Improved Reduction Between SIS Problems over Structured Lattices

ZaHyun Koo[1], Jong-Seon No[1], and Young-Sik Kim[2]

[1] Seoul National University, Republic of Korea
[2] Chosun University, Republic of Korea

Abstract. Lattice-based cryptographic scheme is constructed based on hard problems on a structured lattice such as the short integer solution (SIS) problem and the learning with error (LWE), called ring-SIS (R-SIS), ring-LWE (R-LWE), module-SIS (M-SIS), and module-LWE (M-LWE). Generally, it has been considered that problems defined on the module-lattice are more difficult than the problems defined on the ideal-lattices. However, Albrecht and Deo showed that there is a reduction from M-LWE to R-LWE in the polynomial ring by handling the error rate and modulus. Also, Koo, No, and Kim showed that there is a reduction from M-SIS$_{q^k,m^k,\beta'}$ to R-SIS$_{q,m,\beta}$ under some norm constraint of R-SIS, where $k > 1$. In this paper, we propose the improved reductions related to M-SIS and R-SIS compared to the previous work. To show the improved reduction, we propose the three novel reductions related to M-SIS to R-SIS on the polynomial ring. First, we propose the reduction from R-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m^k,\beta^k}$. Combining one of the previous works, we obtain the reduction between R-SIS problems with distinct parameters preserving the number of samples of R-SIS. Second, we propose the improved reduction from M-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m,\beta}$ with $k \geq 1$ under some norm constraint of R-SIS. Comparing to the previous work, the upper bound of the norm of the solution of M-SIS is decreased. Finally, we propose a reduction between M-SIS with different moduli. Combining these three results implies that R-SIS$_{q,m,\beta}$ is more difficult than M-SIS$_{C,m,\beta'}$, where C is a multiple of q^k for some $k \geq 1$ under some norm constraint of R-SIS, which provides a double extension of the possible range of module ranks for M-SIS compared to the previous work.

Keywords: Lattice-based cryptography · module-short integer solution (M-SIS) problem · ring-short integer solution (R-SIS) problem · short integer solution (SIS) problem.

1 Introduction

Many cryptographic schemes are based on problems that are difficult to solve on computers. Representatively, there are RSA cryptographic scheme based on prime factor decomposition, and 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, both cryptographic schemes have been considered secure. However, due to the development

of quantum computer, it is known that many cryptographic schemes can be broken using quantum algorithms operated over quantum computer [18]. 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, and multivariate polynomial-based cryptography, and so on. Among them, the diverse forms of lattice-based cryptography such as public key cryptographic schemes, signature schemes, and key encapsulation mechanisms are presented in NIST PQC (post-quantum cryptography) standardization competition for the advantages of small-sized key and efficiency [2].

Lattice-based cryptographic schemes are based on hard problems such as the *shortest independent vector problem* (SIVP). This problem reduces to *short integer solution* (SIS) problem and *learning with error* (LWE) problem. The SIS problem introduced by Ajtai in 1996 [1] has been used to construct many cryptographic schemes. The SIS problem is defined as follows: Let $\mathbb{Z}$ and $\mathbb{R}$ denote the set of integers and the set of real numbers, respectively. Let $\mathbb{Z}_q$ denote the set of integers modulo q. For any positive integers m, n, given positive $\beta \in \mathbb{R}$, 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 $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. Many cryptographic schemes such as signature scheme and commitment scheme can be constructed using the SIS problems [12], [7], [14].

The LWE problem introduced by Regev in 2005 [17] have been proposed. The LWE problem has two versions, that is, the search LWE and the decision LWE problems. The search LWE is defined as follows: For given dimension n and positive integer q and the error distribution χ on $\mathbb{Z}$, the search LWE problem is to find $\mathbf{s}$ for many given independent pairs $(\mathbf{a}, \frac{1}{q}\langle \mathbf{a}, \mathbf{s} \rangle + e)$ for $\mathbf{a} \in \mathbb{Z}_q^n$ chosen uniformly at random and error $e \leftarrow \chi$. The decision LWE problem is to distinguish between many arbitrarily independent pairs $(\mathbf{a}, \frac{1}{q}\langle \mathbf{a}, \mathbf{s} \rangle + e)$ and the same number of samples $(\mathbf{c}, d)$, $\mathbf{c} \in \mathbb{Z}_q^n$ and $d \in \mathbb{Z}_q$ from the uniform distribution over $\mathbb{Z}_q^{n+1}$. Many public key cryptographic scheme and homormophic encryption scheme are constructed based on LWE [14], [6], [15].

However, cryptographic schemes based on SIS and LWE are inefficient since the size of the key that in the signature scheme or commitment scheme is too large. To overcome this problem, many cryptographic schemes based on the structured lattices have been proposed, that is, the ideal-lattice and the module-lattice. The ideal-lattice means the lattice with a polynomial ring structure and module-lattice has a module structure, which is an algebraic structure that generalizes ring structure and vector space. 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) [16] and this problem defined over a module-lattice is said to be module-SIS (M-SIS) [11]. Similarly, ring-LWE (R-LWE) [13] and module-LWE (M-LWE) [11] are defined over the structured lattices. It is shown that R-SIS, M-SIS, R-LWE, and M-LWE are as hard as SIVP, which is defined on the structured lattices [11].

Generally, it has been considered that M-SIS (resp. M-LWE) is more difficult than R-SIS (resp. R-LWE) 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 the module defining M-SIS since the polynomial ring defining R-SIS is considered as the module with rank 1. Then the algorithm $\mathcal{A}$ can be used to find the solution of R-SIS. Thus, in lattice-based cryptographic scheme, M-SIS and M-LWE having a module structure is preferred as fundamental difficulties of the scheme due to the reduced key-size and security reason and we do not consider the existence of an algorithm to solve the R-SIS [8], [4], [9], [5].

However, the problems over the module-lattice is not always more difficult than the problems over the ideal-lattice. In the case of LWE over structured lattices, Albrecht and Deo showed that there is a reduction from M-LWE to R-LWE [3] by controlling the error rate and modulus in the M-LWE and R-LWE problems. Specifically, M-LWE with error rate α, modulus q, and the rank of module d reduces to R-LWE with error $\alpha \cdot n^2\sqrt{d}$ and modulus q^d.

In the case of SIS over structured lattices, Koo, No, and Kim showed that R-SIS problem is more difficult than M-SIS in a specific parameter [10]. 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 constraints, the possible range of module ranks that can be reduced to R-SIS is limited to $d < \frac{m+1}{2}$ for sufficiently large modulus q. In addition, this reduction showed the relationship between R-SIS with m samples and modulus q and M-SIS with m^k samples and modulus q^k for some $k > 1$. In other words, this reduction cannot be said that it is established for the same modulus and the same samples.

1.1 Contributions

In this paper, we proposes the improved reduction from M-SIS to R-SIS compared to the previous work [10]. Similar to the previous work, this reduction considers some condition 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 derive a reduction from R-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m^k,\beta^k}$. Combining this reduction with one of the previous work [10], the reduction from R-SIS$_{q^k,m^k,\beta^k}$ to R-SIS$_{q,m,\beta}$, we obtain a reduction in which the number of samples is preserved, that is, there exists a reduction from R-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q,m,\beta}$. Second, we propose the method to reduce the upper bound of the norm of the solution of M-SIS in the reduction from M-SIS to R-SIS shown in the previous work. In the previous work, it can be seen that the upper bound of the norm of the solution of R-SIS increases in the process of finding m distinct solutions of R-SIS. However, in this work, we propose a method to reduce the upper bound of the norm of each solution of R-SIS compared to [10] while finding m distinct solutions of R-SIS. Applying this method to construct the solution of M-SIS through the solutions of R-SIS, it can be seen that the upper bound of the norm of the solution of M-SIS is reduced compared to the previous

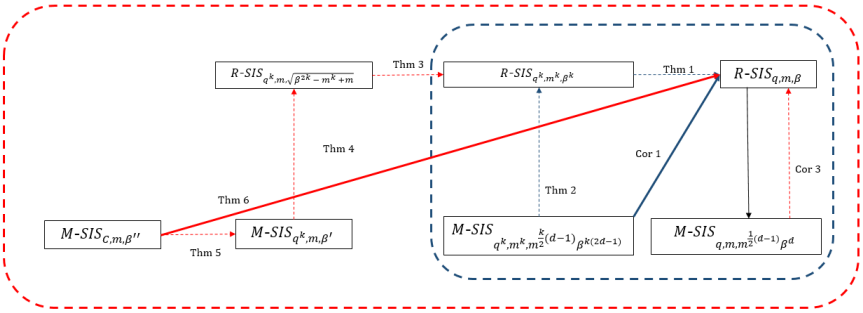


Fig. 1. Reduction between R-SIS and M-SIS for various parameters.

work [10]. This means that we obtain the improved reduction from M-SIS to R-SIS. Due to the reduced upper bound, we obtain that the possible range of module rank that satisfies this reduction increases twice the range of the module rank that satisfies the previous work. Also, the reduction from M-SIS to R-SIS in previous work [10] deals with the case of $k > 1$, but this improved reduction deals with the case of $k \geq 1$ as well. Finally, we propose a reduction between M-SIS with different modulus, that is, there exists a reduction from M-SIS$_{C,m,\beta'}$ to M-SIS$_{q^k,m,\beta}$, where C is a composite number that has a factor q^k for some $k \geq 1$. As the modulus of M-SIS increases, M-SIS becomes easier. Fig. 1 summarizes the relationship among the proposed reductions for the structured SIS problems. Combining three reductions, we propose the following main result (See Section 3.4 and 4 for details):

Main Result (Informal). *For sufficiently large prime q, there exists a reduction from M-SIS$_{C,m,\beta'}$ to R-SIS$_{q,m,\beta}$ with module rank $d < m$, where C is a composite number that has a factor q^k for some $k \geq 1$. In particular, there exists a reduction from M-SIS$_{q,m,\beta'}$ to R-SIS$_{q,m,\beta}$ with module rank $d < m$.*

1.2 Technical Overview

To show the reduction from M-SIS$_{C,m,\beta'}$ to R-SIS$_{q,m,\beta}$, we first derive a reduction from R-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m^k,\beta'}$. To derive this reduction, we choose uniformly and independently the samples $a_1, \ldots, a_m \in R_{q^k}$. Then we append $m^k - m$ zeros and we consider the m^k samples $a_1, \ldots, a_m, 0, \ldots, 0$ of R-SIS. Using the algorithm $\mathcal{A}$ for solving R-SIS$_{q^k,m^k,\beta^k}$, we find the solution $\mathbf{z} = (z_1, \ldots, z_{m^k})$ with $\|\mathbf{z}\| \leq \beta^k$. We need from the first element to the m-th element $(z_1, \ldots, z_m)$ of the solution $\mathbf{z}$ and we need to estimate upper bound of the norm of $(z_1, \ldots, z_m)$.

Second, to show the improved reduction from M-SIS to R-SIS, we should reduce the upper bound of the norm of the solution of R-SIS compare to [10] while finding the distinct m solutions of R-SIS. To reduce this upper bound, we consider the instance of R-SIS, say $a_1, \ldots, a_m \in R_{q^k}$ and write $A = (a_1, \ldots, a_m)$. Using the algorithm for solving R-SIS$_{q^k,m,\beta}$, we find the solution $\mathbf{z}$ by replacing

the i-th position of this vector A with zero. Then we obtain the solution of A by replacing the i-th position of the solution $\mathbf{z}$ with zero.

Finally, to show the reduction from M-SIS$_{C,m,\beta'}$ to R-SIS$_{q^k,m,\beta}$, where C is a composite number that has a factor q^k for some $k \geq 1$, we just embed instances $\mathbf{a}_1, \ldots, \mathbf{a}_m$ of R_C^d as $R_{q^k}^d$. Then we check the change of instances and find a solution of M-SIS$_{q^k,m,\beta'}$, that is, we find $\sum_{i=1}^{m} \mathbf{a}'_i \cdot z_i = 0 \bmod q^k$ with $\|\mathbf{z}\| \leq \beta$. Using these solutions, we find solution of M-SIS$_{C,m,\beta'}$, that is, $\sum_{i=1}^{m} \mathbf{a}_i \cdot \bar{\mathbf{z}}_i = 0 \bmod C$ with $\|\bar{\mathbf{z}}\| \leq \beta'$.

1.3 Organization

The remainder of this paper is organized as follows: In Section 2, SIS problems on ideal and module lattices are introduced and we also introduce the results of previous works. In Section 3, we derive three reductions, that is, the reduction from R-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m^k,\beta^k}$, the improved reduction from M-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m,\beta}$, and the reduction from M-SIS$_{C,m,\beta'}$ to M-SIS$_{q^k,m,\beta}$. Section 4 derives the relation between the modulus and the rank of module when M-SIS reduces to R-SIS and compares it with the previous work. Also, we give some simple examples. Finally, the conclusion and suggested future works are provided in Section 5.

2 Preliminaries

2.1 Structured Lattices

Ideal and module 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 $n = 2^r$ for some positive integer r. 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 additive subgroup of R and for all $r \in R$ and all $x \in I$, $r \cdot x \in I$. The quotient 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 $M \subseteq R^d$ as an R-module 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 [11]. Hereinafter vectors are denoted in bold and if $\mathbf{a}$ is a vector, then its i-th coordinate is denoted by a_i. A matrix is denoted by uppercase letter in bold.

Norms For each $a = a(X) \in R$, let $a(X) = \sum_{i=0}^{n-1} a_i X^i$ for $a_i \in \mathbb{Z}$. Then we define the norm of a as

$$\|a\| = \|a(X)\| = \left(\sum_{i=1}^{n-1} a_i^2 \right)^{1/2}.$$

Similarly, for each $\mathbf{a} = (a_1(X), \ldots, a_d(X)) \in R^d$, we define the norm $\mathbf{a}$ as

$$\|\mathbf{a}\| = \left(\sum_{i=1}^{d} \|a_i(X)\| \right)^{1/2}.$$

Lattices An n-dimensional lattice is a discrete subgroup of $\mathbb{R}^n$, where $\mathbb{R}$ is the set of real numbers. Specifically, for linearly independent vectors $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subseteq \mathbb{R}^n$, the set

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

is a lattice in $\mathbb{R}^n$ with the basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. 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 [11].

2.2 Short Integer Solution Problems

First, we defined the *short integer solution* (SIS) problem over the lattice, which is used in many lattice-based cryptographic schemes such as signature scheme and commitment scheme. This problem defined by Ajtai [1] is given as follows:

Definition 1 ([1]). *The SIS problem is defined as follows: Given* $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ *chosen from the uniform distribution, the SIS is to find* $\mathbf{z} = (z_1, \ldots, z_m)^T \in \mathbb{Z}^m$ *such that* $\mathbf{A} \cdot \mathbf{z} = 0 \bmod q$ *and* $0 < \|\mathbf{z}\| \leq \beta$.

To guarantee the non-trivial solution $\mathbf{z} \in \mathbb{Z}^m$ of SIS, the upper bound β of the norm of the solution of SIS is less than the modulus q. Indeed, if $\beta \geq q$ and $\mathbf{A} \in \mathbb{Z}^{n \times m}$, then we take the solution $\mathbf{z} = (q, 0, \ldots, 0)^T \in \mathbb{Z}^m$ and we obtain $\|\mathbf{z}\| = q \leq \beta$ and $\mathbf{A} \cdot \mathbf{z} = 0 \bmod q$.

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

Definition 2 ([11], [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* $\sum_{i=1}^{m} a_i \cdot z_i = 0 \bmod q$ *and* $0 < \|\mathbf{z}\| \leq \beta$, *where* $\mathbf{z} = (z_1, \ldots, z_m)^T \in R^m$.

Definition 3 ([11], [16]). *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 uniform distribution, the M-SIS problem is to find* $\mathbf{z} = (z_1, \ldots, z_m)^T \in R^m$ *such that* $\sum_{i=1}^{m} \mathbf{a}_i \cdot z_i = 0 \bmod q$ *and* $0 < \|\mathbf{z}\| \leq \beta$.

2.3 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 instances of R-SIS. Then we can consider a_i as the module element $\mathbf{a}_i = (a_i, 0, \ldots, 0) \in R_q^d$. Using the algorithm $\mathcal{A}$, we can find the solution $\mathbf{z} = (z_1, \ldots, z_m)^T \in R^m$ with $\|\mathbf{z}\| \leq \beta$ such that

$$\sum_{i=1}^{m} \mathbf{a}_i \cdot z_i = \left(\sum_{i=1}^{m} a_i \cdot z_i, 0, \ldots, 0 \right) = 0 \bmod q.$$

Since $\sum_{i=1}^{m} a_i \cdot z_i = 0 \bmod q$ and $\|\mathbf{z}\| \leq \beta$, we find the solution of the instances of R-SIS. However, Koo, et al., showed that R-SIS is more difficult than M-SIS under norm constraints of R-SIS [10]. 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 ([10]). *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 Theorem 1, the condition $\beta \geq \sqrt{n \cdot m} \cdot q^{\frac{1}{m}}$ is essential since it is the condition to guarantee the solution of R-SIS$_{q,m,\beta}$. And the solution of R-SIS$_{q^k,m^k,\beta^k}$ is constructed by the solution of R-SIS$_{q,m,\beta}$. Since each solution of $\mathbf{z}$ of R-SIS$_{q,m,\beta}$ is relatively prime to q, the solution of R-SIS$_{q^k,m^k,\beta^k}$ is also relatively prime to q. Thus, we can assume that the solution $\mathbf{z}$ of R-SIS$_{q^k,m^k,\beta^k}$ satisfies $\gcd(\mathbf{z}, q) = 1$.

To 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 difficult since details of the process of the algorithms for solving R-SIS are not known. To resolve this problem, we use the following lemma.

Lemma 1 ([10]). *Let m be a positive integer. Let $k > 1$ be a positive integer 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 $\sum_{i=1}^{m} a_i \cdot \bar{z}_i^{(j)} = 0 \bmod q^k$ for all $j = 1, \ldots, m$.*

In Lemma 1, since the modulus is q^k, we assume that the upper bound β of the norm of the solution of R-SIS$_{q^k,m,\beta}$ is larger than the prime q without loss of generality. This assumption implies that we find distinct m solutions that has the norm with upper bound β^2, that is, the upper bound of the norm of the solution of R-SIS$_{q^k,m,\beta}$ is increased.

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

Theorem 2 ([10]). *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$_{q^k,m,\beta'}$ from R-SIS$_{q^k,m,\beta}$ with $\beta' = m^{\frac{1}{2}(d-1)}\beta^{(2d-1)}$.

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 ([10]). *Let m be a fixed positive integer. Let $k > 1$ be a positive integer and q be a prime. Choose a module rank $d \in \mathbb{N}$ such that*

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

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 $\beta < \sqrt[2d-1]{q/(\sqrt{m})^{(d-1)}}$. 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 an reduction from M-SIS$_{q^k,m^k,\beta'}$ to R-SIS$_{q,m,\beta}$ with $\beta' = m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)}$.

2.4 Observation in Previous Works

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. By modifying (1), we have the range of module rank as follows:

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

To find the relation between the number of sample m and module rank d, we increase the prime q large enough. Then we have

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

for sufficiently large q. 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 $\frac{m+1}{2}$ for sufficiently large q, where $\beta' = m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)}$.

The reduction from M-SIS$_{q^k,m^k,\beta'}$ to R-SIS$_{q,m,\beta}$, where $\beta' = m^{\frac{k}{2}(d-1)}\beta^{k(2d-1)}$, has three limitations. First, the parameter k, which is the exponent of q, is larger than 1. This means that it is impossible that there exists a reduction between M-SIS and R-SIS with the same modulus. Furthermore, the moduli of M-SIS and R-SIS are related to the prime q. Second, the number of instances of M-SIS and that of R-SIS are different. That is, the number of instances is not preserved. Finally, the possible range of module rank d is upper bounded by $\frac{m+1}{2}$.

We propose the method to solve these three problems in the next section. That is, we propose the reduction from M-SIS$_{C,m,\beta'}$ to R-SIS$_{q^k,m,\beta}$ with module rank $d < m$ for sufficiently large q, where C is a composite number that has a factor q^k for some $k \geq 1$.

3 Improved Reduction from M-SIS to R-SIS

In this section, we propose the improved reduction from M-SIS to R-SIS compared to Section 2. First, we propose the reduction from R-SIS to R-SIS that preserves the number of samples of R-SIS. To show this reduction, we show that there exists a reduction from R-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m^k,\beta^k}$, where $\beta' = \sqrt{\beta^{2k} - m^k + m}$ and this result can be combined with Theorem 1.

Second, we propose the improved reduction from M-SIS to R-SIS. In Lemma 1, the solution of M-SIS is constructed by the solutions of R-SIS. To construct the solution of M-SIS, we find distinct solutions of R-SIS. Then the upper bound of the norm of the solution of R-SIS are increased since the assumption $q \leq \beta$. This is the cause of rapidly increasing the upper bound of the norm of the solution of M-SIS. We show that the upper bound of the norm of the solution of R-SIS is decreased by removing the assumption $q \leq \beta$ compared to Lemma 1 when we find distinct m solutions of R-SIS. By reducing this upper bound, we obtain a relaxed upper bound of the norm of the solution of M-SIS. Through the relaxed upper bound, we obtain that the possible range of module rank d is increased to double times that of Section 2.4. (See Section 4.2 for details)

Finally, we propose the reduction between M-SIS problems with different modulus. That is, there exists a reduction from M-SIS$_{C,m,\beta'}$ to M-SIS$_{q^k,m,\beta}$, where q^k is a factor of the composite integer C and $\beta' = \frac{C}{q^k}\beta$. These three reductions can be combined to obtain the improved reduction from M-SIS to R-SIS, that is, there exists a reduction from M-SIS$_{C,m,\beta'}$ to R-SIS$_{q^k,m,\beta}$, where $\beta' = m^{\frac{1}{2}(d-1)}(\beta^k - m^k + m)^{\frac{d}{2}}$ and C is a composite number that has a factor of q^k for some $k \geq 1$.

3.1 Preserving the Number of Samples of R-SIS

In this subsection, we propose that solving R-SIS$_{q^k,m^k,\beta^k}$ is more difficult than solving R-SIS$_{q^k,m,\beta'}$, where $\beta' = \sqrt{\beta^{2k} - m^k + m}$ for any $k \geq 1$. Since the solution of R-SIS$_{q^k,m^k,\beta^k}$ can be constructed from the solution of R-SIS$_{q,m,\beta}$ in Theorem 1, we can assume that the output of the algorithm $\mathcal{A}$ for solving R-SIS$_{q^k,m^k,\beta^k}$ is relatively prime to q. Through this reduction and Theorem 1, we demonstrate the reduction between the R-SIS problems preserving the number of samples of R-SIS.

Theorem 3. *Assume that an algorithm $\mathcal{A}$ exists for solving R-SIS$_{q^k,m^k,\beta^k}$ such that $\mathcal{A}$ outputs a solution $\mathbf{z} \in R^{m^k}$ with $\gcd(\mathbf{z}, q) = 1$. Then there exists an algorithm $\mathcal{A}'$ for solving R-SIS$_{q^k,m,\beta'}$, where $\beta' = \sqrt{\beta^{2k} - m^k + m}$; that is, there exists a reduction from R-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m^k,\beta^k}$, where $\beta' = \sqrt{\beta^{2k} - m^k + m}$.*

Proof. Assume that there exists an algorithm $\mathcal{A}$ for solving R-SIS$_{q^k,m^k,\beta^k}$. Let $a_1, \ldots, a_m \in R_{q^k}$ be chosen independently from the uniform distribution. Then we can write

$$\mathbf{a} = (a_1, \ldots, a_m, a_{m+1}, \ldots, a_{m^k}) = (a_1, \ldots, a_m, 0, \ldots, 0)$$

by appending the $m^k - m$ zeros. Then we can consider $\mathbf{a}$ as the instances of R-SIS$_{q^k,m^k,\beta^k}$. Using the algorithm $\mathcal{A}$, we can find the solution $\mathbf{z} = (z_1, \ldots, z_{m^k}) \in R^{m^k}$ with $\|\mathbf{z}\| \leq \beta^k$ such that

$$\begin{aligned}\sum_{i=1}^{m^k} a_i \cdot z_i &= \sum_{i=1}^{m} a_i \cdot z_i + 0 \cdot z_{m+1} + \ldots + 0 \cdot z_{m^k} \\ &= \sum_{i=1}^{m} a_i \cdot z_i \\ &= 0 \bmod q^k.\end{aligned}$$

Since $\mathbf{z}$ is relatively prime to q

$$\|(z_1, \ldots, z_m, 1, \ldots, 1)\| \leq \|\mathbf{z}\| \leq \beta^k.$$

This implies that $\|(z_1, \ldots, z_m)\| \leq \sqrt{\beta^{2k} - m^k + m}$. Thus, there exists a solution $\mathbf{z}' = (z_1, \ldots, z_m) \in R^m$ with $\|\mathbf{z}'\| \leq \beta'$ such that $\sum_{i=1}^{m} a_i \cdot z_i = 0 \bmod q^k$, where $\beta' = \sqrt{\beta^{2k} - m^k + m}$. □

Combining Theorems 1 and 3, we obtain the reduction between R-SIS problems with different parameters preserving the number of samples of R-SIS, that is, there exists a reduction from R-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q,m,\beta}$, where $\beta' = \sqrt{\beta^{2k} - m^k + m}$ for some $k \geq 1$ as in the following corollary.

Corollary 2. *Let m be a positive integer and q be a prime. Choose the upper bound of the norm $\beta \in \mathbb{R}$ such that $\beta \geq \sqrt{n \cdot m} q^{\frac{1}{m}}$. Assume tha there exists an algorithm $\mathcal{A}$ for solving the R-SIS$_{q,m,\beta}$ problem. Then there exists an algorithm $\mathcal{A}'$ for solving R-SIS$_{q^k,m,\beta'}$ for any integer $k \geq 1$, where $\beta' = \sqrt{\beta^{2k} - m^k + m}$.*

Proof. From Theorem 1, there exists an algorithm $\mathcal{S}$ for solving R-SIS$_{q^k,m^k,\beta^k}$ for any $k \geq 1$. Each solution of R-SIS$_{q^k,m^k,\beta^k}$ is constructed by the product of solutions of R-SIS$_{q,m,\beta}$. Thus, the algorithm $\mathcal{S}$ outputs the solution $\mathbf{z}$ of R-SIS$_{q^k,m^k,\beta^k}$ such that $\mathbf{z}$ is relatively prime to q. From Theorem 3, we obtain the algorithm $\mathcal{A}'$ for solving R-SIS$_{q^k,m,\beta'}$, where $\beta' = \sqrt{\beta^{2k} - m^k + m}$. □

3.2 Reducing the Upper Bound of the Norm for the Solution of M-SIS

In this subsection, we propose the improved reduction from M-SIS to R-SIS. The method of the reduction from M-SIS to R-SIS is the same as that in Theorem 2, but we show how to reduce the upper bound of the norm of the solution of M-SIS. To show the reduction from M-SIS to R-SIS, 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 difficult since details of the process of the algorithms for solving R-SIS are not known. From Lemma 1, we find as many distinct solutions as the number of instances of R-SIS. And thus, the upper bound of the norm of the solution of M-SIS is determined by that of R-SIS.

However, the upper bound of the norm of the solution of R-SIS is increased since we assume $q \leq \beta$ in Lemma 1. Therefore, we remove this assumption and propose a method of reducing the upper bound of the norm of the solution of R-SIS compare to Lemma 1 while finding distinct m solutions of R-SIS. We can achieve a reduced the upper bound of the norm of the solution of M-SIS compared to Theorem 2 through a reduced that of R-SIS. Also, we obtain that the possible range of module rank that can be reduced is doubled than that in Section 2.4. The following lemma shows how to reduce the upper bound of the norm of the solution of R-SIS compared to Lemma 1.

Lemma 2. *Let m be a positive integer. Let $k \geq 1$ be a positive integer and q be a prime. Let β be a real number such that $\sqrt{n \cdot m} \cdot q^{\frac{k}{m}} \leq \beta$. 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 distinct m solutions $\bar{\mathbf{z}}^{(i)} = (\bar{z}_1^{(i)}, \ldots, \bar{z}_m^{(i)})^T$ with $\|\bar{\mathbf{z}}^{(i)}\| \leq \beta$ such that $\sum_{i=1}^m a_j \cdot \bar{z}_j^{(i)} = 0 \mod q^k$ for all $i = 1, \ldots, m$.*

Proof. Let $A = (a_1, \ldots, a_m)$. Since $\binom{m}{m-1} = \binom{m}{1} = m$, we define the distinct subsets $S^{(i)} \subset \{1, 2, \ldots, m\}$ with $|S^{(i)}| = m - 1$ for all $i = 1, 2, \ldots, m$. For each $i = 1, \ldots, m$, we define the vector $A^{(i)} = (a_1^{(i)}, \ldots, a_m^{(i)})$ by $a_j^{(i)} = a_j$ if $j \in S^{(i)}$, and $a_j^{(i)} = 0$ if $j \notin S^{(i)}$. Then we can find a solution $\mathbf{z}^{(i)} = (z_1^{(i)}, \ldots, z_m^{(i)}) \in R^m$

with $\|\mathbf{z}^{(i)}\| \leq \beta$ such that $\sum_{j=1}^{m} a_j^{(i)} \cdot z_j^{(i)} = 0 \bmod q^k$ using the algorithm $\mathcal{A}'$ for all $i = 1, \ldots, m$. Then we obtain

$$\begin{aligned}\sum_{j=1}^{m} a_j^{(i)} \cdot z_j^{(i)} &= \sum_{j \in S^{(i)}} a_j^{(i)} \cdot z_j^{(i)} + \sum_{j \notin S^{(i)}} a_j^{(i)} \cdot z_j^{(i)} \\ &= \sum_{j \in S^{(i)}} a_j^{(i)} \cdot z_j^{(i)} \\ &= 0 \bmod q^k.\end{aligned}$$

Since $\gcd(z_j^{(i)}, q) = 1$, we have $\|z_j^{(i)}\| \geq 1$ and thus

$$\begin{aligned}\beta^2 &\geq \|\mathbf{z}^{(i)}\|^2 \\ &= \|z_1^{(i)}\|^2 + \cdots \|z_m^{(i)}\|^2 \\ &= \sum_{j \in S^{(i)}} \|z_j^{(i)}\|^2 + \sum_{j \notin S^{(i)}} \|z_j^{(i)}\|^2 \\ &\geq \sum_{j \in S^{(i)}} \|z_j^{(i)}\|^2 + 1 \\ &\geq \sum_{j \in S^{(i)}} \|z_j^{(i)}\|^2.\end{aligned}$$

Then, we obtain the inequality $\beta \geq (\sum_{j \in S^{(i)}} \|z_j^{(i)}\|)^{\frac{1}{2}}$. Now, we set the vector $\bar{\mathbf{z}}^{(i)} = (\bar{z}_1^{(i)}, \ldots, \bar{z}_m^{(i)})$ by $\bar{z}_j^{(i)} = z_j^{(i)}$ if $j \in S^{(i)}$, and $\bar{z}_j^{(i)} = 0$ if $j \notin S^{(i)}$. Then we obtain

$$\begin{aligned}\sum_{j=1}^{m} a_j \cdot \bar{z}_j^{(i)} &= \sum_{j \in S^{(i)}} a_j \cdot \bar{z}_j^{(i)} + \sum_{j \notin S^{(i)}} a_j \cdot \bar{z}_j^{(i)} \\ &= \sum_{j \in S^{(i)}} a_j \cdot \bar{z}_j^{(i)} \\ &= \sum_{j \in S^{(i)}} a_j^{(i)} \cdot z_j^{(i)} \\ &= 0 \bmod q^k\end{aligned}$$

with $\|\bar{\mathbf{z}}^{(i)}\| = (\sum_{j \in S^{(i)}} \|z_j^{(i)}\|^2)^{\frac{1}{2}} \leq \beta$ for all $i = 1, \ldots, m$. Thus, we obtain the distinct m solutions $\bar{\mathbf{z}}^{(i)} = (\bar{z}_1^{(i)}, \ldots, \bar{z}_m^{(i)})$ with $\|\bar{\mathbf{z}}^{(i)}\| \leq \beta$ such that $\sum_{j=1}^{m} a_j \cdot \bar{z}_j^{(i)} = 0 \bmod q^k$ for all $i = 1, \ldots, m$. □

Now, we propose the improved reduction from M-SIS to R-SIS using the Lemma 2. The proof of the following theorem is similar to that of Theorem 2. The difference of the proof is to apply the Lemma 2 to the last step that is finding the solution of R-SIS after applying the $d-1$ times Lemma 2 to the instances of R-SIS. Thus, we obtain the reduction from M-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m,\beta}$, where $\beta' = m^{\frac{1}{2}(d-1)}\beta^d$ and β' is less than that of Theorem 2.

Theorem 4. *Let m be a fixed positive integer. Let $k \geq 1$ be a positive integer and q be a prime. Choose a module rank $d \in \mathbb{Z}_{>0}$ such that*

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

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

$$\sqrt{n \cdot m} \cdot q^{\frac{k}{m}} \leq \beta, \tag{2}$$

where $\beta < \left[\sqrt[d]{q^{2k}/m^{d-1}} \right]^{\frac{1}{2}}$. 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 $\beta' = m^{\frac{1}{2}(d-1)}\beta^d$; that is, there exists a reduction from M-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m,\beta}$ with $\beta' = m^{\frac{1}{2}(d-1)}\beta^d$.

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

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

Then each 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 $\bar{\mathbf{z}}_d^{(j)} = (\bar{z}_{d,1}^{(j)}, \ldots, \bar{z}_{d,m}^{(j)})^T$ with $\|\bar{\mathbf{z}}_d^{(j)}\| \leq \beta$ such that $\mathbf{a}_d' \cdot \bar{\mathbf{z}}_d^{(j)} = 0 \bmod q^k$ by Lemma 2 for $j = 1, \ldots, m$. Now, we construct the $m \times m$ solution matrix

$$\bar{\mathbf{Z}}_d = \begin{bmatrix} | & | & \cdots & | \\ \bar{\mathbf{z}}_d^{(1)} & \bar{\mathbf{z}}_d^{(2)} & \cdots & \bar{\mathbf{z}}_d^{(m)} \\ | & | & \cdots & | \end{bmatrix}$$

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

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

Applying the above method $d-1$ times, we obtain the solution matrix

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

Finally, applying Lemma 2 to $\mathbf{a}_1^*$, we find a solution $\mathbf{z}'$ with $\|\mathbf{z}'\| \leq \beta$ such that $\mathbf{A}^* \cdot \mathbf{z}' = \mathbf{0} \bmod q^k$. Then, we have the solution $\mathbf{z} = \bar{\mathbf{Z}}_d \cdots \bar{\mathbf{Z}}_2 \cdot \mathbf{z}'$ for $\mathbf{A}$. Then $\mathbf{A} \cdot \mathbf{z} = \mathbf{0} \bmod q^k$ and

$$\begin{aligned}\|\mathbf{z}\| &= \|\bar{\mathbf{Z}}_d \cdots \bar{\mathbf{Z}}_2 \cdot \mathbf{z}'\| \\ &\leq \left(\sqrt{m} \cdot \beta\right)^{d-1} \cdot \beta \\ &\leq m^{\frac{1}{2}(d-1)} \beta^d.\end{aligned}$$

From (2), we have that the upper bound $\beta' = m^{\frac{1}{2}(d-1)}\beta^d$ on the norm of the solution of M-SIS$_{q^k,m,\beta'}$ is less than q^k since

$$\begin{aligned}m^{\frac{1}{2}(d-1)}\beta^d &< m^{\frac{1}{2}(d-1)} \left(\sqrt[d]{q^{2k}/m^{d-1}}\right)^{\frac{d}{2}} \\ &= q^k.\end{aligned}$$

Thus, we find a non-trivial solution of M-SIS$_{q^k,m,\beta'}$ and show that there exists a reduction from M-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m,\beta}$. □

The difference is that the upper bound of the norm of the solution of M-SIS in Theorem 4 is tighter than that of M-SIS in Theorem 4. Since the upper bound of the norm of the solution of R-SIS is decreased compared to Lemma 1, we obtain a solution of M-SIS with the reduced upper bound of the norm. Also, while in Lemma 1, the assumption $q \leq \beta$ is used, this assumption is removed in Lemma 2. This allows us to consider the case $k = 1$ in Theorem 4, that is, there exists a reduction from M-SIS$_{q,m,\beta'}$ to R-SIS$_{q,m,\beta}$, where $\beta' = m^{\frac{1}{2}(d-1)}\beta^d$.

3.3 Expanding the Modulus of M-SIS

In this subsection, we propose the reduction from M-SIS$_{C,m,\beta'}$ to M-SIS$_{q^k,m,\beta}$, where C is a composite number that has a factor q^k for some $k \geq 1$ and $\beta' = \frac{C}{q^k}\beta$. In Section 2, we showed the reduction between M-SIS and R-SIS with modulus related to q. To overcome this limitation, we propose a method of extending the modulus, which is the composite number divided by q^k for some $k \geq 1$.

Theorem 5. *Let m be an integer. Let $k \geq 1$ be a positive integer and q be a prime. Let C be a composite integer such that q^k divides C. Assume that there exists an algorithm $\mathcal{A}$ for solving M-SIS$_{q^k,m,\beta}$. Then there exists an algorithm $\mathcal{A}'$ for solving M-SIS$_{C,m,\beta'}$, where $\beta' = \frac{C}{q^k}\beta$.*

Proof. Let $\mathbf{a}_1, \ldots, \mathbf{a}_m \in R_C^d$ be chosen independently from uniform distribution, where $\mathbf{a}_i = (a_{i1}, \ldots, a_{id})$ for all $i = 1, \ldots, m$. For $i = 1, \ldots, m$ 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$_{q^k,m,\beta}$, we can find the solution $z_1, \ldots, z_m \in R$ such that

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

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

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

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

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

Since $\frac{C}{q^k}$ is an integer, $\frac{C}{q^k} z_i$ is in R for all $i = 1, \ldots, m$. And we obtain $\|\frac{C}{q^k}\mathbf{z}\| = \frac{C}{q^k}\|\mathbf{z}\| \leq \frac{C}{q^k}\beta$. Thus, $\frac{C}{q^k}\mathbf{z}$ is a solution of the instance of M-SIS$_{q^k,m,\beta'}$, where $\beta' = \frac{C}{q^k}\beta$. □

3.4 Combining of the Theorems

Now, we propose the improved reduction from M-SIS to R-SIS preserving the number of samples and expanding the modulus size as in the following theorem:

Theorem 6. *Let m be a fixed positive integer. Let $k \geq 1$ be a positive integer and q be a prime. Let C be a composite integer such that q^k divides C. Choose a module rank $d \in \mathbb{N}$ such that*

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} < \left[\sqrt[d]{q^{2k}/m^{d-1}} \right]^{\frac{1}{2k}}. \tag{3}$$

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

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

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

Proof. From Corollary 2, there exists the algorithm $\mathcal{S}$ for solving R-SIS$_{q^k,m,\gamma}$, where $\gamma = \sqrt{\beta^{2k} - m^k + m}$. Since we have

$$\begin{aligned}
[n \cdot m \cdot q^{\frac{2k}{m}} + m^k - m]^{\frac{1}{2k}} &\leq [m^k(n \cdot q^{\frac{2k}{m}} + 1)]^{\frac{1}{2k}} \\
&\leq [2 \cdot m^k \cdot n \cdot q^{\frac{2k}{m}}]^{\frac{1}{2k}} \\
&\leq [n^k \cdot m^k \cdot q^{\frac{2k}{m}}]^{\frac{1}{2k}} \\
&= \sqrt{n \cdot m} \cdot q^{\frac{1}{m}} \\
&\leq \beta,
\end{aligned}$$

we obtain $\sqrt{n \cdot m} \cdot q^{\frac{k}{m}} \leq \sqrt{\beta^{2k} - m^k + m} = \gamma$. Since

$$\beta < \left[\sqrt[d]{q^{2k}/m^{d-1}}\right]^{\frac{1}{2k}} < \left[\sqrt[d]{q^{2k}/m^{d-1}} + m^k - m\right]^{\frac{1}{2k}},$$

we have

$$\gamma = \sqrt{\beta^{2k} - m^k + m} < \left[\sqrt[d]{q^{2k}/m^{d-1}}\right]^{\frac{1}{2}}.$$

Thus, we have

$$\sqrt{n \cdot m} \cdot q^{\frac{k}{m}} \leq \gamma = \sqrt{\beta^{2k} - m^k + m} < \left[\sqrt[d]{q^{2k}/m^{d-1}}\right]^{\frac{1}{2}}$$

and from Theorem 4, there exists the algorithm $\mathcal{S}'$ for solving M-SIS$_{q^k,m,\gamma'}$, where $\gamma' = m^{\frac{1}{2}(d-1)}\gamma^d = m^{\frac{1}{2}(d-1)}(\beta^{2k} - m^k + m)^{\frac{d}{2}}$. Finally, applying Theorem 5, we obtain the algorithm $\mathcal{A}'$ for solving M-SIS$_{C,m,\beta'}$, where $\beta' = \frac{C}{q^k}\gamma' = \frac{C}{q^k}m^{\frac{1}{2}(d-1)}(\beta^{2k} - m^k + m)^{\frac{d}{2}}$. Thus, R-SIS$_{q,m,\beta}$ is more difficult than M-SIS$_{C,m,\beta'}$, where $q^k \mid C$ for some $k \geq 1$ and $\beta' = \frac{C}{q^k}m^{\frac{1}{2}(d-1)}(\beta^{2k} - m^k + m)^{\frac{d}{2}}$. □

In particular, if we take $k = 1$ and $C = q$, we obtain the reduction from M-SIS$_{q,m,\beta'}$ to R-SIS$_{q,m,\beta}$, where $\beta' = m^{\frac{1}{2}(d-1)}\beta^d$. The following corollary is given as:

Corollary 3. *Let m be a fixed positive integer. Let q be a prime. Choose a module rank $d \in \mathbb{N}$ such that*

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} < \left[\sqrt[d]{q^2/m^{d-1}}\right]^{\frac{1}{2}}. \tag{4}$$

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

4 Observations

4.1 Hardness of Structured SIS Problems Depending of the Upper Bound

In Corollary 3, we obtain the reduction from M-SIS$_{q,m,\beta'}$ to R-SIS$_{q,m,\beta}$ handling the upper bound of the norm of the solution of R-SIS. In general, the hardness of structured SIS problems depend on the upper bound of the norm of the solution of structured SIS problems. For example, if the upper bound of the norm of the solution of R-SIS is increased, then the hardness of R-SIS is reduced. That is, we have the following theorem.

Theorem 7. *Let m and q be positive integers. Let $\beta', \beta \in \mathbb{R}$ such that $\beta \leq \beta' < q$ and $\beta \geq \sqrt{n \cdot m} q^{\frac{1}{m}}$. 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.*

Proof. Assume that there exists an algorithm $\mathcal{A}$ for solving R-SIS$_{q,m,\beta}$ and $\beta \geq \beta'$. Let $a_1, \ldots, a_m \in R_q$ be chosen uniformly and independently. From the algorithm $\mathcal{A}$, there exists a solution $\mathbf{z} = (z_1, \ldots, z_m)^T \in R^m$ such that $\sum_{i=1}^{m} a_i \cdot z_i = 0 \bmod q$ and $\|\mathbf{z}\| \leq \beta$. Since $\beta \leq \beta'$, the norm of the solution $\mathbf{z}$ is less than β'; that is, $\|\mathbf{z}\| \leq \beta \leq \beta'$. Thus, we find the solution $\mathbf{z}$ such that $\sum_{i=1}^{m} a_i \cdot z_i = 0 \bmod q$ and $\|\mathbf{z}\| \leq \beta'$. The proof is similar to the reduction between M-SIS problems. □

Thus, the hardness of structured SIS problems depends on the upper bound of the norm of the solution of structured SIS; that is, when the upper bound of the norm of the solution of structured SIS increases, the structured SIS problem becomes easier. Thus, combining Corollary 3 and Theorem 7, we obtain the following corollary:

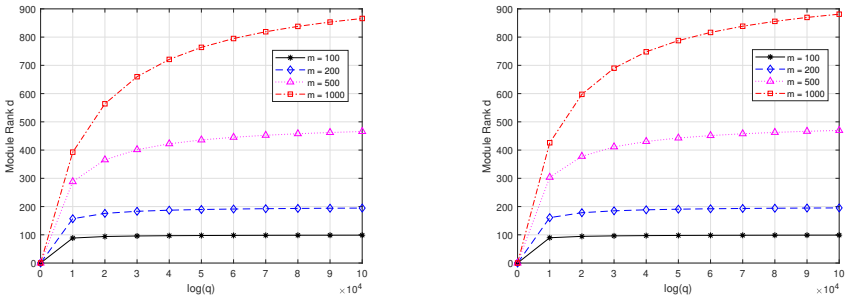
Corollary 4. *Let m be a fixed positive integer. Let q be a prime. Choose a module rank $d \in \mathbb{N}$ such that*

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} < \left[\sqrt[d]{q^2/m^{d-1}} \right]^{\frac{1}{2}}.$$

Let a positive real number $\beta = \sqrt{n \cdot m} \cdot q^{\frac{1}{m}}$ be an upper bound on the norm of the solution of R-SIS$_{q,m,\beta}$. Assume that an algorithm $\mathcal{A}$ exists for solving the R-SIS$_{q,m,\beta}$ problem. Then, an algorithm $\mathcal{A}'$ exists for solving the M-SIS$_{q,m,\beta'}$ problem with module rank d, where $\beta' = \frac{1}{\sqrt{m}} n^{\frac{d}{2}} m^d q^{\frac{d}{m}}$; that is, there exists a reduction from M-SIS$_{q,m,\beta'}$ to R-SIS$_{q,m,\beta}$ with $\beta' = \frac{1}{\sqrt{m}} n^{\frac{d}{2}} m^d q^{\frac{d}{m}}$. In particular, if

$$\frac{1}{\sqrt{m}} n^{\frac{d}{2}} m^d q^{\frac{d}{m}} \leq \beta' < q,$$

then there exists a reduction from M-SIS$_{q,m,\beta'}$ to R-SIS$_{q,m,\beta}$.



(a) $k = 2$ (b) $k = 10$

Fig. 2. Rank of module when $n = 2^{16}$ from (5) in Section 4.2 (a) $k = 2$ (b) $k = 10$.

Proof. From Corollary 3, there exists a reduction from M-SIS$_{q,m,\beta'}$ to R-SIS$_{q,m,\beta}$, where

$$\begin{aligned}\beta' &= m^{\frac{1}{2}(d-1)}\beta^d \\ &= m^{\frac{1}{2}(d-1)}(\sqrt{n \cdot m} \cdot q^{\frac{1}{m}})^d \\ &= \frac{1}{\sqrt{m}} n^{\frac{d}{2}} \cdot m^d \cdot q^{\frac{d}{m}}.\end{aligned}$$

If $\frac{1}{\sqrt{m}} n^{\frac{d}{2}} m^d q^{\frac{d}{m}} \leq \beta' < q$, then there exists from M-SIS$_{q,m,\beta'}$ to R-SIS$_{q,m,\beta}$ from Theorem 7. Thus, this corollary holds. □

Thus, the hardness of M-SIS$_{q,m,\beta'}$ is determined by the upper bound β' of the norm of the solution of M-SIS. Corollary 4 means that for a fixed modulus q and the same number m of instances of M-SIS and R-SIS, the tightness of the upper bound of the norm of the solution of M-SIS determines whether the M-SIS problem is a more difficult of easier than the R-SIS problem for some possible module rank d.

4.2 The Possible Range of Module Ranks

In Theorem 6, the possible module rank d is determined by (3). Since the parameter n is the dimension of the polynomial ring R and m is the number of samples of R-SIS, these are fixed. Thus, d depends on the prime q when the exponent of q, k, is fixed. When we modify (3), we obtain the possible range of module rank d. Modification of (3) is as follows:

$$d < \frac{2km \log q + m \log m}{2k \log q + mk \log n + mk \log m + m \log m}. \tag{5}$$

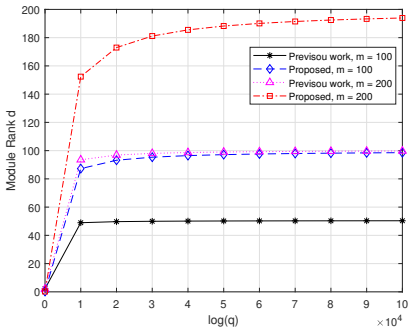


Fig. 3. Comparison of the possible ranges of module ranks.

To find the relation between the prime q and the possible range of module rank d, we try to increase the prime q. Then we have

$$\frac{2km\log q + m\log m}{2k\log q + mk\log n + mk\log m + m\log m} \to m \quad as \quad q \to \infty,$$

and thus the possible range of module rank d is

$$d < m$$

for sufficiently large q. Fig. 2 shows the possible ranks of module with the different parameter and $\log_2(q)$. In the case of Fig. 2(a), the logarithm in modulus q of base 2 varies from 0 to 10^5 with fixed $n = 2^{16}$ and $k = 2$ and in the case of Fig. 2(b), the logarithm in modulus q of base 2 varies from 0 to 10^5 with fixed $n = 2^{16}$ and $k = 10$. As $\log_2(q)$ increases, the possible range of module rank d approach to the number of the instances m. Also, as m increases, the possible range of module rank d becomes even wider and as k increases, it becomes faster in (5) to converge to m.

4.3 Comparison of the Previous Work and the Proposed Work

To find the possible range of module rank d when $k = 1$, we modify (4) as follows

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

Similarly, we obtain the possible range of module rank d as

$$d < m$$

for sufficiently large q. The possible range of module ranks has doubled compared to Section 2.4. Also, in the case of the previous work, we consider the case where the modulus exponent k, is greater than 2, but in this work, we propose the

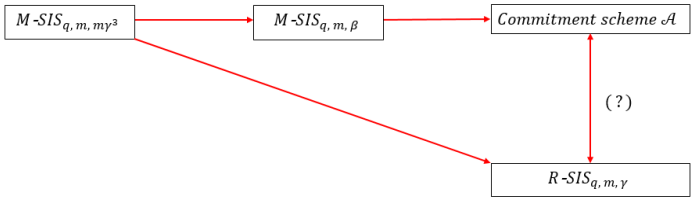


Fig. 4. Application of the proposed method in Section 4.4.

improved reduction for the case of $k = 1$. Fig. 3 shows the comparison of the possible ranges of module ranks of the previous work and the proposed work. In Fig. 3, the logarithm in modulus q of base 2 varies from 0 to 10^5 with fixed $n = 2^{16}$. From Fig. 3, we can see that this work has a possible range of module ranks that are about twice as wide as that of the previous work. Thus, we obtain that for sufficiently large q, there exists a reduction from M-SIS$_{q,m,\beta'}$ to R-SIS$_{q,m,\beta}$ with module rank $d < m$, where $\beta' = m^{\frac{1}{2}(d-1)}\beta^d$. This means that if there is a cryptographic algorithm based on M-SIS$_{q,m,\beta'}$, then we must consider R-SIS$_{q,m,\beta}$ since there is a possibility that the cryptographic scheme may be attacked by the algorithm for solving R-SIS$_{q,m,\beta}$.

4.4 Application

In this section, we consider two possible applications that can be analyzed by the proposed results.

Example 1. In [4], the commitment scheme $\mathcal{A}$ satisfying statistical-hiding is constructed. This scheme is based on the M-SIS$_{q,m,\beta}$ with rank $d = 3$ and dimension $n = 2^9$, where $q \approx 2^{35}$, $m = 18$, and $\beta = \sqrt{18} \times 128 \approx 543.0580$. That is, $\mathcal{A}$ is more difficult than M-SIS$_{q,m,\beta}$. Using (4), we obtain

$$\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} \approx 369.494$$
$$\left[\sqrt[d]{q^2/m^{d-1}}\right]^{\frac{1}{2}} \approx 1240.5.$$

From Theorem 7, we consider the M-SIS$_{q,m,m\gamma^3}$ problem so that M-SIS$_{q,m,\beta}$ is more difficult than M-SIS$_{q,m,m\gamma^3}$. M-SIS$_{q,m,m\gamma^3}$ is reduced to R-SIS$_{q,m,\gamma}$ and we take $\gamma = 369.5$ based on Theorem 7. This means that the relationship between R-SIS and commitment scheme $\mathcal{A}$ cannot be accurately known. In other words, there is a possibility that the commitment scheme $\mathcal{A}$ is attacked by the algorithm that solves the R-SIS$_{q,m,\gamma}$, where q and m are defined as the above. Thus, if there is an algorithm for solving the commitment scheme $\mathcal{A}$, it must be proved that there is an algorithm to solve R-SIS$_{q,m,\gamma}$. This means that in order for the commitment scheme $\mathcal{A}$ to be more secure, the algorithm for solving R-SIS$_{q,m,\gamma}$ must also be considered. Fig. 4 is a summary of Example 1.

Table 1. The parameters of M-SIS in [19]

The module rank d	2	3
The modulus q	$\approx 2^{196}$	$\approx 2^{196}$
The number of instances m	132	132
The dimension of polynomial ring n	2^{10}	2^{10}
The upper bound β	$\approx 2^{126}$	$\approx 2^{126}$
$\sqrt{n \cdot m} q^{\frac{1}{m}}$	≈ 1029.01	≈ 1029.01
$\left[\sqrt[d]{q^2/m^{d-1}}\right]^{\frac{1}{2}}$	$\approx 9349.7 \times 10^{25}$	$\approx 9129.2 \times 10^{15}$

Example 2. The parameters of M-SIS$_{q,m,\beta}$ used in [19] are listed in Table 1.

Since $\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} < \left[\sqrt[d]{q^2/m^{d-1}}\right]^{\frac{1}{2}}$, the M-SIS problem can be reduced to the R-SIS problem. In the case of the module rank $d = 2$, we can find the upper bound of the norm of the solution of R-SIS by solving $\sqrt{132} \times \gamma^2 = 2^{126}$. Then we obtain $\gamma \approx 2721.1 \times 10^{15}$ and $\sqrt{n \cdot m} \cdot q^{\frac{1}{m}} < \gamma < \left[\sqrt[d]{q^2/m^{d-1}}\right]^{\frac{1}{2}}$. Thus, M-SIS$_{q,m,\beta}$ can be reduced to R-SIS$_{q,m,\gamma}$. In the case of the module rank $d = 3$, we obtain $\gamma = 8637.8 \times 10^{11}$. Thus, M-SIS$_{q,m,\beta}$ can be reduced to R-SIS$_{q,m,\gamma}$ in the case of module rank $d = 3$. Therefore, there is a possibility of being attacked due to the relationship between the scheme in [19] and R-SIS$_{q,m,\gamma}$. Thus, if there is an algorithm for solving the scheme in [19], it must be proved that there is an algorithm to solve R-SIS$_{q,m,\gamma}$. This means that in order for the scheme in [19] to be more secure, the algorithm for solving R-SIS$_{q,m,\gamma}$ must also be considered.

5 Conclusion and Future works

In this paper, we showed that the improved reduction from M-SIS$_{C,m,\beta'}$ to R-SIS$_{q,m,\beta}$, where C is a composite number that has a factor q^k for some $k \geq 1$ and $\beta' = \frac{C}{q^k} m^{\frac{1}{2}(d-1)} (\beta^{2k} - m^k + m)^{\frac{d}{2}}$. To show this improved reduction from M-SIS$_{C,m,\beta'}$ to R-SIS$_{q,m,\beta}$, we first showed that there exists a reduction from R-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m^k,\beta^k}$, where $\beta = \sqrt{\beta^{2k} - m^k + m}$. Combining with this result and Theorem 1, we obtained the reduction from R-SIS$_{q^k,m,\beta}$ to R-SIS$_{q,m,\beta}$. Second, we showed the improved reduction from M-SIS$_{q^k,m,\beta'}$ to R-SIS$_{q^k,m,\beta}$, where $\beta' = m^{\frac{1}{2}(d-1)} \beta^d$. Comparing with the previous work, we reduced the upper bound of norm of the solution of M-SIS. This implies that we obtained the possible range of module ranks $d < m$ that is doubled compared to the previous work. Finally, we showed that there exists the reduction from M-SIS$_{C,m,\beta'}$ to M-SIS$_{q^k,m,\beta}$, where C is the multiple of q^k for some $k \geq 1$ and $\beta' = \frac{C}{q^k}\beta$. In particular, the previous work was established for the case of $k > 1$, but this work is also possible to apply for the case of $k = 1$. This means that R-SIS$_{q,m,\beta}$ is more difficult than M-SIS$_{C,m,\beta'}$, where C is divided by q and $\beta' = \frac{C}{q} m^{\frac{1}{2}(d-1)} \beta^d$ with module rank $d < m$ for sufficiently large q.

This reduction is limited because the range of module rank is limited to $d < m$. To extend the range of module rank, we handle the upper bound of the norm of the solution of M-SIS. As we decrease this, the range of module rank is increased. We showed the reduction from M-SIS to R-SIS only for cases with the same modulus and for the composite number C divided by the modulus q^k for some $k \geq 1$.

As a future work, we want to show the reduction from M-SIS to R-SIS for different prime number p and q, that is, we want to show that there exists the reduction from M-SIS$_{p,m,\beta'}$ to R-SIS$_{q,m,\beta}$, where p and q are prime with $p > q$.

References

1. Ajtai, M.: Generating hard instances of lattice problems. In: Proc. 28th Annu. ACM Symp. Theory Comp. pp. 99–108 (1996)
2. Alagic, G., Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y.K., Miller, C., Moody, D., Peralta, R., et al.: Status report on the first round of the NIST post-quantum cryptography standardization process. US Department of Commerce, National Institute of Standards and Technology (2019)
3. Albrecht, M.R., Deo, A.: Large modulus Ring-LWE $\geq$ Module-LWE. In: Proc. ASIACRYPT 2017. vol. 10624 of LNCS, pp. 267–296. Springer, Berlin/Heidelberg, Germany (Dec 2017)
4. Baum, C., Damgård, I., Lyubashevsky, V., Oechsner, S., Peikert, C.: More efficient commitments from structured lattice assumptions. In: International Conference on Security and Cryptography for Networks. pp. 368–385. Springer (2018)
5. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D.: Crystals-kyber: a CCA-secure module-lattice-based KEM. In: 2018 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 353–367. IEEE (2018)
6. Chillotti, I., Gama, N., Georgieva, M., Izabachene, M.: Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In: international conference on the theory and application of cryptology and information security. pp. 3–33. Springer (2016)
7. Ducas, L., Durmus, A., Lepoint, T., Lyubashevsky, V.: Lattice signatures and bimodal Gaussians. In: Proc. CRYPTO 2013. vol. 8042 of LNCS, pp. 40–56. Springer, Berlin/Heidelberg, Germany (Aug 2013)
8. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: Crystals-dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems pp. 238–268 (2018)
9. Esgin, M.F., Steinfeld, R., Sakzad, A., Liu, J.K., Liu, D.: Short lattice-based one-out-of-many proofs and applications to ring signatures. In: International Conference on Applied Cryptography and Network Security. pp. 67–88. Springer (2019)
10. Koo, Z., No, J., Kim, Y.: Reduction from module-SIS to ring-SIS under norm constraint of ring-sis. IEEE Access **8**, 140998–141006 (2020)
11. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography **75**(3), 565–599 (2015)
12. Lyubashevsky, V.: Lattice signatures without trapdoors. In: Proc. EUROCRYPT 2012. vol. 7237 of LNCS, pp. 738–755. Springer, Berlin/Heidelberg, Germany (Apr 2012)

13. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 1–23. Springer (2010)
14. Micciancio, D., Regev, O.: Lattice-based cryptography. In: Post-Quantum Cryptography, pp. 147–191. Springer, Berlin/Heidelberg, Germany (2009)
15. Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem. In: Proceedings of the forty-first annual ACM symposium on Theory of computing. pp. 333–342 (2009)
16. Peikert, C., Rosen, A.: Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In: Proc. TCC 2006. vol. 3876 of LNCS, pp. 145–166. Springer, Berlin/Heidelberg, Germany (Mar 2006)
17. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM (JACM) **56**(6), 1–40 (2009)
18. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review **41**(2), 303–332 (1999)
19. Torres, W.A., Kuchta, V., Steinfeld, R., Sakzad, A., Liu, J.K., Cheng, J.: Lattice RingCT v2.0 with multiple input and multiple output wallets. In: Australasian Conference on Information Security and Privacy. pp. 156–175. Springer (2019)