthday methods. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 145–156. Springer, 2003.

BIBLIOGRAPHY

[Sin15] Vikram Singh. A practical key exchange for the internet using lattice cryptography. *IACR Cryptology ePrint Archive*, 2015:138, 2015.

[TU15] Ehsan Ebrahimi Targhi and Dominique Unruh. Quantum security of the fujisaki-okamoto transform. Technical report, 2015.

[Xag10] D Keita Xagawa. Cryptography with lattices. 2010.

[XXW13] Xiang Xie, Rui Xue, and Minqian Wang. Zero knowledge proofs from ring-lwe. In *International Conference on Cryptology and Network Security*, pages 57–73. Springer, 2013.

[XXZ11] Xiang Xie, Rui Xue, and Rui Zhang. Efficient threshold encryption from lossy trapdoor functions. In *PQCrypto*, pages 163–178. Springer, 2011.

[ZB12] Vinod Vaikuntanathan Zvika Brakerski, Craig Gentry. Fully homomorphic encryption without bootstrapping. In *Innovations in Theoretical Computer Science(ITCS'12)*, 2012.

[ZTH10] Bing Zeng, Xueming Tang, and Chingfang Hsu. A framework for fully-simulatable h-out-of-n oblivious transfer. *arXiv preprint arXiv:1005.0043*, 2010.

국문초록

랜덤선형부호의 복호화 문제(Learning with Errors)는 2005년 Regev가 소개한 이후로 다양한 암호학적 스킴을 설계하는데 이용되고 있다. 최근에는 키교환, 공개키암호, 서명 스킴과 같은 기본적인 암호학적 알고리즘 뿐만아니라 완전 동형암호, 다중 선형함수와 같은 고차원의 암호학적 알고리즘을 설계하는데 이용되고 있다. 한편 최근 양자 컴퓨팅 기술의 급속한 발전으로 인해 이론적인 연구보다는 보다 더 실제로 사용될 수 있는 암호학적 스킴을 연구, 개발하는일이 중요해졌다. 이러한 배경에서, 이 논문에서는 양자 컴퓨터 시대를 대비한 효율적인 공개키 암호 및 commitment 스킴 또한 이와 관련된 영지식 증명 프로토콜과 LWE 문제 기반의 임계암호시스템을 제안한다. 효율성을 위해 특별히 랜덤선형부호의 복호화 문제에서 비밀 벡터를 스파스한 벡터로 생성하는 변형된 형태를 사용하며, 이 변형된 문제의 어려움 및 제안하는 스킴들의 안전성을 제시한다.

주요어휘: 격자, 랜덤선형부호의 복호화 문제, 스파스 백터, 공개키 암호, commitment, 임계 암호시스템

학번: 2014-30074