IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 27, 2021, accepted October 27, 2021, date of publication November 15, 2021, date of current version December 2, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3128139

Improved Reduction Between SIS Problems Over Structured Lattices

ZAHYUN KOO[1], YONGWOO LEE[1], JOON-WOO LEE[1], (Graduate Student Member, IEEE), JONG-SEON NO[1], (Fellow, IEEE), AND YOUNG-SIK KIM[2], (Member, IEEE)

[1]Department of Electrical and Computer Engineering, INMC, Seoul National University, Seoul 08826, South Korea
[2]Department of Information and Communication Engineering, Chosun University, Gwangju 61452, South Korea

Corresponding author: Young-Sik Kim (iamyskim@chosun.ac.kr)

This work was supported by the Samsung Research Funding and Incubation Center for Future Technology of Samsung Electronics under Project SRFC-IT1801-08.

ABSTRACT Many lattice-based cryptographic schemes are constructed based on hard problems on an algebraic structured lattice, such as the short integer solution (SIS) problems. These problems are called ring-SIS (R-SIS) and its generalized version, module-SIS (M-SIS). Generally, it has been considered that problems defined on the module lattice are more difficult than the problems defined on the ideal lattice. However, Koo, No, and Kim showed that R-SIS is more difficult than M-SIS under some norm constraints of R-SIS. However, this reduction has problems in that the rank of the module is limited to about half of the instances of R-SIS, and the comparison is not performed through the same modulus of R-SIS and M-SIS. In this paper, we propose the three reductions. First, we show that R-SIS is more difficult than M-SIS with the same modulus and ring dimension under some constraints of R-SIS. Also, we show that through the reduction from M-SIS to R-SIS with the same modulus, the rank of the module is extended as much as the number of instances of R-SIS from half of the number of instances of R-SIS compared to the previous work. Second, we show that R-SIS is more difficult than M-SIS under some constraints, which is tighter than the M-SIS in the previous work. Finally, we propose that M-SIS with the modulus prime q^k is more difficult than M-SIS with the composite modulus c, such that c is divided by q. Through the three reductions, we conclude that R-SIS with the modulus q is more difficult than M-SIS with the composite modulus c.

INDEX TERMS Lattice-based cryptography, learning with error (LWE), module-short integer solution (M-SIS) problem, ring-short integer solution (R-SIS) problem, short integer solution (SIS) problem.

I. INTRODUCTION

Many cryptographic schemes are based on problems that are difficult to solve on computers, including the RSA based on prime factor decomposition and the elliptic curve cryptographic (ECC) scheme based on the discrete logarithm problem (DLP). Since the prime factor decomposition problem and DLP take a long time to solve on computers, cryptographic schemes based on these problems have been considered secure. However, due to the quantum computer's development, it is known that many cryptographic schemes can be broken using quantum algorithms operated on quantum computers [1]. Therefore, candidates of cryptographic schemes that are resistant to quantum computers have been actively researched. The representative candidates are lattice-based cryptography, code-based cryptography, multivariate polynomial-based cryptography, isogeny-based cryptography. Among them, the diverse forms of lattice-based cryptography such as public-key cryptographic schemes, signature schemes, and key encapsulation mechanisms are submitted in NIST post-quantum cryptography (PQC) standardization competition for the advantages of small-sized key and efficiency as well as security [2].

Lattice-based cryptographic schemes are based on hard problems such as the *shortest independent vector problem* (SIVP), which is known to reduce to *short integer solution* (SIS) problem and *learning with error* (LWE) problem. The SIS problem introduced by Ajtai [3] has been used to construct many lattice-based cryptographic schemes. The SIS problem is defined as follows: Let $\mathbb{Z}$ and $\mathbb{R}$ denote the sets of integers and real numbers, respectively. Let $\mathbb{Z}_q$ denote the set of integers modulo q. For any positive integers m, n, given positive real number $\beta \in \mathbb{R}$, and positive integer q, the SIS problem is to find solution $\mathbf{z} \in \mathbb{Z}^m$ such that $\mathbf{A} \cdot \mathbf{z} = \mathbf{0} \bmod q$ and $0 < \|\mathbf{z}\| \leq \beta$ for uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. A one-way function can be constructed from the

The associate editor coordinating the review of this manuscript and approving it for publication was Neetesh Saxena.

SIS problem [7], and then many cryptographic schemes can be constructed from one-way function [4]–[6].

However, cryptographic schemes based on SIS are inefficient since the size of the key of the signature scheme or commitment scheme is too large. Many cryptographic schemes based on structured lattices such as the ideal and module lattices have been proposed to overcome this problem. The ideal lattice is defined on the lattice with a polynomial ring structure, and the module lattice is defined on a module structure, which is an algebraic structure that generalizes ring structure and vector space. Then we can define the SIS problem over the structured lattices. The SIS problem defined over an ideal lattice is said to be ring-SIS (R-SIS) [8], and the SIS problem defined over a module lattice is said to be module-SIS (M-SIS) [9]. It is shown that R-SIS and M-SIS are as hard as SIVP defined on the ideal lattice and the module-lattice, respectively [9], [10].

A. PREVIOUS WORKS

Generally, it has been considered that M-SIS is a more difficult problem than R-SIS in the polynomial ring. For example, suppose that there is an algorithm $\mathcal{A}$ for solving M-SIS. The instances of R-SIS can be embedded in M-SIS since the polynomial ring defining R-SIS is considered the module with rank one. Then the algorithm $\mathcal{A}$ can be used to find the solution of R-SIS. Thus, in lattice-based cryptographic schemes [11]–[13], [14], M-SIS is preferred due to the fundamental difficulty as well as the reduced key-size and thus, we do not work on the existence of an algorithm to solve the R-SIS.

However, the problems over the module lattice are not always more difficult than the problems over the ideal lattice. In the case of SIS over structured lattices, Koo, No, and Kim showed that the R-SIS problem is more difficult than M-SIS for some specific parameters [15]. In other words, there exists a reduction from M-SIS$_{q^k,m^k,\beta'}$ to R-SIS$_{q,m,\beta}$, where $\beta' = m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)}$. To show this, they assign a specific constraint to the upper bound of the norm of the solution of R-SIS. In particular, due to this constraint, the possible range of module rank that can be reduced to R-SIS is limited to $d < \frac{m+1}{2}$ for sufficiently large modulus q. Also, this reduction showed the relationship between R-SIS with m instances and modulus q and M-SIS with m^k instances and modulus q^k for some $k > 1$. In other words, this reduction cannot be said to be established for the same modulus and the same instances. Also, we can infer tight rank-modulus trade-off reduction from R-SIS to M-SIS through [18]–[20]. First, let nd be a ring-dimension defining R-SIS. Reference [19] proposed that there exists a quantum reduction from R-SIS to R-LWE. Since [18] proposed a tight rank-modulus trade-off reduction from R-LWE to M-LWE with ring dimension n and module-rank d. Finally, we use the dual attack reduction [20] from M-LWE to M-SIS, preserving rank and ring dimension. All these steps preserve the modulus q. However, this reduction does not preserve the ring dimension, that is, not the same ring.

B. CONTRIBUTIONS

In this paper, we propose the improved reduction from M-SIS to R-SIS compared to the previous work [15]. Similar to the previous work, the proposed reduction considers some conditions of the upper bound β on the norm of the solution of R-SIS. However, there are three differences between the previous work and the proposed reduction.

First, we propose a new method to find m distinct solutions of instances of R-SIS$_{q,m,\beta}$. Using this method, we obtain the reduction from M-SIS$_{q,m,\beta_1}$ to R-SIS$_{q,m,\beta}$, where $\beta_1 = (t \cdot \sqrt{m})^{d-1}\beta^d$ in Theorem 3 and t is a positive integer. This reduction preserves the modulus q and ring-dimension n. In particular, we can see that the possible range of module rank that allows the reduction from M-SIS to R-SIS is doubled compared to that in the previous work [15].

Second, we propose that M-SIS$_{q,m,\beta_1}$ is more difficult than M-SIS$_{q^k,m^k,\beta_3}$, where $\beta_3 = m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)}$ for $k \geq 1$. To show this, first, we show the reduction from M-SIS$_{q^k,m^k,\beta^k}$ to M-SIS$_{q,m,\beta}$ in Theorem 4, where there is no constraint on β; that is, β can be $t \cdot \sqrt{m} \cdot \beta$ as in Fig. 1. From this reduction, the modulus and the number of instances of M-SIS$_{q^k,m^k,\beta_2}$ are matched with M-SIS$_{q^k,m^k,\beta_3}$ as in Fig. 1. Then, we show a reduction from M-SIS$_{q^k,m^k,\beta_3}$ to M-SIS$_{q,m,\beta_2}$ for some $k \geq 1$ by comparing the upper bound of M-SIS solutions in Theorem 5.

Third, we propose a reduction between M-SIS problems with different modulus. There is a reduction from M-SIS$_{c,m^k,\gamma}$ to M-SIS$_{q^k,m^k,\beta_2}$, where c is a composite integer with a factor q^k and $\gamma = \frac{c}{q^k}\beta_2$ for some $k \geq 1$ in Theorem 6. Thus, as the modulus of M-SIS becomes large, M-SIS becomes less secure. Combining three reductions, that is, Theorems 3, 4, and 6, we propose the following main result, Theorem 7 (See Subsection IV-C for details):

Main Result 1 (Theorem 7): Let m be a positive integer. Let t be positive integers and q be a prime such that

$$t \leq \sqrt{n \cdot m} \cdot q^{\frac{1}{m}} < \frac{q}{t}.$$

Let c be a composite integer such that c is divided by q^k for some $k \geq 1$. Choose a module rank $d \in \mathbb{Z}_{>0}$ such that

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} < \frac{\sqrt[d]{q \cdot t \cdot \sqrt{m}}}{t \cdot \sqrt{m}}.$$

Let a positive real number β be an upper bound on the norm of the solution of R-SIS$_{q,m,\beta}$ such that

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} \leq \beta < \frac{\sqrt[d]{q \cdot t \cdot \sqrt{m}}}{t \cdot \sqrt{m}}.$$

Assume that an algorithm $\mathcal{A}$ exists for solving R-SIS$_{q,m,\beta}$. Then there exists an algorithm $\mathcal{B}$ for solving M-SIS$_{c,m^k,\gamma}$, where $\gamma = \frac{c}{q^k}(t \cdot \sqrt{m})^{k(d-1)}\beta^{kd}$.

As mentioned in [15], when constructing M-SIS based cryptographic scheme, the algorithm for solving R-SIS for certain parameters should be considered. When we construct the cryptographic scheme based on M-SIS, through the proposed work, it means that we need to consider the tighter parameters compared to the previous work [15].

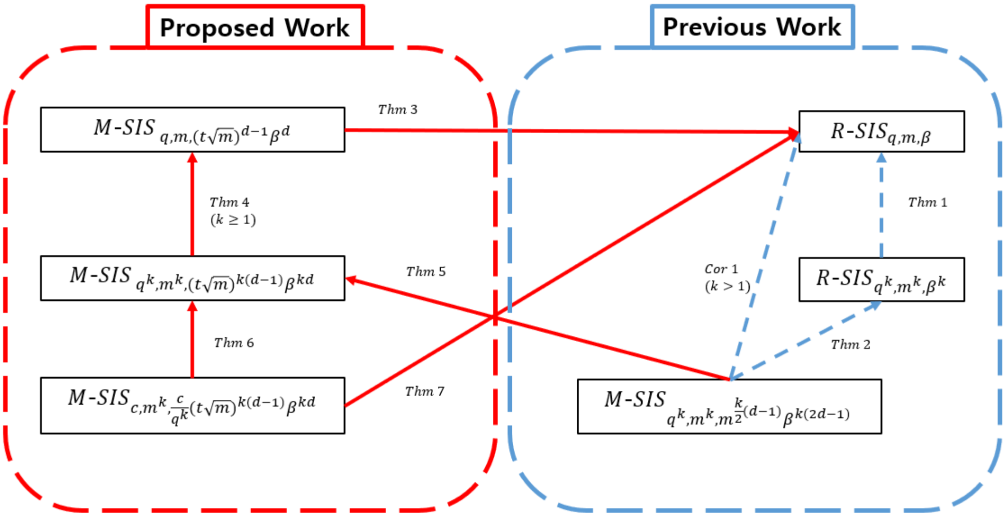

Proposed Work
Previous Work
$M\text{-}SIS_{q,m,(t\sqrt{m})^{d-1}\beta^d}$
Thm 3
$R\text{-}SIS_{q,m,\beta}$
Thm 4
$(k \geq 1)$
Thm 1
$M\text{-}SIS_{q^k,m^k,(t\sqrt{m})^{k(d-1)}\beta^{kd}}$
Thm 5
Cor 1
$(k > 1)$
$R\text{-}SIS_{q^k,m^k,\beta^k}$
Thm 6
Thm 2
$M\text{-}SIS_{c,m^k,\frac{c}{q^k}(t\sqrt{m})^{k(d-1)}\beta^{kd}}$
Thm 7
$M\text{-}SIS_{q^k,m^k,m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)}}$

FIGURE 1. Relationship of reductions between R-SIS and M-SIS for various parameters.

For example, we assume that M-SIS$_{q,m,\beta_1}$, where $m = 10$, $n = 2^8$, $\log(q) \approx 40$, $\log(\beta_1) \approx 50$, $d = 3$, and consider the collision-hash function defined over the module as follows: Let $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_m) \in R_q^d$, where R is a polynomial ring. We define the function $f_A : R^m \to R_q^d$ as $f_A(\mathbf{x}) = \sum_{i=1}^m \mathbf{a}_i \cdot x_i$, where $\mathbf{x} = (x_1, \ldots, x_m)$ with $\|\mathbf{x}\| \leq \frac{\beta_1}{2}$. Collision $\mathbf{x} \neq \mathbf{x}' \in R^m$, where $f_A(\mathbf{x}) = f_A(\mathbf{x}')$, yields the solution $\mathbf{z} = \mathbf{x} - \mathbf{x}'$ with $\|\mathbf{z}\| \leq \beta_1$. Assuming M-SIS$_{q,m,\beta_1}$, it is difficult to find a solution $\|\mathbf{z}\| \leq \beta_1$. If we assume that there exists an algorithm for solving R-SIS$_{q,m,\beta}$, where $\beta \approx 10$, a solution of M-SIS$_{q,m,\beta_1}$ could not be found through previous work [15]. However, due to the tighter parameters of the proposed work, we may be able to find a solution of M-SIS$_{q,m,\beta_1}$ for the same case.

C. ORGANIZATION

The remainder of this paper is organized as follows: In Section II, SIS problems on ideal and module lattices and the results of the previous works are introduced. In Section III, we propose a new method to find m distinct solutions for R-SIS. Using this method, we derive the reduction from M-SIS$_{q,m,(t\cdot\sqrt{m})^{d-1}\beta^d}$ to R-SIS$_{q,m,\beta}$. Also, we show the possible range of module rank of the proposed reduction. And it shows the comparison with the range in [15]. Section IV proposes the various reductions among the M-SIS problems, which lead to the reduction from M-SIS$_{c,m^k,\frac{c}{q^k}(t\cdot\sqrt{m})^{k(d-1)}\beta^{kd}}$ to R-SIS$_{q,m,\beta}$ for the modulus c such that $q^k|c$ for some $k \geq 1$. Finally, the conclusion and suggested future works are provided in Section V.

II. PRELIMINARIES

A. STRUCTURED LATTICES

1) NOTATIONS

Let D be a distribution over some finite set S, and then $x \leftarrow D$ means that x is chosen from the distribution D. Let $\mathcal{A}$ be an algorithm, and then $x \to \mathcal{A}$ means that $\mathcal{A}$ inputs x and $y \leftarrow \mathcal{A}$ means that $\mathcal{A}$ outputs y.

2) IDEALS AND MODULES

Let $\Phi(X)$ be a monic irreducible polynomial of degree n and $\mathbb{Q}$ be the set of rational numbers. We use the $2n$-th cyclotomic polynomial $\Phi(X) = X^n + 1$ with $n = 2^s$ for some positive integer s because many lattice-based cryptosystems use the $2n$-th cyclotomic polynomial $\Phi(X)$. Let K be a number field as $\mathbb{Q}[X]/\langle\Phi(X)\rangle$ and define R as the ring $\mathbb{Z}[X]/\langle\Phi(X)\rangle$. Conveniently, we refer to R as the polynomial ring. A non-empty set $I \subseteq R$ is an ideal of R if I is an additive subgroup of R and for all $r \in R$ and all $x \in I$, $r \cdot x \in I$. The quotient ring R/I is the set of equivalence classes $r + I$ of R modulo I. Let q be the positive integer and define $R_q = R/qR$. Define $M \subseteq K^d$ as an R-module, where R is the ring of integers of K and K is a number field if M is closed under addition and under scalar multiplication by elements of R. It is known that M/qM is isomorphic to R_q^d [9]. The element of R_q^d is denoted by the vector $\mathbf{a}$, whose entry is an element of the polynomial ring, that is, $\mathbf{a} = (a_1(X), \ldots, a_d(X)) \in R_q^d$. A matrix is denoted by an uppercase letter in bold.

3) CANONICAL EMBEDDING

In [9], the canonical embeddings are the n ring homomorphisms $\sigma_j : K \to \mathbb{C}$ for all $j = 1, \ldots, n$, where $\mathbb{C}$ is the set of the complex numbers. They are defined by $\sigma_j(X) = \xi^j$, where ξ is the solution of $X^n + 1$ for any $j \in \mathbb{Z}_{2n}^\times$ with $n = 2^r$ for some positive integer r, where $\mathbb{Z}_{2n}^\times$ denotes the set of integer j module $2n$ such that $\gcd(j, 2n) = 1$. We define the canonical embedding vector as the ring homomorphism $\sigma_C : K \to \mathbb{C}^n$ as $\sigma_C(x) = (\sigma_j(x))_{j \in \mathbb{Z}_{2n}^\times}$ under component-wise addition and multiplication. For any $a \in K$, we define the norm of a as

$$\|a\| = \|\sigma_C(a)\| = \left(\sum_{j \in \mathbb{Z}_{2n}^\times} |\sigma_j(a)|^2\right)^{1/2}.$$

Also, for any $\mathbf{a} = (a_1, \ldots, a_d) \in K^d$, we define the norm of $\mathbf{a}$ as

$$\|\mathbf{a}\| = \left(\sum_{i=1}^{d} \|a_i\|^2\right)^{1/2} = \left(\sum_{i=1}^{d} \sum_{j \in \mathbb{Z}_{2n}^{\times}} |\sigma_j(a_i)|^2\right)^{1/2}.$$

4) LATTICES

An n-dimensional lattice is a discrete subgroup of $\mathbb{R}^m$, where $\mathbb{R}$ is the set of real numbers. Specifically, for linearly independent vectors $\{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$, $\mathbf{b}_i \in \mathbb{R}^m$, for all $i = 1, \ldots, m$, the set

$$\mathcal{L} = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_m) = \left\{\sum_{i=1}^{n} x_i \mathbf{b}_i \ : \ x_i \in \mathbb{Z}\right\}$$

is a lattice in $\mathbb{R}^m$ with the basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$. Also the dual lattice of $\mathcal{L}^*$ is defined as

$$\mathcal{L}^* = \{\mathbf{x} \in \operatorname{span}(\mathcal{L}) \mid \forall \mathbf{v} \in \mathcal{L}, \langle \mathbf{x}, \mathbf{v} \rangle \in \mathbb{Z}\}.$$

A lattice is an *ideal lattice* if it is isomorphic to some ideal I of R. Similarly, a lattice is a *module lattice* if it is isomorphic to some R-module M [9].

B. SHORT INTEGER SOLUTION PROBLEMS

First, we define the *short integer solution* (SIS) problem over the lattice used in many lattice-based cryptographic schemes such as signature schemes and commitment schemes. This problem was first defined by Ajtai [3].

This problem is extended to the structured lattices, which are ideal lattices and module lattices. Since the instances of R-SIS are polynomial, the key size of the signature scheme based on R-SIS can be smaller than that of a signature scheme based on SIS. The module structure is a generalized structure of the ring, and the R-SIS problem can be extended to the problem over module lattice, termed M-SIS. These problems are defined as follows:

Definition 1 ([8], [9], [16]): The problem R-SIS$_{q,m,\beta}$ is defined as follows: Given $a_1, \ldots, a_m \in R_q$ chosen independently from the uniform distribution, the R-SIS problem is to find $z_1, \ldots, z_m \in R$ such that $\sum_{i=1}^{m} a_i \cdot z_i = 0 \mod q$ and $0 < \|\mathbf{z}\| \leq \beta$, where $\mathbf{z} = (z_1, \ldots, z_m)^T \in R^m$.

Definition 2 ([8], [9]): Similarly, the problem M-SIS$_{q,m,\beta}$ is defined as follows: Given $\mathbf{a}_1, \ldots, \mathbf{a}_m \in R_q^d$ chosen independently from the uniform distribution, the M-SIS problem is to find $\mathbf{z} = (z_1, \ldots, z_m)^T \in R^m$ such that $\sum_{i=1}^{m} \mathbf{a}_i \cdot z_i = 0 \mod q$ and $0 < \|\mathbf{z}\| \leq \beta$.

C. REDUCTION FROM M-SIS TO R-SIS

Generally, the M-SIS problem is more difficult than the R-SIS problem. Indeed, suppose that an algorithm $\mathcal{A}$ exists for solving M-SIS and let $a_1, \ldots, a_m \in R_q$ be independently uniform instances of R-SIS. Also, we choose $a_2^{(j)}, \ldots, a_d^{(j)} \in R_q$ from uniform distribution over R_q for all $j = 1, \ldots, m$, where d is a module rank. Then $\mathbf{a}_j = (a_j, a_2^{(j)}, \ldots, a_d^{(j)})$ and $\mathbf{a}_1, \ldots, \mathbf{a}_m$ are instances of M-SIS. Using the algorithm $\mathcal{A}$ for solving M-SIS, we obtain a solution $\mathbf{z} = (z_1, \ldots, z_m)^T$ such that

$$\sum_{i=1}^{m} \mathbf{a}_i \cdot z_i = (\sum_{i=1}^{m} a_i \cdot z_i, \sum_{i=1}^{m} a_2^{(i)} \cdot z_i, \ldots, \sum_{i=1}^{m} a_d^{(i)} \cdot z_i)$$
$$= \mathbf{0} \mod q$$

with $\|\mathbf{z}\| \leq \beta$. Since $\sum_{i=1}^{m} a_i \cdot z_i = 0 \mod q$ and $\|\mathbf{z}\| \leq \beta$, we find the solution of the instance of R-SIS. However, Koo, *et al.*, showed that R-SIS is more difficult than M-SIS under norm constraints of R-SIS [15]. To show the reduction from M-SIS to R-SIS, Koo, *et al.*, showed it in two steps. The first step is that there exists a reduction from R-SIS$_{q^k,m^k,\beta^k}$ to R-SIS$_{q,m,\beta}$ as follows:

Theorem 1 [15]: Let m be a positive integer and q be a prime. Choose the upper bound of the norm, $\beta \in \mathbb{R}$ such that $\beta \geq \sqrt{n \cdot m} \cdot q^{\frac{1}{m}}$ and $q \geq \beta\sqrt{n}\omega(\log n)$. Assume that there exists an algorithm $\mathcal{A}$ for solving the R-SIS$_{q,m,\beta}$ problem. Then there exists an algorithm $\mathcal{A}'$ for solving the R-SIS$_{q^k,m^k,\beta^k}$ for any integer $k \geq 1$, which corresponds to the reduction from R-SIS$_{q^k,m^k,\beta^k}$ to R-SIS$_{q,m,\beta}$.

In the second step, we need to find as many distinct solutions as the number of instances for the same instances of R-SIS. However, finding distinct solutions for the same instances of R-SIS is not straightforward since details of the algorithms' process for solving R-SIS are unknown. To resolve this problem, we use the following lemma.

Lemma 1 [15]: Let m and $k > 1$ be positive integers, and q be a prime. Let β be a real number such that $\max(q, \sqrt{n \cdot m} \cdot q^{\frac{k}{m}}) \leq \beta$. Assume that an algorithm $\mathcal{A}'$ exists for solving R-SIS$_{q^k,m,\beta}$ such that $\mathcal{A}'$ outputs a solution $\mathbf{z} \in R^m$ with $\gcd(\mathbf{z}, q) = 1$. Let $a_1, \ldots, a_m \in R_{q^k}$ be instances of R-SIS$_{q^k,m,\beta}$. Then we can find m distinct solutions $\bar{\mathbf{z}}^{(j)} = (\bar{z}_1^{(j)}, \ldots, \bar{z}_m^{(j)})^T \in R^m$ with $\|\bar{\mathbf{z}}^{(j)}\| \leq \beta^2$ such that $\sum_{i=1}^{m} a_i \cdot \bar{z}_i^{(j)} = 0 \mod q^k$ for all $j = 1, \ldots, m$.

The following theorem shows the second step: a reduction from M-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m,\beta}$ using Lemma 1.

Theorem 2 [15]: Let m be a fixed positive integer. Let $k > 1$ be a positive integer and q be a prime. Choose a module rank $d \in \mathbb{Z}$ such that

$$\max(q, \sqrt{n \cdot m} \cdot q^{\frac{k}{m}}) < \sqrt[2d-1]{q^k/(\sqrt{m})^{(d-1)}}.$$

Let a positive real number β be an upper bound of the norm of the solution of R-SIS$_{q^k,m,\beta}$ such that

$$\max(q, \sqrt{n \cdot m} \cdot q^{\frac{k}{m}}) \leq \beta,$$

where $\beta < \sqrt[2d-1]{q^k/(\sqrt{m})^{(d-1)}}$. Assume that an algorithm $\mathcal{A}'$ exists for solving the R-SIS$_{q^k,m,\beta}$ problem such that $\mathcal{A}'$ outputs a solution $\mathbf{z} \in R^m$ with $\gcd(\mathbf{z}, q) = 1$. Then an algorithm $\mathcal{A}''$ exists for solving the M-SIS$_{q^k,m,\beta'}$ problem with module rank d, where $\beta' = m^{\frac{1}{2}(d-1)}\beta^{(2d-1)}$; that is, there exists a reduction from M-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m,\beta}$.

Combining Theorems 1 and 2, we can show that there exists the reduction from M-SIS$_{q^k,m^k,\beta'}$ to R-SIS$_{q,m,\beta}$ with $\beta'' = m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)}$ as in the following corollary.

Corollary 1 [15]: Let m be a fixed positive integer. Let $k > 1$ be a positive integer and q be a prime. Choose a module rank $d \in \mathbb{Z}$ such that

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} < \sqrt[2d-1]{q^k / (\sqrt{m})^{(d-1)}}. \tag{1}$$

Let a positive real number β be an upper bound on the norm of the solution of R-SIS$_{q,m,\beta}$ such that

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} \leq \beta,$$

where $\beta < \sqrt[2d-1]{q^k / (\sqrt{m})^{(d-1)}}$. Assume that an algorithm $\mathcal{A}$ exists for solving the R-SIS$_{q,m,\beta}$ problem. Then an algorithm $\mathcal{A}''$ exists for solving M-SIS$_{q^k,m^k,\beta''}$ problem with module rank d, where $\beta'' = m^{\frac{k}{2}(d-1)} \beta^{k(2d-1)}$; that is, there exists a reduction from M-SIS$_{q^k,m^k,\beta''}$ to R-SIS$_{q,m,\beta}$.

D. RANGE OF MODULE RANK FOR PREVIOUS WORK

The module rank d is determined by (1) in Corollary 1. Since n is the dimension of the polynomial ring R and m is the number of instances of R-SIS, these parameters are fixed. Thus, the module rank d depends only on the modulus prime q, with fixed parameters n and m. By modifying (1), we have the range of module rank, where the reduction in Corollary 1 is possible, as follows:

$$d < \frac{2(m+1)\log q + 2m \log m + m \log n}{4 \log q + 2m \log m + 2m \log n}. \tag{2}$$

Then we have

$$d < \frac{m+1}{2}$$

for sufficiently large q [15]. Thus, the possible module rank d which enables the reduction from M-SIS$_{q^k,m^k,\beta''}$ to R-SIS$_{q,m,\beta}$ is upper bounded by $\frac{m+1}{2}$ for sufficiently large q, where $\beta'' = m^{\frac{k}{2}(d-1)} \beta^{k(2d-1)}$.

III. IMPROVED REDUCTION FROM M-SIS TO R-SIS

In this section, we propose a new method to find m distinct solutions for instances of R-SIS. In particular, the m distinct solutions are linearly independent over R_q. Using m distinct solutions, we obtain the solution for instances of M-SIS. Similar to the previous work [15], there is a range of module rank that allows the reduction from M-SIS to R-SIS. However, the proposed work shows that the range of module rank is doubled compared to the previous work.

A. IMPROVED REDUCTION FROM M-SIS TO R-SIS FOR THE SAME MODULUS AND THE NUMBER OF INSTANCES

We propose a new method of finding m distinct solutions of instances of R-SIS. Finding distinct solutions for the same instances of R-SIS is difficult since details of the algorithms' process for solving R-SIS are not known. For example, if the algorithm $\mathcal{A}$ for solving R-SIS is deterministic, then this algorithm outputs the same solution for the same instance. To overcome this problem, we devise a method to add randomness before using the algorithm for solving R-SIS.

Lemma 2: Let m be a positive integer and let t be a positive integer. Choose a prime q such that

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} < \frac{q}{t}.$$

Choose a real number β such that

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} \leq \beta < \frac{q}{t}.$$

Suppose that there exists an algorithm $\mathcal{A}$ for solving R-SIS$_{q,m,\beta}$. Let $\mathbf{a} = (a_1, \ldots, a_m) \in R_q^m$ be chosen independently from uniform distribution. Then there exist m linearly independent solutions $\bar{\mathbf{z}}^{(j)} = (\bar{z}_1^{(j)}, \ldots, \bar{z}_m^{(j)}) \in R^m$ such that $\sum_{i=1}^{m} a_i \cdot \bar{z}^{(j)} = 0 \mod q$ with $\|\bar{\mathbf{z}}^{(j)}\| \leq t \cdot \beta$ for all $j = 1, \ldots, m$.

Proof: **(Step 1)** Let $r^{(1)} = (r_1^{(1)}, \ldots, r_m^{(1)}) \leftarrow U(R^m)$ with $\|r^{(1)}\| \leq t$ and let $\mathbf{a}^{(1)} = (a_1 \cdot r_1^{(1)}, \ldots, a_m \cdot r_m^{(1)})$. Then $\mathbf{a}^{(1)}$ is uniform and we can consider $\mathbf{a}^{(1)}$ as an instance of R-SIS$_{q,m,\beta}$. Using the algorithm $\mathcal{A}$ for solving R-SIS$_{q,m,\beta}$, we obtain a non-trivial solution $\mathbf{z}^{(1)} = (z_1^{(1)}, \ldots, z_m^{(1)})$ such that $\sum_{i=1}^{m} a_i \cdot r_i^{(1)} \cdot z_i^{(1)} = 0 \mod q$ with $\|\mathbf{z}^{(1)}\| \leq \beta$. Since $\mathbf{a}^{(1)}$ is uniform, there is a non-zero $r_i^{(1)}$(if $r_i^{(1)}$ is all zero in R, then $a_i^{(1)}$ is not uniform). Denote $\bar{\mathbf{z}}^{(1)} = (r_1^{(1)} \cdot z_1^{(1)}, \ldots, r_m^{(1)} \cdot z_m^{(1)})$ in R^m. Then $\bar{\mathbf{z}}^{(1)}$ is a non-trivial solution of $(a_1, \ldots, a_m)$ with $\|\bar{\mathbf{z}}^{(1)}\| \leq t \cdot \beta$ since $\mathbf{z}^{(1)}$ is a non-trivial solution in R^m and there is a non-zero $r_i^{(1)}$ in R. Since $t \cdot \beta$ is less than q, we consider $r_i^{(1)}, z_i^{(1)} \in R$ as $r_i^{(1)}, z_i^{(1)} \in R_q$ for all $i = 1, \ldots, m$.

(Step 2) Let $r^{(2)} = (r_1^{(2)}, \ldots, r_m^{(2)}) \leftarrow U(R^m)$ with $\|r^{(2)}\| \leq t$ and let $\mathbf{a}^{(2)} = (a_1 \cdot r_1^{(2)}, \ldots, a_m \cdot r_m^{(2)})$. Then $\mathbf{a}^{(2)}$ is uniform and we can consider $\mathbf{a}^{(2)}$ as an instance of R-SIS$_{q,m,\beta}$. Through the above process, we obtain a non-trivial solution $\bar{\mathbf{z}}^{(2)} = (r_1^{(2)} \cdot z_1^{(2)}, \ldots, r_m^{(2)} \cdot z_m^{(2)}) \in R^m$ with $\|\bar{\mathbf{z}}^{(2)}\| \leq t \cdot \beta$. Also, we consider $r_i^{(2)}, z_i^{(2)} \in R$ as $r_i^{(2)}, z_i^{(2)} \in R_q$ for all $i = 1, \ldots, m$.

Let $\bar{\mathbf{z}}^{(1)}$ be fixed. Since $\|\bar{\mathbf{z}}^{(1)}\| \leq t \cdot \beta < q$, each coefficient of $\bar{\mathbf{z}}^{(1)}$ is in $\mathbb{Z}_q$. Thus, $\gcd(\bar{\mathbf{z}}^{(1)}, q) = 1$ because q is a prime. Then we can define

$$S_1 = \mathrm{span}_{R_q}(\bar{\mathbf{z}}^{(1)}) = \{k_1 \cdot \bar{\mathbf{z}}^{(1)} \mid k_1 \in R_q\}$$

and

$$\begin{aligned} T_1 = \{\bar{\mathbf{z}}^{(2)} = (r_1^{(2)} \cdot z_1^{(2)}, \ldots, r_m^{(2)} \cdot z_m^{(2)}) \\ \mid (r_1^{(2)}, \ldots, r_m^{(2)}) \leftarrow U(R^m), \\ (a_1 \cdot r_1^{(2)}, \ldots, a_m \cdot r_m^{(2)}) \rightarrow \mathcal{A}, \\ \text{and } \mathbf{z}^{(2)} = (z_1^{(2)}, \ldots, z_m^{(2)}) \leftarrow \mathcal{A}\}. \end{aligned}$$

Since S_1 is determined by an element $k_1 \in R_q$, we obtain $|S_1| = q^n$. However, $\bar{\mathbf{z}}^{(2)}$ is determined by $r_i^{(2)}$ for all $i = 1, \ldots, m$, whether $\bar{\mathbf{z}}^{(2)}$ belongs to S_1 or not. Thus, we obtain $|T_1| = q^{nm}$. Then $|S_1 \cap T_1| \leq |S_1| \ll |T_1|$. If $\bar{\mathbf{z}}^{(2)}$ is in S_1, then we repeat Step 2 until $\bar{\mathbf{z}}^{(1)}$ and $\bar{\mathbf{z}}^{(2)}$ are linearly independent, which is possible from $|S_1| \ll |T_1|$.

Now, assume that $\bar{\mathbf{z}}^{(1)}, \ldots, \bar{\mathbf{z}}^{(j-1)} \in R^m$ are linearly independent solutions of $(a_1, \ldots, a_m)$ such that $\|\bar{\mathbf{z}}^{(k)}\| \leq t \cdot \beta$ for all $k = 1, \ldots, j-1$.

(Step 3) Let $r^{(j)} = (r_1^{(j)}, \dots, r_m^{(j)}) \leftarrow U(R^m)$ with $\|r^{(j)}\| \leq t$ and let $\mathbf{a}^{(j)} = (a_1 \cdot r_1^{(j)}, \dots, a_m \cdot r_m^{(j)})$. Through the above process, we obtain a solution $\bar{\mathbf{z}}^{(j)} = (r_1^{(j)} \cdot z_1^{(j)}, \dots, r_m^{(j)} \cdot z_m^{(j)})$ such that $\|\bar{\mathbf{z}}^{(j)}\| \leq t \cdot \beta$. Also, we consider $r_i^{(j)}, z_i^{(j)} \in R$ as $r_i^{(j)}, z_i^{(j)} \in R_q$ for all $i = 1, \dots, m$. Let $\bar{\mathbf{z}}^{(1)}, \dots, \bar{\mathbf{z}}^{(j-1)}$ be fixed and let

$$\begin{aligned} S_{j-1} &= \mathrm{span}_{R_q}(\bar{\mathbf{z}}^{(1)}, \dots, \bar{\mathbf{z}}^{(j-1)}) \\ &= \{k_1 \cdot \bar{\mathbf{z}}^{(1)} + \cdots + k_{j-1} \cdot \bar{\mathbf{z}}^{(j-1)} \\ &\qquad \mid k_i \in R_q \text{ for } i = 1, \dots, j-1\} \end{aligned}$$

and

$$\begin{aligned} T_{j-1} = \{\bar{\mathbf{z}}^{(j)} &= (r_1^{(j)} \cdot z_1^{(j)}, \dots, r_m^{(j)} \cdots z_m^{(j)}) \\ &\mid (r_1^{(j)}, \dots, r_m^{(j)}) \leftarrow U(R^m), \\ &(a_1 \cdot r_1^{(j)}, \dots, a_m \cdot r_m^{(j)}) \rightarrow \mathcal{A}, \\ &\text{and } \mathbf{z}^{(j)} = (z_1^{(j)}, \dots, z_m^{(j)}) \leftarrow \mathcal{A}\}. \end{aligned}$$

Then $|S_{j-1}| = q^{n(j-1)}$ since S_{j-1} is determined by elements $k_1, \dots, k_{j-1} \in R_q$. However, $\bar{\mathbf{z}}^{(j)}$ is determined by $r_i^{(j)}$ for all $i = 1, \dots, m$ whether $\bar{\mathbf{z}}^{(j)}$ belongs to S_{j-1} or not. Thus, we obtain $|T_{j-1}| = q^{nm}$. Then $|S_{j-1} \cap T_{j-1}| \leq |S_{j-1}| \ll |T_{j-1}|$. If $\bar{\mathbf{z}}^{(j)}$ is in S_{j-1}, then we repeat Step 3 until $\bar{\mathbf{z}}^{(1)}, \bar{\mathbf{z}}^{(2)}, \dots, \bar{\mathbf{z}}^{(j)}$ are linearly independent, which is also possible from $|S_{j-1}| \ll |T_{j-1}|$. If we repeat this process m times, then we can find m linearly independent solutions $\bar{\mathbf{z}}^{(j)} = (\bar{z}_1^{(j)}, \dots, \bar{z}_m^{(j)}) = (r_1^{(j)} \cdot z_1^{(j)}, \dots, r_m^{(j)} \cdot z_m^{(j)})$ such that $\sum_{i=1}^{m} a_i \cdot r_i^{(j)} \cdot z_i^{(j)} = 0 \mod q$ with $\|\bar{\mathbf{z}}^{(j)}\| \leq t \cdot \beta$ for all $i = 1, \dots, m$. ■

The above solutions are not exact solutions of R-SIS$_{q,m,\beta}$, but we can use these solutions to find the solution of M-SIS. Now, we prove the reduction from M-SIS to R-SIS using Lemma 2. The proof of the following theorem is the same as that of Theorem 2. However, the upper bound of the solution of R-SIS is changed since we use Lemma 2. Also, the condition for β is changed as in the following theorem, where the reduction from M-SIS to R-SIS is satisfied.

Theorem 3: Let m, t be positive integers and q be chosen as in Lemma 2. Choose a module rank $d \in \mathbb{Z}_{>0}$ such that

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} < \frac{\sqrt[d]{q \cdot t \cdot \sqrt{m}}}{t \cdot \sqrt{m}}. \tag{3}$$

Let a positive real number β be an upper bound on the norm of the solution of R-SIS$_{q,m,\beta}$ such that

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} \leq \beta < \frac{\sqrt[d]{q \cdot t \cdot \sqrt{m}}}{t \cdot \sqrt{m}}.$$

Assume that an algorithm $\mathcal{A}$ exists for solving R-SIS$_{q,m,\beta}$. Then there exists an algorithm $\mathcal{A}_1$ for solving M-SIS$_{q,m,\beta_1}$, where $\beta_1 = (t\sqrt{m})^{d-1}\beta^d$.

Proof: Let $\mathbf{a}_1, \dots, \mathbf{a}_m \in R_q^d$ be instances of M-SIS$_{q,m,\beta}$, which are chosen independently from the uniform distribution, where $\mathbf{a}_i = (a_{i1}, \dots, a_{id})^T$ and $a_{ij} \in R_q$. Then we can write the matrix

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1d} & a_{2d} & \cdots & a_{md} \end{bmatrix} = \begin{bmatrix} \mathbf{a}'_1 \\ \mathbf{a}'_2 \\ \vdots \\ \mathbf{a}'_d \end{bmatrix} \in R_q^{d \times m},$$

where $\mathbf{a}'_i = (a_{1i}, \dots, a_{mi})$. Then the i-th row $\mathbf{a}'_i$ of $\mathbf{A}$ is considered as an instance of R-SIS. Consider the last row $\mathbf{a}'_d$ of $\mathbf{A}$. Then there are m distinct solutions $\bar{\mathbf{z}}_d^{(j)} = (\bar{z}_{d,1}^{(j)}, \dots, \bar{z}_{d,m}^{(j)})^T$ with $\|\bar{\mathbf{z}}_d^{(j)}\| \leq t \cdot \beta$ such that $\mathbf{a}'_d \cdot \bar{\mathbf{z}}_d^{(j)} = 0 \bmod q^k$ for $j = 1, \dots, m$ from Lemma 2. Now, we construct the $m \times m$ solution matrix

$$\bar{\mathbf{Z}}_d = \left[\bar{\mathbf{z}}_d^{(1)} \; \bar{\mathbf{z}}_d^{(2)} \; \cdots \; \bar{\mathbf{z}}_d^{(m)}\right]$$

and $\|\bar{\mathbf{Z}}_d\| \leq (t \cdot \sqrt{m}) \cdot \beta$. Then, we have

$$\mathbf{A} \cdot \bar{\mathbf{Z}}_d = \begin{bmatrix} \mathbf{a}''_1 \\ \mathbf{a}''_2 \\ \vdots \\ \mathbf{a}''_{d-1} \\ \mathbf{0} \end{bmatrix} \bmod q,$$

where $\mathbf{a}''_i$ is an m-tuple vector. Applying the above method $d-1$ times, we obtain the solution matrix

$$\mathbf{A}^* = \mathbf{A} \cdot \bar{\mathbf{Z}}_d \cdots \bar{\mathbf{Z}}_2 = \begin{bmatrix} \mathbf{a}^*_1 \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \end{bmatrix} \bmod q.$$

Finally, applying the algorithm $\mathcal{A}$ to $\mathbf{a}^*_1$, we find a solution $\mathbf{z}'$ with $\|\mathbf{z}'\| \leq \beta$ such that $\mathbf{A}^* \cdot \mathbf{z}' = \mathbf{0} \bmod q$. Then, we have the solution $\mathbf{z} = \bar{\mathbf{Z}}_d \cdots \bar{\mathbf{Z}}_2 \cdot \mathbf{z}'$ for $\mathbf{A}$. Then $\mathbf{A} \cdot \mathbf{z} = \mathbf{0} \bmod q$ and

$$\begin{aligned} \|\mathbf{z}\| &= \|\bar{\mathbf{Z}}_d \cdots \bar{\mathbf{Z}}_2 \cdot \mathbf{z}'\| \\ &\leq \left(t \cdot \sqrt{m} \cdot \beta\right)^{d-1} \cdot \beta \\ &= \left(t \cdot \sqrt{m}\right)^{d-1} \beta^d. \end{aligned}$$

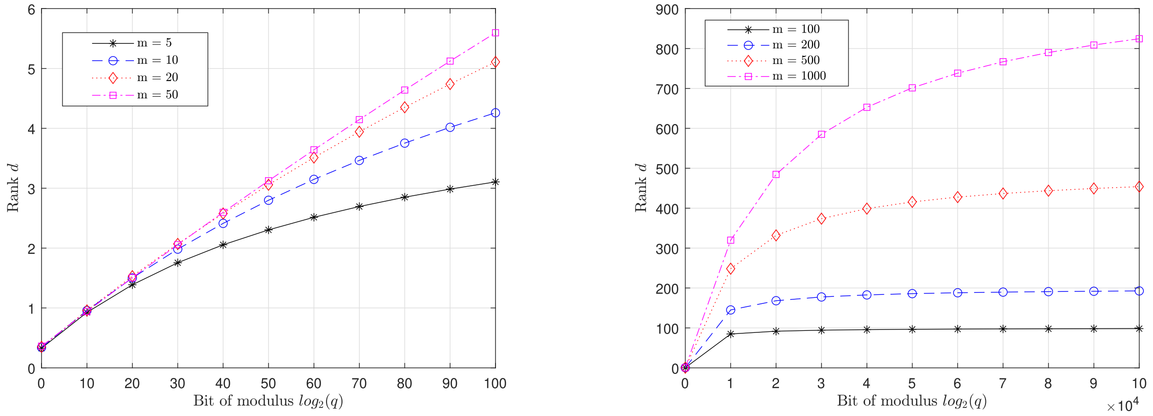
From (3), we have that the upper bound $\beta_1 = (t \cdot \sqrt{m})^{d-1} \cdot \beta^d$ on the norm of the solution of M-SIS$_{q,m,\beta_1}$ is less than q since

$$\begin{aligned} \left(t \cdot \sqrt{m}\right)^{d-1} \beta^d &< \left(t \cdot \sqrt{m}\right)^{d-1} \left(\frac{\sqrt[d]{q \cdot t \cdot \sqrt{m}}}{t \cdot \sqrt{m}}\right)^d \\ &= q. \end{aligned}$$

Thus, we find a non-trivial solution of M-SIS$_{q,m,\beta_1}$ and show that there exists a reduction from M-SIS$_{q,m,\beta_1}$ to R-SIS$_{q,m,\beta}$, where $\beta_1 = (t\sqrt{m})^{d-1}\beta^d$. ■

B. THE POSSIBLE RANGE OF MODULE RANK FOR M-SIS

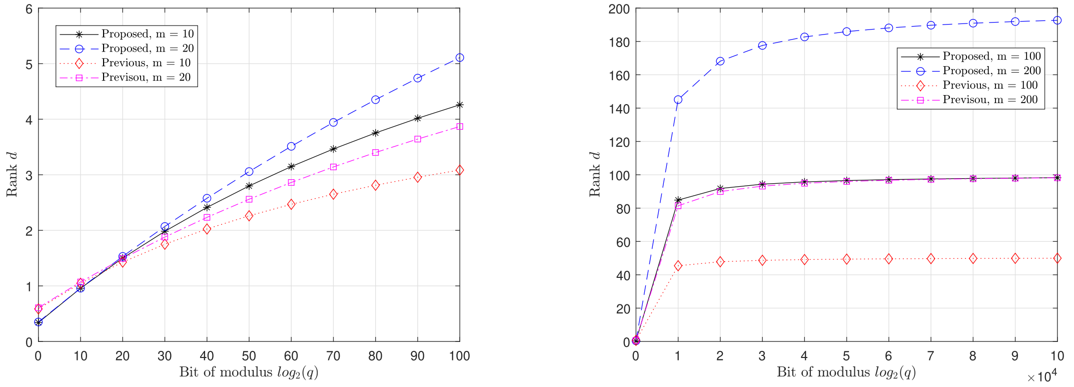
Similar to the previous work [15], the possible range of module rank of M-SIS that satisfies the reduction from M-SIS$_{q,m,\beta_1}$ to R-SIS$_{q,m,\beta}$ depends on (3) in Theorem 3, where $\beta_1 = (t\sqrt{m})^{d-1}\beta^d$. Moreover, n and m are fixed since n and m are the dimension of the polynomial ring R and the number of instances of R-SIS, respectively. Also, given t, the module rank d depends on the modulus q. In this paper,



(a) Module rank for small number bits of modulus

(b) Convergence of module rank

FIGURE 2. Rank of module when $n = 2^{16}$ from (4) in Section III-B.



(a) For small $\log_2 q$

(b) For large $\log_2 q$

FIGURE 3. Comparison of the possible ranges of module ranks for the previous and the proposed works when $n = 2^{16}$.

the new range of module rank d of M-SIS through (3) is derived as

$$d < \frac{2m\log q + m\log m + 2m\log t}{m\log n + 2m\log m + 2\log q + 2m\log t}. \tag{4}$$

Then, for sufficiently large q, we obtain the range of module rank as

$$d < m.$$

This result is twice as large as the range of module rank of the reduction from M-SIS to R-SIS [15]. Fig. 2 shows the possible module ranks with the different parameters and $\log_2 q$ for $n = 2^{16}$, $t = 10$. In the case of Fig. 2(a), the bits of modulus q vary from 0 to 100. In the case of Fig. 2(b), the bits of modulus q vary from 0 to 10^5. As $\log_2 q$ increases, the possible range of module rank d approaches the number of instances m as in Fig. 2(b). Also, as m increases, the possible range of module rank d becomes even wider.

The possible range of module rank is doubled compared to that of the previous result in (2). Also, the previous work considered the case that the modulus exponent k is larger than one, but in this work, we propose the reduction for the case of $k = 1$. Fig. 3 shows the comparison of the possible ranges of module ranks of the previous work [15] and the proposed work for $n = 2^{16}$, $t = 10$. In the case of Fig. 3(a), the bits of modulus q vary from 0 to 100. The range of module rank of the previous work is larger than that of the proposed work in the range 0 to 10, but, in the range 10 to 100, the range of the proposed work is larger than that of previous work. Also, the previous reduction is possible when the exponent k of the modulus of M-SIS is larger than one, but the proposed reduction is also possible when the exponent of k of that of M-SIS is equal to one. In the case of Fig. 3(b), the bits of modulus q vary from 0 to 10^5, and it shows the convergence values of (2) and (4). (2) converges to half of the number of instances of R-SIS, which is the maximum module rank. However, (4) converges to the same number of instances of R-SIS, which is the maximum module rank.

IV. REDUCTION FROM VARIOUS M-SIS PROBLEMS TO R-SIS PROBLEM

In this section, we derive several reductions among the M-SIS problems, which lead to the reduction from M-SIS$_{c,m^k,\frac{c}{q^k}(t\cdot\sqrt{m})^{k(d-1)}\beta^{kd}}$ to R-SIS$_{q,m,\beta}$ for the modulus c such that $q^k|c$.

A. REDUCTION BETWEEN M-SIS PROBLEMS WITH INCREASED MODULUS

First, we derive the reduction from M-SIS$_{q^k,m^k,\beta^k}$ to M-SIS$_{q,m,\beta}$ as in the following theorem, where its proof is the same as that of Theorem 1 in the previous work [15].

Theorem 4: Let m be a positive integer and q be a prime. Let d be a positive integer such that d define a rank of module defining M-SIS$_{q,m,\beta}$ and M-SIS$_{q^k,m^k,\beta^k}$. Assume that there exists an algorithm $\mathcal{A}_1$ for solving the M-SIS$_{q,m,\beta}$ problem. Then there exists an algorithm $\mathcal{A}_2$ for solving the M-SIS$_{q^k,m^k,\beta^k}$ for any integer $k \geq 1$, which corresponds to the reduction from M-SIS$_{q^k,m^k,\beta^k}$ to M-SIS$_{q,m,\beta}$.

Proof: Assume that there exists an algorithm $\mathcal{A}_1$ for solving M-SIS$_{q,m,\beta}$. Assume that $\mathbf{a}_1, \ldots, \mathbf{a}_{m^k} \in R^d_{q^k}$ are chosen independently from uniform distribution over R^d_q. We can write $\mathbf{A} = (\mathbf{a}_1, \ldots, \mathbf{a}_{m^k}) = (\bar{\mathbf{a}}_1, \ldots, \bar{\mathbf{a}}_{m^{k-1}})$, where $\bar{\mathbf{a}}_i$ is an m tuple vector. Using the algorithm $\mathcal{A}_1$, we obtain the solution $\mathbf{z}_i \in R^m$ such that $\bar{\mathbf{a}}_i \cdot \mathbf{z}_i = \mathbf{0} \mod q$ and $\|\mathbf{z}_i\| \leq \beta$. Since $\beta < q$ and q is a prime, $\gcd(\mathbf{z}_i, q) = 1$. Thus, $\bar{\mathbf{a}}_i \cdot \mathbf{z}_i = q \cdot \mathbf{a}'_i$ and $\mathbf{a}'_i = \bar{\mathbf{a}}_i \cdot \mathbf{z}_i / q \in R^d_{q^{k-1}}$ for some $\mathbf{a}'_i \in R^d$. Set $\mathbf{A}' = (\mathbf{a}'_1, \ldots, \mathbf{a}'_{m^{k-1}})$ and use the induction on k. Then we find a solution $\mathbf{z}' = (z'_1, \ldots, z'_{m^{k-1}})^T \in R^{m^{k-1}}$ with $\|\mathbf{z}'\| \leq \beta^{k-1}$ such that $\mathbf{A}' \cdot \mathbf{z}' = 0 \mod q^{k-1}$. Let $\mathbf{z} = (z'_1 \cdot \mathbf{z}_1, \ldots, z'_{m^{k-1}} \cdot \mathbf{z}_{m^{k-1}})^T \in R^{m^k}$. Then, we have

$$\begin{aligned}
\mathbf{A} \cdot \mathbf{z} &= \sum_{i=1}^{m^{k-1}} z'_i \cdot \bar{\mathbf{a}}_i \cdot \mathbf{z}_i \\
&= \sum_{i=1}^{m^{k-1}} z'_i \cdot q \cdot \mathbf{a}'_i \\
&= q \cdot \sum_{i=1}^{m^{k-1}} z'_i \cdot \mathbf{a}'_i \\
&= q \cdot \mathbf{A}' \cdot \mathbf{z}' = 0 \mod q^k
\end{aligned}$$

and $\|\mathbf{z}\| \leq \|\mathbf{z}'\| \cdot \max_i \|\mathbf{z}_i\| \leq \beta^k$. Thus, M-SIS$_{q,m,\beta}$ is more difficult than M-SIS$_{q^k,m^k,\beta^k}$. ■

Using Theorem 4, we can obtain the following reduction.

Corollary 2: There exists the reduction from M-SIS$_{q^k,m^k,\beta_2}$ to M-SIS$_{q,m,\beta_1}$, where $\beta_1 = (t \cdot \sqrt{m})^{d-1}\beta^d$ and $\beta_2 = \beta_1^k$ as in Fig. 1.

B. REDUCTION BETWEEN M-SIS PROBLEMS WITH CHANGED NORM BOUND

In order to derive the reduction from M-SIS$_{q^k,m^k,\beta_3}$ to M-SIS$_{q,m,\beta_1}$ in Fig. 1, we use the reduction from M-SIS$_{q^k,m^k,\beta_3}$ to M-SIS$_{q^k,m^k,\beta_2}$, where

$$\begin{aligned}
\beta_1 &= (t \cdot \sqrt{m})^{d-1}\beta^d, \\
\beta_2 &= \beta_1^k \\
&= (t \cdot \sqrt{m})^{k(d-1)}\beta^{kd}, \\
\beta_3 &= m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)},
\end{aligned}$$

and $k \geq 1$. To derive the reduction, we need to know the following remark.

Remark 1: Let m and q be positive integers. Let $\beta, \beta' \in \mathbb{R}$ such that

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} \leq \beta \leq \beta' < q.$$

Assume that there exists an algorithm $\mathcal{A}$ for solving R-SIS$_{q,m,\beta}$. Then there exists an algorithm $\mathcal{A}'$ for solving R-SIS$_{q,m,\beta'}$. Similarly, assume that there exists an algorithm $\mathcal{A}$ for solving M-SIS$_{q,m,\beta}$. Then there exists an algorithm $\mathcal{A}'$ for solving M-SIS$_{q,m,\beta'}$ with the same module rank.

Thus, we derive the reduction from M-SIS$_{q^k,m^k,\beta_3}$ to M-SIS$_{q^k,m^k,\beta_2}$ as in the following theorem.

Theorem 5: Let m be a positive integer. Let t be positive integers and q a prime such that

$$t \leq \sqrt{n \cdot m} \cdot q^{\frac{1}{m}} < \frac{q}{t}.$$

Choose a module rank $d \in \mathbb{Z}_{>0}$ such that

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} < \frac{\sqrt[d]{q \cdot t \cdot \sqrt{m}}}{t \cdot \sqrt{m}}.$$

Let β be a positive real number such that

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} \leq \beta < \frac{\sqrt[d]{q \cdot t \cdot \sqrt{m}}}{t \cdot \sqrt{m}}.$$

Then M-SIS$_{q^k,m^k,\beta_2}$ is harder than M-SIS$_{q^k,m^k,\beta_3}$, where $\beta_2 = (t \cdot \sqrt{m})^{k(d-1)}\beta^{kd}$, $\beta_3 = m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)}$, and $k \geq 1$.

Proof: Assume that there exists an algorithm $\mathcal{A}_2$ for solving M-SIS$_{q^k,m^k,\beta_2}$, where $\beta_2 = \left(t \cdot \sqrt{m}\right)^{k(d-1)} \beta^{kd}$. Then we need to compare β_2 and β_3 as

$$\begin{aligned}
\frac{\beta_3}{\beta_2} &= \frac{m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)}}{(t \cdot \sqrt{m})^{k(d-1)}\beta^{kd}} \\
&= \left(\frac{\beta}{t}\right)^{k(d-1)} \\
&\geq \left(\frac{\sqrt{n \cdot m} \cdot q^{\frac{1}{m}}}{t}\right)^{k(d-1)},
\end{aligned}$$

which is larger than one if $t \leq \sqrt{n \cdot m} \cdot q^{\frac{1}{m}}$. Thus, we obtain

$$\beta_3 = m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)} \geq (t \cdot \sqrt{m})^{k(d-1)}\beta^{kd} = \beta_2.$$

From Remark 1, there exists an algorithm $\mathcal{A}_3$ for solving M-SIS$_{q^k,m^k,\beta_3}$, where $\beta_3 = m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)}$. ■

From Theorems 3, 5, and Corollary 2, we can derive the reduction from M-SIS$_{q^k,m^k,\beta_3}$ to R-SIS$_{q,m,\beta}$, where $\beta_3 = m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)}$ for $k \geq 1$, where Corollary 1 in the previous work [15] derived the same reduction for $k > 1$.

C. REDUCTION FROM M-SIS WITH COMPOSITE NUMBER AS MODULUS TO R-SIS

In this subsection, we observe the relationship between M-SIS with modulus q^k for prime q and $k \geq 1$ and M-SIS with modulus c as a composite number. In particular, composite number c is divided by prime q^k. The following theorem shows the relationship between two problems.

Theorem 6: Let m, t, and q be chosen as in Theorem 5. Let $k \geq 1$ be a positive integer. Let c be a composite integer such that q^k divides c. Assume that there exists an algorithm $\mathcal{A}$ for solving M-SIS$_{q^k,m^k,\beta_2}$. Then there exists an algorithm $\mathcal{B}$ for solving M-SIS$_{c,m^k,\gamma}$, where $\gamma = \frac{c}{q^k}\beta_2$ and $\beta_2 = (t \cdot \sqrt{m})^{k(d-1)}\beta^{kd}$ for $k \geq 1$.

Proof: Let $\mathbf{a}_1, \ldots, \mathbf{a}_{m^k} \in R_c^d$ be chosen independently from uniform distribution, where $\mathbf{a}_i = (a_{i1}, \ldots, a_{id})$ for all $i = 1, \ldots, m^k$. For $i = 1, \ldots, m^k$ and $j = 1, \ldots, d$, $a_{ij} = a_{ij}^{(0)} + q^k a_{ij}^{(1)} + \cdots + q^{ks} a_{ij}^{(s)}$ for some integer s and thus we write $\mathbf{a}_i = \mathbf{a}_i^{(0)} + q^k \mathbf{a}_i^{(1)} + \cdots + q^{ks} \mathbf{a}_i^{(s)}$. Thus, $\mathbf{a}_i \equiv \mathbf{a}_i^{(0)} \bmod q^k$. From the algorithm $\mathcal{A}$ for solving M-SIS$_{q^k,m^k,\beta_2}$, we can find the solution $z_1, \ldots, z_{m^k} \in R$ such that

$$\mathbf{a}_1^{(0)} \cdot z_1 + \cdots + \mathbf{a}_{m^k}^{(0)} \cdot z_{m^k} = \sum_{i=1}^{m^k} \mathbf{a}_i^{(0)} \cdot z_i = 0 \bmod q^k$$

and $\|\mathbf{z}\| \leq \beta_2$, where $\mathbf{z} = (z_1, \ldots, z_{m^k})^T$. This means that $\sum_{i=1}^{m^k} \mathbf{a}_i^{(0)} \cdot z_i = q^k \cdot \alpha$ for some $\alpha \in R$. Thus, we have

$$\begin{aligned}\sum_{i=1}^{m^k} \mathbf{a}_i \cdot z_i &= \sum_{i=1}^{m^k} \mathbf{a}_i^{(0)} \cdot z_i \\ &\quad + q^k \sum_{i=1}^{m^k} \mathbf{a}_i^{(1)} \cdot z_i + \cdots + q^{ks} \sum_{i=1}^{m^k} \mathbf{a}_i^{(s)} \cdot z_i \\ &= q^k \cdot \alpha + q^k \sum_{i=1}^{m^k} \mathbf{a}_i^{(1)} \cdot z_i + \cdots + q^{ks} \sum_{i=1}^{m^k} \mathbf{a}_i^{(s)} \cdot z_i \\ &= 0 \bmod q^k.\end{aligned}$$

Thus, $\sum_{i=1}^{m^k} \mathbf{a}_i \cdot z_i = q^k \cdot \alpha'$ for some $\alpha' \in R$ and we have

$$\begin{aligned}\frac{c}{q^k} \sum_{i=1}^{m^k} \mathbf{a}_i \cdot z_i &= \sum_{i=1}^{m^k} \mathbf{a}_i \cdot (\frac{c}{q^k} z_i) \\ &= c \cdot \alpha' \\ &= 0 \bmod c.\end{aligned}$$

Since $\frac{c}{q^k}$ is an integer, $\frac{c}{q^k} z_i$ is in R for all $i = 1, \ldots, m^k$. And we obtain $\|\frac{c}{q^k}\mathbf{z}\| = \frac{c}{q^k}\|\mathbf{z}\| \leq \frac{c}{q^k}\beta_2$. Thus, $\frac{c}{q^k}\mathbf{z}$ is a solution of the instance of M-SIS$_{c,m^k,\gamma}$, where $\gamma = \frac{c}{q^k}\beta_2$ and $\beta_2 = (t \cdot \sqrt{m})^{k(d-1)}\beta^{kd}$ for $k \geq 1$. ■

Using Theorems 3, 6, and Corollary 2, we obtain the reduction from M-SIS$_{c,m^k,\gamma}$ to R-SIS$_{q,m,\beta}$, when $\gamma = \frac{c}{q^k}(t \cdot \sqrt{m})^{k(d-1)}\beta^{kd}$ as in the following theorem.

Theorem 7: Let m, t, and q be chosen as in Theorem 5. Let c be a composite integer such that c is divided by q^k for some $k \geq 1$. Choose a module rank $d \in \mathbb{Z}_{>0}$ such that

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} < \frac{\sqrt[d]{q \cdot t \cdot \sqrt{m}}}{t \cdot \sqrt{m}}.$$

Let a positive real number β be an upper bound on the norm of the solution of R-SIS$_{q,m,\beta}$ such that

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} \leq \beta < \frac{\sqrt[d]{q \cdot t \cdot \sqrt{m}}}{t \cdot \sqrt{m}}.$$

Assume that an algorithm $\mathcal{A}$ exists for solving R-SIS$_{q,m,\beta}$. Then there exists an algorithm $\mathcal{B}$ for solving M-SIS$_{c,m^k,\gamma}$, where $\gamma = \frac{c}{q^k}(t \cdot \sqrt{m})^{k(d-1)}\beta^{kd}$.

V. CONCLUSION AND FUTURE WORKS

In this paper, we derived the reduction from M-SIS$_{c,m^k,\gamma}$ to R-SIS$_{q,m,\beta}$, where $\gamma = \frac{c}{q^k}(t\sqrt{m})^{k(d-1)}\beta^{kd}$ and c is a composite integer that has a factor q^k for some $k \geq 1$. To show this reduction, we proposed the three reductions. First, we proposed the reduction from M-SIS$_{q,m,\beta_1}$ to R-SIS$_{q,m,\beta}$, where $\beta_1 = (t\sqrt{m})^{d-1}\beta^d$. To show this reduction, we devised the new method to find m distinct solutions of R-SIS$_{q,m,\beta}$. This new method is to add randomness to the algorithm for solving R-SIS$_{q,m,\beta}$. Thus, we can devise an algorithm that gives m distinct solutions to the same instances of R-SIS. Compared to the previous work [15], this reduction is preserved the same modulus and ring dimension. Also, the possible range of module rank for reduction from M-SIS$_{q,m,\beta}$ to R-SIS$_{q,m,\beta}$ could be doubled compared to [15].

Second, we proposed the reduction from M-SIS$_{q^k,m^k,\beta_2}$ to R-SIS$_{q,m,\beta}$, where $\beta_2 = \beta_1^k = (t\sqrt{m})^{k(d-1)}\beta^{kd}$. To show this reduction, we derived the method extending the reduction from R-SIS$_{q^k,m^k,\beta^k}$ to R-SIS$_{q,m,\beta}$ shown in [15] to the reduction from M-SIS$_{q^k,m^k,\beta_2}$ to M-SIS$_{q,m,\beta_1}$, where $\beta_2 = \beta_1^k = (t\sqrt{m})^{k(d-1)}\beta^{kd}$. Also, we showed that M-SIS$_{q^k,m^k,\beta_2}$ is more difficult than M-SIS$_{q^k,m^k,\beta_3}$ defined in the previous work [15], where $\beta_3 = m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)}$ for $k \geq 1$ using the fact that M-SIS becomes more difficult when the upper bound of M-SIS is tighter. This means that R-SIS is more difficult than M-SIS, which is tighter than the M-SIS in the previous work [15].

Finally, we showed that M-SIS$_{q^k,m^k,\gamma}$ is more difficult than M-SIS$_{c,m^k,\beta_2}$, where c is a composite integer with a factor q^k and $\gamma = \frac{c}{q^k}\beta_2 = \frac{c}{q^k}(t\sqrt{m})^{k(d-1)}\beta^{kd}$. In the previous work [15], all reductions depend on the prime modulus q. However, we proposed the reductions between the M-SIS problems with the different modulus. Combining three reductions, we obtained the reduction from M-SIS$_{c,m^k,\gamma}$ to R-SIS$_{q,m,\beta}$.

As a future work, it is crucial to handle the upper bound of the solution of R-SIS and M-SIS because this upper bound determines the rank of the module. Also, since we showed the results for R-SIS and M-SIS related to only one prime q, we need to derive the relationship between R-SIS and M-SIS with different primes p and q as the modulus.

ACKNOWLEDGMENT

The authors would like to thank the editor and the anonymous reviewers for their constructive comments and suggestions, which improve the quality of this article.

REFERENCES

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, 1999.

[2] G. Alagic, G. Alagic, J. Alperin-Sheriff, D. Apon, and D. Cooper, ''Status report on the first round of the NIST post-quantum cryptography standardization process,'' U.S. Dept. Commerce, NIST, Gaithersburg, MD, USA, Tech. Rep. 8240, 2019. [Online]. Available: https://www.nist.gov/publications/status-report-first-round-nist-post-quantum-cryptography-standardization-process

[3] M. Ajtai, ''Generating hard instances of lattice problems (extended abstract),'' in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 99–108.

[4] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, ''Lattice signatures and bimodal Gaussians,'' in *Proc. CRYPTO* (Lecture Notes in Computer Science), vol. 8042. Berlin, Germany: Springer, Aug. 2013, pp. 40–56.

[5] V. Lyubashevsky, ''Lattice signatures without trapdoors,'' in *Proc. EUROCRYPT* (Lecture Notes in Computer Science), vol. 7237. Berlin, Germany: Springer, Apr. 2012, pp. 738–755.

[6] D. Micciancio and O. Regev, ''Lattice-based cryptography,'' in *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, pp. 147–191.

[7] P. Bertm P.-A. Fouque, A. Roux-Langlois, and M. Sabt, ''Practical implementation of ring-SIS/LWE based signature and IBE,'' in *Proc. Int. Conf. Post-Quantum Cryptogr.* Cham, Switzerland: Springer, 2018, pp. 271–291.

[8] C. Peikert and A. Rosen, ''Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices,'' in *Proc. TCC* (Lecture Notes in Computer Science), vol. 3876. Berlin, Germany: Springer, Mar. 2006, pp. 145–166.

[9] A. Langlois and D. Stehlé, ''Worst-case to average-case reductions for module lattices,'' *Des., Codes Cryptogr.*, vol. 75, no. 3, pp. 565–599, Jun. 2015.

[10] V. Lyubashevsky, C. Peikert, and O. Regev, ''On ideal lattices and learning with errors over rings,'' in *Proc. EUROCRYPTO* (Lecture Notes in Computer Science), vol. 6110. Berlin, Germany: Springer, May 2010, pp. 1–23.

[11] C. Baum, I. Damgard, V. Lyubashevsky, S. Oechsner, and C. Peikert, ''More efficient commitments from structured lattice assumptions,'' in *Proc. Int. Conf. Secur. Cryptogr. Netw.* Cham, Switzerland: Springer, 2018, pp. 368–385.

[12] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, ''CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM,'' in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Apr. 2018, pp. 353–367.

[13] L. Ducas, ''CRYSTALS-dilithium: A lattice-based digital signature scheme,'' *TCHES*, vol. 2018, no. 1, pp. 238–268, Feb. 2018. [Online]. Available: https://tches.iacr.org/index.php/TCHES/article/view/839

[14] M. F. Esgin, R. Steinfeld, A. Sakzad, J. K. Liu, and D. Liu, ''Short lattice-based one-out-of-many proofs and applications to ring signatures,'' in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.* Cham, Switzerland: Springer, 2019, pp. 67–88.

[15] Z. Koo, J.-S. No, and Y.-S. Kim, ''Reduction from module-SIS to ring-SIS under norm constraint of ring-SIS,'' *IEEE Access*, vol. 8, pp. 140998–141006, 2020.

[16] V. Lyubashevsky and D. Micciancio, ''Generalized compact knapsacks are collision resistant,'' in *Proc. ICALP*. Berlin, Germany: Springer, 2006, pp. 144–155.

[17] D. Micciancio and O. Regev, ''Worst-case to average-case reductions based on Gaussian measures,'' *SIAM J. Comput.*, vol. 37, no. 1, pp. 302–367, 2007.

[18] C. Peikert and Z. Pepin, ''Algebraically structured LWE, revisited,'' in *Proc. TCC*. Cham, Switzerland: Springer, 2019, pp. 1–23.

[19] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa, ''Efficient public key encryption based on ideal lattices,'' in *Proc. ASIACRYPT* (Lecture Notes in Computer Science), vol. 5912. Berlin, Germany: Springer 2009, pp. 617–635.

[20] M. R. Albrecht, ''On dual lattice attacks against small-secret LWE and parameter choices in HElib and SEAL,'' in *Proc. EUROCRYPT* (Lecture Notes in Computer Science), vol. 10211. Berlin, Germany: Springer 2017, pp. 103–129.

ZAHYUN KOO received the B.S. degree in mathematics from Dongguk University, Seoul, South Korea, in 2015, and the M.S. degree in mathematics from Seoul National University, Seoul, in 2018, where he is currently pursuing the Ph.D. degree in electrical and computer engineering. His current research interests include lattice-based cryptography and error-correcting codes.

YONGWOO LEE received the B.S. degree in electrical engineering and computer science from the Gwangju Institute of Science and Technology, Gwangju, South Korea, in 2015, and the M.S. degree in electrical and computer engineering from Seoul National University, in 2017, where he is currently pursuing the Ph.D. degree. He is also a submitter for a candidate algorithm (pqsigRM) in the first round for the NIST post quantum cryptography standardization. His current research interests include homomorphic encryption and code-based cryptography.

JOON-WOO LEE (Graduate Student Member, IEEE) received the B.S. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2016, where he is currently pursuing the Ph.D. degree. His current research interests include homomorphic encryption and lattice-based cryptography.

JONG-SEON NO (Fellow, IEEE) received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, South Korea, in 1981 and 1984, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 1988. He was a Senior MTS with Hughes Network Systems, from 1988 to 1990. He was an Associate Professor with the Department of Electronic Engineering, Konkuk University, Seoul, from 1990 to 1999. He joined the Faculty of the Department of Electrical and Computer Engineering, Seoul National University, in 1999, where he is currently a Professor. His research interests include error-correcting codes, cryptography, sequences, LDPC codes, interference alignment, and wireless communication systems. He became an IEEE Fellow through the IEEE Information Theory Society, in 2012. He was a recipient of the IEEE Information Theory Society Chapter of the Year Award, in 2007. From 1996 to 2008, he served as the Founding Chair for the Seoul Chapter of the IEEE Information Theory Society. He was the General Chair of Sequence and Their Applications 2004 (SETA2004), Seoul. He also served as the General Co-Chair for the International Symposium on Information Theory and its Applications 2006 (ISITA2006) and the International Symposium on Information Theory 2009 (ISIT2009), Seoul. He became a member of the National Academy of Engineering of Korea (NAEK), in 2015, where he served as the Division Chair for electrical, electronic, and information engineering, from 2019 to 2020. He served as the Co-Editor-in-Chief for the IEEE Journal of Communications and Networks, from 2012 to 2013.

YOUNG-SIK KIM (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering and computer science from Seoul National University, in 2001, 2003, and 2007, respectively. He joined the Semiconductor Division, Samsung Electronics, where he performed research and development of security hardware IPs for various embedded systems, including modular exponentiation hardware accelerator (called Tornado 2MX2) for RSA and elliptic curve cryptography in smart card products and mobile application processors of Samsung Electronics, in 2010. He is currently a Professor with Chosun University, Gwangju, South Korea. He is also a submitter for two candidate algorithms (McNie and pqsigRM) in the first round for the NIST post quantum cryptography standardization. His research interests include post-quantum cryptography, the IoT security, physical layer security, data hiding, channel coding, and signal design. He is selected as one of 2025's 100 Best Technology Leaders (for crypto-systems) by the National Academy of Engineering of Korea.