Integer Version of Ring-LWE and its Applications

Gu Chunsheng

School of Computer Engineering, Jiangsu University of Technology, China
{chunsheng_gu}@163.com

Abstract. In this work, we describe an integer version of ring-LWE over the polynomial rings and prove that its hardness is equivalent to one of the polynomial ring-LWE. Moreover, we also present a public key cryptosystem using this variant of the polynomial ring-LWE.

Keywords: Ring-LWE, NTRU, public key cryptosystem, ideal lattice

1 Introduction

Many cryptographic schemes based on discrete logarithms and integer factoring problems are no longer secure once the quantum computer becomes a reality. This is because Shor [21] presented an efficient quantum algorithm that solves these hard problems. Currently, the most promising quantum-safe works are based on the hardness of lattice problems like LWE-based cryptosystems [20], Ring-LWE-based cryptosystems [13] and NTRU [11].

Compared with LWE, RLWE over the polynomial rings has an advantage of efficiency. This is because the LWE-based cryptographic schemes have key sizes and computation times that are at least quadratic in the security parameter. To improve the efficiency of these schemes, Lyubashevsky, Peikert, and Regev [13] defined a ring-based variant of LWE (RLWE) that uses algebraic structure, and described a polynomial time quantum reduction from worst-case problems on ideal lattices to the decisional RLWE. The LWE-based schemes can directly adapt to the RLWE-based analogues, whose key sizes and computation times reduce to almost linear in the security parameter. Furthermore, in recent years, several new cryptographic schemes have been proposed around the RLWE problem [4,6,14,15].

However, the RLWE over the polynomial rings also has some shortcomings. First, we can not compare the hardness relationship between the RLWE problems over the different polynomial rings. Second, there exist some weak RLWE instances over the polynomial rings, although these instances do not appear in RLWE-based applications [8,19,9]. Third, for the RLWE problems over the different polynomial rings, their computational efficiency is different and needs to be re-optimized implementation for each of them.

This work is the first step in trying to solve the above problems. That is, we describe an integer version of the ring-LWE over the polynomial rings and unify the framework of RLWEs over the different polynomial rings. We observe that the integer version of the hard problem recently appeared in the work [2]. In [2], Aggarwal, Joux, Prakash, and Santha proposed a new public-key cryptosystem (AJPS) using an integer version of NTRU, whose security relies on the conjectured hardness of the Mersenne low hamming ratio assumption. However, Beunardeau, Connolly, Géraud, and Naccache [3] presented an algorithm that recovers the secret key from the public key much faster than the security estimates in [2].

1.1 Our contribution

Our main contribution is to describe an integer variant of ring-LWE over the polynomial ring and show that its hardness is equivalent to that of the polynomial ring-LWE.

In the RLWE problem, given q a prime integer, and a list of samples $(\mathbf{a}_l, \mathbf{b}_l = \mathbf{a}_l\mathbf{s} + \mathbf{e}_l) \in R_q^2$, where $R_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$, $\mathbf{s} \in R_q$, $\mathbf{a}_l \in R_q$ are chosen independently and uniformly from $\mathbb{Z}_q^n$, and $\mathbf{e}_l$ is chosen independently according to the probability distribution $\chi = D_{\mathbb{Z}^n,\sigma}$, find $\mathbf{s}$. In the first variant of LWE, $\mathbf{s}$ is chosen from the error distribution χ rather than uniformly at random, the choice of other parameters remains unchanged. This variant becomes no easier to solve than the decisional LWE [17,1].

In this work, we introduce an integer version of RLWE over the polynomial rings (I-RLWE). In the I-RLWE problem, we replace x with q and convert RLWE into I-RLWE. Given $p = q^n + 1$, we draw many samples $(a_l, b_l = a_l s + e_l) \in \mathbb{Z}_p^2$, where $\mathbf{a}_l, \mathbf{s} \leftarrow R_q$, $\mathbf{e}_l \leftarrow D_{\mathbb{Z}^n,\sigma}$, and $a_l = \sum_{i=0}^{n} a_{l,i}q^i, s = \sum_{i=0}^{n} s_i q^i$, $e_l = \sum_{i=0}^{n} e_{l,i}q^i$, the problem is to find s. Similarly, we can also generate a variant by sampling from the error distribution $\mathbf{s} \leftarrow \chi$ and generating s. For this case, we also call to sample s from χ.

Our second contribution is to present a public key cryptosystem (PKC) based on I-RLWE. Given a sample of I-RLWE $(a, b = as + 2e) \in \mathbb{Z}_p^2$ that samples s, e from the error distribution χ, and plaintext $m = \sum_{i=0}^{n} m_i q^i$ with $\mathbf{m} \in \{0, 1\}^n$, one first chooses r, e_1, e_2 from χ, and generates a ciphertext as $(c_1 = [ar + 2e_1]_p, c_2 = [br + 2e_2 + m]_p)$. To decrypt the ciphertext (c_1, c_2), one computes $c = [c_2 - c_1 s]_p = [2e_2 + m - 2e_1 s]_p = \sum_{i=0}^{n} c_i q^i$, and recovers the plaintext $\mathbf{m}$ from c. This is because all c_i's that only depend χ are "small". Concrete details see Section 4.

Organization. Section 2 recalls some background. Section 3 describes an integer variant of RLWE and shows its hardness. Section 4 presents a public key cryptosystem using this variant of RLWE.

2 Preliminaries

2.1 Notations

Let $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ denote the ring of integers, the field of rational numbers, and the field of real numbers. Let n be a positive integer and power of 2. Notation $[n]$ denotes the set $\{1, 2, ..., n\}$. Let $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$, $R_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$, and $\mathbb{K} = \mathbb{Q}[x]/\langle x^n + 1\rangle$. Vectors are denoted in bold lowercase (e.g. $\mathbf{a}$), and matrices in bold uppercase (e.g. $\mathbf{A}$). We denote by a_j the j-th entry of a vector $\mathbf{a}$, and $a_{i,j}$ the element of the i-th row and j-th column of $\mathbf{A}$. We denote by $\|\mathbf{a}\|_2$ (abbreviated as $\|\mathbf{a}\|$) the Euclidian norm of $\mathbf{a}$. For $\mathbf{A} \in R^{d\times d}$, we define $\|\mathbf{A}\| = \max\{\|a_{i,j}\|, i, j \in [d]\}$, where $\|a_{i,j}\|$ is the Euclidian norm corresponding to the coefficient vector of $a_{i,j}$.

We denote $[a]_q = a \bmod q \in [0, q-1]$ throughout this work. Similarly, for $\mathbf{a} \in \mathbb{Z}^n$ (or $a \in R$), $[\mathbf{a}]_q$ denotes each entry (or each coefficient) $[a_j]_q \in [0, q-1]$ of $\mathbf{a}$ (or a).

2.2 Lattices and Ideal Lattices

An n-dimensional full-rank lattice $L \subset \mathbb{R}^n$ is the set of all integer linear combinations $\sum_{i=1}^{n} y_i\mathbf{b}_i$ of n linearly independent vectors $\mathbf{b}_i \in \mathbb{R}^n$. If we arrange the vectors $\mathbf{b}_i$ as the columns of matrix $\mathbf{B} \in \mathbb{R}^{n\times n}$, then $L = \{\mathbf{By} : \mathbf{y} \in \mathbb{Z}^n\}$. We say that $\mathbf{B}$ spans L if $\mathbf{B}$ is a basis for L. Given a basis $\mathbf{B}$ of L, we define $P(\mathbf{B}) = \{\mathbf{By}|\mathbf{y} \in \mathbb{R}^n \text{ and } y_i \in [-1/2, 1/2)\}$ as the parallelization corresponding to $\mathbf{B}$. We let $\det(\mathbf{B})$ be the determinant of $\mathbf{B}$.

Given $g \in R$, we let $I = \langle g\rangle$ be the principal ideal lattice in R generated by g, whose $\mathbb{Z}$-basis is $Rot(g) = (g, x \cdot g, ..., x^{n-1} \cdot g)$.

Given $\mathbf{c} \in \mathbb{R}^n$, $\sigma > 0$, the Gaussian distribution of a lattice L is defined as $D_{L,\sigma,\mathbf{c}} = \rho_{\sigma,\mathbf{c}}(\mathbf{x})/\rho_{\sigma,\mathbf{c}}(L)$ for $\mathbf{x} \in L$, where $\rho_{\sigma,\mathbf{c}}(\mathbf{x}) = \exp(-\pi\|\mathbf{x} - \mathbf{c}\|^2/\sigma^2))$, $\rho_{\sigma,\mathbf{c}}(L) = \sum_{\mathbf{x}\in L} \rho_{\sigma,\mathbf{c}}(\mathbf{x})$. In the following, we will write $D_{L,\sigma,\mathbf{0}}$ as $D_{L,\sigma}$. We denote a Gaussian sample as $x \leftarrow D_{L,\sigma}$ (or $d \leftarrow D_{I,\sigma}$) over the lattice L (or ideal lattice I).

Micciancio and Regev [16] introduced the smoothing parameter of lattices. For an n-dimensional lattice L, and positive real $\epsilon > 0$, we define its smoothing parameter $\eta_\epsilon(L)$ to be the smallest s such that $\rho_{1/s}(L^*\backslash\{0\}) \leq \epsilon$, where L^* is the dual lattice of L.

Lemma 2.1 (Lemma 3.3 [16]). For any n-dimensional lattice L and positive real $\epsilon > 0$, $\eta_\epsilon(L) \leq \sqrt{\ln(2n(1 + 1/\epsilon))/\pi} \cdot \lambda_n(L)$.

Lemma 2.2 (Lemma 4.4 [16]). For any n-dimensional lattice L, vector $\mathbf{c} \in \mathbb{R}^n$ and reals $0 < \epsilon < 1$, $s \geq \eta_\epsilon(L)$, we have

$$\Pr_{\mathbf{x}\leftarrow D_{L,s,\mathbf{c}}}\{\|\mathbf{x} - \mathbf{c}\| > s\sqrt{n}\} \leq \frac{1+\epsilon}{1-\epsilon} \cdot 2^{-n}.$$

2.3 Ring-LWE in Polynomial Rings

Throughout this paper, we only consider the integer version of ring-LWE for the special ring R. However, we notice if the expansion factor of a polynomial ring $R = \mathbb{Z}_q[x]/\langle f(x)\rangle$ is small, then one can directly generate the integer version of this ring using our method. For the ring-LWE defined by the number fields [13], we will further study their integer versions.

For simplicity, we define the ring-LWE over the polynomial rings. We sample a secret $\mathbf{s} \in R$ from some Gaussian distribution instead of uniform distribution over R_q, since the latter is easily be transformed into the former [17,1].

Definition 2.3 (Ring-LWE Distribution). Let Ψ be a Gaussian distribution with parameter σ over R. Given a secret $\mathbf{s} \leftarrow D_{\mathbb{Z}^n,\sigma}$, a sample from the ring-LWE distribution $A_{\mathbf{s},\sigma}$ over $R_q \times R_q$ is generated by choosing $\mathbf{a} \leftarrow R_q$, $\mathbf{e} \leftarrow D_{\mathbb{Z}^n,\sigma}$, and outputting $(\mathbf{a}, \mathbf{b} = \mathbf{as} + \mathbf{e}) \in R_q \times R_q$.

Definition 2.4 (Computational Ring-LWE). The computational ring-LWE problem, denoted $\mathrm{RLWE}_{q,\sigma}$, is defined as follows: given arbitrary many independent samples from $A_{\mathbf{s},\sigma}$, find $\mathbf{s}$.

Definition 2.5 (Decisional Ring-LWE). The decisional ring-LWE problem, denoted $\mathrm{DRLWE}_{q,\sigma}$, is to distinguish with non-negligible advantage between arbitrary many independent samples from $A_{\mathbf{s},\sigma}$, and the same number of uniformly random and independent samples from $R_q \times R_q$.

According to [7], the ring-LWE over the polynomial ring $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ is equivalent to the hard ring-LWE defined in [13].

Lemma 2.6 (Theorem 3.6 [13]). Let $\mathbb{K}$ be the mth cyclotomic number field having dimension $n = \varphi(m)$ and $R = O_{\mathbb{K}}$ be its ring of integers. Let $\alpha < \sqrt{\log n/n}$, and $q \geq 2$, $q = 1 \mod m$ be a poly(n)-bounded prime such that $\alpha q \geq \omega(\sqrt{\log n})$. Then there is a polynomial-time quantum reduction from $O(\sqrt{n}/\alpha)$-approximate SIVP (or SVP) on ideal lattices in $\mathbb{K}$ to $\mathrm{DRLWE}_{q,\sigma}$, where $\sigma = \alpha(n/\log n)^{1/4}$.

3 Integer version of Ring-LWE

Here we describe an integer variant of the ring-LWE over the polynomial rings, and prove that its hardness is equivalent to that of the polynomial RLWE.

For simplicity, let n be the security parameter, $q > n^3$ be a prime, $p = q^n + 1$, χ be a Gaussian distribution with parameter $\sigma = \sqrt{n}$ over R, unless otherwise stated.

Definition 3.1 (I-RLWE Distribution). Given a secret $s = \sum_{i=0}^{n-1} s_i q^i$ with $\mathbf{s} \leftarrow D_{\mathbb{Z}^n,\sigma}$, a sample from the I-RLWE distribution $A_{s,\sigma}$ over $\mathbb{Z}_p \times \mathbb{Z}_p$ is generated by choosing at random $a \leftarrow \mathbb{Z}_p$, $e = \sum_{i=0}^{n-1} e_i q^i$ with $\mathbf{e} \leftarrow D_{\mathbb{Z}^n,\sigma}$, and outputting $(a, b = as + e) \in \mathbb{Z}_p \times \mathbb{Z}_p$.

Definition 3.2 (Computational I-RLWE). The computational integer ring-LWE problem, denoted $\text{I-RLWE}_{q,\sigma}$, is defined as follows: given arbitrary many independent samples from $A_{s,\sigma}$, find s.

Definition 3.3 (Decisional I-RLWE). The decisional integer ring-LWE problem, denoted I-DRLWE$_{q,\sigma}$, is to distinguish with non-negligible advantage between arbitrary many independent samples from $A_{s,\sigma}$, and the same number of uniformly random and independent samples from $\mathbb{Z}_p \times \mathbb{Z}_p$.

Before giving the hardness of I-RLWE, we first prove the following several lemmas.

Given an element $\mathbf{f} \in R$, if all coefficients $f_i, i \in \{0, \cdots, n-1\}$ of $\mathbf{f}$ are small, then we can generate an integer modulo p corresponding to $\mathbf{f}$.

Lemma 3.4 Suppose that $f = \left[\sum_{i=0}^{n-1} f_i q^i\right]_p = \sum_{i=0}^{n-1} h_i q^i$ with $|f_i| < q/2 - 1$. Then

$$h_i = [f_i - \overline{h}_{i-1}]_q = \begin{cases} f_i - \overline{h}_{i-1} & f_i - \overline{h}_{i-1} \geq 0 \\ f_i - \overline{h}_{i-1} + q & f_i - \overline{h}_{i-1} < 0 \end{cases}$$

where for $i \in [n-1]$,

$$\overline{h}_{i-1} = \begin{cases} 0 & h_{i-1} \leq q/2 \\ 1 & h_{i-1} > q/2 \end{cases};$$

for $i = 0$,

$$\overline{h}_{-1} = \overline{h}_{n-1} = \begin{cases} 0 & h_{n-1} \leq q/2 \\ -1 & h_{n-1} > q/2 \end{cases}.$$

Proof. First, we determine $\overline{h}_{n-1}$ by f_{n-1} as follows:

Case 1: $f_{n-1} < 0$.

Since $h_{n-1} = [f_{n-1} - \overline{h}_{n-2}]_q$ and $\overline{h}_{n-2} \geq 0$, we have $f_{n-1} - \overline{h}_{n-2} < 0$. So, $h_{n-1} > q/2$ and $\overline{h}_{-1} = -1$.

Case 2: $f_{n-1} > 0$.

By $\overline{h}_{n-2} \leq 1$, we get $f_{n-1} - \overline{h}_{n-2} \geq 0$. So, $h_{n-1} < q/2$ and $\overline{h}_{n-1} = 0$.

Case 3: $f_{n-1} = 0$.

In this case, $\overline{h}_{n-1}$ depends on f_{n-2}. $\overline{h}_{-1} = -1$ when $f_{n-2} < 0$, and $\overline{h}_{n-1} = 0$ when $f_{n-1} > 0$.

Similarly, if $f_{n-2} = 0$, then $\overline{h}_{n-1}$ recursively depends on $f_{n-3}, \cdots, f_1$.

Now we use the induction method to prove the result.

For induction basis, consider $i = 0$.

If $\overline{h}_{n-1} = -1$, then $h_{n-1} > q/2$. So, $f = \sum_{i=0}^{n-1} h_i q^i > \sum_{i=0}^{n-1} |f_i| q^i$ by $|f_i| < q/2 - 1$. As a result, $f_{n-1} < 0$.

Again, by $|f_i| < q/2 - 1$, we have $-p < \sum_{i=0}^{n-1} f_i q^i < 0$. Hence,

$$\begin{aligned} f &= \sum_{i=0}^{n-1} f_i q^i + p \\ &= \sum_{i=0}^{n-1} f_i q^i + q^n + 1 \\ &= (f_{n-1} + q)q^{n-1} + \sum_{i=1}^{n-2} f_i q^i + f_0 + 1 \\ &= (f_{n-1} + q)q^{n-1} + \sum_{i=1}^{n-2} f_i q^i + f_0 - \overline{h}_{n-1} \end{aligned}$$

That is, $h_0 = [f]_q = [f_0 - \overline{h}_{n-1}]_q$. Hence, if $f_0 - \overline{h}_{n-1} < 0$, then $h_0 = f_0 - \overline{h}_{n-1} + q$, otherwise $h_0 = f_0 - \overline{h}_{n-1}$.

If $\overline{h}_{n-1} = 0$, then $0 \le h_{n-1} \le q/2$. So, $f = \sum_{i=0}^{n-1} h_i q^i = \sum_{i=0}^{n-1} f_i q^i$ by $|f_i| < q/2 - 1$. Consequence, $f_{n-1} \ge 0$. Hence, $h_0 = [f]_q = [f_0]_q = [f_0 - \overline{h}_{n-1}]_q$.

By induction step, we assume that h_i is correct for $i \le k$.

Now, we prove $i = k+1$.

Since $f = \left[\sum_{i=0}^{n-1} f_i q^i\right]_p = \sum_{i=0}^{n-1} f_i q^i + rp$ for some $r \in \{0,1\}$, we have

$$\begin{aligned} [f]_{q^{k+2}} &= \left[\sum_{i=0}^{n-1} f_i q^i + rp\right]_{q^{k+2}} \\ &= \left[\sum_{i=0}^{k+1} f_i q^i + r\right]_{q^{k+2}} \\ &= \sum_{i=0}^{k+1} h_i q^i \end{aligned}.$$

If $h_k > q/2$, then $\overline{h}_k = 1$ and $f_k - \overline{h}_{k-1} < 0$. So, $-q^{k+1}/2 < \sum_{i=0}^{k} f_i q^i + r < 0$ by $|f_i| < q/2 - 1$. That is, $\sum_{i=0}^{k} h_i q^i = q^{k+1} + \sum_{i=0}^{k} f_i q^i + r$. Thus,

$$\begin{aligned} \left[\sum_{i=0}^{k+1} f_i q^i + r\right]_{q^{k+2}} &= \left[(f_{k+1}-1)q^{k+1} + q^{k+1} + \sum_{i=0}^{k} f_i q^i + r\right]_{q^{k+2}} \\ &= \left[(f_{k+1}-1)q^{k+1} + \sum_{i=0}^{k} h_i q^i\right]_{q^{k+2}} \\ &= \sum_{i=0}^{k+1} h_i q^i \end{aligned}$$

Hence, we obtain $h_{k+1} = [f_{k+1} - 1]_q = [f_{k+1} - \overline{h}_k]_q$.

If $h_k < q/2$, then $\overline{h}_k = 0$ and $f_k - \overline{h}_{k-1} > 0$. Similarly, we can get $h_{k+1} = [f_{k+1}]_q = [f_{k+1} - \overline{h}_k]_q$. ∎

Given two ring elements $\mathbf{f}, \mathbf{g} \in R$, if their coefficients are all "small", then the corresponding integer of their product is equal to the product of their corresponding integers modulo p.

Lemma 3.5 Suppose that $f = \left[\sum_{i=0}^{n-1} f_i q^i\right]_p$, $g = \left[\sum_{i=0}^{n-1} g_i q^i\right]_p$ with $\mathbf{f} \leftarrow D_{\mathbb{Z}^n,\sigma}$, $\mathbf{g} \leftarrow D_{\mathbb{Z}^n,\sigma}$. Then $h = [fg]_p = \sum_{i=0}^{n-1} h_i q^i$, where

$$\begin{aligned} h_i &= \left[\sum_{[j+k]_n = i} (-1)^{\lfloor (j+k)/n \rfloor} f_j g_k - \overline{h}_{i-1}\right]_q, \\ \overline{h}_{i-1} &= \begin{cases} 0 & h_{i-1} \le q/2 \\ 1 & h_{i-1} > q/2 \end{cases}, i \in [n-1]; \\ \overline{h}_{i-1} = \overline{h}_{n-1} &= \begin{cases} 0 & h_{n-1} \le q/2 \\ -1 & h_{n-1} > q/2 \end{cases}, i = 0. \end{aligned}$$

Proof. By $f = \left[\sum_{j=0}^{n-1} f_j q^j\right]_p$, $g = \left[\sum_{k=0}^{n-1} g_k q^k\right]_p$, we have

$$\begin{aligned} h &= [fg]_p \\ &= [\sum_{j=0}^{n-1} f_j q^j \times \sum_{k=0}^{n-1} g_k q^k]_p \\ &= [\sum_{i=0}^{n-1} a_i q^i]_p, \end{aligned}$$

where $a_i = \sum_{[j+k]_n=i} (-1)^{\lfloor (j+k)/n \rfloor} f_j g_k, i = 0, 1, \cdots, n-1$.

By Lemma 2.2, $|f_j| < n$, $|g_k| < n$ with overwhelming probability. So, we have $|a_i| \leq \sum_{[j+k]_n=i} |f_j||g_k| \leq n^3 < q/2 - 1$.

Hence, the result is directly obtained by Lemma 3.4. ∎

In Lemma 3.5, we only consider the product of two ring elements with "small" coefficients. However, in the RLWE problem, only the coefficients of one element are "small" , the coefficients of another element are uniformly distributed modulo q. So, in the following lemma, we give the relationship between the product of the corresponding integers of two elements and the corresponding integer of the product of two elements.

Lemma 3.6 Given $\mathbf{a} \leftarrow R_q$, $\mathbf{s} \leftarrow D_{\mathbb{Z}^n,\sigma}$, $\mathbf{b} = \mathbf{as} \in R_q$, suppose that

$$a = \left[\sum_{i=0}^{n-1} a_i q^i\right]_p, b = \left[\sum_{i=0}^{n-1} b_i q^i\right]_p, s = \left[\sum_{i=0}^{n-1} s_i q^i\right]_p.$$

Then,

$$[as - b]_p = \sum_{i=0}^{n-1} r_i q^i,$$

where

$$\begin{cases} |r_i| < n^2 - n + 3 & r_i \leq q/2 \\ |r_i - q| < n^2 - n + 3 & r_i > q/2 \end{cases}.$$

Proof. By $\mathbf{b} = \mathbf{as} \in R_q$, we have

$$\begin{aligned} b_i &= \left[\sum_{[j+k]_n=i} (-1)^{\lfloor (j+k)/n \rfloor} a_j s_k\right]_q \\ &= \sum_{[j+k]_n=i} (-1)^{\lfloor (j+k)/n \rfloor} a_j s_k + c_{b_i} q \end{aligned}$$

Since $\mathbf{s} \leftarrow D_{\mathbb{Z}^n,\sigma}$, $|s_k| < n$ by Lemma 2.2. By $\mathbf{a} \leftarrow R_q$, $|a_j| < q$. So

$$\begin{aligned} |\sum_{[j+k]_n=i} (-1)^{\lfloor (j+k)/n \rfloor} a_j s_k| &\leqq \sum_{[j+k]_n=i} |a_j||s_k| \\ &\leqq \sum_{[j+k]_n=i} (n-1)|a_j| \\ &< n(n-1)q \end{aligned}$$

Hence $|c_{b_i}| < n(n-1)+1$.

Let $h = [as]_p = \sum_{i=0}^{n-1} h_i q^i$. Then,

$$\begin{aligned} h_i &= \left[\sum_{[j+k]_n=i} (-1)^{\lfloor (j+k)/n \rfloor} a_j s_k + c_{b_{i-1}} - \overline{h}_{i-1}\right]_q \\ &= \left[b_i - c_{b_i} q + c_{b_{i-1}} - \overline{h}_{i-1}\right]_q \\ &= \left[b_i + c_{b_{i-1}} - \overline{h}_{i-1}\right]_q, \end{aligned}$$

where for $i \in [n-1]$,

$$\overline{h}_{i-1} = \begin{cases} 0 & 0 \le b_{i-1} + c_{b_{i-2}} - \overline{h}_{i-2} < q \\ 1 & b_{i-1} + c_{b_{i-2}} - \overline{h}_{i-2} < 0 \\ -1 & b_{i-1} + c_{b_{i-2}} - \overline{h}_{i-2} \ge q \end{cases};$$

for $i = 0$,

$$\overline{h}_{-1} = \overline{h}_{n-1} = \begin{cases} 0 & 0 \le b_{n-1} + c_{b_{n-2}} - \overline{h}_{n-2} < q \\ -1 & b_{n-1} + c_{b_{n-2}} - \overline{h}_{n-2} < 0 \\ 1 & b_{n-1} + c_{b_{n-2}} - \overline{h}_{n-2} \ge q \end{cases}.$$

Thus, we obtain

$$\begin{aligned} [as-b]_p &= [h-b]_p \\ &= [\sum_{i=0}^{n-1} (h_i - b_i) q^i]_p \\ &= \left[(-c_{b_{n-1}} + \overline{h}_{n-1}) q^0 + \sum_{i=1}^{n-1} (c_{b_{i-1}} - \overline{h}_{i-1}) q^i\right]_p \\ &= \sum_{i=0}^{n-1} r_i q^i, \end{aligned}$$

Since $|c_{b_i}| + |\overline{h}_i| < n^2 - n + 2 < q/2 - 1$, $i \in \{0, 1, \cdots, n-1\}$, so by Lemma 3.4

$$r_i = \begin{cases} [-c_{b_{n-1}} + \overline{h}_{n-1} + \overline{r}_{n-1}]_q & i = 0 \\ [c_{b_{i-1}} - \overline{h}_{i-1} - \overline{r}_{i-1}]_q & i \in [n-1]. \end{cases}$$

where, for $i \in [n-1]$,

$$\overline{r}_{i-1} = \begin{cases} 0 & r_{i-1} \le q/2 \\ 1 & r_{i-1} > q/2 \end{cases};$$

for $i = 0$,

$$\overline{r}_{-1} = \overline{r}_{n-1} = \begin{cases} 0 & r_{n-1} \le q/2 \\ -1 & r_{n-1} > q/2 \end{cases}.$$

The result follows by $|c_{b_i}| + |\overline{h}_i| + |\overline{r}_{i-1}| < n^2 - n + 3$. $\blacksquare$

After the above preparations, we now come to the position of the main results in this work. In the following Lemma 3.7, we convert a sample of RLWE into a sample of I-RLWE, whose noise increases a n factor than that of the origin RLWE sample. In contrast, in Lemma 3.8, we convert a sample of I-RLWE into a sample of RLWE, also at the expense of increasing noise.

Lemma 3.7 Given a sample of RLWE $(\mathbf{a}, \mathbf{b}^{'} = \mathbf{as} + \mathbf{e}) \in R_q \times R_q$, there exists a polynomial time algorithm, which transforms this sample into a sample of I-RLWE $(a, b^{'} = as + e^{'}) \in \mathbb{Z}_p \times \mathbb{Z}_p$, such that

$$a = \sum\nolimits_{i=0}^{n-1} a_i q^i, b^{'} = \sum\nolimits_{i=0}^{n-1} b_i^{'} q^i, s = \sum\nolimits_{i=0}^{n-1} s_i q^i,$$
$$e^{'} = \sum\nolimits_{i=0}^{n-1} e_i^{'} q^i, \text{where} \begin{cases} |e_i^{'}| < n^2 + 6 & e_i^{'} \leq q/2 \\ |e_i^{'} - q| < n^2 + 6 & e_i^{'} > q/2 \end{cases}$$

Proof. We denote $\mathbf{b} = \mathbf{as} \in R_q$, and $\mathbf{b}^{'} = \mathbf{b} + \mathbf{e} \in R_q$.

Let $h = [as]_p = \sum\nolimits_{i=0}^{n-1} h_i q^i$, $b = \left[\sum\nolimits_{i=0}^{n-1} b_i q^i\right]_p$.

By Lemma 3.6,

$$[b - h]_p = [\sum\nolimits_{i=0}^{n-1} (b_i - h_i) q^i]_p = \sum\nolimits_{i=0}^{n-1} r_i q^i,$$

where $b_i - h_i = r_i + k_i q$ with $r_i \in [0, q-1]$, $|k_i| \leq 1$.

By Lemma 2.2, $|e_i| < n$. So, $b_i^{'} = [b_i + e_i]_q = b_i + e_i + d_i q$ such that $|d_i| \leq 1$. That is, $b^{'} = \sum\nolimits_{i=0}^{n-1} b_i^{'} q^i = \sum\nolimits_{i=0}^{n-1} (b_i + e_i + d_i q) q^i$.

Hence,

$$\begin{aligned} [b^{'} - as]_p &= [b^{'} - h]_p \\ &= [\sum\nolimits_{i=0}^{n-1} (b_i^{'} - h_i) q^i]_p \\ &= [\sum\nolimits_{i=0}^{n-1} (b_i + e_i + d_i q - h_i) q^i]_p \\ &= [\sum\nolimits_{i=0}^{n-1} ((b_i - h_i) + e_i + d_i q) q^i]_p \\ &= [\sum\nolimits_{i=0}^{n-1} (r_i + k_i q + e_i + d_i q) q^i]_p \\ &= [(r_0 - k_{n-1} + e_0 - d_{n-1}) q^0 + \sum\nolimits_{i=1}^{n-1} (r_i + k_{i-1} + e_i + d_{i-1}) q^i]_p \\ &= \sum\nolimits_{i=0}^{n-1} e_i^{'} q^i \end{aligned}$$

It is not difficult to verify $e_i^{'} = r_i + k_{i-1} + e_i + d_{i-1} - \overline{e}_{i-1}^{'}$, where for $i \in [n-1]$,

$$\overline{e}_{i-1}^{'} = \begin{cases} 0 & 0 \leq r_{i-1} + k_{i-2} + e_{i-1} + d_{i-2} + \overline{e}_{i-2}^{'} < q \\ 1 & r_{i-1} + k_{i-2} + e_{i-1} + d_{i-2} + \overline{e}_{i-2}^{'} < 0 \\ -1 & r_{i-1} + k_{i-2} + e_{i-1} + d_{i-2} + \overline{e}_{i-2}^{'} \geq q \end{cases};$$

for $i = 0$,

$$\overline{e}^{'}_{i-1} = \begin{cases} 0 & 0 \le r_{i-1} + k_{i-2} + e_{i-1} + d_{i-2} + \overline{e}^{'}_{i-2} < q \\ -1 & r_{i-1} + k_{i-2} + e_{i-1} + d_{i-2} + \overline{e}^{'}_{i-2} < 0 \\ 1 & r_{i-1} + k_{i-2} + e_{i-1} + d_{i-2} + \overline{e}^{'}_{i-2} \ge q \end{cases}.$$

Let $\widetilde{r}_i = \begin{cases} r_i & r_i \le q/2 \\ r_i - q & r_i > q/2 \end{cases}$, and $\widetilde{e}^{'}_i = \widetilde{r}_i + k_{i-1} + e_i + d_{i-1} - \overline{e}^{'}_{i-1}$.

Since $|e_i| < n$, $|k_{i-1}| \le 1$, $|d_{i-1}| \le 1$, $|\overline{e}^{'}_{i-1}| \le 1$, and $|\widetilde{r}_i| < n^2 - n + 3$ by Lemma 3.6, we obtain $|\widetilde{e}^{'}_i| < n^2 + 6$.

The proof is complete. ∎

Lemma 3.8 Given a sample of I-RLWE $(a, b^{'} = as + e) \in \mathbb{Z}_p \times \mathbb{Z}_p$, there exists a polynomial time algorithm, which transforms this sample into a sample of RLWE $(\mathbf{a}, \mathbf{b}^{'} = \mathbf{as} + \mathbf{e}^{'}) \in R_q \times R_q$, such that

$$\begin{cases} |e^{'}_i| < n^2 + 3 & e^{'}_i \le q/2 \\ |e^{'}_i - q| < n^2 + 3 & e^{'}_i > q/2 \end{cases}$$

Proof. By $a = \sum_{i=0}^{n-1} a_i q^i$, $b^{'} = \sum_{i=0}^{n-1} b^{'}_i q^i$, $s = \sum_{i=0}^{n-1} s_i q^i$, we generate

$$\mathbf{a} = (a_0, a_1, \cdots, a_{n-1}),$$
$$\mathbf{b}^{'} = (b^{'}_0, b^{'}_1, \cdots, b^{'}_{n-1}).$$

We denote $\mathbf{b} = \mathbf{as} \in R_q$, and $b = \sum_{i=0}^{n-1} b_i q^i$.

Let $h = [as]_p = \sum_{i=0}^{n-1} h_i q^i$. Then by Lemma 3.6,

$$\begin{aligned} h_i &= \left[\sum_{[j+k]_n = i} (-1)^{\lfloor (j+k)/n \rfloor} a_j s_k + c_{b_{i-1}} - \overline{h}_{i-1}\right]_q \\ &= \left[b_i + c_{b_{i-1}} - \overline{h}_{i-1}\right]_q, \end{aligned}$$

By $e = \sum_{i=0}^{n-1} e_i q^i$, we get

$$\begin{aligned} b^{'} &= [as + e]_p \\ &= [\sum_{i=0}^{n-1} (h_i + e_i) q^i]_p \\ &= [\sum_{i=0}^{n-1} (b_i + c_{b_{i-1}} - \overline{h}_{i-1} + e_i) q^i]_p \\ &= \sum_{i=0}^{n-1} b^{'}_i q^i \end{aligned}$$

Hence, $b^{'}_i = b_i + c_{b_{i-1}} - \overline{h}_{i-1} + e_i + \overline{b}^{'}_{i-1}$, where for $i \in [n-1]$,

$$\overline{b}^{'}_{i-1} = \begin{cases} 0 & 0 \le b_{i-1} + c_{b_{i-2}} - \overline{h}_{i-2} + e_{i-1} + \overline{b}^{'}_{i-2} < q \\ 1 & b_{i-1} + c_{b_{i-2}} - \overline{h}_{i-2} + e_{i-1} + \overline{b}^{'}_{i-2} < 0 \\ -1 & b_{i-1} + c_{b_{i-2}} - \overline{h}_{i-2} + e_{i-1} + \overline{b}^{'}_{i-2} \ge q \end{cases};$$

for $i = 0$,

$$\overline{b}^{'}_{i-1} = \begin{cases} 0 & 0 \leq b_{i-1} + c_{b_{i-2}} - \overline{h}_{i-2} + e_{i-1} + \overline{b}^{'}_{i-2} < q \\ -1 & b_{i-1} + c_{b_{i-2}} - \overline{h}_{i-2} + e_{i-1} + \overline{b}^{'}_{i-2} < 0 \\ 1 & b_{i-1} + c_{b_{i-2}} - \overline{h}_{i-2} + e_{i-1} + \overline{b}^{'}_{i-2} \geq q \end{cases}.$$

Now by $\mathbf{b}^{'} = \mathbf{as} + \mathbf{e}^{'} = \mathbf{b} + \mathbf{e}^{'} \in R_q$, we have

$$e^{'}_i = [b^{'}_i - b_i]_q = [c_{b_{i-1}} - \overline{h}_{i-1} + e_i + \overline{b}^{'}_{i-1}]_q.$$

Since $|e_i| < n$, $|c_{b_i}| < n(n-1) + 1$ by Lemma 2.2, 3.6, thus we have,

$$|c_{b_{i-1}} - \overline{h}_{i-1} + e_i + \overline{b}^{'}_{i-1}| < n(n-1) + 1 + 1 + n + 1 = n^2 + 3.$$

The proof is complete. ∎

For simplicity, in the proofs of Lemma 3.7, 3.8, we directly use n as the noise upper bound of a new sample, instead of $O(\sqrt{n}\sigma)$ by Lemma 2.2. In fact, we have showed that the Gaussian noise parameter in the converting samples becomes $O(n\sigma)$. Of course, we can also add a Gaussian noise with parameter $O(n\sigma)$ to a converted sample to refresh its noise. Thus, we have obtained the following results from Lemma 3.7, 3.8.

Theorem 3.9 The decisional ring-LWE problem $\mathrm{DRLWE}_{q,\sigma}$ is reduced to the decisional integer ring-LWE problem $\text{I-DRLWE}_{q,O(n\sigma)}$. Moreover, the decisional integer ring-LWE problem $\text{I-DRLWE}_{q,\sigma}$ is reduced to the decisional ring-LWE problem $\mathrm{DRLWE}_{q,O(n\sigma)}$.

Proof. By Lemma 3.7, 3.8, the result directly follows from the transformation of samples between them. ∎

4 Public key cryptosystem

In this section, we first present a public key cryptosystem based on the integer version of ring-LWE over the polynomial rings (I-RLWE), then show its correctness and security.

4.1 Construction

Let n be the security parameter.

Key Generation: $(pk, sk) \leftarrow \mathrm{KeyGen}(1^n)$.

(1) Choose a prime $q = O(n^3)$, and set $p = q^n + 1$.

(2) Choose at random $a \leftarrow \mathbb{Z}_p$.

(3) Sample $\mathbf{s} \leftarrow D_{\mathbb{Z}^n,\sigma}$, $\mathbf{e} \leftarrow D_{\mathbb{Z}^n,\sigma}$ with $\sigma = O(\sqrt{n})$.

(4) Set $s = \sum_{i=0}^{n-1} s_i q^i$, $e = \sum_{i=0}^{n-1} 2e_i q^i$.

(5) Set $b = [as + e]_p$.

(6) Output the public key $pk = \{q, (a, b)\}$, and the secret key $sk = \{s\}$.

Encryption: $(c_1, c_2) \leftarrow \mathrm{Enc}(pk, \mathbf{m})$.

(1) Given a plaintext $\mathbf{m} \in \{0,1\}^n$, set $m = \sum_{i=0}^{n-1} m_i q^i$.

(2) Sample $\mathbf{r} \leftarrow D_{\mathbb{Z}^n,\sigma}$, $\mathbf{e}_1, \mathbf{e}_2 \leftarrow D_{\mathbb{Z}^n,\sigma}$.

(3) Set $r = \sum_{i=0}^{n-1} r_i q^i$, $e_j = \sum_{i=0}^{n-1} 2e_{j_i} q^i, j \in [2]$.

(4) Compute $c_1 = [ar + e_1]_p$, $c_2 = [br + e_2 + m]_p$.

(5) Output (c_1, c_2) a ciphertext.

Decryption: $\mathbf{m} \leftarrow \mathrm{Dec}(sk, (c_1, c_2))$.

```
(1) Given $sk$ and a ciphertext $(c_1, c_2)$, compute $t_0 = [c_2 - c_1 s]_p$.
(2) For $i = 0, 1, \cdots, n-1$
        (2.1) Compute $d_i = [t_i]_q$.
        (2.2) Compute $t_{i+1} = \lfloor t_i / q \rfloor$.
        (2.3) If $d_i > q/2$, then set $d_i = d_i - q$, $t_{i+1} = t_{i+1} + 1$.
(3) Set $d_0 = d_0 - 1$ if $d_{n-1} < 0$.
(4) Set $m_i = [d_i]_2, i \in \{0, 1, \cdots, n-1\}$.
(5) Output the plaintext $\mathbf{m}$.
```

Remark 4.1 (1) Our scheme uses the parity of noise in a ciphertext to encode a plaintext. Similar to [13], we can also use $\lfloor q/2 \rfloor$ to compute $m = \sum_{i=0}^{n-1} (m_i \lfloor q/2 \rfloor) q^i$ and generate a ciphertext. In this case, the decryption algorithm seem to be easier. That is, it directly determines the ith plaintext bit by checking d_i. If $q/4 < d_i < (3/4)q$, then $m_i = 1$; otherwise $m_i = 0$.

(2) To improve the efficiency of our scheme, we can use some special number $q = 2^t$ with a positive integer t. This is because the encryption and decryption algorithms take less time. Furthermore, the multiplication between two large integers can directly apply FFT-based algorithms [10], as a result, our scheme can use an arbitrary positive integer n instead of $n = 2^k$ in RLWE that is to use FFT-based algorithms.

(3) The NTRU scheme over the polynomial rings [11,22] can be directly converted into an integer scheme of NTRU. For example, consider the NTRU scheme in [22]. Let $q = 2^t, p = q^n - 1$ with a prime n, the public key $\mathbf{h} = \mathbf{3f}/(\mathbf{3g}{+}\mathbf{1}) \in \mathbb{Z}_q[x]/\langle x^n - 1 \rangle$, and the secret key $\mathbf{s} = \mathbf{3g}{+}\mathbf{1} \in \mathbb{Z}[x]/\langle x^n - 1 \rangle$. Then, one can generate an integer scheme of NTRU as follows: the public key is $h = \left[\sum_{i=0}^{n-1} h_i q^i \right]_p$, and the secret key $s = \left[\sum_{i=0}^{n-1} s_i q^i \right]_p$.

4.2 Correctness

For the correctness of our scheme, we only require to prove that the algorithm Dec correctly recover the plaintext in a ciphertext.

Lemma 4.2 Given sk and a ciphertext (c_1, c_2), the algorithm Dec correctly decrypts the plaintext $\mathbf{m}$.

Proof. By Enc, we have $c_1 = [ar+e_1]_p$, $c_2 = [br+e_2+m]_p$. Since $b = [as+e]_p$, by Dec, we get

$$\begin{aligned} t_0 &= [c_2 - c_1 s]_p \\ &= [br + e_2 + m - (ar + e_1)s]_p \\ &= [er + e_2 - e_1 s + m]_p \\ &= \sum\nolimits_{i=0}^{n-1} d_i q^i. \end{aligned}$$

Since $r = \sum\nolimits_{i=0}^{n-1} r_i q^i$, $s = \sum\nolimits_{i=0}^{n-1} s_i q^i$, $e = \sum\nolimits_{i=0}^{n-1} 2e_i q^i$, $e_j = \sum\nolimits_{i=0}^{n-1} 2e_{j_i} q^i$, we obtain

$$\begin{aligned} er &= [\sum\nolimits_{i=0}^{n-1}(2\sum\nolimits_{[j+k]_n=i}(-1)^{\lfloor (j+k)/n \rfloor} e_j r_k)q^i]_p = [\sum\nolimits_{i=0}^{n-1} 2u_i q^i]_p \\ e_1 s &= [\sum\nolimits_{i=0}^{n-1}(2\sum\nolimits_{[j+k]_n=i}(-1)^{\lfloor (j+k)/n \rfloor} e_{1_j} s_k)q^i]_p = [\sum\nolimits_{i=0}^{n-1} 2v_i q^i]_p \\ t_0 &= [er + e_2 - e_1 s + m]_p = [\sum\nolimits_{i=0}^{n-1}(2u_i + 2e_{2_i} - 2v_i + m_i)q^i]_p = \sum\nolimits_{i=0}^{n-1} d_i q^i \end{aligned}$$

Using Lemma 2.2, we get $|2u_i| < 2n^3$, $|2v_i| < 2n^3$, $|2e_{1_i}| < 2n$. So,

$$|2u_i + 2e_{2_i} - 2v_i + m_i| < 4n^3 + 2n + 1 < q/2 - 1, i \in \{0, 1, \cdots, n-1\}.$$

By Lemma 3.4, $d_i = [2u_i + 2e_{2_i} - 2v_i + m_i - \overline{d}_{i-1}]_q, i \in \{0, 1, \cdots, n-1\}$.
For $i = 0$, we have

$$\begin{aligned} d_0 &= [2u_0 + 2e_{2_0} - 2v_0 + m_0 - \overline{d}_{n-1}]_q \\ &= \begin{cases} 2u_0 + 2e_{2_0} - 2v_0 + m_0 - \overline{d}_{n-1} & 2u_0 + 2e_{2_0} - 2v_0 + m_0 - \overline{d}_{n-1} \geq 0 \\ 2u_0 + 2e_{2_0} - 2v_0 + m_0 - \overline{d}_{n-1} + q & 2u_0 + 2e_{2_0} - 2v_0 + m_0 - \overline{d}_{n-1} < 0 \end{cases} \end{aligned}$$

By Step (2.3), if $d_0 > q/2$, then $d_0 = d_0 - q = 2u_0 + 2e_{2_0} - 2v_0 + m_0 - \overline{d}_{n-1}$, otherwise $d_0 = 2u_0 + 2e_{2_0} - 2v_0 + m_0 - \overline{d}_{n-1}$.

Using Step (3), the algorithm Dec subtracts $\overline{d}_{n-1}$ according to the sign of d_{n-1}, and obtain $d_0 = 2u_0 + 2e_{2_0} - 2v_0 + m_0$. Thus, $m_0 = [d_0]_2$ by Step (4).

Similarly, Dec can correctly recover all other bits of the plaintext $\mathbf{m}$ by $m_i = [d_i]_2, i \in \{1, \cdots, n-1\}$. ■

4.3 Security

Similar to [13], the semantic security of our scheme follows from two applications of the pseudorandomness of I-RLWE. So, the security of our public key cryptosystem depends on the hardness of I-RLWE, which is equivalent to the hardness of RLWE by Theorem 3.9.

5 Implementation and Comparison

To evaluate the encryption and decryption capabilities of the proposed approach, and access its consuming time on different security level, we conduct one group of experiments. The experiment environment setup is as follows. We implemented our NTRU-type public key cryptosystem over the NTL library. All programs were run on the physical machine, which has a 3.20GHz Intel Core i5-3470 processor, and 8GB of RAM.

Table 1 is our concrete parameter settings, and Table 2 is the performance comparison of I-RLWE and RLWE.

From our experiments result, we notice that if we directly encrypt plaintexts by applying our public key scheme, its performance is relatively weak, especially for the ciphertext expansion rate. However, if we use our public key scheme for key encapsulation mechanism, our scheme will be relatively practical.

Table 1. The concrete parameter settings of our implementation

Problem	Security level (bits)	n	q (prime)	σ	p	the size of pk (bits)	the size of sk (bits)
RLWE	80	512	134217757	23		28672	14336
RLWE	168	1024	1073741827	32		63488	31744
RLWE	200	1024	16411	2		30720	15360
RLWE	232	2048	32771	2		65536	32768
I-RLWE	80	512	134217757	23	q^n+1	28672	14336
I-RLWE	168	1024	1073741827	32	q^n+1	63488	31744
I-RLWE	200	1024	16411	2	q^n+1	30720	15360
I-RLWE	232	2048	32771	2	q^n+1	65536	32768

Table 2. The performance comparison of I-RLWE and RLWE

Problem	Security level (bits)	Length per plaintext (bits)	Length per ciphertext (bits)	Expansion rate	Time per encryption (ms)	Time per decryption (ms)	Successful rate (%)
RLWE	80	512	28672	56	22.06	16.54	100
RLWE	168	1024	63488	62	51.55	35.16	100
RLWE	200	1024	30720	30	39.29	19.00	100
RLWE	232	2048	65536	32	84.18	41.13	100
I-RLWE	80	512	28672	56	16.58	13.52	100
I-RLWE	168	1024	63488	62	66.81	113.78	100
I-RLWE	200	1024	30720	30	20.12	24.56	100
I-RLWE	232	2048	65536	32	77.93	99.06	100

Table 3. The concrete parameter settings of our NTRU-type scheme

Security level	λ	ρ	β	n	x^n+1	the size of pk	the size of sk
(bits)				(prime)	(the number of factors)	(bits)	(bits)
80	120	30	3600	18013	2	18013	3600
112	144	36	5184	25931	2	25931	5184
128	160	40	6400	32003	2	32001	6400
160	200	50	10000	50021	2	50021	10000

Table 4. The performance of our NTRU-type scheme

Security	Length per	Length per	Expansion	Time per	Time per	Testing	Successful
level	plaintext	ciphertext	rate	encryption	decryption	frequency	rate
(bits)	(bits)	(bits)		(ms)	(ms)		(%)
80	120	18013	150	3.382	3.198	2000	100
112	144	25931	180	5.744	5.547	2000	100
128	160	32003	200	7.693	8.209	2000	100
160	200	50021	250	11.613	15.735	2000	100

To further evaluate the performance of our scheme. In the following, we present computational experiments of our NTRU-type scheme. Table 3 is our concrete parameter settings. We define different security level with different parameter values. Table 4 is the performance result of our NTRU-type scheme. Note that the estimate of the security level mainly relies upon the time complexity of the classical meet-in-the-middle attack on our NTRU-type scheme.

When security level is 80 (λ=120, ρ=30, β=3600, n=18013), we have 100% successful rate for testing frequency=2000, and average excryption/decryption time is about 3ms with 150 expansion rate. When security level is 160 (λ=200, ρ=50, β=10000, n=50021), we have 100% successful rate for testing frequency=2000, and average excryption/decryption time is about 15ms with 250 expansion rate. From our experiments result, we can notice that if we directly encrypt plaintexts by applying our public key scheme, its performance is relatively weak, especially for the ciphertext expansion rate. However, if we use our public key scheme for key encapsulation mechanism, our scheme will be relatively practical and effective.

It should be noted that we did not optimize our implementation and only illustrate the relative practicality of our construction.

According to the parameter settings of NTRU, the vector (g, f) in L_1 has size $(d_f + d_g)^{1/2}$, where d_f, d_g are the number of the non-zero coefficients of f, g, respectively. Since $\det(L_1) = q^n$, the Gaussian heuristic suggests that (g, f) is in general the shortest vector in L_1. However, the current lattice reduction algorithm that find (g, f) requires exponential in the security parameter n.

Similarly, for our NTRU-type system, given the public key $h = g/f$ over $\mathbb{Z}_2[x]/(x^n + 1)$, we can also construct a lattice from h. Owing to using the unbalanced private key f, we only need to use the 2β rows of the circulant matrix H generated by h. The reaseon is that $fh = (s+1)h + s(x^{2\beta}h) = f_1h + f_2h$. As a reasult, we write a matrix form as follows:

$$L_2 = \begin{pmatrix} 2I_{n\times n} & 0 & 0 \\ H[\ 0 :\ \beta - 1] & I_{\beta\times\beta} & 0 \\ H[2\beta : 3\beta - 1] & 0 & I_{\beta\times\beta} \end{pmatrix} \qquad (1)$$

where H is a circulant matrix generated from h, $H[i : j]$ represents the submatrix of the i-th row to the j-th row of H.

By our parameter settings, the vector (g, f_1, f_2) in L_2 has size $(3\rho+1)^{1/2}$ or $(3\rho-1)^{1/2}$. Since $\det(L_2) = 2^n$, the Gaussian heuristic suggests that (g, f_1, f_2) is usually the shortest vector in L_2. When n is large enough, the lattice reduction algorithm that computes (g, f_1, f_2) requires time complexity at about $2^{O(n)}$.

6 Conclusions and discussions

In this work, we describe an integer version of RLWE over the polynomial rings and show that its hardness is equivalent to the polynomial RLWE. This one-dimensional LWE problem with structural noise is corresponding to the hard one-dimensional LWE problem with exponential modulus in the security parameter [5]. This point is also consistent with the result in [5] that shows the tradeoff between the dimension and the modulus of LWE instances.

Furthermore, the I-RLWE problem also provides a new perspective on the difficulty of the problem. That is, the difficulty of the problem is not only related to the magnitude of noise, but also to the dispersion of noise.

For the I-RLWE problem, if we keep the number of noise bits of the problem unchanged, but put these scattered, structured noise together, then we obtain a corresponding one-dimensional LWE problem.

For example, for I-RLWE with $q > n^3$ and $\sigma \leq \sqrt{n}$, currently there exists no efficient algorithm that solves I-RLWE. However, for the corresponding one-dimensional LWE with $p = q^n > n^{3n}$ and $\alpha = \sigma^n$, there exists an efficient algorithm that solves this one-dimensional LWE.

Without loss of generality, given a sample of the one-dimensional LWE $(a, b = a \times s + e \mod p)$, where $a \leftarrow U(\mathbb{Z}_p)$, and $s, e \leftarrow \chi = D_{\mathbb{Z},\alpha}$, we generate the lattice $L(\mathbf{B})$ with

$$\mathbf{B} = \begin{pmatrix} b & 0 & x \\ a & 1 & 0 \\ p & 0 & 0 \end{pmatrix}.$$

According to Minkowski's first theorem, $\lambda_1(L) \leq \sqrt{3}|\det(\mathbf{B})|^{1/3}$. Again, $\mathbf{v} = (e, -s, x) \in L$ and $\|\mathbf{v}\| \ll \sqrt{3}|\det(\mathbf{B})|^{1/3}$. So, $\mathbf{v}$ is very likely the shortest vector of L, and can be obtained by using the LLL algorithm [**?**]. As a result, the one-dimensional LWE with the above parameters is not secure.

On the other hand, for the one-dimensional LWE with $\alpha > p^{1/2}$, the above lattice attack does not work.

So, our analysis demonstrates that the hardness of I-RLWE relies on not only the size of noise, but also the dispersion of noise.

Acknowledgement: This work was supported by the National Natural Science Foundation of China (Nos. 61672270, 61702236, and 61602216) and Changzhou Sci&Tech Program (Grant No.CJ20179027).

References

1. B Applebaum, D Cash, C Peikert, and A Sahai. Fast cryptographic primitives and circular secure encryption based on hard learning problems. CRYPTO 2009, LNCS 5677, pp. 595-618.
2. D Aggarwal, A Joux, A Prakash, and M Santha. A new public-key cryptosystem via Mersenne numbers. Cryptology ePrint Archive, Report 2017/481, 2017. http://eprint.iacr.org/2017/481.
3. M Beunardeau, A Connolly, R Géraud, and D Naccache. On the Hardness of the Mersenne Low Hamming Ratio Assumption. Cryptology ePrint Archive, Report 2017/522, 2017. http://eprint.iacr.org/2017/522.
4. Z Brakerski, C Gentry, and V Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. ICTS, 2012, pp. 309-325.
5. Z Brakerski, A Langlois, C Peikert, O Regev, and D Stehlè. Classical hardness of learning with errors. STOC 2013, pp. 575-584.
6. Z Brakerski, V Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011, LNCS 6841, pp. 505-524.
7. L Ducas, A Durmus. Ring-LWE in Polynomial Rings, PKC 2012, pp. 34-51.
8. K Eisenträger, S Hallgren, and K E Lauter. Weak instances of PLWE. SAC, 2014, pp. 183-194.
9. Y Elias, K E Lauter, E Ozman, and K E Stange. Provably weak instances of ring-LWE. CRYPTO 2015, pp. 63-92.
10. von zur Gathen J, Gerhard J. Modern Computer Algebra. 3rd edition. Cambridge, England: Cambridge University Press, 2013.
11. J Hoffstein, J Pipher, and J H Silverman. NTRU: A ring-based public key cryptosystem. ANTS, 1998, pp. 267-288.
12. V. Lyubashevsky, D. Micciancio. Generalized Compact Knapsacks Are Collision Resistant, ICALP 2006: Automata, Languages and Programming, LNCS 4052, pp. 144-155. The full version of this extended abstract appears in ECCC TR05-142.
13. V Lyubashevsky, C Peikert, and O Regev. On ideal lattices and learning with errors over rings. Journal of ACM 60, 6, Article 43 (November 2013), 35 pages.
14. A Langlois and D Stehlé. Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography, 2015, 75(3), pp. 565-599.
15. A Lòpez-Alt, E Tromer, and V Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. STOC, 2012, pp. 1219-1234.
16. D Micciancio and O Regev. Worst-Case to Average-Case Reductions Based on Gaussian Measures, SIAM Journal on Computing, 37(1):267-302, 2007.
17. D Micciancio and O Regev. Lattice-based cryptography. Post Quantum Cryptography, pp. 147-191. Springer, February 2009.
18. C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem. STOC 2009, pp. 333-342.

19. C Peikert. How (Not) to Instantiate Ring-LWE. Security and Cryptography for Networks (SCN 2016), LNCS 9841, pp. 411-430.
20. O Regev. On lattices, learning with errors, random linear codes, and cryptography. Journal of ACM, 56(6), pp.1-40, 2009.
21. P W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 1997, 26(5): 1484-1509.
22. D Stehlé and R Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. EUROCRYPT 2011, LNCS 6632, pp. 27-47.