East Asian Math. J.
Vol. 38 (2022), No. 0*, pp. 085–094
http://dx.doi.org/10.7858/eamj.2022.007

# ZERO-KNOWLEDGE PROOFS FROM SPLWE-BASED COMMITMENTS

Jinsu Kim and Dooyoung Kim*

Abstract. Recently, an LWE-based commitment scheme is proposed. Their construction is statistically hiding as well as computationally binding. On the other hand, the construction of related zero-knowledge protocols is left as an open problem. In this paper, we present zero-knowledge protocols with hardness based on the LWE problem. we show how to instantiate efficient zero-knowledge protocols that can be used to prove linear and sum relations among these commitments. In addition, we show how the variant of LWE, spLWE problem, can be used to instantiate efficient zero-knowledge protocols.

## 1. Introduction

Since Ajtai ([1]) proved reductions from the worst-case to the average-case for some lattice problems, lattice-based cryptography has developed rapidly. cryptographers can design provably secure schemes and protocols unless all instances of lattice problems are easy to solve. In 2004, Regev introduced the Learning with Errors (LWE) ([13]). it makes possible a lot of important cryptographic primitives like encryption, signature, key-exchange based on it with a strong security guarantee. ([11], [5], [8]) This is necessary as it is one of the promising candidates as an alternative for the factoring and discrete logarithm problem in post-quantum era.

Commitment schemes ([3]) are one of the basic primitives in cryptography. They allow one to publicly commit to a secret message or value. The committed value can not be changed by anyone and remains as secret information until the committer determines to reveal it. Commitment schemes also have a lot of applications. They can be found as key tools in many cryptographic services such as secret sharing, zero-knowledge protocols, and others. Arguably,

Received October 14, 2021; Accepted January 13, 2022.
2010 *Mathematics Subject Classification.* 11A11.
*Key words and phrases.* Zero-knowledge proof, LWE, spLWE, Commitment, Linear relation, Sum relation.
This research was supported by Korea Naval Academy Institute for Ocean Research(2022).
*Corresponding author.


(pISSN 1226-6973, eISSN 2287-2833)

when converted to zero-knowledge protocols, they allow a committer to convince a challenger without leakage about secret key and opening information. In particular, this property enforces honest behavior by adversaries. This leads to secure protocols against a malicious attacker. In lattice-based cryptography, several pieces of research are proposed in terms of post-quantum security. It is proposed LPN-based commitment schemes and zero-knowledge protocols by [9]. An improved version of [9] was presented in [15]. They use Ring-LWE problem to design secure commitment schemes and zero-knowledge protocols. Unlike the schemes and protocols in [15], Ring-LWE based-encryption schemes are constructed in advance, and used as building blocks for the commitment schemes and protocols in ([2], [6], [7]). In [7], commitment schemes and their companion zero-knowledge protocols are efficient in the sense that they achieve negligible soundness error with a single iteration of the zero-knowledge protocol. In [10], an LWE-based commitment scheme is presented. They use the spLWE problem, a sparse secret variant of LWE, as a base problem to improve its efficiency. On the other hand, the construction of related zero-knowledge protocols is left as an open problem.

In this work, we present LWE-based zero-knowledge protocols for proving knowledge, and for linear, sum relations on committed values. Due to the rejection sampling lemma in [12], Our protocols also achieve negligible soundness error with a single iteration of the zero-knowledge protocol. To improve their efficiency, we show spLWE-based instantiation of the protocols.

The rest of the paper consists of as follows. In Section 2, we give backgrounds for spLWE problem and the spLWE-based commitment. Section 3 present the three main zero-knowledge protocols for proving knowledge, and for linear, sum relations on committed values. Finally, Section 4 provides the concluding remarks and future works.

## 2. Background and Notation

Throughout the paper, matrices will be denoted by capital bold letters, and vectors will be denoted by small letters, $\vec{v}$. We will write $\|\vec{v}\|$ for the Euclidian norm of vectors. For a distribution $\mathcal{D}$, $a \leftarrow \mathcal{D}$ denotes choosing an element according to the distribution of $\mathcal{D}$ and $\vec{a} \leftarrow \mathcal{D}^m$ means that each component of $\vec{a}$ 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 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 $[\vec{v}]_i$ means the its $i$-th component of $\vec{v}$.

### 2.1. Discrete Gaussian Distribution

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

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

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 as $D_{L,\vec{v},s}(\vec{x}) = D_{L,\vec{v},\sigma}(\vec{x}) = \rho_{\vec{v},\sigma}(\vec{x})/\rho_{\vec{v},\sigma}(L)$ where

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

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 a discrete Gaussian distribution.

**Lemma 2.1** ([4], Lemma 2.4)**.** *For any real $s > 0$ and $T > 0$, and any vector $\boldsymbol{x} \in \mathbb{R}^n$, we have*

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

**Lemma 2.2** ([12], 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 $k > 1$, $Pr\left[\|\vec{z}\| > k\sigma\sqrt{m}; \vec{z} \leftarrow D^m_\sigma\right] < k^m \exp(m - mk^2/2)$.*

### 2.2. LWE and spLWE

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

**Definition 2.1** (Learning with Errors (LWE))**.** *For integers $n, q \geq 1$, an error distribution $\phi$ over $\mathbb{R}$, and a distribution $\mathcal{D}$ over $\mathbb{Z}^n_q$, $LWE_{n,q,\phi}(\mathcal{D})$, is to distinguish (given arbitrarily many independent samples) the uniform distribution over $\mathbb{T}^n_q \times \mathbb{T}$ from $A_{q,\vec{s},\phi}$ 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 $(\mathbf{a}, b) = (\mathbf{a}, \langle \mathbf{a}, \mathbf{s}\rangle + e) \in \mathbb{T}^n_q \times \mathbb{T}$ sampled according to $A_{q,\vec{s},\phi}$, and these are also equivalently defined on $\mathbb{Z}^n_q \times \mathbb{Z}_q$ rather than $\mathbb{T}^n_q \times \mathbb{T}$ for discrete (Gaussian) error distributions over $\mathbb{Z}_q$.

Let $\mathrm{LWE}_{n,m,q,\phi}(\mathcal{D})$ denotes the case when the number of samples are bounded by $m \in \mathbb{N}$. We simply denote $\mathrm{LWE}_{n,q,\phi}$ when the secret distribution $\mathcal{D}$ is $\mathcal{U}(\mathbb{Z}^n_q)$. In many cases, $\phi$ is a (discrete) Gaussian distribution so we simply denote by $\mathrm{LWE}_{n,m,q,s}$ instead of $\mathrm{LWE}_{n,m,q,\phi}$. We remark that in the above definition, $A_{q,\vec{s},\phi}$ can be substituted by the distribution over $\mathbb{Z}^n_q \times \mathbb{Z}_q$ for a distribution $\phi$ on $\mathbb{Z}$ by sampling $\vec{a} \leftarrow \mathbb{Z}^n_q$. Clearly, these two problems are equivalent.

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 $\theta$, we write $spLWE_{n,m,q,s,\rho,\theta}$ as the problem $LWE_{n,m,q,s}(\mathcal{U}(X_{n,\rho,\theta}))$. We also consider a variant of $LWE$, $LWE_{n,q,\leq\alpha}$, in which the amount of noise is some unknown $\beta \leq \alpha$. Similarly, $spLWE_{n,q,\leq\alpha,\rho,\theta}$ can be defined by the same way.

### 2.3. spLWE-based Commitment

In [10], they present $spLWE$-based commitment schemes. The setup algorithm chooses a $spLWE$ dimension $n$, the number of sample $m$, a weight $\theta$, a bound of non-zero coefficient $\rho$, a prime modulus $q$, a message space rank $l$, and a bound of elements in a challenge set $\beta$, and set width parameters $s_1, s_2, s_3$, and rejection sampling parameters $\alpha_1, \alpha_2$. The commitment algorithm computes the commitment vector $\vec{c}$ with public random matrices $\mathbf{A}, \mathbf{B}$ and randomness vectors $\vec{r}, \vec{e}$. The verification algorithm checks if the commitment computed from opening informations $(\vec{m}', \vec{r}', \vec{e}', f')$ is indeed the commitment $\vec{c}$, and the norm of randomness vector used in the commitment $\vec{c}$ is sufficiently small.

- 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 $(seed_A, seed_B)$.
- Com$(\vec{m} \in \mathbb{Z}_q^n)$: 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 $\vec{r} \leftarrow X_{n,\rho,\theta}$, $\vec{e} \leftarrow D^m_{\mathbb{Z},s_1}$, compute $\vec{c} = Com(\vec{m}, \vec{r}, \vec{e}) = \mathbf{A}\vec{m} + \mathbf{B}\vec{r} + \vec{e} \mod q$.
- Ver$(\vec{c}, (\vec{m}', \vec{r}', \vec{e}', f'))$: Given a commitment $\vec{c}$ with a opening information $(\vec{m}, \vec{r}, \vec{e}, f)$, the verifier accepts if and only if $\mathbf{A}\vec{m}' + \mathbf{B}(f'^{-1}\vec{r}') + f'^{-1}\vec{e}' = \vec{c}, \|\vec{r}'\|_\infty \leq 24s_2/\sqrt{2\pi}, \|\vec{e}'\|_\infty \leq 24s_3/\sqrt{2\pi}, |f'| \leq \beta$.

## 3. Zero-Knowledge Proofs of Knowledge

In this section, we present zero-knowledge protocols that can be constructed from the spLWE-based commitment scheme. Our design approach is based on the well known technique, cut-and-choose proof in [14]. We also use the rejection sampling as introduced by Lyubashevsky to prevent leakage of error information.

**Lemma 3.1** ([12] 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 $\vec{v} \leftarrow D, \vec{z} \leftarrow D^n_\sigma$ and output $(\vec{z}, \vec{v})$ with probability $\frac{D^n_\sigma(\vec{z})}{MD^n_{\vec{v},\sigma}(\vec{z})}$.*
- *$A2$ : draw $\vec{v} \leftarrow D, \vec{z} \leftarrow D^n_\sigma$ 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 $\alpha \in \mathbb{R}_{>0}$, we have $M = \exp(12/\alpha + 1/(2\alpha^2))$ and the outputs of $A_1$ and $A_2$ are within statistical distance $2^{-100}/M$.*

### 3.1. Proof for Committed Messages

Let $\vec{c} = \mathbf{A}\vec{m} + \mathbf{B}\vec{r} + \vec{e} \mod q$ be a commitment that is published by the prover. The prover can prove that $\vec{c}$ is a commitment of the message $\vec{m}$. This can be done by showing that the prover can prove he knows a valid randomness of $\vec{c}$ without revealing it. In this case, the public input is $(\vec{c}, \vec{m})$ and the private input is $(\vec{r}, \vec{e})$:

- P computes $\vec{t} = \mathbf{B}\vec{\rho} + \vec{\eta} \mod q$ where $\vec{\rho} \leftarrow D^n_{\sigma_2}, \vec{\eta} \leftarrow D^m_{\sigma_3}$, 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 $\vec{s}_r = \vec{\rho} + d\vec{r} \mod q, \vec{s}_e = \vec{\eta} + d\vec{e} \mod q$. If $d = 0$, P sends $\vec{s}_m = 0, \vec{s}_r, \vec{s}_e$ to V. Otherwise, P sends $\vec{s}_m = 0, \vec{s}_r, \vec{s}_e$ 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 iff $\vec{s}_m = 0$, $\vec{t} + d\vec{c} = \mathbf{B}\vec{s}_r + \vec{s}_e$, $\|\vec{s}_r\|_\infty \leq 12\sigma_2$, and $\|\vec{s}_e\|_\infty \leq 12\sigma_3$.

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

**Theorem 3.1.** *The protocol is a $\Sigma'$-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 Honest-Verifier Zero-Knowledge property of this protocol.

- Completeness: The verifier accepts with overwhelming probability if the protocol is not aborted by the prover, and the accepting probability is close to $\frac{1}{2\beta+1} + \frac{2\beta}{(2\beta+1)M_2 M_3}$ overwhelmingly.
- Special Soundness: Given a commitment $\vec{c}$ and a pair of accepting transcripts $(\vec{t}, d, (0, \vec{s}_r, \vec{s}_e))$, $(\vec{t}, d, (0, \vec{s}'_r, \vec{s}'_e))$ where $d \neq d'$, we can extract a valid 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 $\vec{s}_m = 0, \vec{s}_r = \vec{\rho}, \vec{s}_e = \vec{\eta}$ to V. Thus $\vec{t} + d\vec{c} = \vec{t} = \mathbf{B}\vec{\rho} + \vec{\eta} = \mathbf{B}\vec{s}_r + \vec{s}_e \mod q$. Since $\vec{\rho} \leftarrow D^n_{\sigma_2}, \vec{\eta} \leftarrow D^m_{\sigma_3}$, $\|\vec{s}_r\|_\infty = \|\vec{\rho}\|_\infty \leq 12\sigma_2$, and $\|\vec{s}_e\|_\infty = \|\vec{\eta}\|_\infty \leq 12\sigma_3$ with overwhelming probability by lemma 2.1.

In the case $d \neq 0$, P sends $\vec{s}_m = 0, \vec{s}_r = \vec{\rho} + d\vec{r}, \vec{s}_e = \vec{\eta} + d\vec{e}$ to V with probability close to $\frac{1}{M_2 M_3}$ overwhelmingly by the rejection sampling lemma. Thus $\mathbf{B}\vec{s}_r + \vec{s}_e = \mathbf{B}\vec{\rho} + \vec{\eta} + d(\mathbf{B}\vec{r} + \vec{e}) = \vec{t} + d\vec{c}$. Note that the distribution of $\vec{s}_r = \vec{\rho} + d\vec{r}, \vec{s}_e = \vec{\eta} + d\vec{e}$ are statistically close to $D^n_{\sigma_2}, D^m_{\sigma_3}$ respectively by the rejection sampling lemma. Hence, $\|\vec{s}_r\|_\infty \leq 12\sigma_2$, and $\|\vec{s}_e\|_\infty \leq 12\sigma_3$ with overwhelming probability by lemma 2.1. Therefore, V accepts with probability close to $\frac{1}{2\beta+1} + \frac{2\beta}{(2\beta+1)M_2 M_3}$ overwhelmingly.

Special Soundness: Suppose two accepting transcripts $(\vec{t}, d, (0, \vec{s}_r, \vec{s}_e))$, and $(\vec{t}, d, (0, \vec{s}'_r, \vec{s}'_e))$ where $d \neq d'$ are given. Then the following equations are hold:

$$\vec{t} + d\vec{c} = \mathbf{B}\vec{s}_r + \vec{s}_e \mod q$$
$$\vec{t} + d'\vec{c} = \mathbf{B}\vec{s}'_r + \vec{s}'_e \mod q$$

By subtracting the above equations, we get:

$$(d - d')\vec{c} = \mathbf{B}(\vec{s}_r - \vec{s}'_r) + (\vec{s}_e - \vec{s}'_e) \mod q$$

In other words, we have a witness $((\vec{s}_r - \vec{s}'_r), (\vec{s}_e - \vec{s}'_e), d - d')$ for $(\mathbf{B}, \vec{c})$ such that $\|\vec{s}_r - \vec{s}'_r\|_\infty \leq 24\sigma_2$, and $\|\vec{s}_e - \vec{s}'_e\|_\infty \leq 24\sigma_3$.

Honest-Verifier Zero-Knowledge: Let $\vec{c}$ and challenge $d$ are given as inputs. First, the simulator samples $\vec{s}'_m = 0, \vec{s}'_r \leftarrow D^n_{\sigma_2}$, and $\vec{s}'_e \leftarrow D^m_{\sigma_3}$, and computes $\vec{t} = \mathbf{A}\vec{s}'_m + \mathbf{B}\vec{s}'_r + \vec{s}'_e - d\vec{c}$. In the case $d = 0$, the simulator outputs $(\vec{t}, 0, (\vec{s}'_m, \vec{s}'_r, \vec{s}'_e))$. This is statistically indistinguishable from accepting transcripts of the real protocol, since the distribution of response $(\vec{s}'_m, \vec{s}'_r, \vec{s}'_e)$ is statistically indistinguishable from the distribution of real response by the rejection sampling lemma, and $\vec{t}$ is uniquely determined by $\vec{s}'_m, \vec{s}'_r, \vec{s}'_e$, and $d$ in the real protocol and in the simulation. When $d \neq 0$, the simulator outputs $(\vec{t}, d, (\vec{s}'_m, \vec{s}'_r, \vec{s}'_e))$ with probability $\frac{1}{M_2 M_3}$. Otherwise, the simulator outputs $(\vec{t}_0, d, \perp)$ where $\vec{t}_0 \leftarrow \mathbb{Z}^m_q$. The non-aborting case of this simulation is indistinguishable from the non-aborting case of the real protocol similarly. $\mathbf{B}\vec{\rho} + \vec{\eta} \mod q$ in $\vec{t} = \mathbf{B}\vec{\rho} + \vec{\eta} \mod q$ 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 $\vec{t}_0$, which is sampled from uniform random distribution over $\mathbb{Z}^m_q$.

□

### 3.2. Proof of Linear Relation

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

- P computes $\vec{t}_i = \mathbf{A}\vec{\mu}_i + \mathbf{B}\vec{\rho}_i + \vec{\eta}_i \mod q$ for $i = 1, 2$ where $\vec{\mu}_1 \leftarrow \mathbb{Z}^l_q, \vec{\mu}_2 = g(\vec{\mu}_1), \vec{\rho}_i \leftarrow D^n_{\sigma_2}, \vec{\eta}_i \leftarrow D^m_{\sigma_3}$ for $i = 1, 2$, and sends $\vec{t}_1, \vec{t}_2$ 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 $\vec{s}_{m,i} = \vec{\mu}_i + d\vec{m}_i \mod q, \vec{s}_{r,i} = \vec{\rho}_i + d\vec{r}_i \mod q, \vec{s}_{e,i} = \vec{\eta}_i + d\vec{e}_i \mod q$ for $i = 1, 2$. If $d = 0$, P sends $\vec{s}_{m,i}, \vec{s}_{r,i}, \vec{s}_{e,i}$ for $i = 1, 2$ to V. Otherwise, P sends $\vec{s}_{m,i}, \vec{s}_{r,i}, \vec{s}_{e,i}$ for $i = 1, 2$ to V with probability $p = \prod_{i=1}^{2} D^n_{\sigma_2}(\vec{\rho}_i)/M_{2,i} D^n_{d\vec{r}_i,\sigma_2}(\vec{\rho}_i) \times D^n_{\sigma_2}(\vec{\eta}_i)/M_{3,i} D^n_{d\vec{e}_i,\sigma_2}(\vec{\eta}_i)$, and $\perp$ with probability $1 - p$.

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

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

**Theorem 3.2.** *The protocol is a $\Sigma'$-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 $\vec{c}_1, \vec{c}_2$ and a pair of accepting transcripts
$$(\vec{t}_1, \vec{t}_2, d, (\vec{s}_{m,1}, \vec{s}_{m,2}, \vec{s}_{r,1}, \vec{s}_{r,2}, \vec{s}_{e,1}, \vec{s}_{e,2}))$$
$$(\vec{t}_1, \vec{t}_2, d', (\vec{s}'_{m,1}, \vec{s}'_{m,2}, \vec{s}'_{r,1}, \vec{s}'_{r,2}, \vec{s}'_{e,1}, \vec{s}'_{e,2}))$$
where $d \neq d'$, we can extract a valid opening information of $\vec{c}_1$, and $\vec{c}_2$.
- 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 Honest-Verifier Zero-Knowledge property of this protocol as in the previous case.

Completeness: When $d = 0$, P sends $\vec{s}_{m,i} = \vec{\mu}_i, \vec{s}_{r,i} = \vec{\rho}_i, \vec{s}_{e,i} = \vec{\eta}_i$ to V for $i = 1, 2$. Thus $\vec{t}_i + d\vec{c}_i = \vec{t}_i = \mathbf{A}\vec{\mu}_i + \mathbf{B}\vec{\rho}_i + \vec{\eta}_i = \mathbf{A}\vec{s}_{m,i} + \mathbf{B}\vec{s}_{r,i} + \vec{s}_{e,i} \mod q$ for $i = 1, 2$. Since $\vec{\rho}_i \leftarrow D^n_{\sigma_2}, \vec{\eta}_i \leftarrow D^m_{\sigma_3}$, $\|\vec{s}_{r,i}\|_\infty = \|\vec{\rho}_i\|_\infty \leq 12\sigma_2$, and $\|\vec{s}_{e,i}\|_\infty = \|\vec{\eta}_i\|_\infty \leq 12\sigma_3$ for $i = 1, 2$ with overwhelming probability by lemma 2.1. Note that $\vec{s}_{m,2} = \vec{\mu}_2 = g(\vec{\mu}_1) = g(\vec{s}_{m,1})$

In the case $d \neq 0$, P sends $\vec{s}_{m,i} = \vec{\mu}_i + d\vec{m}_i, \vec{s}_{r,i} = \vec{\rho}_i + d\vec{r}_i, \vec{s}_{e,i} = \vec{\eta}_i + d\vec{e}_i$ 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 $\mathbf{A}\vec{s}_{m,i} + \mathbf{B}\vec{s}_{r,i} + \vec{s}_{e,i} = \mathbf{A}\vec{\mu}_i + \mathbf{B}\vec{\rho}_i + \vec{\eta}_i + d(\mathbf{A}\vec{m}_i + \mathbf{B}\vec{r}_i + \vec{e}_i) = \vec{t}_i + d\vec{c}_i$ for $i = 1, 2$. Note that the distributions of $\vec{s}_{r,i} = \vec{\rho}_i + d\vec{r}_i, \vec{s}_{e,i} = \vec{\eta}_i + d\vec{e}_i$ for $i = 1, 2$ are statistically close to $D^n_{\sigma_2}, D^m_{\sigma_3}$ respectively by the rejection sampling lemma. Hence, $\|\vec{s}_{r,i}\|_\infty \leq 12\sigma_2$, and $\|\vec{s}_{e,i}\|_\infty \leq 12\sigma_3$ for $i = 1, 2$ with overwhelming probability by lemma 2.1, and $\vec{s}_{m,2} = \vec{\mu}_2 + d\vec{m}_2 = g(\vec{\mu}_1) + dg(\vec{m}_1) = g(\vec{s}_{m,1})$. 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
$$(\vec{t}_1, \vec{t}_2, d, (\vec{s}_{m,1}, \vec{s}_{m,2}, \vec{s}_{r,1}, \vec{s}_{r,2}, \vec{s}_{e,1}, \vec{s}_{e,2})),$$
$$(\vec{t}_1, \vec{t}_2, d', (\vec{s}'_{m,1}, \vec{s}'_{m,2}, \vec{s}'_{r,1}, \vec{s}'_{r,2}, \vec{s}'_{e,1}, \vec{s}'_{e,2}))$$
where $d \neq d'$. Then the following equations are hold:
$$\vec{t}_i + d\vec{c}_i = \mathbf{A}\vec{s}_{m,i} + \mathbf{B}\vec{s}_{r,i} + \vec{s}_{e,i} \mod q$$

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

By subtracting the above equations, we get:

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

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

Honest-Verifier Zero-Knowledge: Let $\vec{c}_1, \vec{c}_2$ and challenge $d$ are given as inputs. First, the simulator samples $\vec{s}'_{m,1} \leftarrow \mathbb{Z}_q^l, \vec{s}'_{r,i} \leftarrow D_{\sigma_2}^n$, $\vec{s}'_{e,i} \leftarrow D_{\sigma_3}^m$, and computes $\vec{s}'_{m,2} = g(\vec{s}'_{m,1})$, $\vec{t}_i = \mathbf{A}\vec{s}'_{m,i} + \mathbf{B}\vec{s}'_{r,i} + \vec{s}'_{e,i} - d\vec{c}_i$ for $i = 1, 2$. In the case $d = 0$, the simulator outputs $(\vec{t}_1, \vec{t}_2, 0, (\vec{s}'_{m,1}, \vec{s}'_{m,2}, \vec{s}'_{r,1}, \vec{s}'_{r,2}, \vec{s}'_{e,1}, \vec{s}'_{e,2}))$. This is statistically indistinguishable from accepting transcripts of the real protocol, since the distribution of response $(\vec{s}'_{m,1}, \vec{s}'_{m,2}, \vec{s}'_{r,1}, \vec{s}'_{r,2}, \vec{s}'_{e,1}, \vec{s}'_{e,2})$ is statistically indistinguishable from the the distribution of real response by the rejection sampling lemma, and $\vec{t}_i$ is uniquely determined by $\vec{s}'_{m,i}, \vec{s}'_{r,i}, \vec{s}'_{e,i}$, and $d$ in the real protocol and in the simulation. When $d \neq 0$, the simulator outputs $(\vec{t}_1, \vec{t}_2, 0, (\vec{s}'_{m,1}, \vec{s}'_{m,2}, \vec{s}'_{r,1}, \vec{s}'_{r,2}, \vec{s}'_{e,1}, \vec{s}'_{e,2}))$ with probability $\prod_{i=1}^2 M_{2,i}M_{3,i}$. Otherwise, the simulator outputs $(\vec{t}_{0,1}, \vec{t}_{0,2}, d, \perp)$ where $\vec{t}_{0,i} \leftarrow \mathbb{Z}_q^m$ for $i = 1, 2$. The non-aborting case of this simulation is indistinguishable from the non-aborting case of the real protocol similarly. $\mathbf{B}\vec{\rho}_i + \vec{\eta}_i \mod q$ in $\vec{t}_i = \mathbf{A}\vec{\mu}_i + \mathbf{B}\vec{\rho}_i + \vec{\eta}_i \mod q$ in real protocol can be regarded as an instance of $LWE_{n,m,q,\sigma_3}(D_{\sigma_2}^n)$, which is hard under the condition, $spLWE_{n,m+n,q,s_1,\rho,\theta}$ is hard. Thus $\vec{t}_i$ is computationally indistinguishable from $\vec{t}_{0,i}$, which is sampled from uniform random distribution over $\mathbb{Z}_q^m$ □

### 3.3. Proof of Sum

We now describe our zero-knowledge proof of sum. Let $\vec{c}_i = \mathbf{A}\vec{m}_i + \mathbf{B}\vec{r}_i + \vec{e}_i \mod q$ for $i = 1, 2, 3$ be commitments that are published by the prover such that $\vec{m}_3 = \vec{m}_1 + \vec{m}_2$. The goal of following protocol is to prove the sum relation of committed 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 $\vec{c}_i$ for $i = 1, 2, 3$, and the private inputs are $(\vec{r}_i, \vec{e}_i)$ for $i = 1, 2, 3$:

- P computes $\vec{t}_i = \mathbf{A}\vec{\mu}_i + \mathbf{B}\vec{\rho}_i + \vec{\eta}_i \mod q$ for $i = 1, 2, 3$ where $\vec{\mu}_1, \vec{\mu}_2 \leftarrow \mathbb{Z}_q^l, \vec{\mu}_3 = \vec{\mu}_1 + \vec{\mu}_2, \vec{\rho}_i \leftarrow D_{\sigma_2}^n, \vec{\eta}_i \leftarrow D_{\sigma_3}^m$ for $i = 1, 2, 3$, and sends $\vec{t}_1, \vec{t}_2, \vec{t}_3$ 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 $\vec{s}_{m,i} = \vec{\mu}_i + d\vec{m}_i \mod q, \vec{s}_{r,i} = \vec{\rho}_i + d\vec{r}_i \mod q, \vec{s}_{e,i} = \vec{\eta}_i + d\vec{e}_i \mod q$ for $i = 1, 2, 3$. If $d = 0$, P sends $\vec{s}_{m,i}, \vec{s}_{r,i}, \vec{s}_{e,i}$ for $i = 1, 2, 3$ to V. Otherwise, P sends $\vec{s}_{m,i}, \vec{s}_{r,i}, \vec{s}_{e,i}$ for $i = 1, 2, 3$ to V with probability $p = \prod_{i=1}^3 D_{\sigma_2}^n(\vec{\rho}_i)/M_{2,i}D_{d\vec{r}_i,\sigma_2}^n(\vec{\rho}_i) \times D_{\sigma_3}^n(\vec{\eta}_i)/M_{3,i}D_{d\vec{e}_i,\sigma_2}^n(\vec{\eta}_i)$, and $\perp$ with probability $1 - p$.

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

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

**Theorem 3.3.** *The protocol is a $\Sigma'$-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 $\vec{c}_1, \vec{c}_2, \vec{c}_3$ and a pair of accepting transcripts

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

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

  where $d \neq d'$, we can extract a valid opening information of $\vec{c}_1$, $\vec{c}_2$ and $\vec{c}_3$.
- 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 knowledge of this protocol as in the previous case, proof of linear relation. The only difference is $\vec{s}_{m,3} = \vec{s}_{m,1} + \vec{s}_{m,2}$. In this case, the simulator set the $\vec{s}'_{m,3}$ as $\vec{s}'_{m,3} = \vec{s}'_{m,1} + \vec{s}'_{m,2}$ for $\vec{s}'_{m,1}, \vec{s}'_{m,2} \leftarrow \mathbb{Z}_q^l$. □

## 4. Concluding Remarks

In this work, we give spLWE-based constructions for zero-knowledge protocols of knowledge of committed messages, and for proving linear, and sum relations among such messages. In order to achieve negligible soundness error in our protocols, we use rejection sampling. Finally, we address an open problem stated in previous work in [10].

For future works, we consider the construction of additional zero-knowledge protocols for proving the bound of error in spLWE. In terms of efficiency, we would like to more concretely analyze the error size in the commitment scheme and zero-knowledge protocols. The more commitments are added, the bigger the error size grows. As a result, the verification algorithm does not accept the input as a valid one.

## Acknowledgment

This work is supported by internal funds in Naval Academy, Republic of Korea.

## References


[1] M. Ajtai, Generating hard instances of lattice problems, Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, (1996), 99-108.

[2] G. Asharov, A. Jain, A. López-Alt, E. Tromer, V. Vaikuntanathan, D. Wichs, Multiparty computation with low communication, computation and interaction via threshold FHE, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Berlin, Heidelberg, (2012), 483-501.

[3] M. Blum, Coin flipping by telephone a protocol for solving impossible problems, ACM SIGACT News, 15(1), (1983), 23-27.

[4] W. Banaszczyk, Inequalities for convex bodies and polar reciprocal lattices in $\mathbb{R}^n$, Discrete & Computational Geometry, 13(2), (1995), 217-231.

[5] S. Bai, S. Galbraith, An improved compression technique for signatures based on learning with errors, RSA Conference, Springer, Cham, (2014), 28-47.

[6] F. Benhamouda, J. Camenisch, S. Krenn, V. Lyubashevsky, G. Neven, Better zero-knowledge proofs for lattice encryption and their application to group signatures, International Conference on the Theory and Application of Cryptology and Information Security, Springer, Berlin, Heidelberg, (2014), 551-572.

[7] F. Benhamouda, S. Krenn, V. Lyubashevsky, K. Pietrzak, Efficient zero-knowledge proofs for commitments from learning with errors over rings, European symposium on research in computer security, Springer, Cham, (2015), 305-325.

[8] J. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, D. Stebila, Frodo: Take off the ring! practical, quantum-secure key exchange from LWE, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, (2016), 1006-1018.

[9] A. Jain, S. Krenn, K. Pietrzak, A. Tentes, Commitments and efficient zero-knowledge proofs from learning parity with noise, International Conference on the Theory and Application of Cryptology and Information Security, Springer, Berlin, Heidelberg, (2012), 663-680.

[10] J. Kim, A Post-Quantum Commitment Scheme based on spLWE, IJCSNS International Journal of Computer Science and Network Security, 20(12), (2020), 265-271.

[11] R. Lindner, C. Peikert, Better key sizes (and attacks) for LWE-based encryption, RSA Conference, Springer, Berlin, Heidelberg, (2011), 99-108.

[12] V. Lyubashevsky, Lattice signatures without trapdoors, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Berlin, Heidelberg, (2012), 738-755.

[13] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, Proceedings of the thirty-seventh annual ACM symposium on Theory of computing, (2005), 84-93.

[14] C. P. Schnorr, Efficient signature generation by smart cards, Journal of cryptology, 4(3), (1991), 161-174.

[15] X. Xie, R. Xue, M. Wang, Zero knowledge proofs from Ring-LWE, International Conference on Cryptology and Network Security, Springer, Cham, (2013), 57-73.



Jinsu Kim
Jungwon-ro, Jinhae-gu, Changwon-si, Gyeongsangnam-do, Republic of Korea, 51698
*E-mail address*: nemokjs1@gmail.com

Dooyoung Kim
Jungwon-ro, Jinhae-gu, Changwon-si, Gyeongsangnam-do, Republic of Korea, 51698
*E-mail address*: dykim07@outlook.com