Algebraic isomorphic spaces of ideal lattices, reduction of Ring-SIS problem, and new reduction of Ring-LWE problem

Zhuang Shan(单壮)[1], Leyou Zhang(张乐友)[1,*], Qing Wu(吴青)[2], Qiqi Lai(来齐齐)[3]

September 19, 2023

Abstract

This paper mainly studies an open problem in modern cryptography, namely the Ring-SIS reduction problem. In order to prove the hardness of the Ring-SIS problem, this paper introduces the concepts of the one-dimensional SIS problem, the Ring-SIS$|_{x=0}$ problem, and the variant knapsack problem. The equivalence relations between the three are first established, on which the connection between the Ring-SIS$|_{x=0}$ problem and the Ring-SIS problem is built. This proves that the hardness of the Ring-SIS problem is no less than that of the variant knapsack problem and no more than that of the SIS problem. Additionally, we reduce the Ring-LWE problem to the Ring-SIS problem, which guarantees the security of encryption schemes based on Ring-LWE to a certain degree. Lastly, this article proves that the difficulty of the Ring-SIS problem and the Ring-LWE problem is moderate with respect to the spatial dimension or polynomial degree.

Keywords: Ring-SIS problem, shortest trapdoor in ideal lattices, Ring-LWE problem, knapsack problem, SIVP.

1 Introduction

The main research problem of this article is to reduce the Ring-SIS problem [LPR10] to the SIS problem, and the Ring-SIS problem refers to $f_1, \ldots, f_m \in \mathcal{R}_q$, where $\mathcal{R}_q$ is a polynomial ring with modulus q, find m polynomials $g_1, \ldots,$ whose coefficients are not all 0, $g_m \in \mathcal{R}_{\{0,\pm 1\}}$, such that

$$f_1 g_1 + \cdots + f_m g_m = 0 \bmod q\mathcal{R}.$$

Currently, lattice cryptography is an important research field in post-quantum cryptography. In 2005, Regev completed the reduction work of the learning with error problem (LWE), reducing it to a difficult problem in the classic lattice, that is, the closet vector problem and the shortest vector problem [Reg05]. Regev's work ensured the theoretical foundation of lattice cryptography. In 1996, Ajtai gave a new lattice difficulty problem, namely the shortest integer problem (SIS, [Ajt96]). Subsequently, Micciancio and Peikert gave a more concise conclusion and combined it with the LWE problem to serve as a one-way trapdoor function for the encryption scheme based on the LWE problem [MP13]. Moreover, the SIS problem itself provides the security guarantee of the trapdoor function. This achievement makes the world of lattice cryptography more dynamic.

With in-depth research on encryption schemes based on the LWE problem, everyone found that the computational overhead of this type of scheme is not very ideal. Therefore, it is hoped that there

[1] School of Mathematics and Statistics, Xidian University, Xi'an 710126, China; arcsec30@163.com

[2] School of Automation, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

[3] School of Computer Science, Shaanxi Normal University, Xi'an, China

will be a new difficult problem that can inherit the difficulty of LWE and at the same time ensure the operating efficiency of the solution. In 2010, Lyubashevsky, Peikert, and Regev proposed a learning with error problem on polynomial rings, namely the Ring-LWE problem [LPR10], establishing an isomorphic relationship with the ideal lattice. And reduce it to the bounded coding problem on the ideal lattice (Ideal-BDD). The Ring-LWE problem is similar in form to the LWE problem, and its calculation time is much less than that of the LWE problem.

However, the Ideal-BDD problem itself is also a variant of the BDD problem, and the reduction work has not yet been completed. Therefore, simply reducing the Ring-LWE problem to the Ideal-BDD problem may not necessarily explain the difficulty. In addition, similar to the encryption scheme based on LWE, the encryption scheme based on Ring-LWE also requires the Ring-SIS problem as a trapdoor function, and Lyubashevsky, Peikert, and Regev mentioned "Indeed, the perspectives and techniques that have so far been employed for the Ring-SIS problem appear insufficient for adapting the more involved hardness proofs for LWE to the ring setting" in the article [LPR10]. Steven Yue mentioned on the Zhihu website that the Ring-SIS problem is still an open problem [MP13]. Therefore, the reduction of the Ring-SIS problem is an urgent problem that needs to be solved in current lattice cryptography.

1.1 Our work

The main work of this paper is to reduce the Ring-SIS problem to the SIS problem. Similar to the article by Micciancio and Peikert [MP13], we also divide the article into three parts, namely Ring-SIS to Ring-SIS Reduction, Direct Reduction and Ring-SIS to Ring-LWE Reduction.

1.1.1 Ring-SIS to Ring-SIS Reduction

Let Ring-SIS(m, n, q, β) be a problem, where m, n are positive integers, q is a prime number, and β is a positive number. This part is divided into two steps, namely

1. When there is an oracle that can solve Ring-SIS(m, n, q, β) in polynomial time, there is also an efficient algorithm that can solve Ring text$-$SIS$(m' = tm, n, q, \beta)$, and the number of times the algorithm queries the oracle is t times;

2. When there is an oracle that can solve Ring-SIS(m, n, q, β) in polynomial time, there is also an efficient algorithm that can solve Ring text$-$SIS$(m, n' = tn, q, \beta)$, and the number of times this algorithm queries the oracle at least t times.

For **first step**, we can divide it according to the number of polynomials in Ring-SIS$(m' = tm, n, q, \beta)$. More specifically, $f_1, \ldots, f_{m'} \in \mathcal{R}_q$ is divided into t parts, each part is exactly Ring-SIS(m, n, q, β), at this time, use the Ring-SIS(m, n, q, β) oracle to solve its sutras. The solution for each part together, it is the solution of Ring-SIS$(m' = tm, n, q, \beta)$. At this time, we need to ask t times Ring -SIS(m, n, q, β) oracle.

For **second step**, according to the properties of polynomials, that is, when $f(x)g(x) = (a_0 + a_1x + \cdots a_{n-1}x^{n-1})(b_0 + b_1x + \cdots b_{n-1}x^{n-1}) \bmod (x^n + 1) = 0$, then there is $f_{t,k}(x)g_{t,k}(x) = (a_0x^k + a_1x^{k+t} + \cdots a_{n-1}x^{k+(n-1)t})(b_0x^k + b_1x^{k+t} + \cdots b_{n-1}x^{k+(n-1)t}) \bmod (x^{nt} + 1) = 0$, where $k \in [0, t)$.

According to this property, we have obtained a very important theorem, that is, when $F^T(x) := (f^{(1)}(x), f^{(2)}(x), \cdots, f^{(m)}(x))$, $G(x) := (g^{(1)}(x), g^{(2)}(x), \cdots, g^{(m)}(x))$, if there is

$$F^T(x)G(x) = \sum_i^m f^{(l)}(x)g^{(l)}(x) \bmod (x^n + 1) = 0,$$

then there is

$$F_{t,k}^T(x)G_{t,k}(x) = \sum_l^{\mathrm{m}} f_{t,k}^{(l)}(x)g_{t,k}^{(l)}(x) \bmod (x^{nt} + 1) = 0$$

for $F_{t,k}^T(x) := (f_{t,k}^{(1)}(x), f_{t,k}^{(2)}(x), \cdots, f_{t,k}^{(m)}(x))$, $G(x) := (g_{t,k}^{(1)}(x), g_{t,k}^{(2)}(x), \cdots, g_{t,k}^{(m)}(x))$. Among them, $k \in [0, t)$. This conclusion is very important. According to this conclusion, we can extract an n order polynomial in Ring-SIS$(m, n' = tn, q, \beta)$, thus forming a Ring-SIS(m, n, q, β) problem. We can get the solution to a part of the Ring-SIS$(m, n' = tn, q, \beta)$ problem that is divided into parts of the Ring-SIS(m, n, q, β) problem by asking the Ring-SIS(m, n, q, β) oracle m times.

According to the above properties, it can be seen that after the first query m times Ring-SIS(m, n, q, β) oracle gets the solution, it will be compared with Ring-SIS$(m, n' = tn, q, \beta)$ problem, the n' terms of the $n' - 1$ degree polynomial of the original problem are reduced by n terms, because we asked Ring-SIS(m, n, q, β) once, so after action, it is still Ring-SIS$(m, n' = tn, q, \beta)$ problem, except that each polynomial is missing n terms.

Repeat this method there are only n terms left in each polynomial of the Ring-SIS$(m, n' = tn, q, \beta)$ problem, and we can directly use Ring-SIS(m, n, q, β) is solved by the oracle. Combining these solutions is the final solution to the Ring-SIS$(m, n' = tn, q, \beta)$ problem. Then a total of $(tn-n)/n+1 = (t-1)+1 = t$ times are asked Ring-SIS(m, n, q, β) oracle.

1.1.2 Direct Reduction

We reduce the Ring-SIS problem to the SIS problem by establishing an isomorphic relationship between the two, thus proving the difficulty of the Ring-SIS problem. However, we cannot directly reduce the Ring-SIS problem to the SIS problem, so we thought of a way. We consider the variants of the SIS problem and the Ring-SIS problem, that is, the one-dimensional SIS problem and the Ring-SIS$|_{x=0}$ problem. The so-called one-dimensional SIS problem refers to $\alpha^T = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{M}_{mn\times 1}(\mathbb{Z}_q)$, $\alpha_i^T \in \mathcal{M}_{n\times 1}(\mathbb{Z}_q)$, find $z = (z_1, z_2, \ldots, z_n) \in \mathcal{M}_{1\times mn}(\mathbb{Z}_q)$, $z_i \in \mathcal{M}_{1\times n}(\mathbb{Z}_q)$, $\|z\| \leq \beta$, such that

$$z\alpha = \sum_{i}^{m} z_i\alpha_i = (z_1, z_2, \ldots, z_m)(\alpha_1, \alpha_2, \ldots, \alpha_m)^T = 0.$$

Where $\mathcal{M}_{m\times n}(\mathbb{Z}_q)$ represents a matrix of order $m \times n$ and the coefficients are elements in $\mathbb{Z}_q$[Qiu10]. The corresponding Ring-SIS$|_{x=0}$ problem refers to $f_1, \ldots, f_m \in \mathcal{R}_q$, where $\mathcal{R}_q$ is a polynomial ring with modulus q, find a set of polynomials $g_1, \ldots, g_m \in \mathcal{R}_{\{0,\pm 1\}}$ whose coefficients are not all 0, such that

$$f_1g_1 + \cdots + f_mg_m|_{x=0} = 0 \bmod q\mathcal{R}.$$

The purpose of this is to establish an isomorphic relationship between the Ring-SIS$|_{x=0}$ problem and the one-dimensional SIS problem(one-dimensional SIS problem).

When the isomorphism relationship is established, we follow the conclusion of Lemma 9, that is, if space A and space B are isomorphic, then if for $\mathcal{A}$ in space A is an abstract hard problem if and only if $\mathcal{B}$ in the corresponding space B is also a hard problem. When the isomorphic relationship between the Ring-SIS$|_{x=0}$ problem and the one-dimensional SIS problem is established, we assume that there are collision-resolving oracles for the two, and obtain the collision-resolving oracle of the Ring-SIS$|_{x=0}$ problem that needs to be asked to solve the Ring-SIS problem. The number of times the oracle needs to be asked and the number of times the one-dimensional SIS question that needs to be asked to crack the SIS problem collides with the oracle. In the end, the number of times the two are obtained is "roughly the same" in terms of probability, so this illustrates the connection between the Ring-SIS problem and the SIS problem.

Although the demonstration of this proof in this article may not be sufficient, one thing we are sure of is that the one-dimensional SIS problem is difficult, and the difficulty of the Ring-SIS problem is not lower than that of the one-dimensional SIS problem, but not higher than that of the SIS problem.

1.1.3 Ring-SIS to Ring-LWE Reduction

Let $n \geq 1$, and $p = p(n) \leq \text{poly}(n)$ be prime numbers, now consider a set of 'equations of with error'

$$\begin{aligned} \langle s, a_1 \rangle &\approx_\chi b_1 (\text{mod} q), \\ \langle s, a_2 \rangle &\approx_\chi b_2 (\text{mod} q), \\ &\vdots \\ \langle s, a_n \rangle &\approx_\chi b_n (\text{mod} q). \end{aligned}$$

Among them, $s \in \mathcal{M}_{m\times 1}(\mathbb{Z}_q)$, a_i is in $\mathcal{M}_{m\times 1}(\mathbb{Z}_q)$ independently selected uniformly, $b_i \in \mathbb{Z}_q$. There is a perturbation $e_i \in_R \chi \subset \mathbb{Z}_q$ in the above equation such that for each i, there are $b_i = \langle s, a_i \rangle + e_i$. We put these n 'equations of with error' together and get

$$b = As + e, \text{ here } b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}, A = \begin{pmatrix} a_1^T \\ a_2^T \\ \vdots \\ a_n^T \end{pmatrix}, e = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}. \tag{1}$$

The learning with error problem $\text{LWE}_{q,\chi}$ refers to finding s from (1). This problem occupies a very important position in the hardness assumptions of lattice cryptography, so that various variants based on the LWE problem have been proposed accordingly. For example, the learning with rounding problem [BPR12], the Evasive learning with error problem [Wee22], and the learning parity with noise problem [MP13] etc.

In 2005, Regev gave a proof of the difficulty of the LWE problem. So for the connection between the LWE problem and the SIS problem [Yuea, Yueb], we have that when there is an oracle that can solve the LWE problem within a time polynomial, there is also an effective algorithm that can solve the SIS problem. This is because for the LWE problem $b = As + e$, where $A \in \mathcal{M}_{m\times n}(\mathbb{Z}_q)$, $s \in \mathcal{M}_{m\times 1}(\{0, \pm 1\})$, and $e_i \in \chi$. So we can use the collision-resolving oracle of the LWE problem to query $b - e = As$ twice, and get $As_1 = b - e = As_2 (s_1, s_2 \in \{0, 1\})$, so we have $Au = A(s_1 - s_2) = 0 (u \in \{0, \pm 1\})$, at this time u is the solution to the SIS problem.

Then the same relationship exists between Ring-SIS and Ring-LWE. The difference is that the Ring-LWE problem is only "one-dimensional", that is, finding the polynomial s from $b = as+e$, where $a, s \in \mathcal{R}_q$, and $x \leftarrow \chi$. The Ring-SIS problem is to solve m polynomials. In fact, the encryption scheme based on the Ring-LWE problem also requires multiple $b = as + e$ to set the public key and private key, so the relationship between m Ring-LWE problems and Ring-SIS is the same as the LWE problem and SIS The relationship between the problems is consistent.

2 Preliminaries

Lattice. Each element of a lattice in $\mathbb{R}^n$ can be expressed linearly by n linearly independent vector integer coefficients. This set of linearly independent vectors is called a lattice basis, and we know that the lattice basis is not unique. Given a set of lattice bases $(v_1, \ldots, v_n)$ in the lattice $\mathcal{L}$, then the fundamental parallelelepiped is

$$\mathcal{P}(v_1, \ldots, v_n) = \left\{ \sum_{i=1}^{n} k_i v_i \middle| k_i \in [0, 1) \right\}.$$

If the lattice base $(v_1, \ldots, v_n)$ is determined, we can use the symbol $\mathcal{P}(\mathcal{L})$ to replace $\mathcal{P}(v_1, \ldots, v_n)$. $\forall x \in \mathbb{R}^n$, we can project it onto $\mathcal{P}(\mathcal{L})$. According to the properties of projection [CZY22], there is a unique $y \in \mathcal{P}(\mathcal{L})$ makes $y - x \in \mathcal{L}$. We use the symbol $\det(\mathcal{L})$ to represent the volume of the fundamental parallelelepiped of the lattice $\mathcal{L}$. In other words, the symbol $\det(\mathcal{L})$ represents the determinant of a

matrix composed of a set of lattice bases $(v_1, \ldots, v_n)$. For a given n dimensional lattice, the $\det(\mathcal{L})$ size of any set of lattice bases of the lattice is constant. We simply prove this theorem.

Given n lattice $\mathcal{L}$, $(v_1, \ldots, v_n)$ and $(u_1, \ldots, u_n)$ are two arbitrary groups of lattice $\mathcal{L}$ respectively lattice bases. Therefore we have $v_i = \sum_{j=1}^{n} m_{ij} u_j$ and $u_i = \sum_{j=1}^{n} m'_{ij} v_j, i \in \{1, \ldots, n\}$, therefore there are two integer matrices M and M' such that

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = M \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} \text{ and } \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = M' \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

It is easy to prove that M and M' are inverse to each other, and M and M' are both integer matrices, so there are $\det(M)\det(M') = 1$ and $\det(M) = \det(M') = \pm 1$, so $\det(v_1, \ldots, v_n) = \pm \det(u_1, \ldots, u_n)$.

Isomorphic mapping of polynomial $\mathbb{Z}[x]/<x^n + 1>$ to ideal lattice $\mathcal{I}$.

Definition 1. *An ideal lattice is a subset of rings or domains that satisfies the following two properties:*

1. *Additive closure: If any two elements in the ideal are added, the result is still in the ideal. In other words, for any elements a and b in the ideal, $a + b$ also belongs to that ideal.*
2. *Multiplicative absorptivity: If an element in the ideal is multiplied by any element in the ring (or field), the result is still in the ideal. In other words, for any element a in the ideal and any element r in the ring (or field), ar and ra belong to that ideal.*

For a commutative ring, we can further require that the ideal be closed for both addition and multiplication. Such an ideal is called a true ideal.

Definition 2. *Referring to the definition of ideal, the ideal lattice $\mathcal{I}$ is a subset of the lattice $\mathcal{L}$ that satisfies the following two properties:*

1. *Additive closure: If any two elements in an ideal lattice are added, the result is still in the ideal lattice. In other words, for any elements a and b in an ideal lattice, $a + b$ also belongs to that ideal lattice.*
2. *Multiplicative absorptivity: If an element in an ideal lattice is multiplied by an element in any other ideal lattice, the result remains in the ideal lattice. In other words, for any element a in the ideal and any element r in another ideal lattice, both ar and ra belong to that ideal lattice.*

Corollary 1. *The ideal lattice $\mathcal{I}$ is a true idea of the lattice $\mathcal{L}$.*

For $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ is mapped to

$$Rot(f) = a_0 I + a_1 X + \cdots + a_{n-1} X^{n-1} \in \tilde{\mathcal{R}}.$$

Among them, $\tilde{\mathcal{R}}$ is the mapping of all $\mathbb{Z}[x]/<x^n + 1>$ to the elements in the ideal lattice $\mathcal{I}$ collection, and

$$X = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

So there is

$$Rot(f) = \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix},$$

it is easy to prove that this mapping relationship is isomorphic.

SIS problem [Ajt96, dZ]. Given the integers n, m, q and the positive number β. The shortest integer solution problem is to randomly select vector $\alpha_i \in \mathcal{M}_{n\times 1}(\mathbb{Z}_q)$, $m \in \{1,\ldots,m\}$. The matrix $A \in \mathcal{M}_{n\times m}(\mathbb{Z}_q)$, find the non-zero integer coefficient vector $z \in \mathcal{M}_{m\times 1}(\mathbb{Z}_q)$, $\|z\| \le \beta$, such that

$$f_A(z) := Az = \sum_i^m \alpha_i z_i = 0 \in \mathbb{Z}_q^n.$$

Given the lattice $\mathcal{L}$, the representation of the SIS problem on the lattice is

$$\mathcal{L}^{\perp}(A) = \{z \in \mathbb{Z}^m : Az = 0 \in \mathbb{Z}_q^n\}.$$

A variant of the SIS problem

$$\mathcal{L}_u^{\perp}(A) = \{z \in \mathbb{Z}^m : Az = u \in \mathbb{Z}_q^n\} = c + \mathcal{L}^{\perp}(A).$$

Among them, c is the solution of any non-homogeneous SIS, that is, $Ac = u$. The variant of the SIS problem are usually used to construct the one-way trapdoor function of encryption schemes.

Ring-SIS problem [Yuec, LPR10]. Given $f_1, \ldots, f_m \in \mathcal{R}_q$, where $\mathcal{R}_q$ is a polynomial ring with modulus q, find m polynomials $g_1, \ldots,$ whose coefficients are not all 0, $g_m \in \mathcal{R}_{\{0,\pm 1\}}$, such that

$$f_1 g_1 + \cdots + f_m g_m = 0 \bmod q\mathcal{R}.$$

In $\mathbb{Z}[x]/<x^n - 1>$, the Ring-SIS problem is not difficult. The reason is that $x^n - 1$ is reducible, that is

$$x^n - 1 = (1 - x)(1 + x + x^2 + \cdots + x^{n-1}).$$

We let $\tilde{g}(x) := 1 + x + x^2 + \cdots + x^{n-1} \in \mathbb{Z}[x]/<x^n - 1>$, so there is

$$(1 - x)\tilde{g}(x) = x^n - 1 = 0. \tag{2}$$

On the other hand, for the Ring-SIS problem $\mathcal{F}(x) = (f_1(x), f_2(x), \ldots, f_m(x))$. That is, find $\mathcal{G}(x) = (g_1(x), g_2(x), \ldots, g_m(x))$, such that

$$\mathcal{F}(x)\mathcal{G}(x) = \sum_{i=1}^m f_i g_i = 0.$$

We let $\mathcal{G}(x) = (\tilde{g}(x), 0, \ldots, 0)$, if for the solution of $\mathcal{F}(x)$ is $\mathcal{G}(x)$, only $f_1(x)\tilde{g}(x) = 0 \bmod q\mathcal{R}$.

So what kind of $\tilde{g}(x)$ can satisfy this condition?

In fact, we assume that $f_1(x)$ is a multiple of the polynomial $x - 1$, that is, $f_1(x) = f'(x)(x - 1)$ then there is

$$f_1(x)\tilde{g}(x) = f'(x)(x - 1)\tilde{g}(x) = 0 \bmod q\mathcal{R}.$$

In other words, as long as $f_1(x) = f'(x)(x - 1)$ is satisfied, it is the solution of $\mathcal{F}(x)$. So what is the probability of this happening? We have the following lemma.

Lemma 1. *If $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ is a multiple of $(x - 1)$, then $\sum_{i=0}^{n-1} a_i = 0$.*

Proof. We use mathematical induction. When $n = 1$, if $f(x) = f'(x)(x - 1)$, then $f'(x) = \lambda \in \mathbb{Z}_q$. At this time, there is

$$f(x) = \lambda - \lambda x = a_0 + a_1 x,$$

so there is $a_0 + a_1 = 0$. Assume that it is true when $n = k$. When $n = k + 1$, we assume that $f'(x) = b_0 + b_1 x + \cdots + b_k x^k$ and

$$\begin{aligned} f(x) = f'(x)(x - 1) &= (b_0 + b_1 x + \cdots + b_k x^k)(x - 1) \\ &= (b_0 + b_1 x + \cdots + b_{k-1}x^{k-1})(x - 1) + b_k x^k(x - 1) \\ &= \underbrace{a_0 + a_1 x + \cdots + a_k x^k}_{\text{(a)}} + \underbrace{b_k x^k(x - 1)}_{\text{(b)}}. \end{aligned}$$

Because it is true when $k = n$, then the sum of the coefficients of the (a) equation is 0, and it is easy to prove that the sum of the coefficients of the (b) equation is also 0. Therefore, the proposition is true. □

Lemma 2 ([Yuec])**.** *If* $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in \mathbb{Z}_q[x]$*, then the probability of* $\sum_{i=0}^{n-1} a_i = 0$ *occurring is* $1/q$*.*

Since the first $n-1$ coefficients are all random numbers in the integer ring $\mathbb{Z}_q$, so $\sum_{i=0}^{n-2} a_i$ is also in the integer ring $\mathbb{Z}_q$ random number. Randomly select a_{n-1}, then the probability of satisfying $\sum_{i=0}^{n-1} a_i = 0$ is $1/q$. The cracking probability of $1/q$ is very large for password security, so the Ring-SIS problem of polynomial $\mathbb{Z}[x]/<x^n - 1>$ is not difficult for the security of the password scheme.

Lemma 3. *If* $f(x)g(x) = (a_0+a_1x+\cdots a_{n-1}x^{n-1})(b_0+b_1x+\cdots b_{n-1}x^{n-1}) \bmod (x^n+1) = 0$*, then there is* $f_{t,k}(x)g_{t,k}(x) = (a_0x^k+a_1x^{k+t}+\cdots a_{n-1}x^{k+(n-1)t})(b_0x^k+b_1x^{k+t}+\cdots b_{n-1}x^{k+(n-1)t}) \bmod (x^{nt}+1) = 0$*, where* $k \in [0, t)$*.*

Proof. According to the conditions, because $f(x)g(x) = (a_0+a_1x+\cdots a_{n-1}x^{n-1})(b_0+b_1x+\cdots b_{n-1}x^{n-1}) \bmod (x^n + 1) = 0$, so there is

$$\begin{array}{lll} & \left(a_0b_0 + (-1)\sum_{j=1}^{n-1} a_jb_{n-j}\right) & \\ + & \left(\sum_{i=1}^{2} a_{i-1}b_{2-i} + (-1)\sum_{j=2}^{n-1} a_jb_{n+1-j}\right) & x \\ + & \left(\sum_{i=1}^{3} a_{i-1}b_{3-i} + (-1)\sum_{j=3}^{n-1} a_jb_{n+2-j}\right) & x^2 \qquad \bmod (x^n + 1) = 0. \\ \vdots & & \\ + & \left(\sum_{i=1}^{n} a_{i-1}b_{n-i}\right) & x^{n-1} \end{array}$$

So we get

$$\begin{array}{lll} & \left(a_0b_0 + (-1)\sum_{j=1}^{n-1} a_jb_{n-j}\right) & x^{2k} \bmod (x^{nt} + 1) \\ + & \left(\sum_{i=1}^{2} a_{i-1}b_{2-i} + (-1)\sum_{j=2}^{n-1} a_jb_{n+1-j}\right) & x^{2k+t} \bmod (x^{nt} + 1) \\ + & \left(\sum_{i=1}^{3} a_{i-1}b_{3-i} + (-1)\sum_{j=3}^{n-1} a_jb_{n+2-j}\right) & x^{2k+2t} \bmod (x^{nt} + 1) \qquad = 0. \\ \vdots & & \\ + & \left(\sum_{i=1}^{n} a_{i-1}b_{n-i}\right) & x^{2k+(n-1)m} \bmod (x^{nt} + 1) \end{array}$$

□

Corollary 2. *Let* $F^T(x) := (f^{(1)}(x), f^{(2)}(x), \cdots, f^{(m)}(x))$*,* $G(x) := (g^{(1)}(x), g^{(2)}(x), \cdots, g^{(m)}(x))$*, if there is*

$$F^T(x)G(x) = \sum_{i}^{m} f^{(l)}(x)g^{(l)}(x) \bmod (x^n + 1) = 0.$$

Then for $F^T_{t,k}(x) := (f^{(1)}_{t,k}(x), f^{(2)}_{t,k}(x), \cdots, f^{(m)}_{t,k}(x))$*,* $G(x) := (g^{(1)}_{t,k}(x), g^{(2)}_{t,k}(x), \cdots, g^{(m)}_{t,k}(x))$*, there are*

$$F^T_{t,k}(x)G_{t,k}(x) = \sum_{l}^{\mathrm{m}} f^{(l)}_{t,k}(x)g^{(l)}_{t,k}(x) \bmod (x^{nt} + 1) = 0.$$

Among them, $k \in [0, t)$*.*

Proof. Let the lth component (polynomial) of $F^T(x)$ be

$$f^{(l)}(x) := a^{(l)}_0 + a^{(l)}_1 x + \cdots a^{(l)}_{n-1}x^{n-1}.$$

So we get

$$
\begin{aligned}
F^T(x)G(x) &= \sum_{l}^{n} f^{(l)}(x)g^{(l)}(x) \\
&= \sum_{l}^{\mathrm{m}} \left(a_0^{(l)}b_0^{(l)} + (-1)\sum_{j=1}^{n-1} a_{j=1}^{(l)}b_{n-j}^{(l)}\right) \\
&+ \sum_{l}^{\mathrm{m}} \left(\sum_{i=1}^{2} a_{i-1}^{(l)}b_{2-i}^{(l)} + (-1)\sum_{j=2}^{n-1} a_j^{(l)}b_{n+1-j}^{(l)}\right) \quad x \\
&+ \sum_{l}^{\mathrm{m}} \left(\sum_{i=1}^{3} a_{i-1}^{(l)}b_{3-i}^{(l)} + (-1)\sum_{j=3}^{n-1} a_j^{(l)}b_{n+2-j}^{(l)}\right) \quad x^2 \qquad \bmod (x^n+1) = 0. \\
&\vdots \\
&+ \sum_{l}^{\mathrm{m}} \left(\sum_{i=1}^{n} a_{i-1}^{(l)}b_{n-i}^{(l)}\right) \quad x^{n-1}
\end{aligned}
$$

And we have

$$
\begin{aligned}
F_{t,k}^T(x)G_{t,k}(x) &= \sum_{l}^{\mathrm{m}} f_{t,k}^{(l)}(x)g_{t,k}^{(l)}(x) \bmod (x^{nt}+1) \\
&= \sum_{l}^{\mathrm{m}} \left(a_0^{(l)}b_0^{(l)} + (-1)\sum_{j=1}^{n-1} a_j^{(l)}b_{n-j}^{(l)}\right) \quad x^{2k} \bmod (x^{nt}+1) \\
&+ \sum_{l}^{\mathrm{m}} \left(\sum_{i=1}^{2} a_{i-1}^{(l)}b_{2-i}^{(l)} + (-1)\sum_{j=2}^{n-1} a_j^{(l)}b_{n+1-j}^{(l)}\right) \quad x^{2k+t} \bmod (x^{nt}+1) \\
&+ \sum_{l}^{\mathrm{m}} \left(\sum_{i=1}^{3} a_{i-1}^{(l)}b_{3-i}^{(l)} + (-1)\sum_{j=3}^{n-1} a_j^{(l)}b_{n+2-j}^{(l)}\right) \quad x^{2k+2t} \bmod (x^{nt}+1) \qquad = 0. \\
&\vdots \\
&+ \sum_{l}^{\mathrm{m}} \left(\sum_{i=1}^{n} a_{i-1}^{(l)}b_{n-i}^{(l)}\right) \quad x^{2k+(n-1)t} \bmod (x^{nt}+1)
\end{aligned}
$$

□

Lemma 4. *When* $f(x)g(x) \bmod (x^n+1) = 0$, $f(x)g(x)x \bmod (x^n+1) = 0$. *More generally , if* $\sum_{i=1}^{m} f(x)g(x) \bmod (x^n+1) = 0$, $\sum_{i=1}^{m} f(x)g(x)x \bmod (x^n+1) = 0$.

Proof. When $f(x)g(x) \bmod (x^n+1) = 0$, we have

$$
\begin{aligned}
&\left(a_0b_0 + (-1)\sum_{j=1}^{n-1} a_jb_{n-j}\right) \\
+ &\left(\sum_{i=1}^{2} a_{i-1}b_{2-i} + (-1)\sum_{j=2}^{n-1} a_jb_{n+1-j}\right) \quad x \\
+ &\left(\sum_{i=1}^{3} a_{i-1}b_{3-i} + (-1)\sum_{j=3}^{n-1} a_jb_{n+2-j}\right) \quad x^2 \qquad \bmod (x^n+1) = 0. \\
&\vdots \\
+ &\left(\sum_{i=1}^{n} a_{i-1}b_{n-i}\right) \quad x^{n-1}
\end{aligned}
$$

Therefore, there is

$$
\begin{aligned}
0 &= \left(a_0b_0 + (-1)\sum_{j=1}^{n-1} a_jb_{n-j}\right) \\
&= \left(\sum_{i=1}^{2} a_{i-1}b_{2-i} + (-1)\sum_{j=2}^{n-1} a_jb_{n+1-j}\right) \\
&\vdots \\
&= \left(\sum_{i=1}^{n} a_{i-1}b_{n-i}\right).
\end{aligned}
$$

So, we know that

$$
\left(
\begin{aligned}
&\left(a_0b_0 + (-1)\sum_{j=1}^{n-1} a_jb_{n-j}\right) \\
+ &\left(\sum_{i=1}^{2} a_{i-1}b_{2-i} + (-1)\sum_{j=2}^{n-1} a_jb_{n+1-j}\right) \quad x \\
+ &\left(\sum_{i=1}^{3} a_{i-1}b_{3-i} + (-1)\sum_{j=3}^{n-1} a_jb_{n+2-j}\right) \quad x^2 \\
&\vdots \\
+ &\left(\sum_{i=1}^{n} a_{i-1}b_{n-i}\right) \quad x^{n-1}
\end{aligned}
\right) x \bmod (x^n+1) = 0.
$$

According to the Corollary 2, if $\sum_{i=1}^{m} f(x)g(x) \bmod (x^n+1) = 0$, then $\sum_{i=1}^{m} f(x)g(x)x \bmod (x^n+1) = 0$. □

Corollary 3. *When* $f(x)g(x) \bmod (x^n+1) = 0$, $f(x)g(x)x^k \bmod (x^n+1) = 0$. *More generally, if* $\sum_{i=1}^{m} f(x)g(x) \bmod (x^n+1) = 0$, $\sum_{i=1}^{m} f(x)g(x)x^k \bmod (x^n+1) = 0$, $k \in \mathbb{Z}$.

3 Hardness of Ring-SIS with Small Modulus

Lemma 5. *For any integer* m, q, *even number* n *and* $\mathcal{X} \subset \mathcal{M}_{m\times 1}(\widetilde{\mathcal{R}}_q)$, *such that* $\forall x, x' \in \mathcal{X}$, *there are* $\gcd(x-x', q) = 1$ *and* $\|x-x'\| \leq \beta$. *Then if there is a collision-resolving query oracle* $\mathcal{W}$ *for* Ring-SIS$(m, n^k, q, \mathcal{X})$, *then there is also a solution* Ring-SIS$(m, n^{k+1}, q^{k+1}, \beta^{k+1})$ *algorithm, and ask the number of oracle* $\mathcal{W}$ *at least* n.

Proof. According to the definition of the Ring-SIS$(m, n^{k+1}, q^{k+1}, \beta^{k+1})$ problem, we can think that we find solution

$$G(x) := (g^1(x), g^2(x), \cdots, g^m(x)), g^i(x) \in \mathbb{Z}_q[x]/<x^{n^{k+1}}+1>, i \in \{1, \ldots, m\}.$$

Make $F^T(x)G(x) = 0$, where

$$F(x) := (f^1(x), f^2(x), \cdots, f^m(x)), f^i(x) \in \mathbb{Z}_q[x]/<x^{n^{k+1}}+1>, i \in \{1, \ldots, m\}.$$

We use the method of Definition 7 in the Appendix to Ring-SIS$(m, n^{k+1}, q^{k+1}, \beta^{k+1})$ extracts the first Ring-SIS$(m, n^k, q, \mathcal{X})$, that is

$$(\underline{F}^{(0)})^T(x) := (\underline{f}^{(1,0)}(x), \underline{f}^{(2,0)}(x), \cdots, \underline{f}^{(m,0)}(x)), \underline{f}^{(i,0)}(x) \in \mathbb{Z}_q[x]/<x^{n^k}+1>, i \in \{1, \ldots, m\}.$$

Here,

$$\underline{f}^{(i,0)}(x) = \underline{a}_0^{(i,0)} + \underline{a}_1^{(i,0)}x + \cdots \underline{a}_{n^k-1}^{(i,0)}x^{n^k-1}.$$

And use the collision-resolving query oracle $\mathcal{W}$ of Ring-SIS$(m, n^k, q, \mathcal{X})$ to $\underline{G}^{(0)}(x)$ is used to find m solutions, and

$$\underline{G}^{(0)}(x) := (\underline{g}^{(1,0)}(x), \underline{g}^{(2,0)}(x), \cdots, \underline{g}^{(m,0)}(x)),$$
$$\underline{g}^{(i,0)}(x) \in \mathbb{Z}_q[x]/<x^{n^k}+1>, i \in \{1, \ldots, n\}$$

is obtained. Where,

$$\underline{g}^{(i,0)}(x) = b_0^{(i,0)} + b_1^{(i,0)}x + \cdots b_{n^k-1}^{(i,0)}x^{n^k-1}.$$

We will turn it into

$$g^{(i,0)}(x) = b_0^{(i,0)} + b_1^{(i,0)}x^n + \cdots + b_{n^k-1}^{(i,0)}x^{(n^k-1)n}.$$

Construct

$$G^{(0)}(x) := (g^{(1,0)}(x), g^{(2,0)}(x), \cdots, g^{(m,0)}(x)), g^{(i,0)}(x) \in \mathbb{Z}_q[x]/<x^{n^k}+1>, i \in \{1, \ldots, n\}.$$

According to the Corollary 2, we have $(\underline{F}^{(0)}(x))^T\underline{G}^{(0)}(x) = 0$. We let

$$F(x) := (f^{(1)}(x), f^{(2)}(x), \cdots, f^{(m)}(x)), f^{(i)}(x) \in \mathbb{Z}_q[x]/<x^{n^{k+1}}+1>, i \in \{1, \ldots, m\}.$$

Among them,

$$f^{(i)}(x) = \mathcal{F}_0^{(i)} + \cdots + \mathcal{F}_{n-1}^{(i)}, \mathcal{F}_\lambda = a_0x^\lambda + a_1x^{\lambda+n} + \cdots + a_{n^k-1}x^{\lambda+(n^k-1)n}, \lambda \in \{1, \ldots, n\}.$$

So we set $F(x) = F^{(0)}(x)$, and calculate

$$F^{(1)}(x) = ((F^{(0)}(x))^T G_1^{(0)}(x), \underbrace{0, \ldots, 0}_{m-1}),$$
$$(F^{(0)}(x))^T G_i^{(0)}(x) \in \mathbb{Z}_q[x]/<x^{n^{k+1}}+1>, i \in \{1, \ldots, m\}.$$

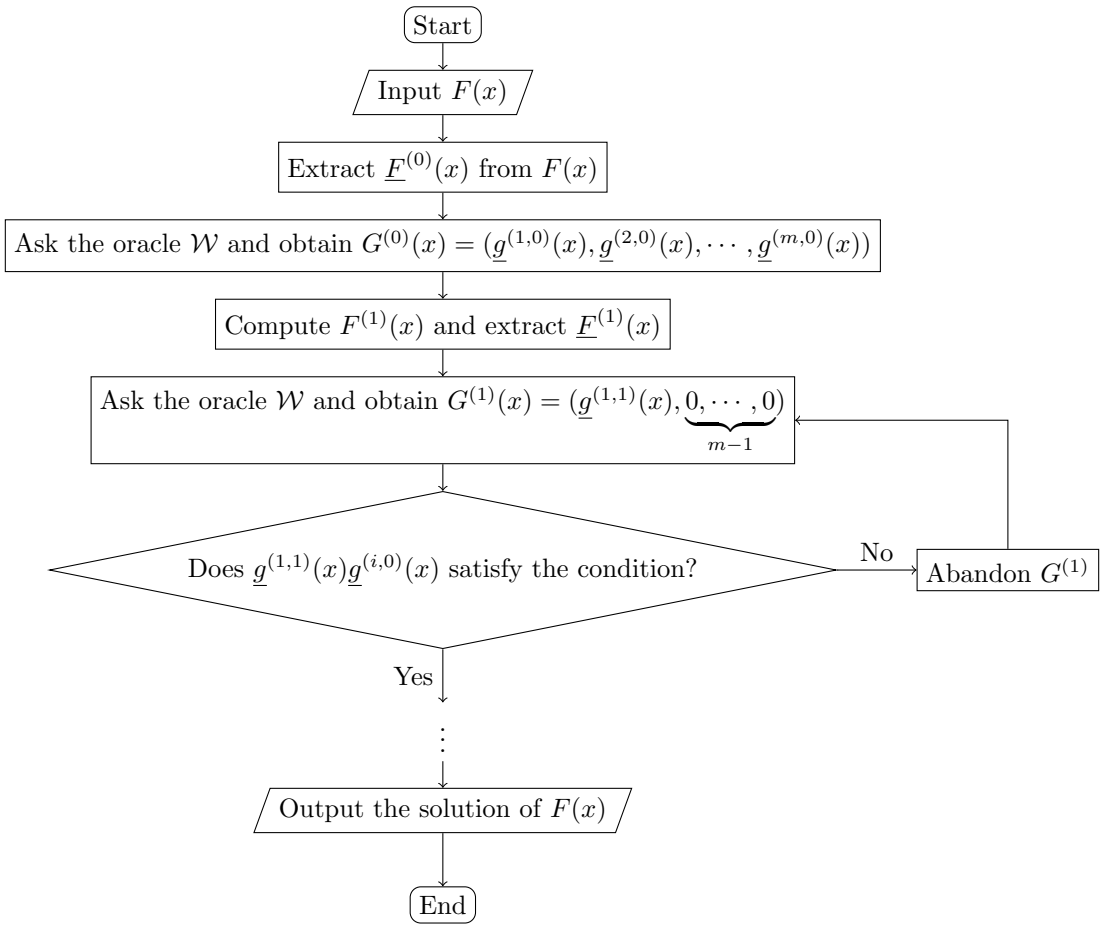


Figure 1: Solution Ring-SIS$(m, n^{k+1}, q^{k+1}, \beta^{k+1})$ algorithm

This is still a Ring-SIS$(m, n^{k+1}, q^{k+1}, \beta^{k+1})$ problem. But what is different from $F(x)$ is that since $(\underline{F}^{(0)}(x))^T \underline{G}^{(0)}(x) = 0$, so the polynomials in $F^{(1)}(x)$ all have less n^k terms.

Continue to follow the above method until finally each polynomial of $F^{(n-1)}(x)$ has only n^k terms left, so it can be solved by using the oracle again and determine if the product with the previous solution belongs to $\mathcal{R}_{\{0,\pm 1\}}$. According to this method to solve the Ring-SIS$(m, n^{k+1}, q^{k+1}, \beta^{k+1})$ problem, then we ask the oracle at least

$$\left(\frac{n^{k+1} - n^k}{n^k}\right) + 1 = n(\text{times}).$$

□

Remark 1. *According to the above process, it can be summarized as*

$$G(x) = (\tilde{g}_1, \ldots, \tilde{g}_m).$$

Here,

$$\tilde{g}_i = \prod_{j=1}^{n} g^{(1,j)} \left(\sum_{i=1}^{m} g^{(i,0)}\right).$$

3.1 Ring-SIS to Ring-SIS Reduction

Lemma 6. *For any integer n, m, q and $\mathcal{X} \subset \mathcal{M}_{m\times 1}(\widetilde{\mathcal{R}}_q)$, such that $\forall x, x' \in \mathcal{X}$, there are $\gcd(x - x', q) = 1$ and $\|x - x'\| \leq \beta$. Then for the integer c, we have a direct reduction from the collision-resolving query algorithm of* Ring-SIS(m, n^c, q^c, β^c) *to the collision-resolving query algorithm of* Ring-SIS$(m, n, q, \mathcal{X})$. *This algorithm reduces in polynomial time of its input size and makes $(n^{c-1} - 1) + 1$ calls to its oracle.*

Proof. See the appendix for detailed proof. □

Lemma 7. *For any integer m, q, even number n and $\mathcal{X} \subset \mathcal{M}_{m\times 1}(\widetilde{\mathcal{R}}_q)$, such that $\forall x, x' \in \mathcal{X}$, there are $\gcd(x - x', q) = 1$ and $\|x - x'\| \leq \beta$. Then for the integer c, we have a direct reduction from the collision-resolving query algorithm of* Ring-SIS(m^c, n, q, β) *to the collision-resolving query algorithm of* Ring-SIS$(m, n, q, \mathcal{X})$. *This algorithm reduces in polynomial time of its input size and makes m^{c-1} calls to its oracle at least.*

Proof. Suppose $F(x) = (f_1(x), f_2(x), \ldots, f_{m^c}(x))$, which is divided into m^{c-1} parts, that is

$$\begin{aligned} F_1(x) &= \big(f_1(x), f_2(x), \ldots, f_m(x)\big), \\ F_2(x) &= \big(f_{m+1}(x), f_{m+2}(x), \ldots, f_{2m}(x)\big), \\ &\vdots \\ F_{m^{c-1}}(x) &= \big(f_{m^c-m+1}(x), f_{m^c-m+2}(x), \ldots, f_{m^c}(x)\big). \end{aligned}$$

So $F_i(x)$ is Ring-SIS$(m, n, q, \mathcal{X})$ question, $i \in \{1, 2, \ldots, m^{c-1}\}$. So we only need to ask m^{c-1} times Ring-SIS$(m, n, q, \mathcal{X})$ collision-resolving oracle to solve Ring-SIS(m^c, n, q, β) question. □

Remark 2. *When n and m are close, the conclusions of Lemma 6 and Lemma 7 are "roughly the same" from the perspective of the collision-resolving oracle querying* Ring-SIS$(m, n, q, \mathcal{X})$. *But in fact, the computational complexity of Lemma 6 is much greater than that of Lemma 7. Therefore, assuming that* Ring-SIS$(m, n, q, \mathcal{X})$ *is attacked one day, it is far safer to increase the order of the polynomial than to increase the number of polynomials (or the dimension of* Ring-SIS$(m, n, q, \mathcal{X})$*).*

3.2 Direct Reduction

Lemma 8. *$As = 0$, is equivalent to $xB = 0$. Where $A \in \mathcal{M}_{n\times m}(\mathbb{Z})$, $s \in \mathcal{M}_{m\times 1}(\mathbb{Z})$; $x \in \mathcal{M}_{1\times m}(\mathbb{Z})$,$B \in \mathcal{M}_{m\times n}(\mathbb{Z})$.*

Lemma 9. *If space A and space B are isomorphic, then if $\mathcal{A}$ in space A is an abstract difficult problem, if and only if $\mathcal{B}$ in the corresponding space B is also a difficult question.*

Proof. Assuming that spaces A and B are isomorphic, we denote an abstract difficult problem in space A as $\mathcal{A}$ and the corresponding problem in space B as $\mathcal{B}$. By the definition of isomorphism, there exists a bijective function $f : A \to B$ that preserves the structure and properties in A. Therefore, we can map elements in A to elements in B through f. Now let us prove that if $\mathcal{A}$ is a hard problem, then $\mathcal{B}$ is also a hard problem: Suppose in the space A, for the problem $\mathcal{A}$, we suppose there is a polynomial-time algorithm that solves $\mathcal{A}$. That is, we can compute in polynomial time a result that satisfies $\mathcal{A}$ in A. According to the definition of isomorphism, we can define a mapping function $h : A \to B$, where $h(a) = f(a)$. Since f is a bijective function, h is also a bijective function.

Now let us consider the problem $\mathcal{B}$ in the space B. Given an input x', we can map it back to the space A through the inverse mapping h^{-1} of the function h, and get the corresponding input $x = h^{-1}(x')$. We can then compute the result that satisfies $\mathcal{A}$ in space A using a polynomial-time algorithm that solves problem $\mathcal{A}$ in space A. Finally, we map the result back to the space B through the function h, and get the result that satisfies $\mathcal{B}$ in the space B. The entire process can be completed in polynomial time.

Therefore, if $\mathcal{A}$ is a hard problem, then $\mathcal{B}$ is also a hard problem. □

Lemma 10. *If space A and space B are isomorphic, space C and space D are isomorphic. Then space $A \times B$ and space $C \times D$ are also isomorphic.*

Proof. First, we know that A and B are isomorphic, then there is a bijection $f : A \to B$ that preserves the operations and inverse operations in A. Similarly, we know that C and D are isomorphic, and there exists a bijection $g : C \to D$ that preserves the operations and inverse operations in C. We can define a new mapping $h : A \times B \to C \times D$, mapping the elements (a, b) in $A \times B$ to the elements in $C \times D$ (c, d), where $c = f(a)$ and $d = g(b)$.

Now we show that h is a bijective function.

1. **Mapping is injective**. Suppose there are two different elements $(a1, b1)$ and $(a2, b2)$ belonging to $A \times B$, and $h(a1, b1) = h(a2, b2)$. Then according to the definition of h, $f(a1) = f(a2)$ and $g(b1) = g(b2)$. Since f and g are both bijective functions, we can get $a1 = a2$ and $b1 = b2$. Therefore, h is injective.

2. **Mapping is surjective**. For any (c, d) belonging to $C \times D$, we can choose $a = f^{-1}(c)$ and $b = g^{-1}(d)$ to construct element (a, b) belongs to $A \times B$. By definition, $h(a, b) = (f(a), g(b)) = (c, d)$. Therefore, h is surjective.

3. **Mapping is homomorphic**. Assume $(a1, b1)$ and $(a2, b2)$ belong to $A \times B$, let us prove that $h((a1, b1) + (a2, b2)) = h(a1, b1) + h(a2, b2)$ and $h(-(a1, b1)) = -(h(a1, b1))$. From the definitions of vector addition and scalar multiplication and the properties of f and g we can get these two equations. Therefore, h holds operations and inverse operations.

In summary, we proved that there is a bijective function mapping the elements in $A \times B$ to the elements in $C \times D$, and this mapping preserves operations and inverse operations. Therefore, $A \times B$ is isomorphic to $C \times D$. □

Lemma 11. *If space A, space B and space E are isomorphic, space C, space D and space F are isomorphic. Then space $A \times B \times E$ It is also isomorphic to the space $C \times D \times F$.*

Proof. According to Lemma 10, we know that if space A and space B are isomorphic, space C and space D are isomorphic. Then the space $A \times B$ and the space $C \times D$ are also isomorphic. That is, there is a mapping $h : A \times B \to C \times D$, such that the mapping is homomorphic and one to one. So we let the space $X := A \times B$ and the space $Y := C \times D$, so the space X and the space Y are isomorphic. Combined with the Lemma 10 , we have the space $A \times B \times E$ and the space $C \times D \times F$ which are also isomorphic. □

Lemma 12 ([MP13], TH3.8)**.** *Let m, n be integers, $\beta \geq \beta_\infty > 0$ be real numbers, and $q \geq \beta \cdot n^{\Omega(1)}$ be the modulus of an integer numbers with no more than* $\mathrm{poly}(n)$ *integer divisors less than β_∞, set $S = \{z \in \mathcal{M}_{m\times 1}(\mathbb{Z}) \setminus \{0\} | \, \|z\| \leq \beta \wedge \|z\|_\infty \leq \beta_\infty\}$. Then for $\gamma = \max\{1, \beta\beta_\infty/q\} \cdot O(\beta\sqrt{n})$, there is a difficult problem from n dimensional lattice efficient reduction of the $S-$collision-resolving search algorithm in* $\mathrm{SIS}(m, n, q)$ *from* $\mathrm{SIVP}_\gamma^\eta$.

Corollary 4 (When $n = 1$, the case of Lemma 12, we call it the *one-dimensional* SIS *problem*)**.** *Let m be an integer, $\beta \geq \beta_\infty > 0$ be a real number, and $q \geq \beta$ be the modulus of an integer with no more than* $\mathrm{poly}(1)$ *integer divisors less than β_∞, the set $S = \{z \in \mathcal{M}_{m\times 1}(\mathbb{Z}) \setminus \{0\} | \, \|z\| \leq \beta \wedge \|z\|_\infty \leq \beta_\infty\}$. Then for $\gamma = \max\{1, \beta\beta_\infty/q\} \cdot O(\beta\sqrt{n})$, there is a difficult problem from n dimensional lattice efficient reduction of the $S-$collision-resolving search algorithm in* $\mathrm{SIS}(m, 1, q)$ *from* $\mathrm{SIVP}_\gamma^\eta$.

Definition 3 (Knapsack Problem[MH78])**.** *Given an integer set $a = (a_1, \ldots, a_n)$ and an integer z, find a solution $s = (s_1, \ldots, s_n)$ such that $\sum_{i=1}^n a_i s_i = z$, where $s_i \in \{0, 1\}$.*

Definition 4 (Variant Knapsack Problem)**.** *Given an integer set $a = (a_1, \ldots, a_n)$ and an integer z, find a solution $s = (s_1, \ldots, s_n)$ such that $\sum_{i=1}^n a_i s_i = z$, where $s_i \in \{0, \pm 1\}$.*

Definition 5 (One-dimensional SIS variant problem)**.** *For* $\alpha^T = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{M}_{mn\times 1}(\mathbb{Z}_q)$, $\alpha_i^T \in \mathcal{M}_{n\times 1}(\mathbb{Z}_q)$, *find* $z = (z_1, z_2, \ldots, z_n) \in \mathcal{M}_{1\times mn}(\{0, \pm 1\})$, $z_i \in \mathcal{M}_{1\times n}(\{0, \pm 1\})$, $\|z\| \leq \beta$, *such that*

$$z\alpha = \sum_i z_i\alpha_i = (z_1, z_2, \ldots, z_n)(\alpha_1, \alpha_2, \ldots, \alpha_n)^T = 0.$$

Lemma 13. *The Variant Knapsack Problem is equivalent to the one-dimensional* SIS *problem.*

Lemma 14. *If the* SIS *problem is hard, then the one-dimensional* SIS *variant problem is also hard.*

Proof. The correctness of Lemma 14 is obvious. We set $m' = mn$, so the one-dimensional SIS variant problem is transformed into the SIS problem. Therefore, m' satisfies the condition that the two are equivalent. □

Theorem 1. *The* Ring-SIS$|_{x=0}$ *problem is equivalent in difficulty to the one-dimensional* SIS *variant problem in the classical lattice.*

$$sA = \mathcal{M}_{1\times mn}(\mathbb{Z}_q) \times \mathcal{M}_{mn\times 1}(\mathbb{Z}_q) \mapsto \mathcal{M}_{1\times 1}(\mathbb{Z}_q).$$

$$s_f A_f = (\mathbb{Z}_q^n[x]/<x^m + 1>) \times (\mathbb{Z}_q^n[x]/<x^m + 1>)|_{x=0} \mapsto \mathbb{Z}_q[x]/<x + 1>.$$

The first mapping (a certain row)

$$\begin{aligned} g :&\mathbb{Z}_q^n[x]/<x^m + 1> \to \mathcal{M}_{1\times mn}(\mathbb{Z}_q) \\ &a_0 + a_1x + \cdots + a_{m-1}x^{m-1} \mapsto (a_0, a_1, \cdots, a_{m-1}). \end{aligned}$$

Second mapping (a certain column)

$$\begin{aligned} h :&\mathbb{Z}_q^n[x]/<x^m + 1> \to \mathcal{M}_{mn\times 1}(\mathbb{Z}_q) \\ &b_0 + b_1x + \cdots + b_{m-1}x^{m-1} \mapsto (b_0, -b_{m-1}, \cdots, -b_1). \end{aligned}$$

Then there is

$$\begin{aligned} &(a_0 + a_1x + \cdots + a_{m-1}x^{m-1})(b_0 + b_1x + \cdots + b_{m-1}x^{m-1}) \bmod q \bmod (x^m + 1)|_{x=0} \\ &\qquad = a_0b_0 - a_1b_{m-1} - \cdots - a_{m-1}b \\ &\qquad = g((a_0, a_1, \cdots, a_{m-1})) \cdot h((b_0, -b_{m-1}, \cdots, -b_1)). \end{aligned}$$

Therefore in the space $\mathcal{M}_{1\times mn}(\mathbb{Z}_q) \times \mathcal{M}_{mn\times 1}(\mathbb{Z}_q)$ the inner product and the product defined in space $(\mathbb{Z}_q^n[x]/<x^m+1>) \times (\mathbb{Z}_q^n[x]/<x^m+1>)$ is homomorphic, and it is easy to prove that this operation is also a bijection.

According to the Lemma 10, it can be seen that the corresponding Ring-SIS$|_{x=0}$ on the ring is also difficult.

Theorem 2. *If the* Ring-SIS$|_{x=0}$ *problem is hard, then the* Ring-SIS *problem is also hard.*

Proof. For the Ring-SIS problem, if there is an algorithm $\mathcal{W}$ that can solve the Ring-SIS problem, that is, find $f(x) \in \mathbb{Z}_q^{m_2}[x]$, such that

$$(f_1(x), \cdots, f_m(x)) \cdot (g_1(x), \cdots, g_m(x)) = \sum_i^m f_i(x)g_i(x) = 0 \tag{3}$$

This also means that the coefficient before x^0 in the equation(3) is also 0, then $f(x) \in \mathbb{Z}_q^{m_2}[x]$ is also an Ring-SIS$|_{x=0}$ problem solution

$$(f_1(x), \cdots, f_m(x)) \cdot (g_1(x), \cdots, g_m(x))|_{x=0} = \sum_i^m f_i(x)g_i(x)|_{x=0} = 0.$$

This is contradictory to the conclusion of Theorem 1, so the Ring-SIS problem is also difficult. □

Theorem 3. *Problem* Ring-SIS$(m, n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$ *is "roughly the same" as difficult as problem* SIS$(m, n, q, \mathcal{D}^m_{\mathcal{L},\alpha q})$.

Proof. Due to the existence of the one-dimensional SIS problem collision-resolving oracle, the oracle can solve s_i for any form of $\sum_{i=1}^{m} s_i \alpha_i^1$. In order to be able to solve the SIS problem, we use Gauss's rule to convert the equation (4) into a ladder form and then use the one-dimensional SIS problem collision-resolving oracle to solve it. It is assumed that the SIS problem can be solved by asking $O(n)$ times. The dimensional SIS problem can be solved by colliding with the oracle.

$$As = \sum_{i=1}^{m} s_i \alpha_i = \begin{matrix} \sum_{i=1}^{m} s_i \alpha_i^{(1)} \\ \sum_{i=1}^{m} s_i \alpha_i^{(2)} \\ \sum_{i=1}^{m} s_i \alpha_i^{(3)} \\ \vdots \\ \sum_{i=1}^{m} s_i \alpha_i^{(n)} \end{matrix} \tag{4}$$

Among them, $A = (\alpha_1, \ldots, \alpha_m)$, and $\alpha_i = (\alpha_i^{(1)}, \ldots, \alpha_i^{(n)})$. The Ring-SIS problem also requires $O(n)$ times of querying Ring-SIS$|_{x=0}$ to solve the problem until it collides with the oracle.

$$\begin{array}{ccc} \text{One-dimensional SIS problem} & \overset{O(n) \text{ inquiries}}{\Rightarrow} & \text{SIS problem} \\ \Updownarrow & & \\ \text{Ring-SIS}|_{x=0} \text{ problem} & \overset{O(n) \text{ inquiries}}{\Rightarrow} & \text{Ring-SIS problem} \end{array}$$

According to the form $F(x)G(x) = 0$, we have

$$\begin{aligned} F^T(x)G(x) &= \sum_{l}^{m} f^{(l)}(x) g^{(l)}(x) \\ &= \sum_{l}^{\mathrm{m}} \left(a_0^{(l)} b_0^{(l)} + (-1) \sum_{j=1}^{n-1} a_j^{(l)} b_{n-j}^{(l)} \right) \\ &+ \sum_{l}^{\mathrm{m}} \left(\sum_{i=1}^{2} a_{i-1}^{(l)} b_{2-i}^{(l)} + (-1) \sum_{j=2}^{n-1} a_j^{(l)} b_{n+1-j}^{(l)} \right) \quad x \\ &+ \sum_{l}^{\mathrm{m}} \left(\sum_{i=1}^{3} a_{i-1}^{(l)} b_{3-i}^{(l)} + (-1) \sum_{j=3}^{n-1} a_j^{(l)} b_{n+2-j}^{(l)} \right) \quad x^2 \qquad \bmod (x^n + 1) = 0. \\ &\vdots \\ &+ \sum_{l}^{\mathrm{m}} \left(\sum_{i=1}^{n} a_{i-1}^{(l)} b_{n-i}^{(l)} \right) \quad x^{n-1} \end{aligned} \tag{5}$$

We rewrite the equation (5) as

$$\begin{aligned} &\sum_{l}^{\mathrm{m}} a_0^{(l)} b_0^{(l)} + (-1) \sum_{j=1}^{n-2} \left(\sum_{l}^{\mathrm{m}} a_j^{(l)} b_{n-j}^{(l)} \right) &&= 0 \\ &\sum_{i}^{2} \left(\sum_{l}^{\mathrm{m}} a_{i-1}^{(l)} b_{2-i}^{(l)} \right) + (-1) \sum_{j=2}^{n-3} \left(\sum_{l}^{\mathrm{m}} a_j^{(l)} b_{n+1-j}^{(l)} \right) &&= 0 \\ &\sum_{i}^{3} \left(\sum_{l}^{\mathrm{m}} a_{i-1}^{(l)} b_{3-i}^{(l)} \right) + (-1) \sum_{j=3}^{n-4} \left(\sum_{l}^{\mathrm{m}} a_j^{(l)} b_{n+2-j}^{(l)} \right) &&= 0 \\ &&&\vdots \\ &\sum_{i}^{n} \left(\sum_{l}^{\mathrm{m}} a_{i-1}^{(l)} b_{n-i}^{(l)} \right) &&= 0 \end{aligned} \tag{6}$$

The equation (4) is consistent with the equation (6). We also need to convert it into a ladder form, and then use the Ring-SIS$|_{x=0}$ problem collision-resolving oracle to solve it. Therefore, the number of times that the Ring-SIS$|_{x=0}$ questions need to be asked to solve the Ring-SIS problem is the same as the number of one-dimensional SIS questions that need to be asked to solve the SIS problem, which can also be $O(n)$ times. Therefore, judging from the number of times the oracle is asked, the difficulty of the SIS problem is similar to that of the Ring-SIS problem. □

Remark 3. *Although the proof of Theorem 3 may not be sufficient, there is one thing we are certain about. That is, if the one-dimensional SIS problem is difficult, then the Ring-SIS$|_{x=0}$ problem is also difficult, which implies that the difficulty level of the Ring-SIS problem is no lower than that of the Ring-SIS$|_{x=0}$ problem and no higher than that of the SIS problem, due to the following theorem.*

Theorem 4. *If there exists a oracle that can solve the SIS problem in polynomial time, then there also exists an efficient algorithm to solve the Ring-SIS problem.*

Proof. If there exists a collision-resolving oracle that can solve the SIS problem in polynomial time, i.e., find $s = (s_1, \ldots, s_m)$, $s_i \in \mathbb{Z}_1$, such that

$$\sum_{i=1}^{m} \alpha_i s_i = 0,$$

we can construct an isomorphism mapping the vector $\alpha_i = (\alpha_i^1, \ldots, \alpha_i^n)$ to $f_i(x) = \alpha_i^{(1)} + \alpha_i^{(2)} x + \cdots + \alpha_i^{(n)} x^{n-1}$. Similarly, s_i is mapped to $g_i(x) = s_i$. Therefore, we have

$$\sum_{i=1}^{m} f_i g_i = 0.$$

Thus, $s = (s_1, \ldots, s_m)$ is also a solution to the Ring-SIS problem. □

4 Hardness of Ring-LWE with Small Uniform Errors

Lemma 15. *If there exists a collision-resolving oracle that can solve the* Ring-LWE$(m, n, q, \mathcal{D}_{\mathcal{R},\alpha q})|_{x=0}$ *problem in polynomial time, then there also exists an efficient algorithm to solve the* LWE$(m, 1, q, \mathcal{D}_{\mathcal{L},\alpha q})$ *problem in polynomial time. Similarly, the reverse is also true.*

Proof. According to Theorem 1, assuming the existence of an oracle that solves the LWE$(m, 1, q, \mathcal{D}_{\mathcal{L},\alpha q})$ problem, i.e., finds $s \in \{0, \pm 1\}$ such that $b = As + e$, where $A \in \mathcal{M}_{1\times mn}(\mathbb{Z}_q)$ and $b, e \in \mathbb{Z}_q$. We can establish the following isomorphism mapping, namely

$$\begin{gathered} b = sA + e \\ \downarrow \\ b_f|_{x=0} = (s_f \cdot a + e_f)|_{x=0}. \end{gathered}$$

Here, $s_f \in \mathcal{R}_{\{0,\pm 1\}}, a \in \mathcal{R}_q$, $e_f = e + e_1 x + \cdots + e_{n-1} x^{n-1}, e_i \in \{1, 2, \ldots, q-1\}, i \in \{1, \ldots, n-1\}$. Clearly, we have established an equivalence between the LWE$(m, 1, q, \mathcal{D}_{\mathcal{L},\alpha q})$ and Ring-LWE$(m, n, q, \mathcal{D}_{\mathcal{R},\alpha q})|_{x=0}$ problems. By Lemma 9, we know that the existence of an oracle for LWE$(m, 1, q, \mathcal{D}_{\mathcal{L},\alpha q})$ is equivalent to the existence of an efficient algorithm to solve Ring-LWE$(m, n, q, \mathcal{D}_{\mathcal{R},\alpha q})|_{x=0}$. □

Lemma 16. *If there exists an oracle that can solve the* Ring-LWE$(m, n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$ *problem, then there must exist an efficient algorithm to solve the* Ring-LWE$(m, n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})|_{x=0}$ *problem.*

Proof. Let's assume that there exists an oracle $\mathcal{W}$ that can solve the Ring-LWE$(m, n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$ problem. In other words, it can find $s \in \mathcal{R}_{\{0,\pm 1\}}$ within polynomial time such that

$$b = as + e, \text{where } a \in \mathcal{R}_q, e \in \mathcal{D}_{\mathcal{R},\alpha q}.$$

Since $b = as + e$ is a polynomial, the same equation holds for the constant term of b, which is

$$b|_{x=0} = (as + e)|_{x=0}, \text{where } a \in \mathcal{R}_q, e \in \mathcal{D}_{\mathcal{R},\alpha q}.$$

Therefore, $s \in \mathcal{R}_{\{0,\pm 1\}}$ is also a solution to the Ring-LWE$(m, n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})|_{x=0}$ problem. □

Lemma 17 ([MP13], Th 2.13). *Assuming that we can factorize q into $q = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ in $\mathrm{poly}(n)$ polynomial time, let $0 < \alpha \leq 1/\omega_n$. If the* LWE $(m, n, q, \mathcal{D}^m_{\mathbb{Z},\alpha q})$ *problem is hard, where $m(n) = n^{O(1)}$, then* LWE$(m', n, q, \mathcal{D}^m_{\mathbb{Z},\alpha' q})$ *is also pseudorandom for any $m'(n) = n^{O(1)}$ and*

$$\alpha' \geq \max\{\alpha, \omega_n^{1+1/\ell} \cdot \alpha^{1/\ell}, \omega_n/p_1^{e_1}, \ldots, \omega_n/p_k^{e_k}\},$$

where ℓ is an upper bound on p_i such that $p_i < \omega_n/\alpha'$.

Corollary 5. *Assuming that we can factorize q into $q = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ in polynomial time, let $0 < \alpha \leq 1/\omega$. If the* LWE $(m, 1, q, \mathcal{D}^m_{\mathbb{Z},\alpha q})$ *problem is hard, where m is any integer, then* LWE$(m', 1, q, \mathcal{D}^m_{\mathbb{Z},\alpha' q})$ *is also pseudorandom for any m' and*

$$\alpha' \geq \max\{\alpha, \omega^{1+1/\ell} \cdot \alpha^{1/\ell}, \omega/p_1^{e_1}, \ldots, \omega/p_k^{e_k}\},$$

where ℓ is an upper bound on p_i such that $p_i < \omega/\alpha'$.

Lemma 18. *Assuming we can factorize $q = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ in polynomial time, where p_i are primes and e_i are positive integers. Let $0 < \alpha \leq 1/\omega_n$. If the* Ring-LWE$(m, n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$ *problem is hard, where $m(n) = n^{O(1)}$, then* Ring-LWE$(m', n, q, \mathcal{D}^m_{\mathcal{R},\alpha' q})$ *is also pseudorandom for any $m'(n) = n^{O(1)}$, and*

$$\alpha' \geq \max\{\alpha, \omega_n^{1+1/\ell} \cdot \alpha^{1/\ell}, \omega_n/p_1^{e_1}, \ldots, \omega_n/p_k^{e_k}\},$$

where ℓ is an upper bound on primes p_i such that $p_i < \omega_n/\alpha'$.

Proof. If there exists an oracle that solves the Ring-LWE$(m, n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$ problem, then there must exist an algorithm to solve the Ring-LWE$(m, n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})|_{x=0}$ problem. According to Lemma 16, we know that the Ring-LWE$(m, n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})|_{x=0}$ problem is equivalent to the LWE$(m, 1, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$ problem. Therefore, there also exists an algorithm to solve the LWE$(m, 1, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$ problem. Based on Corollary 5, we can conclude that there exists an algorithm to solve the LWE$(m', 1, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$ problem.

Using the equivalence between Ring-LWE$(m', n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})|_{x=0}$ problem and LWE$(m', 1, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$ problem again, we can obtain a solution to the Ring-LWE$(m', n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})|_{x=0}$ problem, and thus obtain an algorithm for solving Ring-LWE$(m', n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$ problem using the conclusion of Lemma 16. □

Theorem 5. *If there exists an oracle $\mathcal{W}$ capable of solving* Ring-LWE$(n, q, \mathcal{D}_{\mathcal{R},\alpha q})$*, then there also exists an algorithm $\mathcal{W}'$ that can construct collision queries for* Ring-LWE$(m, n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$*, and thereby solve the* Ring-SIS$(m, n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$ *problem.*

Proof. For a Ring-LWE$(n, q, \mathcal{D}_{\mathcal{R},\alpha q})$ problem, given $(a_i, b_i) \in \mathcal{R}_q \times \mathcal{R}_q$, the goal is to find $s_i \in \mathcal{R}_{\{0,\pm 1\}}$ such that

$$b_i = a_i s_i + e_i.$$

Here, a_i and b_i are ring elements in $\mathcal{R}_q$, and s_i is the secret key while $e_i \in \chi$ is a small error term. If there exists an oracle $\mathcal{W}$ capable of solving the Ring-LWE$(n, q, \mathcal{D}_{\mathcal{R},\alpha q})$ problem, then for a m-fold Ring-LWE$(n, q, \mathcal{D}_{\mathcal{R},\alpha q})$ problem, i.e., Ring-LWE$(m, n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$, we only need to query the oracle $\mathcal{W}$ m times in order to obtain $s_i \in \mathcal{R}_{\{0,\pm 1\}}$ such that

$$\big(b_1 = a_1 s_1 + e_1, \ldots, b_m = a_m s_m + e_m\big). \tag{7}$$

as in Equation (7). Let $F(x) = (a_1, \ldots, a_m)$, and consider $G(x) = (t_1, \ldots, t_m)$ as a special solution to the Ring-SIS$(m, n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$ problem, such that

$$F^T(x)G(x) = a_1 t_1 + \cdots + a_m t_m = 0,$$

and $a_i t_i = 0$ for $i \in \{1, \ldots, m\}$.

Using the oracle machine $\mathcal{W}$ again m times, we obtain $y_i = s_i + t_i$ for $i \in \{1, \ldots, m\}$, such that

$$\big(b_1 = a_1(s_1 + t_1) + e_1, \ldots, b_m = a_m(s_m + t_m) + e_m\big). \tag{8}$$

By combining the information from Equation (7) and Equation (8), we can obtain a solution to the Ring-SIS$(m, n, q, \mathcal{D}^m_{\mathcal{R},\alpha q})$ problem. □

5 Reduction and Signature Scheme Construction based on Ring-ISIS Problem

Ring-ISIS problem. Given $f_1, \ldots, f_m \in \mathcal{R}_q$, where $\mathcal{R}_q$ is a polynomial ring with modulus q, find m polynomials $g_1, \ldots$, whose coefficients are not all 0, $g_m \in \mathcal{R}_{\{0,\pm 1\}}$, such that

$$f_1 g_1 + \cdots + f_m g_m = b \bmod q\mathcal{R} \in \mathcal{R}_q.$$

Lemma 19. *Ring-SIS problem is equivalent to Ring-ISIS problem.*

Proof.

$$f_1 g_1 + \cdots + f_m g_m = b \bmod q\mathcal{R}$$
$$\Leftrightarrow f_1 g_1 + \cdots + f_m g_m - b \cdot 1 = 0 \bmod q\mathcal{R}.$$

Let $f_{m+1} = b$ and $g_{m+1} = -1$. Thus, $(g_1, \ldots, g_m, -1) \in \mathcal{R}^{m+1}_{\{0,\pm 1\}}$ is a short solution to the Ring-SIS problem $(f_1, \ldots, f_m, b)$. □

Algorithm 1 Ring-SIS Trapdoor Algorithm

1. **Setup**. Let $\overline{F} = (f_1, \ldots, f_m) \in \mathcal{R}_q^m$. Randomly choose $u \in \mathcal{R}_q$. The method of mapping $\overline{F}$ to a matrix $\overline{A} \in \mathbb{Z}_q^{m \times n}$ and mapping u to $b \in \mathbb{Z}_q^n$ can be done using the formula (**??**).
2. $\mathbf{GenTrap}^{\boldsymbol{\mathcal{D}}}(\overline{\boldsymbol{A}}, \boldsymbol{H}) \rightarrow (\boldsymbol{A}, \boldsymbol{R})$[MP12]. Where R is the trapdoor value for ISIS, and A is a matrix indistinguishable from $\overline{A}$. Similarly, using the method in formula (**??**), A can be mapped to $F \in \mathcal{R}_q^m$.
3. $\mathbf{Sample}^{\boldsymbol{\mathcal{O}}}(\boldsymbol{R}, \overline{\boldsymbol{A}}, \boldsymbol{H}, \boldsymbol{b}, \boldsymbol{s}) \rightarrow \boldsymbol{g} \in \boldsymbol{\mathcal{L}_b^{\perp}(A)} \subset \mathbb{Z}^{\boldsymbol{m}}_{\boldsymbol{\{0,\pm 1\}}}$[MP12]. Where $H \in \mathbb{Z}_q^{n \times n}$ is an invertible integer matrix, and s is the Gaussian parameter.
4. **Return**. Let $S = g$, and return S and F. At this point, each element of S can be understood as a 0-degree polynomial.

Note 1. *The essence of the Ring-ISIS trapdoor algorithm is Micciancio and Peikert's ISIS trapdoor algorithm, hence its correctness is evident.*

Algorithm 2

Setup. Let $H : \mathcal{R}_{\{0,1\}} \rightarrow \mathcal{R}^m_{\{0,\pm 1\}}$ be a hash function, and let $\overline{F} = (f_1, \ldots, f_m) \in \mathcal{R}_q^m$. Randomly choose $u \in \mathcal{R}_q$. Obtain F and S using the Ring-SIS trapdoor algorithm. Set

$$pk = (F, u), \quad sk = S.$$

$\mathbf{Sign}(\boldsymbol{m})$. Randomly choose $A_f \in \mathcal{R}_q^{m \times m}$, and compute

$$\sigma_m^{(1)} = S + A_f S + H(m), \quad \sigma_m^{(2)} = F^T A_f S.$$

$\mathbf{Verify}(\boldsymbol{\sigma_m^{(1)}}, \boldsymbol{\sigma_m^{(2)}}, \boldsymbol{m})$. Verify if

$$F^T \sigma_m^{(1)} \stackrel{?}{=} u + \sigma_m^{(2)} + F^T H(m).$$

Definition 6 ([GSM18], EU-CMA)**.** *If there does not exist an adversary $\mathcal{A}$ that, after making q_s queries, is still unable to mount an attack with non-negligible advantage ε within time t, we say that the signature scheme is (t, q_s, ε) secure.*

Theorem 6. *Suppose the hash function H is a random oracle. If the Ring-ISIS problem is hard, the Algorithm 2 is provably secure in the EU-CMA security model with reduction loss $L = q_H$, where q_H is the number of hash queries to the random oracle.*

Proof. Suppose there exists an adversary $\mathcal{A}$ who can (t, q_s, ε)-break the signature scheme in the EU-CMA security model. We construct a simulator $\mathcal{B}$ to solve the Ring-ISIS problem. Given as input a problem instance $(F, b) \in \mathcal{R}_q^m \times \mathcal{R}_q$ over the Ring-ISIS problem, $\mathcal{B}$ controls the random oracle, runs $\mathcal{A}$, and works as follows.

Setup. $\mathcal{B}$ chooses a hash function $H : \mathcal{R}_{\{0,1\}} \to \mathcal{R}_{\{0,\pm1\}}^m$ and a vector $F = (f_1, \ldots, f_m) \in \mathcal{R}_q^m$. Randomly selects a vector $S = (s_1, \ldots, s_m) \in \mathcal{R}_{\{0,\pm1\}}^m$ such that $F^T S = u$, and

H-Query. The adversary makes hash queries in this phase. Before receiving queries from the adversary, $\mathcal{B}$ randomly chooses an integer $i^* \in [1, q_H]$, where qH denotes the number of hash queries to the random oracle. Then, $\mathcal{B}$ prepares a hash list to record all queries and responses as follows, where the hash list is empty at the beginning.

Let the i-th hash query be m_i. If mi is already in the hash list, $\mathcal{B}$ responds to this query following the hash list. Otherwise, $\mathcal{B}$ randomly chooses B_i from $\mathcal{R}_{\{0,\pm1\}}^m$ and sets $H(m_i)$ as

$$F^T H(m_i) = \begin{cases} b, & \text{if } i = i^*; \\ F^T B_i, & \text{otherwise.} \end{cases}$$

The simulator $\mathcal{B}$ responds to this query with $H(m_i)$ and adds $(i, m_i, B_i, H(m_i))$ to the hash list.

Query. The adversary makes signature queries in this phase. For a signature query on m_i, if m_i is the i^*-th queried message in the hash list, abort. Otherwise, we have $H(m_i) = B_i$.

$\mathcal{B}$ computes $\sigma_{m_i}^{(1)}, \sigma_{m_i}^{(2)}$ as

$$\sigma_m^{(1)} = S + A_f S + H(m), \sigma_m^{(2)} = F^T A_f S.$$

According to the signature definition and simulation, we have

$$F^T \sigma_m^{(1)} = u + \sigma_m^{(2)} + F^T H(m).$$

Therefore, $\sigma_{m_i}^{(1)}, \sigma_{m_i}^{(2)}$ is a valid signature of m_i.

Forgery. The adversary returns a forged signature $\sigma_{m^*}^{(1)}, \sigma_{m^*}^{(2)}$ on some m^* that has not been queried. If m^* is not the i^*-th queried message in the hash list, abort. Otherwise, we have $F^T H(m^*) = b$.

According to the definition of signature and simulation, we know that

$$F^T \sigma_{m^*}^{(1)} = u + \sigma_{m^*}^{(2)} + F^T H(m^*) = u + \sigma_{m^*}^{(2)} + b.$$

At this point, the simulator $\mathcal{B}$ can compute

$$F^T H(m^*) = b, H(m^*) = C_i.$$

C_i is a solution to the Ring-SIS problem (F, b). The correctness analysis of this simulation is as follows.

Indistinguishable simulation. The correctness of the simulation has been explained above. The randomness of the simulation includes all random numbers in the key generation and the responses to hash queries. They are

$$F^T B_1, \cdots, F^T B_{i^*-1}, b, F^T B_{i^*+1}, \cdots, F^T B_{q_H}.$$

According to the setting of the simulation, where B_i, b are randomly chosen, it is easy to see that they are random and independent from the point of view of the adversary. Therefore, the simulation is indistinguishable from the real attack.

Probability of successful simulation and useful attack. If the simulator successfully guesses i^*, all queried signatures are simulatable, and the forged signature is reducible because the message m_{i^*}

cannot be chosen for a signature query, and it will be used for the signature forgery. Therefore, the probability of successful simulation and useful attack is $\frac{1}{q_H}$ for q_H queries.

Advantage and time cost. Suppose the adversary breaks the scheme with (t, q_s, ε) after making q_H queries to the random oracle. The advantage of solving the Ring-SIS problem is therefore $\frac{\varepsilon}{q_H}$. Let T_s denote the time cost of the simulation. We have $T_s = O(q_H + q_s)$, which is mainly dominated by the oracle response and the signature generation. Therefore, $\mathcal{B}$ will solve the Ring-SIS problem with $(t + T_s, \varepsilon/q_H)$.

This completes the proof of the theorem. □

Open problem 1. *The trapdoor provided in this paper clearly does not reflect Ring-ISIS, as the core of the algorithm is Micciancio and Peikert's ISIS trapdoor algorithm. By solving a non-homogeneous matrix equation and lattice shifting, the output values obtained are solutions to ISIS, which is evidently not what we desire. Therefore, a genuine Ring-ISIS trapdoor algorithm is needed.*

Open problem 2. *Since the signature scheme in this paper is directly constructed using Ring-ISIS problem, its security, theoretically speaking, is higher compared to signature schemes based on NTRU problem and is more concise in format than signature schemes based on Ring-LWE problem.*

However, the computational complexity of this scheme in the paper is significantly higher than both, which is also a weakness of this proposed scheme.

References

[Ajt96] Miklós Ajtai. Generating hard instances of lattice problems. *Electron. Colloquium Comput. Complex.*, TR96, 1996.

[BPR12] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In *Advances in Cryptology – EUROCRYPT 2012*, pages 719–737. Springer Berlin Heidelberg, 2012.

[CZY22] Luchuan Ceng, Lijun Zhu, and Tzu Chien Yin. Modified subgradient extragradient algorithms for systems of generalized equilibria with constraints. *AIMS Mathematics*, 8(2):57–74, 2022.

[dZ] dabei Z. Sis problem, `https://dabeiz.github.io/2020/04/28/SIS/`.

[GSM18] Fuchun Guo, Willy Susilo, and Yi Mu. Digital signatures with random oracles. In *Introduction to Security Reduction*, pages 147–165. Springer, 2018.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Advances in Cryptology – EUROCRYPT 2010*, pages 1–23, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[MH78] R. Merkle and M. Hellman. Hiding information and signatures in trapdoor knapsacks. *IEEE Transactions on Information Theory*, 24(5):525–530, 1978.

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, pages 700–718, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[MP13] Daniele Micciancio and Chris Peikert. Hardness of sis and lwe with small parameters. In *Advances in Cryptology – CRYPTO 2013*, pages 21–39, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[Qiu10] Weisheng Qiu. *Advanced Algebra (Volume 1) - Innovative Textbook for College Advanced Algebra Courses*. Higher Education Press, Beijing, 2010.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, page 84 – 93. Association for Computing Machinery, 2005.

[Wee22] Hoeteck Wee. Optimal broadcast encryption and cp-abe from evasive lattice assumptions. In *Advances in Cryptology – EUROCRYPT 2022*, pages 217–241. Springer International Publishing, 2022.

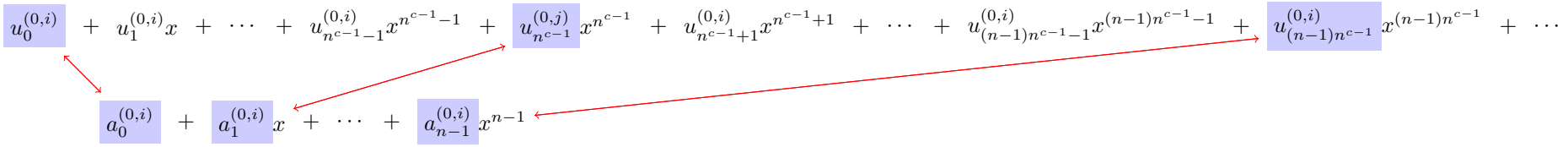
[Yuea] Steven Yue. Lattice learning notes 05: Owf based on sis, `https://zhuanlan.zhihu.com/p/163168725`.

[Yueb] Steven Yue. Lattice learning notes 06: The hardness proof of sis problem, `https://zhuanlan.zhihu.com/p/163641008`.

[Yuec] Steven Yue. Lattice learning notes 09: Ring-sis and ideal lattice, `https://zhuanlan.zhihu.com/p/184851285`.

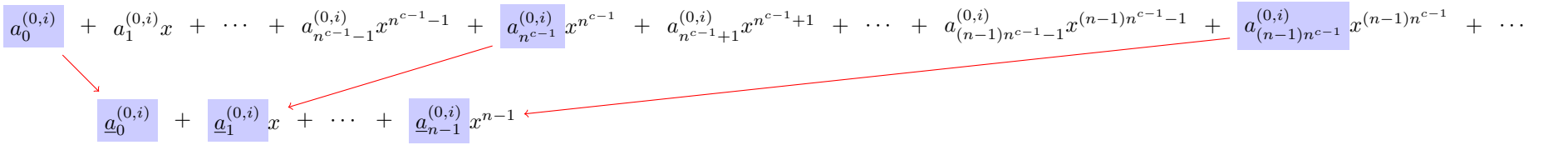
Appendix

Definition 7 (Polynomial degree extension method)**.**

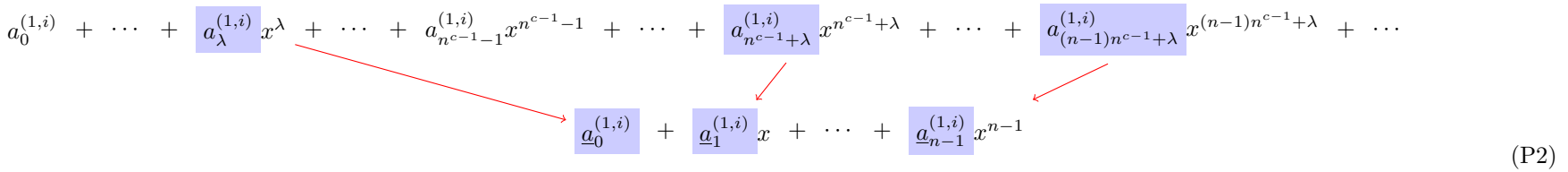


We refer to it as " polynomial degree extension", and conversely, we call it " polynomial degree reduction".

Proof of Lemma 6. First, we use the approach defined in Definition 7 to extract a $\underline{F}^{(0)}(x)$ Ring-SIS(m, n, q^c, β^c) problem from $F(x) = F^{(0)}(x) =$ Ring-SIS(m, n^c, q^c, β^c), as stated in Equation (P1).



(P1)



(P2)

Let $\underline{F}^{(0)}(x) := (\underline{f}^{(0,1)}, \underline{f}^{(0,2)}, \ldots, \underline{f}^{(0,m)})$, here $\underline{f}^{(0,i)} = \underline{a}_0^{(0,i)} + \underline{a}_1^{(0,i)}x + \cdots \underline{a}_{n-1}^{(0,i)}x^{n-1}$. According to the Ring-SIS$(m, n, q, \mathcal{X})$ oracle, we can make m queries to $\underline{F}^{(0)}(x)$ and obtain

$$\underline{G}^{(0)}(x) := (\underline{g}^{(1,0)}(x), \underline{g}^{(2,0)}(x), \cdots, \underline{g}^{(m,0)}(x)), \underline{g}^{(i,0)}(x) \in \mathbb{Z}_q[x]/<x^{n^k}+1>, i \in \{1, \ldots, n\}.$$

Here, $\underline{g}^{(i,0)}(x) = b_0^{(i,0)} + b_1^{(i,0)}x + \cdots b_{n^k-1}^{(i,0)}x^{n^k-1}$.

Likewise. We transform it into

$$g^{(i,0)}(x) = b_0^{(i,0)} + b_1^{(i,0)}x^n + \cdots + b_{n^k-1}^{(i,0)}x^{(n^k-1)n}.$$

We construct

$$G^{(0)}(x) := (g^{(1,0)}(x), g^{(2,0)}(x), \ldots, g^{(m,0)}(x)), g^{(i,0)}(x) \in \mathbb{Z}_q[x]/\langle x^{n^k}+1\rangle, i \in \{1, \ldots, n\}.$$

We define $F^{(1)}(x) = ((F^{(0)}(x))^T G_1^{(0)}(x), \underbrace{0, \ldots, 0}_{m-1})$. At this point, $F^{(1)}(x)$ is also a Ring-SIS(m, n^c, q^c, β^c) problem. We extract a $\underline{F}^{(1)}(x)$ from $F^{(1)}(x)$, which is a Ring-SIS(m, n, q^c, β^c) problem, as stated in Equation (P2).

We let $\underline{F}^{(1)}(x) = (\underline{f}^{(1,1)}, \underbrace{0, \ldots, 0}_{m-1})$, where $\underline{f}^{(1,1)} = \underline{a}_0^{(1,1)} + \underline{a}_1^{(1,1)}x + \cdots + \underline{a}_{n-1}^{(1,1)}x^{n-1}$. Using the Ring-SIS$(m, n, q, \mathcal{X})$ oracle, we make m queries to $\underline{F}^{(0)}(x)$ and obtain

$$\begin{aligned}\underline{G}^{(1)}(x) :&= (\underline{g}^{(1,1)}(x), \underline{g}^{(2,1)}(x), \cdots, \underline{g}^{(m,1)}(x)),\\ &\underline{g}^{(i,0)}(x) \in \mathbb{Z}_q[x]/<x^{n^k}+1>, i \in \{1, \ldots, n\}.\end{aligned}$$

Where,

$$\underline{g}^{(i,1)}(x) = b_0^{(i,1)} + b_1^{(i,1)}x + \cdots b_{n^k-1}^{(i,1)}x^{n^k-1}.$$

We could rewrite it as

$$g^{(i,1)}(x) = b_0^{(i,1)} + b_1^{(i,1)}x^n + \cdots + b_{n^k-1}^{(i,1)}x^{(n^k-1)n}.$$

Construct a part of solution, that is

$$G^{(1)}(x) := (g^{(1,1)}(x), \underbrace{0, \cdots, 0}_{m-1}), g^{(i,1)}(x) \in \mathbb{Z}_q[x]/<x^{n^k}+1>, i \in \{1, \ldots, n\}.$$

Suppose that $F^{(2)}(x) = ((F^{(1)}(x))^T G_1^{(1)}(x), \underbrace{0, \cdots, 0}_{m-1})$, and $F^{(2)}(x)$ is a Ring-SIS(m, n^c, q^c, β^c) problem. The solution to the recursive problem $F(x) = F^{(0)}(x) =$ Ring-SIS(m, n^c, q^c, β^c) is given by

$$G(x) = (\tilde{g}_1, \ldots, \tilde{g}_m),$$

where

$$\tilde{g}_i = \prod_{j=1}^{n} g^{(1,j)} \left(\sum_{i=1}^{m} g^{(i,0)} \right).$$

To verify that $G(x)$ is a solution to the problem $F(x) = F^{(0)}(x) =$ Ring-SIS(m, n^c, q^c, β^c), we only need to calculate $F^T(x)G(x) = 0$. For convenience, let's define

$$F(x) := (f^{(1)}(x), f^{(2)}(x), \cdots, f^{(m)}(x)), f^{(i)}(x) \in \mathbb{Z}_q[x]/<x^{n^{k+1}}+1>, i \in \{1, \ldots, m\}.$$

where,

$$f^{(i)}(x) = \mathcal{F}_0^{(i)} + \cdots + \mathcal{F}_{n^c-1}^{(i)}, \mathcal{F}_\lambda = a_0 x^\lambda + a_1 x^{\lambda+n} + \cdots + a_{n^k-1}x^{\lambda+(n^k-1)n}, \lambda \in \{1, \ldots, n\}.$$

Then we have

$$F^T(x)G(x) = \sum_{k=1}^{m} (\mathcal{F}_0^{(i)} + \cdots + \mathcal{F}_{n^c-1}^{(i)}) \left(\prod_{j=1}^{n} g^{(1,j)} \left(\sum_{i=1}^{m} g^{(i,0)} \right) \right).$$

Since $\sum_{i=1}^{m} (\mathcal{F}_0^{(i)} \sum_{j_1=1}^{m} g_i^{j_1}) = 0$, we have

$$F^T(x)G(x) = \sum_{i=1}^{m}(\mathcal{F}_0^{(i)} + \cdots + \mathcal{F}_{n^c-1}^{(i)}) \left(\prod_{j=1}^{n} g^{(1,j)} \left(\sum_{i=1}^{m} g^{(i,0)} \right) \right)$$
$$= \sum_{i=1}^{m} \left(\mathcal{F}_1^{(i)}(\sum_{i=1}^{m} g^{(i,0)}) + \cdots + \mathcal{F}_{n^c-1}^{(i)}(\sum_{i=1}^{m} g^{(i,0)}) \right) \prod_{j=1}^{n} g^{(1,j)}.$$

Also, since

$$\sum_{i=1}^{m} \left(\mathcal{F}_1^{(i)}(\sum_{i=1}^{m} g^{(i,0)}) \right) = 0,$$

we have

$$F^T(x)G(x) = \sum_{i=1}^{m}(\mathcal{F}_0^{(i)} + \cdots + \mathcal{F}_{n^c-1}^{(i)}) \left(\prod_{j=1}^{n} g^{(1,j)} \left(\sum_{i=1}^{m} g^{(i,0)} \right) \right)$$
$$= \sum_{i=1}^{m} \left(\mathcal{F}_1^{(i)}(\sum_{i=1}^{m} g^{(i,0)}) + \cdots + \mathcal{F}_{n^c-1}^{(i)}(\sum_{i=1}^{m} g^{(i,0)}) \right) \prod_{j=1}^{n} g^{(1,j)}$$
$$= \sum_{i=1}^{m} \left(\mathcal{F}_2^{(i)}(\sum_{i=1}^{m} g^{(i,0)}) g^{(1,1)} + \cdots + \mathcal{F}_{n^c-1}^{(i)}(\sum_{i=1}^{m} g^{(i,0)}) g^{(1,1)} \right) \prod_{j=2}^{n} g^{(1,j)}.$$

If we continue this way, it is easy to prove that $G(x)$ is a solution to the Ring-SIS(m, n^c, q^c, β^c) problem. In this case, it will take a total of $(n^c - n)/n + 1 = n^{c-1}$ queries at least. □