Inner Product Ring LWE Problem, Reduction, New Trapdoor Algorithm for Inner Product Ring LWE Problem and Ring SIS Problem

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

Abstract

Lattice cryptography is currently a major research focus in public-key encryption, renowned for its ability to resist quantum attacks. The introduction of ideal lattices (ring lattices) has elevated the theoretical framework of lattice cryptography. Ideal lattice cryptography, compared to classical lattice cryptography, achieves more acceptable operational efficiency through fast Fourier transforms. However, to date, issues of impracticality or insecurity persist in ideal lattice problems. In order to provide a reasonable and secure trapdoor algorithm, this paper introduces the concept of "Inner Product Ring LWE" and establishes its quantum resistance and indistinguishability using knowledge of time complexity, fixed-point theory, and statistical distances. Inner product Ring LWE is easier to construct trapdoor algorithms compared to Ring LWE. Additionally, leveraging the properties of NTRU, we propose a more secure Ring SIS trapdoor algorithm.

Keywords: Ring LWE; Ring SIS; Trapdoor algorithm.

1 Introduction

Trapdoor algorithms are a key focus of current research in public-key cryptography. Whether a difficult problem can be used to construct public-key encryption depends on whether it can be embedded in a trapdoor algorithm to generate a private key. Take the knapsack problem for example: because the knapsack problem cannot be embedded into a trapdoor, the subset sum problem was introduced. This facilitates the construction of a trapdoor, thereby enabling the generation of a private key.

Before 1997, the Diffie-Hellman problem and the RSA problem were the fundamental hard problems relied upon by public-key encryption algorithms. In 1997, Peter W. Shor demonstrated that both the Diffie-Hellman problem and the RSA problem can be broken in polynomial time on a quantum computer [Sho97]. If the underlying problem of an encryption algorithm can be broken in polynomial time by an algorithm, then that algorithm is no longer secure. Therefore, cryptographers shifted their focus to lattice problems, which offer cryptographic schemes resistant to quantum attacks.

In 2002, Oded Regev published a paper in Stoc where he primarily reduced the Shortest Vector Problem (SVP) to the Hidden Subgroup Problem (HSP) in the asymmetric setting [Reg02]. This reduction implies that if there exists an efficient algorithm to solve SVP in polynomial time, then there also exists an efficient algorithm to solve HSP in polynomial time. HSP is a classic problem in quantum

[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, 710062, Shaanxi, China

computing for which no efficient algorithm is currently known, hence SVP inherits resistance to quantum attacks. However, embedding SVP into trapdoor algorithms is non-trivial. In 2005, Oded Regev further reduced the Learning With Errors (LWE) problem to SVP [Reg05], where LWE is susceptible to trapdoor embedding. In 2003, Dinur et al. introduced another lattice problem suitable for trapdoor embedding, namely the Shortest Integer Solution (SIS) problem [DKRS03]. In 2013, Micciancio and Peikert reduced SIS to the LWE problem [MP13].

In 2008, Gentry, Peikert, and Vaikuntanathan provided a comprehensive overview of lattice-based cryptography and introduced the Learning With Errors (LWE) trapdoor algorithm [GPV08]. In 2012, Micciancio and Peikert extended this work by presenting both LWE and Short Integer Solution (SIS) trapdoor algorithms [MP12]. LWE trapdoor algorithms are commonly used in constructing public-key encryption schemes such as Attribute-Based Encryption (ABE) [ARYY23], while SIS trapdoor algorithms are typically applied in signature schemes [PTDH23]. In 2020, Micciancio et al. further refined LWE and SIS trapdoor algorithms [GMPW20].

Although lattice cryptography offers resistance against quantum attacks, the time complexity of encryption algorithms based on the Learning With Errors (LWE) and Short Integer Solution (SIS) problems reaches $O(n^2)$, due to their fundamental matrix-vector operations. Particularly for LWE, each encryption typically handles only 1 bit at a time. To overcome this challenge, Lyubashevsky, Peikert, and Regev introduced the Ring LWE problem in 2010, which represents an ideal lattice variant. In their work, they established an isomorphism between a specific lattice space (ideal lattice space) and the space of polynomials over a ring, thereby defining Ring LWE as an ideal lattice problem. Encryption algorithms based on Ring LWE, coupled with the fast Fourier transform technique from NTRU, achieve a reduced time complexity of $O(n \log n)$ ([HPS98], p. 269). In 2018, Stephens-Davidowitz introduced the corresponding Ring-SIS problem [SD18].

In the same year, Genise and Micciancio respectively proposed Ring-SIS trapdoor algorithms using Ring LWE and the knapsack problem [GM18], thus filling a gap in trapdoor constructions for ideal lattice problems. However, a trapdoor algorithm for Ring LWE has yet to be constructed. Currently, Ring LWE trapdoor algorithms in use mostly fall into two categories: one directly transitions from Micciancio and Peikert's LWE trapdoor algorithm to Ring LWE, and the other applies Genise and Micciancio's Ring SIS trapdoor algorithm to Ring LWE. Nevertheless, neither category provides a satisfactory trapdoor algorithm for Ring LWE. Therefore, there is a need for a proper Ring LWE trapdoor algorithm to support ideal lattice-based public-key cryptographic schemes.

The main contribution of this paper is to address the aforementioned issues as much as possible. In order to easily embed trapdoor algorithms while preserving the advantages of ideal lattice problems, we propose a new ideal lattice problem called the Inner Product Ring LWE problem. We demonstrate the hardness and indistinguishability of the new Ring LWE problem and provide a trapdoor algorithm for the Inner Product Ring LWE problem. Additionally, we present a more reasonable and secure trapdoor algorithm for Ring-SIS.

1.1 Detailed Analysis

The current Ring LWE trapdoors resemble those of [MP12], but they are not suitable for Ring LWE. Additionally, there are many adaptations borrowing from Nicholas Genise and Daniele Micciancio's Ring SIS signature trapdoors.

Let $\mathcal{R}_q$ denote a power of 2 cyclotomic ring, with parameters set as $m = 2$, $k = \lceil \log q \rceil$, $\overline{m} = m + k$. There exists an algorithm GenTrap that produces a vector $\overline{A} \in \mathcal{R}^{1 \times \overline{m}}$ and a trapdoor $R \in \mathcal{R}_q^{m \times k}$ with tag $h \in \mathcal{R}_q$ satisfying the following:

1. $\overline{A} = [A|AR + hG]$, where G is the trapdoor matrix, $G = [1, 2, \ldots, 2^{k-1}]$, and $A = [a|1] \in \mathcal{R}_q^{1\times 2}$, with $a \leftarrow \mathcal{R}_q$.
2. R is distributed as a Gaussian $\mathcal{D}^{2\times k}$ for some $s = \alpha q$, where $\alpha > 0$ is a RLWE error term, $\alpha q > \omega(\sqrt{\log n})$.
3. h is an invertible element in $\mathcal{R}_q$.
4. $\overline{A}$ is computationally pseudorandom (excluding the component set to 1) under (decisional) RLWE_D where $D = \mathcal{D}_{R,s}$.

Figure 1: LWE trapdoor algorithm [MP12]

Furthermore, there's an alternative approach resembling the Ring SIS signature trapdoors:

1. Select $k = \lfloor \log_b(q) + 1 \rfloor$, σ, q, and n, where $b \geq 2$ is a base for the G-lattice.
2. Choose $a \leftarrow \mathcal{R}_q$.
3. Generate $r = (r_1, \ldots, r_k)$, where $i \in [k]$, $r_i \leftarrow \mathcal{D}_{\mathcal{R},\sigma}$.
4. Generate $e = (e_1, \ldots, e_k)$, where $i \in [k]$, $e_i \leftarrow \mathcal{D}_{\mathcal{R},\sigma}$.
5. Calculate $\overline{g} = (1, a, g_1 - (ar_1 + e_1), \ldots, g_k - (ar_k + e_k))$, where $i \in [k]$, $g_i \leftarrow b^{i-1}$.

Figure 2: Ring SIS trapdoor algorithm(Output $\overline{g}$)[GM18]

Return $(\overline{g}, T_{\overline{g}} = (r, e))$, and **Perturb**$(\cdot)$ to generate a perturbation p, enabling y obeying spherical Gaussian distribution with the parameter σ_s. Finally, the algorithm produces a preimage y that satisfies the condition $\overline{g}^T y = u$, where $y \leftarrow \mathcal{D}_{\mathcal{L},\sigma_s}$, $z \in \mathcal{R}_q^k$, $u \in \mathcal{R}_q$ and $p \in \mathcal{R}_q^m$ for $m = k + 2$.

1. $p \leftarrow$ **Perturb**$((r, e)(b + 1)\sigma, \sigma_s, q, n)$.
2. $z \leftarrow$ **SampleG**$(\sigma, q, u - \overline{g}p)$.
3. Compute $y = [p_1 + ez, p_2 + rz, p_3 + z_1, \ldots, p_m + z_k]$.

Figure 3: Ring SIS trapdoor algorithm(Output y)[GM18]

These trapdoors aim to address the challenges specific to Ring LWE scenarios, offering tailored solutions for improved security and efficiency.

Fact 1. *The G matrix from [MP12] cannot be directly applied to Ring LWE trapdoors because, for Ring LWE, solving $b = as + e$, where $a, s \in \mathcal{R}_q$, involves elements from a univariate polynomial ring, making direct adaptation infeasible.*

Fact 2. *Similarly, Ring SIS trapdoors cannot be directly applied to Ring LWE trapdoors. This is because in the trapdoor algorithm from [GM18], the resulting $\overline{g}$ and y satisfy $\overline{g}^T y = gz = u$, where Ring SIS essentially consists of vectors composed of multiple sets of elements from univariate polynomial rings, whereas Ring LWE only has one set.*

1.2 Overview

Firstly, we define the Inner Product Ring LWE as follows: for any $f_1, f_2, b \in \mathcal{R}_q$, find (g_1, g_2) such that $b = f_1 g_1 + f_2 g_2 + e$. To prove the pseudo-randomness and quantum resistance of Inner Product Ring LWE, we define $\mathbb{P}_{\mathcal{S}_q}$ as the probability set for any $i \in \mathbb{Z}_q$. Now, calculate the value when $\Pr(i) \in \mathbb{P}_{\overline{\mathcal{S}}_{q^2}} := \mathbb{P}_{\mathcal{S}_q} \times \mathbb{P}_{\mathcal{S}_q}$. Define its maximum value as $\Pr(\mathfrak{A})$, with the corresponding element $\mathfrak{A} \in \mathbb{Z}_{q^2}$. At this point, we are calculating the probability of $a_1 s_1 = b_1 \to \mathbb{Z}_{q^2}$, then we calculate $\Pr(i) \in (\mathbb{P}_{\overline{\mathcal{S}}_{q^2}} \uplus \mathbb{P}_{\overline{\mathcal{S}}_{q^2}}) \bmod q^2$, which is the probability of $a_1 s_1 + a_2 s_2 = b_2 \to \mathbb{Z}_{q^2}$, and so on. We find that this relationship is consistent with the relationship $i_{n+1} = T_{i_n} i_n$, where

$$T_{i_n} = \begin{pmatrix} i_n^{(0)} & i_n^{(q^2-1)} & \cdots & i_n^{(1)} \\ i_n^{(1)} & i_n^{(0)} & \cdots & i_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ i_n^{(q^2-1)} & i_n^{(q^2-2)} & \cdots & i_n^{(0)} \end{pmatrix},$$

$i_n^{(j)} = \Pr(j)$. So the idea arose whether we could leverage the theory of fixed points to prove the convergence of this sequence, and perhaps even establish the hardness of Inner Product Ring LWE? Indeed, it is affirmative, because $\{T_{i_n} i_n\}_{n=1}$ satisfies the conditions of the fixed-point theorem, namely, $\{T_{i_n} i_n\}$ is a Cauchy sequence, and it converges to

$$v := \overbrace{\left(\frac{1}{q^2}, \frac{1}{q^2}, \ldots, \frac{1}{q^2}\right)}^{q^2}.$$

However, it is worth noting that T_{i_n} has more than one fixed point. So why does it only converge to v? This is because the other fixed points take the form $i^{(k)} = 1$, $i^{(l)} = 0$, where $l \neq k$, $k \in \mathbb{Z}_{q^2}$. However, the previous analysis on probabilities indicates that $i_n^{(j)} < 1$. Therefore, it will only converge to v. Furthermore, we can obtain

$$\|i_{n+1} - i_n\| \leq \kappa \|i_n - i_{n-1}\| \leq \cdots \leq \kappa^{n-1} \|i_2 - i_1\|.$$

Therefore, as long as κ^{n-1} meets the requirement.

To make Inner Product Ring LWE resistant to quantum attacks, reduce the difficulty of breaking Inner Product Ring LWE to the Dihedral Coset Problem. Cite the conclusion from [BKSW18], which states that the Extrapolated Dihedral Coset Problem can be reduced to the Dihedral Coset Problem. It is hoped that the Inner Product Ring LWE is also difficult. Therefore, we assume there exists an efficient algorithm $\mathcal{W}$ that can solve the Inner Product Ring LWE in polynomial time. Using this algorithm, we solve the Extrapolated Dihedral Coset Problem, leading to

$$m O(\mathcal{W}) \geq O(\Lambda, \beta) \geq O((2n)!) \text{ or } O(e^{2n}).$$

Let $m = \text{ploy}(n)$, it known that

$$O(\mathcal{W}) \geq \frac{O(\Lambda, \beta)}{\text{ploy}(n)} \geq \frac{O((2n)!)}{\text{ploy}(n)} \text{ or } \frac{O(e^{2n})}{\text{ploy}(n)}.$$

This contradicts the assumption that there exists an efficient algorithm $\mathcal{W}$ that can solve the Inner Product Ring LWE problem in polynomial time, therefore proving the theorem.

2 Preliminary

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, use the symbol $\mathcal{P}(\mathcal{L})$ to replace $\mathcal{P}(v_1, \ldots, v_n)$. $\forall x \in \mathbb{R}^n$, project it onto $\mathcal{P}(\mathcal{L})$. According to the properties of projection, there is a unique $y \in \mathcal{P}(\mathcal{L})$ makes $y - x \in \mathcal{L}$. 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.

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, there is $v_i = \sum_{j=1}^{n} m_{ij} u_j$ 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, 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

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

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

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

So there is

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

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

SIS problem [Ajt96, dZ20]. Given the integers n, m, q and the positive number β. The shortest integer solution problem is to randomly select vector $\alpha_i \in \mathbb{Z}_q^{n\times 1}$, $i \in \{1,\ldots,m\}$. The matrix $A \in \mathbb{Z}_q^{n\times m}$, find the non-zero integer coefficient vector $z \in \mathbb{Z}_q^{m\times 1}$, $\|z\| \le \beta$, 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 [Yue20, LPR10, SD18]. Given f_1, ..., $f_m \in \mathcal{R}_q$, where $\mathcal{R}_q$ is a polynomial ring with modulus q, find m polynomials g_1, ..., g_m whose coefficients are not all 0, $g_i \in \mathcal{R}_{\{0,\pm 1\}}, i \in \{1,\ldots,m\}$, 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

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

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

$$(1-x)\tilde{g}(x) = x^n - 1 = 0. \tag{2.1}$$

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

$$\mathcal{F}(x)\mathcal{G}(x) = \sum_{i=1}^m f_i g_i = 0, \text{let } \mathcal{G}(x) = (\tilde{g}(x), \overbrace{0,\ldots,0}^{m-1}).$$

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, 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?

Lemma 1. *If* $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ *is a multiple of* $(x-1)$*, then* $\sum_{i=0}^{n-1} a_i = 0$*.*

Proof. 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 $n = k+1$, assume that $f'(x) = b_0 + b_1x + \cdots + b_kx^k$ and

$$\begin{aligned} f(x) = f'(x)(x-1) &= (b_0 + b_1x + \cdots + b_kx^k)(x-1) \\ &= (b_0 + b_1x + \cdots + b_{k-1}x^{k-1})(x-1) + b_kx^k(x-1) \\ &= \underbrace{a_0 + a_1x + \cdots + a_kx^k}_{\text{(a)}} + \underbrace{b_kx^k(x-1)}_{\text{(b)}}. \end{aligned}$$

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 ([Yue20])**.** *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 ([Nor66])**.** *For* $q \in \mathbb{Z}$*, the prime distribution over the set* $\mathcal{S}_q = \{1, \ldots, q\}$ *satisfies the following relationship:*

$$\lim_{q\to\infty} \frac{\pi(q)}{\int_2^q \frac{1}{\ln(t)} dt} = 1,$$

where $\pi(q)$ *denotes the number of primes.*

Definition 3 ([GSM18], page 32, Section 4.1.6)**.** *We say that* $\varepsilon(n)$ *is negligible associated with* n *if* $\varepsilon(n)$ *can be expressed as*

$$\varepsilon(n) = \frac{1}{O(e^n)},$$

and the notation $O(n)$ *represents a quantity that grows at most as fast as* n *approaches infinity.*

3 Definition and Reduction of Inner Product Ring-LWE

Definition 4 (Inner Product Ring-LWE Problem)**.** *For any* $a_1, a_2, b \in \mathcal{R}_q$*, find* (s_1, s_2) *such that* $b = a_1s_1 + a_2s_2 + e$*.*

3.1 Inner product Ring LWE resistance to quantum attacks

Definition 5 (Dihedral Coset Problem)**.** *Given a security parameter* κ*, an instance from* DCP_q^ℓ*, where* N *denotes the modulus and* ℓ *represents the number of states. Each state is expressed as*

$$|0\rangle|x_i\rangle + |1\rangle|(x_i + s) \bmod q\rangle, \text{ for } i \le \ell,$$

and stores $1 + \lceil \log_2 q \rceil$ *bits, where* $x \in_R \mathbb{Z}_q$*,* $s \in \mathbb{Z}_q$*. If* s *can be recovered with probability poly*$(1/\log q)$ *in poly*$(\log q)$ *time, then the* DCP_q^ℓ *problem is considered broken.*

Definition 6 (Extrapolated Dihedral Coset Problem)**.** *Given a security parameter κ, an instance from $EDCP^{\ell}n, q, \rho$, where q denotes the modulus, ρ is a probability density function, and ℓ represents the number of states. Each state is expressed as*

$$\sum j \in supp(\rho)\rho(j)|j\rangle|(x_i + js) \bmod q\rangle, \quad for\ i \leq \ell,$$

and stores $1+\lceil \log_2 q \rceil$ bits, where $x_i \in_R \mathbb{Z}_q^n$, $s \in \mathbb{Z}_q^n$. If s can be recovered with probability poly$(1/(n \log q))$ in poly$(n \log q)$ time, then the $EDCP^{\ell}_{n,q,\rho}$ problem is considered broken.

Lemma 4. *If there exists an algorithm that solves the $EDCP^{\ell}_{n,q,\rho}$ problem, then there also exists an algorithm that solves the DCP^{ℓ}_{q} problem.*

Proof. Let

$$|b\rangle = \frac{1}{\sqrt{2}}|0\rangle|x_i\rangle + \frac{1}{\sqrt{2}}|1\rangle|(x_i + s) \bmod q\rangle.$$

Thus, $\rho(0)|0\rangle = \frac{1}{\sqrt{2}}|0\rangle$ and $\rho(1)|1\rangle = \frac{1}{\sqrt{2}}|1\rangle$. Therefore, DCP^{ℓ}_{q} is a special case of $EDCP^{\ell}_{n,q,\rho}$. Hence, if there exists an algorithm that solves $EDCP^{\ell}_{n,q,\rho}$, then there also exists an algorithm that solves DCP^{ℓ}_{q}. □

Lemma 5. *Let $(n, q, r = \Omega(\sqrt{\kappa}))$ be an instance of G-EDCP, and (n, q, α) an instance of LWE. If there exists an algorithm to solve $LWE_{n,q,\alpha}$, then there exists an algorithm to solve $G\text{-}EDCP^{\ell}_{n,q,\rho_r}$.*

Theorem 1. *Let (n, q, α) be an instance of inner product Ring LWE. Assuming G-EDCP is hard, there is no efficient algorithm that can solve inner product Ring LWE in polynomial time.*

Proof. For an instance of inner product Ring LWE,

$$\begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} + e = b.$$

Let $a = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$, which can be transformed into a circulant matrix form as

$$A := \begin{pmatrix} a_0 & -a_{n-1} & \cdots & -a_1 \\ a_1 & a_0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{pmatrix}.$$

Thus,

$$\begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} + e = b \Rightarrow \begin{pmatrix} A_1 & A_2 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} + e = b.$$

Here, $a = (a_0, a_1, \ldots, a_{n-1}) \leftarrow a = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$. By contradiction, assume there exists an efficient algorithm $\mathcal{W}$ that solves Inner Product Ring LWE in polynomial time. From $\begin{pmatrix} A_1 & A_2 \end{pmatrix}$, take the first row as α_1, where $\alpha_1 s + e_1 = b_1$, with e_1 and b_1 being the first components of e and b. Similarly, derive $\alpha_2, \ldots, \alpha_m$ from $m-1$ inner product Ring LWE, let

$$\Lambda = (\alpha_1, \alpha_2, \ldots, \alpha_m), \beta = (b_1, b_2, \ldots, b_m), \varepsilon = (e_1, e_2, \ldots, e_m).$$

Thus,

$$\beta = \Lambda s + \varepsilon. \tag{3.1}$$

Assume the time complexity to find s from Equation (3.1) is $O(\Lambda, \beta)$. According to Lemma 5, we have

$$mO(\mathcal{W}) \geq O(\Lambda, \beta) \geq O((2n)!) \text{ or } O(e^{2n}).$$

Let $m = \text{poly}(n)$, then

$$O(\mathcal{W}) \geq \frac{O(\Lambda, \beta)}{\text{poly}(n)} \geq \frac{O((2n)!)}{\text{poly}(n)} \text{ or } \frac{O(e^{2n})}{\text{poly}(n)}.$$

This contradicts the assumption "there exists an efficient algorithm $\mathcal{W}$ that can solve inner product Ring-LWE in polynomial time", hence the theorem holds. □

3.2 Inner product Ring LWE pseudorandomness

Claim 1. *Let $\pi(q)$ denote the number of prime numbers in the set $\mathcal{S}_q$, and let $P_q := \{p_1, \ldots, p_{\pi(q)}\}$ be the set of all prime numbers. Then, the number of prime numbers in the set $\mathcal{S}_q \times \mathcal{S}_q$ is still $\pi(q)$, and we have*

$$\overline{\mathcal{S}}_{q^2} := \mathcal{S}_q \times \mathcal{S}_q = \mathcal{S}_{q^2} \setminus \left\{\mathcal{S}_q \times (P_{q^2} \setminus P_q)\right\}.$$

Claim 2. *For the set $\mathcal{S}_q$, for an element $a \in \overline{\mathcal{S}}_{q^2}$ with prime factorization $\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_\ell^{\alpha_\ell}$, the probability of a occurring in the set $\overline{\mathcal{S}}_{q^2}$ is*

$$\Pr(a) := \frac{CN_q(a)}{q^2} = \sum_{\mathfrak{P}_1, \mathfrak{P}_2 \in \overline{\mathcal{S}}_q} \frac{2}{q^2},$$

where $\mathfrak{P}_1 = \mathfrak{p}_1^{\alpha_1'} \cdots \mathfrak{p}_\ell^{\alpha_\ell'}$, $\mathfrak{P}_2 = \mathfrak{p}_1^{\alpha_1''} \cdots \mathfrak{p}_\ell^{\alpha_\ell''}$, $\alpha_i' + \alpha_i'' = \alpha_i$, $i \in \mathcal{S}$.

Claim 3. *For the set $\mathcal{S}_q$, where each event occurs with probability q^{-1}, then for the set $\mathcal{S}_q \times \mathcal{S}_q$, the probability of each event a occurring is*

$$\Pr(a) = \begin{cases} \dfrac{1}{q^2}, & a = 1, \\ \dfrac{2}{q^2}, & a \text{ is prime}, \\ \dfrac{CN_q(a)}{q^2}, & a \text{ is composite}. \end{cases}$$

Claim 4. *For $\mathfrak{A} \in \overline{\mathcal{S}}_{q^2}$, and assuming*

$$\Pr(\mathfrak{A}) = \max_{a \in \overline{\mathcal{S}}_{q^2}} \Pr(a) = \frac{CN_q(\mathfrak{A})}{q^2},$$

then for any $k \in (\overline{\mathcal{S}}_{q^2} + \overline{\mathcal{S}}_{q^2}) \bmod q^2 \to \mathcal{S}_{q^2}$, we have

$$0 \leq \Pr(\mathfrak{A}) = \frac{CN_q(\mathfrak{A})}{q^2}.$$

Proof.

$$\begin{aligned} \Pr(k) &= \sum_{i=1}^{k} \Pr(i) \Pr(k+i-1) + \sum_{i=k+1}^{q+k-1} \Pr(i) \Pr(q+k+1-i) \\ &= \sum_{i=1}^{k} \frac{a_i}{q^2} \frac{a_{k+i-1}}{q^2} + \sum_{i=k+1}^{q+k-1} \frac{a_i}{q^2} \frac{a_{q+k+1-i}}{q^2} \\ &\leq \frac{CN_q(\mathfrak{A})}{q^2} \sum_{i=1}^{q^2} \frac{a_i}{q^2} = \frac{CN_q(\mathfrak{A})}{q^2}, \end{aligned}$$

and

$$\Pr(k) = \sum_{i=1}^{k} \Pr(i) \Pr(k+i-1) + \sum_{i=k+1}^{q+k-1} \Pr(i) \Pr(q+k+1-i) \geq 0.$$

□

Definition 7 ([Ceg12], Definition 2.1.6)**.** *Let $\mathcal{H}$ be a Hilbert space, and let $T : \mathcal{H} \to \mathcal{H}$ be an operator. If $T(\cdot)$ satisfies*

$$\|Tx - Ty\| < \|x - y\|, \ \forall x, \ y \in \mathcal{H},$$

then $T(\cdot)$ is called a contraction operator.

Lemma 6 ([Ceg12], Proposition 2.1.11)**.** *If $\mathcal{H}$ is a closed set (every Cauchy sequence in $\mathcal{H}$ converges to a point within $\mathcal{H}$), and $T(\cdot)$ is a contraction operator, and $Fix(T)$ is a closed convex set, then the algorithm $x_{n+1} = Tx_n$ converges to some $x \in Fix(T)$, where $Fix(T)$ denotes the set of fixed points of the operator $T(\cdot)$.*

Remark 1. *The convergence mentioned in Lemma 6 should be considered as strong convergence. However, this paper does not discuss the difference between strong and weak convergence, because in finite dimensions strong and weak convergence are equivalent.*

Fact 3. *Suppose that* $\mathbb{P}_{\mathcal{S}_q} := \{\Pr(0), \ldots, \Pr(q-1)\}$*, then* $\mathbb{P}_{\overline{\mathcal{S}}_{q^2}}$.

Fact 4. *Suppose that* $\mathbb{P}_{\overline{\mathcal{S}}_{q^2}} = \{\Pr(0), \ldots, \Pr(q^2-1)\}$*, then*

$$\mathbb{P}_{\mathcal{S}_{q^2}} := \{\acute{\Pr}(0), \ldots, \acute{\Pr}(q^2)\} := \mathbb{P}_{\overline{\mathcal{S}}_{q^2}} \uplus \mathbb{P}_{\overline{\mathcal{S}}_{q^2}} \bmod q^2. \text{ Here,}$$

$$\begin{aligned}
\acute{\Pr}(0) &= \Pr(0)\Pr(0) + \sum_{j=1}^{q^2} \Pr(j)\Pr(q^2-j),\\
\acute{\Pr}(1) &= \sum_{i=1}^{2} \Pr(i-1)\Pr(2-i) + \sum_{j=2}^{q^2} \Pr(j)\Pr(q^2+1-j),\\
&\vdots\\
\acute{\Pr}(q^2-1) &= \sum_{i=1}^{q^2} \Pr(i-1)\Pr(n-i).
\end{aligned}$$

Furthermore, there is also

$$\mathbb{P}'_{\mathcal{S}_{q^2}} := \{\acute{\Pr}(0), \ldots, \acute{\Pr}(q^2-1)\} := \mathbb{P}_{\mathcal{S}_{q^2}} \uplus \mathbb{P}_{\mathcal{S}_{q^2}} \bmod q^2. \text{ Here,}$$

$$\begin{aligned}
\acute{\Pr}(0) &= \acute{\Pr}(0)\acute{\Pr}(0) + \sum_{j=1}^{q^2} \acute{\Pr}(j)\acute{\Pr}(q^2-j),\\
\acute{\Pr}(1) &= \sum_{i=1}^{2} \acute{\Pr}(i-1)\acute{\Pr}(2-i) + \sum_{j=2}^{q^2} \acute{\Pr}(j)\acute{\Pr}(q^2+1-j),\\
&\vdots\\
\acute{\Pr}(q^2-1) &= \sum_{i=1}^{q^2} \acute{\Pr}(i-1)\acute{\Pr}(n-i).
\end{aligned} \tag{3.2}$$

The equation (3.2) *can be rewritten as*

$$\mathbb{P}'_{\mathcal{S}_{q^2}} = \begin{pmatrix} \Pr'(0) & \Pr'(q^2-1) & \cdots & \Pr'(1) \\ \Pr'(1) & \Pr'(0) & \cdots & \Pr'(2) \\ \vdots & \vdots & \ddots & \vdots \\ \Pr'(q^2-1) & \Pr'(q^2-2) & \cdots & \Pr'(0) \end{pmatrix} \begin{pmatrix} \Pr'(0) \\ \Pr'(1) \\ \vdots \\ \Pr'(q^2-1) \end{pmatrix} = M_{\mathbb{P}_{\mathcal{S}_{q^2}}} \mathbb{P}_{\mathcal{S}_{q^2}}.$$

Fact 5. *For the sequence* $\mathbb{P}^{(n)}_{\mathcal{S}_{q^2}} = M_{\mathbb{P}^{(n-1)}_{\mathcal{S}_{q^2}}} \mathbb{P}^{(n-1)}_{\mathcal{S}_{q^2}}$*, define*

$$\mathbb{P}^{(n)}_{\mathcal{S}_{q^2}} = (a_n^{(0)}, a_n^{(1)}, \ldots, a_n^{(q^2-1)}) = \left(\frac{1}{q^2} + \Delta_n^{(0)}, \frac{1}{q^2} + \Delta_n^{(1)}, \ldots, \frac{1}{q^2} + \Delta_n^{(q^2-1)}\right).$$

Claim 5. *The sequence* $\mathbb{P}^{(n)}_{\mathcal{S}_{q^2}} = M_{\mathbb{P}^{(n-1)}_{\mathcal{S}_{q^2}}} \mathbb{P}^{(n-1)}_{\mathcal{S}_{q^2}}$ *is a Cauchy sequence.*

Proof. To prove that $\mathbb{P}^{(n)}_{\mathcal{S}_{q^2}} = M_{\mathbb{P}^{(n-1)}_{\mathcal{S}_{q^2}}} \mathbb{P}^{(n-1)}_{\mathcal{S}_{q^2}}$ forms a Cauchy sequence, it suffices to show that for any $\delta > 0$, there exists an $N > 0$ such that for any $n > N$,

$$\left\| \mathbb{P}^{(n)}_{\mathcal{S}_{q^2}} - \mathbb{P}^{(n-1)}_{\mathcal{S}_{q^2}} \right\| \leq \delta.$$

Because

$$\mathbb{P}^{(n)}_{\mathcal{S}_{q^2}} - \mathbb{P}^{(n-1)}_{\mathcal{S}_{q^2}} = \begin{pmatrix} \Delta_0^{(n-1)} & \Delta_{q^2-1}^{(n-1)} & \cdots & \Delta_1^{(n-1)} \\ \Delta_1^{(n-1)} & \Delta_0^{(n-1)} & \cdots & \Delta_2^{(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{q^2-1}^{(n-1)} & \Delta_{q^2-2}^{(n-1)} & \cdots & \Delta_0^{(n-1)} \end{pmatrix} \begin{pmatrix} \Delta_0^{(n-1)} \\ \Delta_1^{(n-1)} \\ \vdots \\ \Delta_{q^2-1}^{(n-1)} \end{pmatrix}.$$

And

$$\begin{aligned} &\left\| \begin{pmatrix} \Pr'(0) & \Pr'(q^2-1) & \cdots & \Pr'(1) \\ \Pr'(1) & \Pr'(0) & \cdots & \Pr'(2) \\ \vdots & \vdots & \ddots & \vdots \\ \Pr'(q^2-1) & \Pr'(q^2-2) & \cdots & \Pr'(0) \end{pmatrix} \right\| \\ &= \sqrt{q^4 \left(\sum_{i=1}^{k} (\frac{a_i}{q^2} - \frac{1}{q^2})(\frac{a_{k+i-1}}{q^2} - \frac{1}{q^2}) + \sum_{i=k+1}^{q+k-1} (\frac{a_i}{q^2} - \frac{1}{q^2})(\frac{a_{q+k+1-i}}{q^2} - \frac{1}{q^2}) \right)^2} \\ &\leq \sqrt{(\frac{CN_q(\mathfrak{A})}{q^2} - \frac{1}{q^2}) \sum_{i=1}^{q^2} (\frac{a_i}{q^2} - \frac{1}{q^2})} = \frac{\sqrt{CN_q(\mathfrak{A}) - 1}}{q} \end{aligned}$$

So, it is obtained that

$$\left\| \mathbb{P}^{(n)}_{\{0,1,2\}} - \mathbb{P}^{(n-1)}_{\{0,1,2\}} \right\| \leq \left(\frac{\sqrt{CN_q(\mathfrak{A}) - 1}}{q} \right)^{n-1} \left\| \mathbb{P}^{(1)}_{\{0,1,2\}} - \mathbb{P}^{(0)}_{\{0,1,2\}} \right\| \leq \sqrt{CN_q(\mathfrak{A}) - 1} \left(\frac{\sqrt{CN_q(\mathfrak{A}) - 1}}{q} \right)^n.$$

□

Lemma 7. *For any initial vector $a_0 = (a_0^{(0)}, a_0^{(1)}, \ldots, a_0^{(q^2-1)})$, where $a_0^{(i)} \in [0, \frac{CN_q(\mathfrak{A})}{q^2}]$ and $\sum_{i=0}^{2} a_0^{(i)} = 1$, the matrix M_{a_0} is generated as follows:*

$$M_{a_0} = \begin{pmatrix} a_0^{(0)} & a_0^{(q^2-1)} & \cdots & a_0^{(1)} \\ a_0^{(1)} & a_0^{(0)} & \cdots & a_0^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ a_0^{(q^2-1)} & a_0^{(q^2-2)} & \cdots & a_0^{(0)} \end{pmatrix}.$$

Then, let $a_{n+1} := M_{a_n} a_n := T a_n$, then $\{a_n\}_{n=0}^{\infty}$ is a Cauchy sequence and converges to $v = (\overbrace{\frac{1}{q^2}, \frac{1}{q^2}, \ldots, \frac{1}{q^2}}^{q^2})$.

Proof. According to Claim 5, we know that $\begin{pmatrix} \Delta_0^{(n-1)} & \Delta_{q^2-1}^{(n-1)} & \cdots & \Delta_1^{(n-1)} \\ \Delta_1^{(n-1)} & \Delta_0^{(n-1)} & \cdots & \Delta_2^{(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{q^2-1}^{(n-1)} & \Delta_{q^2-2}^{(n-1)} & \cdots & \Delta_0^{(n-1)} \end{pmatrix}$ is a contraction operator, and

$$\left\| \begin{pmatrix} \Delta_0^{(n-1)} & \Delta_{q^2-1}^{(n-1)} & \cdots & \Delta_1^{(n-1)} \\ \Delta_1^{(n-1)} & \Delta_0^{(n-1)} & \cdots & \Delta_2^{(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{q^2-1}^{(n-1)} & \Delta_{q^2-2}^{(n-1)} & \cdots & \Delta_0^{(n-1)} \end{pmatrix} \right\| \leq \frac{\sqrt{CN_q(\mathfrak{A}) - 1}}{q}.$$

Therefore, the matrix $\begin{pmatrix} \Delta_0^{(n-1)} & \Delta_{q^2-1}^{(n-1)} & \cdots & \Delta_1^{(n-1)} \\ \Delta_1^{(n-1)} & \Delta_0^{(n-1)} & \cdots & \Delta_2^{(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{q^2-1}^{(n-1)} & \Delta_{q^2-2}^{(n-1)} & \cdots & \Delta_0^{(n-1)} \end{pmatrix}$ is contractive, with $(\overbrace{0, 0, \ldots, 0}^{q^2})$ being both a convergent point and a fixed point of this matrix sequence. Moreover, since $a_{n+1} := M_{a_n} a_n$ has been

proven to be a Cauchy sequence, the sequence $\{a_n\}_{n=0}^{\infty}$ converges, and it converges to the fixed point of $T(\cdot)$. □

Theorem 2. *Given $\{a_j\}_{j=0}^{2}$ and $\{s_j\}_{j=1}^{2}$ such that $a_j \in_R \mathbb{Z}_q$, $s \in \mathbb{Z}_q$. Then for any $i = 0, 1, \ldots, q^2 - 1$, we have*

$$\max_{i=0,1,\ldots,q^2-1} \left| \Pr\left(\sum_{j=0}^{2} (a_j s_j) = i \right) - \Pr(u = i) \right| \leq \sqrt{CN_q(\mathfrak{A}) - 1} \left(\frac{\sqrt{CN_q(\mathfrak{A}) - 1}}{q} \right)^n .$$

Corollary 2. *For any $a \in \mathcal{R}_q$, $s \in \mathcal{R}_q$, and $u \in_R \mathcal{R}_q$, then the indistinguishability probability between as and u is bounded by $\sqrt{CN_q(\mathfrak{A}) - 1} \left(\frac{\sqrt{CN_q(\mathfrak{A})-1}}{q} \right)^n$.*

Corollary 3. *For any $a_1, a_2, s_1, s_2, e \in \mathcal{R}_q$, and $u \in_R \mathcal{R}_q$, then the indistinguishability probability between $a_1 s_1 + a_2 s_2 + e$ and u is bounded by $O\left(\sqrt{CN_q(\mathfrak{A}) - 1} \left(\frac{\sqrt{CN_q(\mathfrak{A})-1}}{q} \right)^n \right)$.*

Proof.

$$\begin{aligned} a_1 s_1 + a_2 s_2 + e &\approx_C u_1 + a_2 s_2 + e \\ &\approx_C u_2 + e \\ &\approx_C u_3. \end{aligned}$$

□

4 Trapdoor Function Construction

4.1 Inner Product Ring LWE Trapdoor

Let $g = 2^{n-1}$, $gz + e = b \Rightarrow 2^{n-1} z + e = b$. Thus,

$$\begin{aligned} gz + e &= gz_0 + gz_1 x + \cdots + gz_{n-1} x^{n-1} + e \\ &= b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} + e. \end{aligned}$$

Therefore,

$$z_i = \begin{cases} 1, & b_i \geq \frac{3q}{4}, \\ 0, & b_i < \frac{q}{4}. \end{cases}$$

Let $a = (c, g - ct)$, where $c, t \in_R \mathcal{R}_q$. Thus,

$$a \begin{pmatrix} t \\ 1 \end{pmatrix} z + e = (c, g - ct) \begin{pmatrix} t \\ 1 \end{pmatrix} z + e = gz + e = b.$$

Therefore,

$$x = \begin{pmatrix} tz \\ z \end{pmatrix}.$$

However, this causes a distributional shift in x, with covariance

$$\mathbf{COV} = r^2 \begin{pmatrix} T \\ I \end{pmatrix} \begin{pmatrix} T & I \end{pmatrix}$$

of Gaussian distribution. Here, $T = \mathbf{Rot}(t)$. We need to compensate with another Gaussian distribution $\sigma^2 I - \mathbf{COV}$, i.e., draw a vector p from the Gaussian distribution $\sigma^2 I - \mathbf{COV}$, to compute

$$2^{n-1}z + e = b - ap = b - \begin{pmatrix} c & 2^{n-1} - ct \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}.$$

0. Input $a_1, a_2, b \in \mathcal{R}_q$, let $g = 2^{n-1}$.
1. Randomly choose $c, t \in \mathcal{R}_q$, and select a vector $\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$ from the Gaussian distribution of $\sigma^2 I - \mathbf{COV}$.
2. Compute z such that $b - (c, g - ct)(p_1, p_2)^T = gz + e$.

$$z_i = \begin{cases} 1, & |b - (c, g - ct)(p_1, p_2)^T|_i \geq \frac{3g}{4}, \\ 0, & |b - (c, g - ct)(p_1, p_2)^T|_i < \frac{g}{4}. \end{cases}$$

3. Output $a = (c, g - ct)$, $s = \begin{pmatrix} tz \\ z \end{pmatrix}$.

Figure 4: Trapdoor algorithm for Inner Product Ring LWE

Theorem 3. *For $a_1, a_2, c, t, u_1, u_2 \in_R \mathcal{R}_q$, where $g = 2^{n-1}$, it holds that $(c, g - ct) \approx_C (u_1, u_2)$.*

Proof. Since $g - ct$ is an affine transformation of ct, and c itself is a random element in $\mathcal{R}_q$, it suffices that $ct \approx_C u_2$. According to Corollary 2, for any $a \in \mathcal{R}_q$, $s \in \mathcal{R}_q$, and $u \in_R \mathcal{R}_q$, the indistinguishability probability between as and u is bounded by $\sqrt{CN_q(\mathfrak{A}) - 1} \left(\frac{\sqrt{CN_q(\mathfrak{A})-1}}{q} \right)^n$, completing the proof. □

4.2 Ring SIS New Trapdoor

Claim 6. *Let $q = 2^n$, $k \leq q$, $z = (z_0, z_1, \ldots, z_{k-1})^T \in \mathbb{Z}^k_{\{0,\pm 1\}}$, $G^T = (G_0 = 1, G_1 = 2, \ldots, G_{k-1} = 2^{k-1})$. Then, by iterating over all z, it is possible to ensure that for any $u \in \mathbb{Z}_q$, $G^T z = u$.*

Claim 7. *Let $q = 2^n$, $k \leq q$, $\mathcal{Z} = (\mathcal{Z}_0, \mathcal{Z}_1, \ldots, \mathcal{Z}_{k-1})^T \in \mathcal{R}^k_{\{0,\pm 1\}}$, $G^T = (G_0 = 1, G_1 = 2, \ldots, G_{k-1} = 2^{k-1})$. Then, by iterating over all $\mathcal{Z}$, it is possible to ensure that for any $u \in \mathcal{R}_q$, $G^T \mathcal{Z} = u$.*

Proof. Let

$$F^T = \left(h = gf^{-1}, a, G_1 - (as_1 + ge_1), \ldots, G_k - (as_k + ge_k)\right),$$
$$Z^T = \left(f \sum_{i=1}^{k} e_i x_i, \sum_{i=1}^{k} s_i x_i, x_1, \ldots, x_k\right).$$

Verify that

$$\begin{aligned} F^T Z &= hf(\sum_{i=1}^{k} e_i x_i) + a(\sum_{i=1}^{k} s_i x_i) + \sum_{i=1}^{k}(G_i - (as_i + ge_i)) \\ &= gf^{-1} f(\sum_{i=1}^{k} e_i x_i) + a(\sum_{i=1}^{k} s_i x_i) + \sum_{i=1}^{k}(G_i - (as_i + ge_i))x_i \\ &= \sum_{i=1}^{k} G_i x_i = u. \end{aligned}$$

For $Z^T = (f \sum_{i=1}^{k} e_i x_i, \sum_{i=1}^{k} s_i x_i, x_1, \ldots, x_k)$, its covariance is

$$\mathbf{COV} = r^2 \begin{pmatrix} R_1 \\ R_2 \\ I \end{pmatrix} \begin{pmatrix} R_1 & R_2 & I \end{pmatrix}$$

where $R_1 = [f\mathbf{Rot}(e_1), \ldots, f\mathbf{Rot}(e_k)]$, $R_2 = [\mathbf{Rot}(s_1), \ldots, \mathbf{Rot}(s_k)]$. Thus, we need compensation vectors from the Gaussian distribution of $\sigma^2 I - r^2\mathbf{COV}$. □

0. Input $u \in \mathcal{R}_q$, let $G^T = (1, 2, \ldots, 2^{k-1})$.
1. Randomly select $h, a, \{s\}_{n=0}^{k-1}, \{e\}_{n=0}^{k-1} \in \mathcal{R}_q$, and select vector $p^T = (p_1, \ldots, p_k)$ from the Gaussian distribution $\sigma^2 I - r^2\mathbf{COV}$. Here, $h = gf^{-1}$ is an instance of the NTRU problem.
2. Let $F^T = (h, a, G_1 - (as_1 + ge_1), \ldots, G_k - (as_k + ge_k))$, find $\mathcal{Z}$ such that $u - F^T p = G^T \mathcal{Z}$.
3. Output F^T, $Z^T = (f\sum_{i=1}^{k} e_i x_i, \sum_{i=1}^{k} s_i x_i, x_1, \ldots, x_k) + p$.

Figure 5: Trapdoor algorithm for Ring SIS

Definition 8 ([ABD16], note this may not be the first definition of the NTRU problem in the article)**.** *Given $h \in R_q$, find $(g, f) \in R_q^2$ such that $gh - f = 0 \pmod q$, or $h = g^{-1}f \pmod q$.*

Lemma 8 ([FPMSW23])**.** *If there exists an efficient algorithm $\mathcal{W}$ to solve the NTRU problem in polynomial time, then there also exists an efficient algorithm $\mathcal{W}'$ to solve the id-HSVP problem in polynomial time.*

Theorem 4. *Let $h = gf^{-1}$ be an instance of the NTRU problem, $G_0 = 1, G_1 = 2, \ldots, G_{k-1} = 2^{k-1}$, and $a, \{s_i\}_{i=1}^{k}$, $\{e_i\}_{i=1}^{k}$, $\{u_i\}_{i=1}^{k+2} \in \mathcal{R}_q$. Then,*

$$F^T = (h, a, G_1 - (as_1 + ge_1), \ldots, G_k - (as_k + ge_k)) \approx_C (u_{k+1}, u_{k+2}, u_1, \ldots, u_k).$$

Proof. Since $h = gf^{-1}$ is an instance of the NTRU problem, by Lemma 8 and $a \in \mathcal{R}_q$, we have $(h, a) \approx_C (u_{k+1}, u_{k+2})$. Because $G_i - (as_i + ge_i)$ is affine, it suffices to consider the randomness of $as_i + ge_i$. According to Corollary 3, $as_i + ge_i \approx_C u_i$. Therefore, the theorem is proved. □

5 Conclusion

This paper analyzes the issues with current ideal lattice trapdoor algorithms and provides a reasonable ideal lattice trapdoor algorithm. Since Ring LWE is not suitable for trapdoor construction, we propose a new problem based on Ring LWE, specifically Inner Product Ring LWE. We reduce inner product Ring LWE to hidden subgroup problems to ensure its quantum resistance, and demonstrate its indistinguishability from randomly selected elements.

References

[ABD16] Martin Albrecht, Shi Bai, and Léo Ducas. A subfield lattice attack on overstretched ntru assumptions. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016*, pages 153–178, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

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

[ARYY23] Shweta Agrawal, Mélissa Rossi, Anshu Yadav, and Shota Yamada. Constant input attribute based (and predicate) encryption from evasive and tensor lwe. In *Advances in Cryptology – CRYPTO 2023*, pages 532–564, Cham, 2023. Springer Nature Switzerland.

[BKSW18] Zvika Brakerski, Elena Kirshanova, Damien Stehlé, and Weiqiang Wen. Learning with errors and extrapolated dihedral cosets. In *Public-Key Cryptography – PKC 2018*, pages 702–727. Springer International Publishing, 2018.

[Ceg12] Andrzej Cegielski. *Iterative Methods for Fixed Point Problems in Hilbert Spaces*. 2012.

[DKRS03] Irit Dinur, Guy Kindler, Ran Raz, and Shmuel Safra. Approximating CVP to within almost-polynomial factors is NP-hard. *Combinatorica*, 23:205–243, 2003.

[dZ20] dabei Z. Sis problem, 2020.

[FPMSW23] Joël Felderhoff, Alice Pellet-Mary, Damien Stehlé, and Benjamin Wesolowski. Ideal-svp is hard for small-norm uniform prime ideals. In *Theory of Cryptography*, pages 63–92, Cham, 2023. Springer Nature Switzerland.

[GM18] Nicholas Genise and Daniele Micciancio. Faster gaussian sampling for trapdoor lattices with arbitrary modulus. In *Advances in Cryptology – EUROCRYPT 2018*, pages 174–203, Cham, 2018. Springer International Publishing.

[GMPW20] Nicholas Genise, Daniele Micciancio, Chris Peikert, and Michael Walter. Improved discrete gaussian and subgaussian analysis for lattice cryptography. In *Public-Key Cryptography – PKC 2020*, pages 623–651, Cham, 2020. Springer International Publishing.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, page 197 – 206, New York, NY, USA, 2008. Association for Computing Machinery.

[GSM18] Fuchun Guo, Willy Susilo, and Yi Mu. *Introduction to Security Reduction*. 2018.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. Ntru: A ring-based public key cryptosystem. In Joe P. Buhler, editor, *Algorithmic Number Theory*, pages 267–288, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg.

[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.

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *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 Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013*, pages 21–39, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[Nor66] Levinson Norman. On the elementary proof of the prime number theorem. *Proceedings of the Edinburgh Mathematical Society*, 15(2):141–146, 1966.

[PTDH23] Sihang Pu, Sri AravindaKrishnan Thyagarajan, Nico Döttling, and Lucjan Hanzlik. Post quantum fuzzy stealth signatures and applications. CCS '23, page 371 – 385, New York, NY, USA, 2023. Association for Computing Machinery.

[Reg02] Oded Regev. Quantum computation and lattice problems. In *Proceedings of the 43rd Symposium on Foundations of Computer Science*, FOCS '02, page 520 – 529, USA, 2002. IEEE Computer Society.

[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*, pages 84–93. Association for Computing Machinery, 2005.

[SD18] Noah Stephens-Davidowitz. Ring-sis and ideal lattices, 2018.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484 – 1509, oct 1997.

[Yue20] Steven Yue. Lattice learning notes 09: Ring-sis and ideal lattice, 2020.