A Post-Quantum Commitment Scheme based on spLWE

Jinsu Kim†

†Faculty of mathematics, Naval Academy, Gyungnam, 51704 Republic of Korea

Summary

We propose a new post-quantum commitment scheme whose security is based on the hardness of *spLWE* assumption. This scheme satisfies computational hiding and perfect binding properties. To the best of our knowledge, our scheme is the first *LWE*-based commitment scheme where the message space is a whole vector space over $\mathbb{Z}_q$. This property is efficient and useful when constructing zero-knowledge proofs for actively secure threshold encryptions based on LWE. In order to improve its performance, we exploit *spLWE* that is a sparse secret variant of *LWE*. Our implementation shows that the proposed scheme takes tens of milliseconds for committing, and verifying. As an application, we give a zero-knowledge proof for opening information of commitments which can be used for the active security.

Key words:

Post-Quantum, commitment, zero-knowledge proof, LWE, spLWE

1. Introduction

Lattice-based cryptography has developed and improved in terms of efficiency rapidly. Due to the seminal work of Ajtai [1] who proved reductions from the worst-case to the average-case for some lattice problems, cryptographers can design provably secure schemes and protocols unless all instances of lattice problems are easy to solve. This is necessary as it is an important candidate as a post-quantum alternative for the factoring, and discrete logarithm problem. In 2004, Regev introduced the Learning with Errors (*LWE*) [2]. This work also shows that there are connections between some worst-case lattice problems (the shortest independent vectors problem, the shortest vector problem with a gap) and *LWE*. With a strong security guarantee, it is of important versatile cryptographic primitives including encryption, signature, commitment based on it. ([3-8])

Commitment schemes [9] which are interested in this paper are basic building blocks in design of cryptographic protocols and have a lot of applications including a classical application, coin flipping over telephone. Intuitively, they can be described as electronic version of lockable box. Probably the best-known commitment scheme is the Pederson commitment scheme [10]. However, its security is based on the discrete logarithm assumption which can be broken by using quantum computers. It is essential to design post-quantum cryptographic commitments.

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 decryption and threshold signatures. In threshold decryption, the decryption key of an original public-key encryption scheme is split to N shares and then distributed to N servers, so that any t servers can decrypt collaboratively. By giving suitable proofs for partial decryption via some zero-knowledge proofs, malicious behaviors of partial decryption servers can be detected. This prevents unusual or incorrect decryption results. In order to construct zero-knowledge proofs that checks each server performs decryption honestly and correctly, it is essential to consider commitment schemes which can commit arbitrary vector over $\mathbb{Z}_q$.

There are several related works for this topic: A commitment scheme based on *SIS* problem was introduced in [11]. However, the message space is only binary. The *LWE*-based commitment scheme [12] 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 [13].

In this paper, we propose a post-quantum commitment scheme with homomorphic property which can commit to arbitrary vectors over $\mathbb{Z}_q$. Our commitment scheme satisfies computational hiding

Manuscript received December 5, 2020.
Manuscript revised December 20, 2020
https://doi.org/10.22937/IJCSNS.2020.20.12.30
.

and perfect binding properties under *LWE*-assumption. In order to improve its performance, we exploit *spLWE* assumption that is a variant of LWE assumption with sparse secret vectors. We can reduce the size of parameters and communication overheads from *spLWE*-based instantiation. As an application, we give a zero-knowledge proof of knowledge which can be used for actively secure LWE-based threshold cryptosystems. We adopt the relaxing idea of verifying conditions of commitment scheme as in [14]. This enables the proposed zero-knowledge proofs achieve negligible soundness error without multiple iterations.

2. Preliminaries

We use upper-case bold letters to denote matrices, and lower-case, letters with arrow accent for column vectors. For a distribution D, $a \leftarrow D$ denotes choosing an element according to the distribution of D and $\vec{a} \leftarrow D^m$ means that each component of $\vec{a}$ is sampled independently from D. For a given set A, $\mathcal{U}(A)$ means a uniform distribution on the set A and $a \leftarrow A$ denotes choosing an element according to the uniform distribution on A. We denote by $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z} = \{0,1 \cdots, q-1\}$ and $T = \mathbb{R}/\mathbb{Z}$ the additive group of real numbers modulo 1, and T_q the a subgroup of 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 $[x]_i$ means the its i-th component. A function $f(\lambda)$ is called *negligible*, $f(\lambda) = negl(\lambda)$ if $f(\lambda) = o(\lambda^{-c})$ for any $c > 0$, i.e., f decrease faster than any inverse polynomial.

2.1 Commitment Schemes

Commitment schemes can be regard as a digital version of a secure box. One 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 [13], [14]. 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 parameter.
- $Com(pk, m)$: 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.
- $Ver(pk, c, m, d)$: 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 1with overwhelming probability for all $m \in \mathcal{M}$ whenever the inputs were computed honestly:

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

- $Computational\ \ Hiding$: 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:

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

$$\leq \frac{1}{2} + negl(k).$$

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

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

2.2 Zero-Knowledge Proofs and Σ-Protocols

A zero-knowledge proof of knowledge is a two party (prover, P and verifier, V) 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 [15]) Proof of knowledges are usually designed by using Σ-protocols [16], [17]. Our zero-knowledge proof of knowledge is an instantiation of the following definition, which is a generalization of the standard notion of Σ -protocols, and is introduced by Benhamouda et al. [14] in order to achieve negligible soundness error probability of their protocols without parallel repetitions.

Definition 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.

Here, $\alpha > 0$ means even an honest prover sometimes fails to prove knowledge correctly. 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, a dishonest prover can answer correctly at most one challenge, i.e. the soundness error is $1/|C|$. ([17]). 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 an honest-verifier.

2.3 Discrete Gaussian Distribution over Lattice

A lattice $L \subseteq \mathbb{R}^m$ is a set of integer linear combinations of a $\{\overrightarrow{b_1}, \cdots, \overrightarrow{b_n}\}$ which is a subset of independent column vectors in $\mathbb{R}^m$, $L = \{\sum_{i=1}^{n} a_i \overrightarrow{b_i} : a_i \in \mathbb{Z}\}$. For given $s > 0$, a discrete Gaussian distribution over a lattice $L \subseteq \mathbb{R}^m$ centered at $\vec{v} \in \mathbb{R}^m$ is defined as $D_{L,\vec{v},s}(\vec{x}) = \rho_{\vec{v},s}(\vec{x})/\rho_{\vec{v},s}(L)$ for any $\vec{x} \in L$, where $\rho_{\vec{v},s}(\vec{x}) = \exp(-\pi|\vec{x} - \vec{v}|^2/s^2)$ and $\rho_s(L) := \sum_{\vec{x} \in L} \rho_{\vec{v},s}(\vec{x})$. We note that the standard deviation is $\sigma = s/\sqrt{2\pi}$. Alternatively, we can represent the Gaussian function $\rho_{\vec{v},s}(\vec{x})$ as $\rho_{\vec{v},\sigma}(\vec{x})$ then the discrete Gaussian distribution $D_{L,\vec{v},s}(\vec{x})$ is defined, $D_{L,\vec{v},s}(\vec{x}) = D_{L,\vec{v},\sigma}(\vec{x}) = \rho_{\vec{v},\sigma}(\vec{x})/\rho_{\vec{v},\sigma}(L)$ where $\rho_{\vec{v},\sigma}(\vec{x}) = \exp(-|\vec{x} - \vec{v}|^2/2\sigma^2)$ and $\rho_{\vec{v},\sigma}(L) := \sum_{\vec{x} \in L} \rho_{\vec{v},\sigma}(\vec{x})$. When $L = \mathbb{Z}, \vec{v} = 0$, we omit the subscript L, $\vec{v}$ respectively and denote $D_{\mathbb{Z}^m,\vec{v},\sigma}(\vec{x})$ by $D^m_{\vec{v},\sigma}(\vec{x})$. We collect some useful lemmas related to bounds of a discrete Gaussian distribution. The lemmas will be used to prove completeness and soundness of the respective zero-knowledge protocols.

Lemma 1([18], Lemma 4.4)
For any $k > 0$,

$$Pr[|z| > k\sigma; z \leftarrow D_\sigma] \leq 2\exp(-k^2/2).$$

for any $k > 1$,

$$Pr\left[|\vec{z}| > k\sigma\sqrt{m}; \vec{z} \leftarrow D^m_\sigma\right] < k^m \exp(m - mk^2/2).$$

3. *spLWE*-based Commitment Scheme

In this section, we propose a post-quantum commitment scheme based on $spLWE$. The security of our commitment scheme and zero-knowledge proof is guaranteed by $spLWE$ (learning with errors) assumption. $spLWE$ is a variant of LWE with sparse and small secrets. This problem is harder than LWE under some suitable parameters as shown in [19].

More precisely, LWE, and $spLWE$ is defined as follows. For integers $n, q \geq 1$, a vector $\vec{s} \in \mathbb{Z}_q^n$, let $A_{q,\vec{s},\sigma}$ be the distribution of the pairs $(\vec{a}, b = \langle \vec{a}, \vec{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where $\vec{a} \leftarrow \mathbb{Z}_q^n$ and $e \leftarrow D_\sigma$. For integers $n, q \geq 1$, and a distribution $\mathcal{D}$ over $\mathbb{Z}_q^n$, $LWE_{n,q,\sigma}(\mathcal{D})$ is to distinguish (given arbitrarily many independent samples) the uniform distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ from $A_{q,\vec{s},\sigma}$ with a fixed sample $\$\vec{s} \leftarrow \mathcal{D}$. We note that a search variant of LWE is the problem of recovering $\vec{s}$ from $(\vec{a}, b) = \langle \vec{a}, \vec{s} \rangle + e \in \mathbb{Z}_q^n \times \mathbb{Z}_q^n$ sampled according to $A_{q,\vec{s},\sigma}$. Let $LWE_{n,m,q,\sigma}(\mathcal{D})$ denotes the case when the number of samples are bounded by $m \in N$. A typical choice of the secret distribution $\mathcal{D}$ is $\mathcal{U}(\mathbb{Z}_q^n)$ or the error distribution D_σ. For a set $X_{n,\rho,\theta}$ which consists of the vectors $\vec{s} \in \mathbb{Z}^n$ whose nonzero components are in $\{\pm 1, \pm 2, \pm 4, \cdots, \pm \rho\}$, and the number of nonzero components is θ, we define $spLWE_{n,m,q,s,\rho,\theta}$ as the problem $LWE_{n,m,q,s}\left(\mathcal{U}(X_{n,\rho,\theta})\right)$.

3.1 Our $spLWE$-based Commitment scheme

Our $spLWE$-based commitment scheme is simple and efficient. Informally, for dimension n, the number of samples m, and modulus q, the commitment with message space $\mathbb{Z}_q^l$ is of the form $A\vec{m} + B\vec{r} + \vec{e} \bmod q$, where $(A, B) \in \mathbb{Z}_q^{m \times l} \times \mathbb{Z}_q^{m \times n}$ is a public random matrix, $\vec{r} \in \mathbb{Z}_q^n$ is a uniformly random vector, and $\vec{e} \in \mathbb{Z}_q^m$ is a short error vector. Our scheme consists of three sub-algorithms, (Setup, Com, Ver). 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 $\vec{c}$ with public random matrices A, B and randomness vectors $\vec{r}, \vec{e}$. The verification algorithm checks if the commitment computed from opening information $\overrightarrow{m'}, \overrightarrow{r'}, \overrightarrow{e'}, f'$ is indeed the commitment $\vec{c}$, and the norm of randomness vector used in the commitment $\vec{c}$ is sufficiently small.

- Setup$\left(1^{\kappa}, 1^{k}\right)$: 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 $s_2 = \alpha_1 \beta \rho \sqrt{2\pi\theta}$, $s_3 = 2\alpha_2 s_1 \beta \sqrt{m}$ 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 $(seed_A, seed_B)$.
- Com $\left(\vec{m} \in \mathbb{Z}_q^n\right)$: Generate random matrices $A \leftarrow Gen(seed_A), B \leftarrow Gen(seed_B)$ where $(A, B) \in \mathbb{Z}_q^{m \times l} \times \mathbb{Z}_q^{m \times n}$ and sample $\vec{r} \leftarrow X_{n,\rho,\theta}$, $\vec{e} \leftarrow D_{\mathbb{Z},\, s_1}^{m}$, compute $\vec{c} = Com(\vec{m}, \vec{r}, \vec{e}) = A\vec{m} + B\vec{r} + \vec{e} \bmod q$.
- Ver $\left(\vec{c}, \left(\overrightarrow{m'}, \overrightarrow{r'}, \overrightarrow{e'}, f'\right)\right)$: Given a commitment $\vec{c}$ with an opening information $(\vec{m}, \vec{r}, \vec{e}, f)$, the verifier accepts if and only if $A\overrightarrow{m'} + B\left(f'^{-1}\overrightarrow{r'}\right) + f'^{-1}\overrightarrow{e'} = \vec{c}$, $\left\|\overrightarrow{r'}\right\|_{\infty} \leq 24 s_2/\sqrt{2\pi}$, $\left\|\overrightarrow{e'}\right\|_{\infty} \leq 24 s_3/\sqrt{2\pi}$, $|f'| \leq \beta$.

This commitment scheme is computationally hiding under LWE assumption. In particular, the distribution of $B\vec{r} + \vec{e}$ mod q is statistically close to the uniform distribution. It can hide message information. The scheme is perfect binding. This property follows from that $A\left(\vec{m} - \overrightarrow{m'}\right) + B\left(\vec{r} - \overrightarrow{r'}\right) = \vec{e} - \overrightarrow{e'} \bmod q$ does not hold overwhelmingly for sufficiently large q and m, since $\left\|\vec{e} - \overrightarrow{e'}\right\|$ is small. 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 $\vec{r}$'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 more suitable for efficient instantiations.

Theorem 1. Let $m = kn$ with $k > 2$, $l = n$ and $\beta \leq 2^{\frac{n}{4}-1} - \frac{1}{2}$. Assuming the hardness of $spLWE_{n,m,q,s_1,\rho,\theta}$ 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 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 $\|\vec{r}\|_{\infty} \leq \rho < s_2 < 24 s_2/\sqrt{2\pi}$ for $\vec{r} \leftarrow X_{n,\rho,\theta}$, $\|\vec{e}\|_{\infty} \leq 12 s_1/\sqrt{2\pi}$ with probability $1 - 2^{-100}$ for $\vec{e} \leftarrow D_{\mathbb{Z},s_1}^{m}$, which is strictly less than $24 s_3/\sqrt{2\pi}$ and $f' = 1 \leq \beta$.

- Computational Hiding : Under the $spLWE_{n,m,q,s_1,\rho,\theta}$-assumption, $B\vec{r} + \vec{e} \bmod q$ is pseudo-random, thus $A\vec{m} + B\vec{r} + \vec{e} \bmod q$ is also pseudo-random.

- Statistical Binding: Let $\vec{c}$ be a commitment with two opening information $(\vec{m}, \vec{r}, \vec{e}, f)$, $\left(\overrightarrow{m'}, \overrightarrow{r'}, \overrightarrow{e'}, f'\right)$ where $\vec{m} \neq \overrightarrow{m'}$. Then $A\vec{m} + B(f^{-1}\vec{r}) + f^{-1}\vec{e} = \vec{c} = A\overrightarrow{m'} + B\left(f'^{-1}\overrightarrow{r'}\right) + f'^{-1}\overrightarrow{e'} \bmod q$ and so $A\left(\vec{m} - \overrightarrow{m'}\right) + B\left(f^{-1}\vec{r} - f'^{-1}\overrightarrow{r'}\right) = f'^{-1}\overrightarrow{e'} - f^{-1}\vec{e}$ $\bmod q$. Let $\overrightarrow{m''} = \vec{m} - \overrightarrow{m'} \neq 0$. Now, we have that

$$Pr\left[\begin{matrix} A\overrightarrow{m''} + B\left(f^{-1}\vec{r} - f'^{-1}\overrightarrow{r'}\right) = \left(f'^{-1}\overrightarrow{e'} - f^{-1}\vec{e}\right) \\ \bmod q\colon A \leftarrow \mathbb{Z}_q^{m \times l}, B \leftarrow \mathbb{Z}_q^{m \times n} \end{matrix}\right] = \frac{1}{q^m}.$$

By taking union bound over all $\overrightarrow{m''}, \vec{r}, \overrightarrow{r'}, \vec{e}, \overrightarrow{e'}, f, f'$, we have the overall probability that there exist $\overrightarrow{m''} \neq 0$ satisfying the above equation 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. ■

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. We also exploit box-muller transformation to generate discretized Gaussian distribution. Our implementation is performed on PC (Mac Pro) with CPU 2.6GHz Intel Core i5 without parallelization. In order to achieve the binding property, we must set the parameters that satisfy

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

is negligible. On the other hand, the $spLWE_{n,m,q,s_1,\rho,\theta}$ problem is hard. Since the primal and dual attacks are the known best attacks for LWE. Therefore, we follow attack strategy in [19] that considers a variety of attack methodology for $spLWE$. As in [19], the parameters in $spLWE_{n,m,q,s_1,\rho,\theta}$ satisfy the classical and quantum security.

Table 1: Implementation result for 256-bit message

κ, k	Setup(μs)	Com(ms)	Ver(ms)
72	32.0	11.2	13.1
96	56.1	18.6	20.8
128	91.2	33.5	35.7

4. Application: Zero-Knowledge Proofs of Knowledge

In order to prove zero-knowledge of protocols and security of threshold cryptosystems, it is essential that one can construct a simulator that statistically simulates the accepting transcripts and the entire view of an adversary who can see partial decryptions of ciphertexts and has some secret key shares respectively. The following lemmas will be exploited for these purposes.

Lemma 2([18] 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 $\sigma \in \omega\left(T\sqrt{\log n}\right)$. 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 $\vec{v} \leftarrow D, \vec{z} \leftarrow D_\sigma^n$ and output $(\vec{z}, \vec{v})$ with probability $\frac{D_\sigma^n(\vec{z})}{MD_{\vec{v},\sigma}^n(\vec{z})}$.
- A_2 : draw $\vec{v} \leftarrow D, \vec{z} \leftarrow D_\sigma^n$ and output $(\vec{z}, \vec{v})$ 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 $\alpha \in$¥$R_{>0}$, we have $M = \exp\left(12/\alpha + 1/(2\alpha^2)\right)$ 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. Another simple idea about hiding small terms is adding a value which is chosen randomly from a relatively large interval. this technique is known as "smudging".

Lemma 3([20], 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.

4.1. Proof for Opening Information

In this section, we describe our zero-knowledge proof of opening information as an application. Let $\vec{c} = A\vec{m} + B\vec{r} + \vec{e} \mod q$ be a commitment that is published by the prover. The prover can prove that he knows a valid opening information of $\vec{c}$ from the following protocol. The public input is $\vec{c}$ and the private input is $(\vec{m}, \vec{r}, \vec{e})$:

- P computes $\vec{t} = A\vec{\mu} + B\vec{\rho} + \vec{\eta}$ where $\vec{\mu} \leftarrow \mathbb{Z}_q^l, \vec{\rho} \leftarrow D_{\sigma_2}^n, \vec{\eta} \leftarrow D_{\sigma_3}^m$, and sends $\vec{t}$ 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 $\overrightarrow{s_m} = \vec{\mu} + d\vec{m}\ mod\ q, \overrightarrow{s_r} = \vec{\rho} + d\vec{r}\ mod\ q, \overrightarrow{s_e} = \vec{\eta} + d\vec{e}\ mod\ q$. If $d = 0$, P sends $\overrightarrow{s_m}, \overrightarrow{s_r}, \overrightarrow{s_e}$ to V. Otherwise, P sends $\overrightarrow{s_m}, \overrightarrow{s_r}, \overrightarrow{s_e}$ to V with probability $p = D^n_{\sigma_2}(\vec{\rho}) / M_2 D^n_{d\vec{r},\sigma_2}(\vec{\rho}) \times D^n_{\sigma_3}(\vec{\eta}) / M_3 D^n_{d\vec{e},\sigma_3}(\vec{\eta})$, and $\perp$ with probability $1 - p$.
- V accepts if $\vec{t} + d\vec{c} = A\overrightarrow{s_m} + B\overrightarrow{s_r} + \overrightarrow{s_e}\ mod\ q$, $\|\overrightarrow{s_r}\|_\infty \le 12\sigma_2$, and $\|\overrightarrow{s_e}\|_\infty \le 12\sigma_3$. We prove that the above protocol is indeed a zero-knowledge proof.

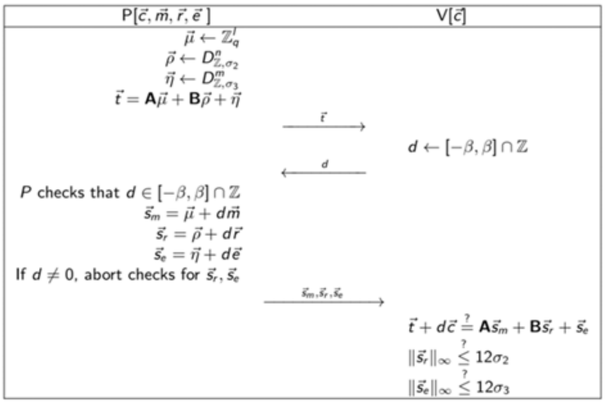
$P[\vec{c}, \vec{m}, \vec{r}, \vec{e}\,]$
$V[\vec{c}]$
$\vec{\mu} \leftarrow \mathbb{Z}^l_q$
$\vec{\rho} \leftarrow D^n_{\mathbb{Z},\sigma_2}$
$\vec{\eta} \leftarrow D^m_{\mathbb{Z},\sigma_3}$
$\vec{t} = \mathbf{A}\vec{\mu} + \mathbf{B}\vec{\rho} + \vec{\eta}$
$\vec{t}$
$d \leftarrow [-\beta, \beta] \cap \mathbb{Z}$
d
P checks that $d \in [-\beta, \beta] \cap \mathbb{Z}$
$\vec{s}_m = \vec{\mu} + d\vec{m}$
$\vec{s}_r = \vec{\rho} + d\vec{r}$
$\vec{s}_e = \vec{\eta} + d\vec{e}$
If $d \neq 0$, abort checks for $\vec{s}_r, \vec{s}_e$
$\vec{s}_m, \vec{s}_r, \vec{s}_e$
$\vec{t} + d\vec{c} \overset{?}{=} \mathbf{A}\vec{s}_m + \mathbf{B}\vec{s}_r + \vec{s}_e$
$\|\vec{s}_r\|_\infty \overset{?}{\le} 12\sigma_2$
$\|\vec{s}_e\|_\infty \overset{?}{\le} 12\sigma_3$

Fig. 1 proof of opening information

Theorem 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 $\vec{c}$ and a pair of accepting transcripts $\left(\vec{t}, d, (\overrightarrow{s_m}, \overrightarrow{s_r}, \overrightarrow{s_e})\right)$, $\left(\vec{t}, d, (\overrightarrow{s'_m}, \overrightarrow{s'_r}, \overrightarrow{s'_e})\right)$ where $d \neq d'$, we can extract a vaild opening information of $\vec{c}$.
- 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 $\overrightarrow{s_m} = \vec{\mu}$, $\overrightarrow{s_r} = \vec{\rho}$, $\overrightarrow{s_e} = \vec{\eta}$ to V. Thus $\vec{t} + d\vec{c} = \vec{t} = A\vec{\mu} + B\vec{\rho} + \vec{\eta} = A\overrightarrow{s_m} + B\overrightarrow{s_r} + \overrightarrow{s_e}\ mod\ q$. Since $\vec{\rho} \leftarrow D^n_{\sigma_2}$, $\vec{\eta} \leftarrow D^m_{\sigma_3}$, $\|\overrightarrow{s_r}\|_\infty = \|\vec{\rho}\|_\infty \le 12\sigma_2$, and $\|\overrightarrow{s_e}\|_\infty = \|\vec{\eta}\|_\infty \le 12\sigma_3$,with overwhelming probability. In the case $d \neq 0$, P sends $\overrightarrow{s_m} = \vec{\mu} + d\vec{m}$, $\overrightarrow{s_r} = \vec{\rho} + d\vec{r}$, $\overrightarrow{s_e} = \vec{\eta} + d\vec{e}$ to V with probability close to $\frac{1}{M_2M_3}$ overwhelmingly by the rejection sampling lemma. Thus $A\overrightarrow{s_m} + B\overrightarrow{s_r} + \overrightarrow{s_e} = A\vec{\mu} + B\vec{\rho} + \vec{\eta} + d(A\vec{m} + B\vec{r} + \vec{e}) = \vec{t} + d\,\vec{c}$. Note that the distribution of $\overrightarrow{s_r} = \vec{\rho} + d\vec{r}$, $\overrightarrow{s_e} = \vec{\eta} + d\vec{e}$ are statistically close to $D^n_{\sigma_2}$, $D^m_{\sigma_3}$ respectively by the rejection sampling lemma. Hence, $\|\overrightarrow{s_r}\|_\infty \le 12\sigma_2$, and $\|\overrightarrow{s_e}\|_\infty \le 12\sigma_3$ with overwhelming probability. 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 $\left(\vec{t}, d, (\overrightarrow{s_m}, \overrightarrow{s_r}, \overrightarrow{s_e})\right)$, $\left(\vec{t}, d, (\overrightarrow{s'_m}, \overrightarrow{s'_r}, \overrightarrow{s'_e})\right)$ where $d \neq d'$ are given. Then the following equations are hold:

$$\vec{t} + d\vec{c} = A\overrightarrow{s_m} + B\overrightarrow{s_r} + \overrightarrow{s_e}\ mod\ q$$
$$\vec{t} + d'\vec{c} = A\overrightarrow{s'_m} + B\overrightarrow{s'_r} + \overrightarrow{s'_e}\ mod\ q$$

By subtracting the above equations, we get:

$$(d - d')\vec{c} = A(\overrightarrow{s_m} - \overrightarrow{s'_m}) + B(\overrightarrow{s_r} - \overrightarrow{s'_r}) + (\overrightarrow{s_e} - \overrightarrow{s'_e})\ mod\ q$$

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

Honest-Verifier Zero-Knowledge: Let $\vec{c}$ and challenge d are given as inputs. First, the simulator samples $\overrightarrow{s'_m} \leftarrow \mathbb{Z}^l_q, \overrightarrow{s'_r} \leftarrow D^n_{\sigma_2}$, and $\overrightarrow{s'_e} \leftarrow D^m_{\sigma_3}$, and computes $\vec{t} = A\overrightarrow{s'_m} + B\overrightarrow{s'_r} + \overrightarrow{s'_e} - d\vec{c}$. In the case $d = 0$, the simulator outputs $\left(\vec{t}, 0, (\overrightarrow{s'_m}, \overrightarrow{s'_r}, \overrightarrow{s'_e})\right)$. This is statistically indistinguishable from accepting transcripts of the real protocol, since the distribution of response $(\overrightarrow{s'_m}, \overrightarrow{s'_r}, \overrightarrow{s'_e})$ is statistically indistinguishable from the the distribution of real response by the rejection sampling lemma, and $\vec{t}$ is uniquely determined by $\overrightarrow{s'_m}, \overrightarrow{s'_r}, \overrightarrow{s'_e}$, and d in the real protocol and in the simulation. When $d \neq 0$, the simulator outputs $\left(\vec{t}, 0, (\overrightarrow{s'_m}, \overrightarrow{s'_r}, \overrightarrow{s'_e})\right)$ with probability $\frac{1}{M_2M_3}$. Otherwise, the simulator outputs ($\overrightarrow{t_0}$, d, $\perp$) where $\overrightarrow{t_0} \leftarrow \mathbb{Z}^m_q$.

The non-aborting case of this simulation is indistinguishable from the non-aborting case of the real protocol similarly. $B\vec{\rho} + \vec{\eta}\ mod\ q$ in $\vec{t} = A\vec{\mu} + B\vec{\rho} + \vec{\eta}\ mod\ q$ in real protocol can be regarded as an instance of $LWE_{n,m,q,\sigma_3}(D^n_{\sigma_2})$, which is hard under the condition, $spLWE_{n,m+n,q,s_1,\rho,\theta}$ is hard. Thus $\vec{t}$ is computationally indistinguishable from $\overrightarrow{t_0}$, which is sampled from uniform random distribution over $\mathbb{Z}^m_q$.

5. Conclusion

We present a post-quantum commitment scheme with its related proof of knowledge which security is based on the hardness of *spLWE* that is a sparse secret variant of *LWE*. These are simple and efficient. In particular, these primitives are efficient and useful when constructing zero-knowledge proofs for actively secure threshold encryptions based on LWE. Our implementation shows that the proposed scheme takes tens of milliseconds for committing, and verifying. This justifies the usefulness of *spLWE* in practical implementation.

References

[1] M. Ajtai, “Generating hard instances of lattice problems,” In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp. 99–108, 1996.

[2] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography,” In STOC, pp. 84–93, 2005.

[3] Z. Brakerski, V. Vaikuntanathan, “Efficient fully homomorphic encryption from (standard) LWE,” SIAM Journal on Computing, Vol.43(2), pp.831-871, 2014.

[4] R. Lindner, C Peikert, “Better key sizes (and attacks) for LWE-based encryption,” In Cryptographers’ Track at the RSA Conference, pp. 319-339, 2011.

[5] V. Lyubashevsky, “Lattice signatures without trapdoors,” In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 738-755, 2012.

[6] L. Ducas, A. Durmus, T. Lepoint, V. Lyubashevsky, “Lattice signatures and bimodal Gaussians,” In Annual Cryptology Conference, pp. 40-56, 2013.

[7] R. del Pino, V. Lyubashevsky, G. Seiler, “Short discrete log proofs for FHE and ring-LWE ciphertexts,” In IACR International Workshop on Public Key Cryptography, pp. 344-373, 2019.

[8] R. Silva, C. Antonio, D. A., R. Dahab, “LWE-based identification schemes,” In 2011 IEEE Information Theory Workshop, pp. 292-296, 2011.

[9] M. Blum, “Coin flipping by telephone: A protocol for solving impossible problems,” Advances in Cryptology-A Report on CRYPTO’81, 1982.

[10] T.P. Pedersen, “Non-interactive and information-theoretic secure verifiable secret sharing,” In Annual international cryptology conference, pp. 129-140, 1991.

[11] A. Kawachi, K. Tanaka, K. Xagawa, “Concurrently secure identification schemes based on the worst-case hardness of lattice problems,” In International Conference on the Theory and Application of Cryptology and Information Security, pp.372-389, 2008.

[12] Z. Bing, T. Xueming, C. Hsu, “A framework for fully-simulatable h-out-of-n oblivious transfer,” arXiv preprint arXiv:1005.0043, 2010.

[13] A. Jain, S. Krenn, K. Pietrzak, A. Tentes, “Commitments and efficient zero-knowledge proofs from learning parity with noise,” In Advances in Cryptology–ASIACRYPT 2012, pp. 663– 680, 2012.

[14] F. Benhamouda, S. Krenn, V. Lyubashevsky, K. Pietrzak, “Efficient zero-knowledge proofs for commitments from learning with errors over rings,” In European symposium on research in computer security, pp. 305-325, 2015.

[15] M. Bellare, O. Goldreich, “On defining proofs of knowledge,” In Annual International Cryptology Conference, pp. 390-420. 1992.

[16] R. Cramer, “Modular design of secure yet practical cryptographic protocol, PhD thesis, University of Amsterdam. 1996.

[17] I. Damgard, “On σ -protocols of knowledge,” 2010. Available at http://www.cs.au.dk/~ivan/Sigma.pdf.

[18] V. Lyubashevsky, “Lattice signatures without trapdoors,” In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 738-755, 2012.

[19] J. H. Cheon, K. Han, J. Kim, C. Lee, Y. Son, “A Practical Post-Quantum Public-Key Cryptosystem Based on spLWE,” In International Conference on Information Security and Cryptology, pp. 51-74. 2016.

[20] L. Kohl, “New tools for multi-party computation,” IACR Cryptology ePrint Archive, 2016:417, 2016.

Jinsu Kim received the B.S. M.S. and D.S. degrees in Mathematical Science from Seoul National University in 2008, 2012 and 2018, respectively. He now with naval academy in Republic of Korea.