Integer Version of Ring-LWE and Its Applications

Chunsheng Gu(✉)

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

Abstract. In this work, we introduce an integer version of ring-LWE (I-RLWE) over the polynomial rings and present a public key encryption based on I-RLWE. The security of our scheme relies on the computational hardness assumption of the I-RLWE problem.

Keywords: Ring-LWE · NTRU · Public key encryption · 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 computational number theory 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].

The LWE-based cryptographic schemes have strong security confidence. However, they also 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].

On one hand, the schemes based on RLWE over the polynomial rings (RLWE) have an advantage of efficiency. On the other hand, the RLWE-based schemes also have some shortcomings. Especially, 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 trying to solve the above problem. That is, we introduce an integer version of the ring-LWE (I-RLWE) over the polynomial ring that unifies the framework of RLWEs over the different polynomial rings, and present a new

W. Meng and S. Furnell (Eds.): SocialSec 2019, CCIS 1095, pp. 110–122, 2019.
https://doi.org/10.1007/978-981-15-0758-8_9

public key encryption based on I-RLWE. 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 (I-RLWE) and present a I-RLWE-based public key encryption.

In the RLWE over the polynomial ring, 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 [1,17].

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 over the polynomial ring 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 encryption (PKE) 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 Sect. 4.

Organization. Section 2 recalls some background. Section 3 describes an integer variant of RLWE over the polynomial ring and some related properties. Section 4 presents a public key encryption using this variant of RLWE. Finally, we conclude this paper.

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

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

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 $\mathbf{x} \leftarrow D_{L,\sigma}$ (or $\mathbf{x} \leftarrow D_{I,\sigma}$) 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 recall 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 [1,17].

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

This section introduces an integer variant of the ring-LWE over the polynomial rings, and describes some related properties.

For simplicity, we let n be the security parameter, $q > n^3$ a prime, $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ a ring, $p = q^n + 1$, 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 $\mathbb{Z}_p \times \mathbb{Z}_p$.

In the following, we describe several related properties of I-RLWE using 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

$$h_i = \left[\sum_{[j+k]_n = i} (-1)^{\lfloor (j+k)/n \rfloor} f_j g_k - \overline{h}_{i-1}\right]_q,$$

$$\overline{h}_{i-1} = \begin{cases} 0 & h_{i-1} \le q/2 \\ 1 & h_{i-1} > q/2 \end{cases}, i \in [n-1];$$

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

Proof. By $f = [\sum_{j=0}^{n-1} f_j q^j]_p$, $g = [\sum_{k=0}^{n-1} g_k q^k]_p$, 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 over the polynomial ring, 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,

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

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

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

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 $|c_{b_i}| + |\overline{h}_i| + |\overline{r}_{i-1}| < n^2 - n + 3$. ■

4 Public Key Encryption

In this section, we first present a public key encryption based on the I-RLWE problem. Then we show its correctness and give its security assumption.

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 $\mathbf{h} = \mathbf{3f}/(\mathbf{3g+1}) \in \mathbb{Z}_q[x]/\langle x^n - 1\rangle$, and the secret key $\mathbf{s} = \mathbf{3g+1} \in \mathbb{Z}[x]/\langle x^n - 1\rangle$. 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

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

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

$$er = [\sum_{i=0}^{n-1} (2 \sum_{[j+k]_n = i} (-1)^{\lfloor (j+k)/n \rfloor} e_j r_k) q^i]_p = [\sum_{i=0}^{n-1} 2u_i q^i]_p$$

$$e_1 s = [\sum_{i=0}^{n-1} (2 \sum_{[j+k]_n = i} (-1)^{\lfloor (j+k)/n \rfloor} e_{1_j} s_k) q^i]_p = [\sum_{i=0}^{n-1} 2v_i q^i]_p$$

$$t_0 = [er + e_2 - e_1 s + m]_p = [\sum_{i=0}^{n-1} (2u_i + 2e_{2_i} - 2v_i + m_i) q^i]_p = \sum_{i=0}^{n-1} d_i q^i$$

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

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

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 Assumption

The security of our public key encryption is based on the following assumption.

Definition 4.3 I-DRLWE$_{q,\sigma}$ Assumption. For any probabilistic distinguisher D that solves the I-DRLWE$_{q,\sigma}$ problem, its advantage ϵ is negligible in security parameter n.

Lemma 4.4. Under I-DRLWE$_{q,\sigma}$ assumption, the public key encryption scheme (Enc, Dec) described in Sect. 4 is secure against chosen plaintext attack.

Proof. Given m_0, m_1 corresponding to plaintext vectors $\mathbf{m}_0, \mathbf{m}_1 \in \{0,1\}^n$, let $c_{i,1} = [ar_i + e_{i,1}]_p$, $c_{i,2} = [br_i + e_{i,2} + m_i]_p$ be the ciphertexts of $m_i, i = 0, 1$, where $\mathbf{r}_i \leftarrow D_{\mathbb{Z}^n,\sigma}$, $\mathbf{e}_{i,1}, \mathbf{e}_{i,2} \leftarrow D_{\mathbb{Z}^n,\sigma}$. We denote $\mathbf{c}_i = (c_{i,1}, c_{i,2}), i = 0, 1$.

By contradiction, assume that there exists a polynomial time algorithm B, so that

$$|\Pr[B(\mathbf{c}_0) = 1] - \Pr[B(\mathbf{c}_1) = 1]| \geq n^{-O(1)}. \tag{1}$$

We assume $\mathbf{c} \leftarrow U(\mathbb{Z}_p^2)$. By I-DRLWE$_{q,\sigma}$ assumption, for any polynomial time algorithm A

$$|\Pr[A(\mathbf{c}_i) = 1] - \Pr[A(\mathbf{c}) = 1]| \leq \mathrm{negl}_i(n), \quad i = 0, 1. \tag{2}$$

Therefore,

$$\begin{aligned} &|\Pr[B(\mathbf{c}_0) = 1] - \Pr[B(\mathbf{c}_1) = 1]| \\ &\leq |\Pr[B(c_0) = 1] - \Pr[A(\mathbf{c}) = 1] + \Pr[A(\mathbf{c}) = 1] - \Pr[B(\mathbf{c}_1) = 1]| \\ &\leq |\Pr[B(\mathbf{c}_0) = 1] - \Pr[A(\mathbf{c}) = 1]| + |\Pr[A(\mathbf{c}) = 1] - \Pr[B(\mathbf{c}_1) = 1]| \\ &\leq \mathrm{negl}_0(n) + \mathrm{negl}_1(n) \\ &= \mathrm{negl}(n), \end{aligned} \tag{3}$$

where $\mathrm{negl}_0(n), \mathrm{negl}_1(n)$, and $\mathrm{negl}(n)$ are negligible functions in n.

This is a contradiction for the expression (1) and (3). ■

5 Conclusions

In this work, we introduce an integer version of ring-LWE (I-RLWE) over the polynomial rings, and present a public key encryption based on I-RLWE whose security relies on a new computational hardness assumption of the I-RLWE problem.

In the future, we will build the relationship between RLWE over the polynomial ring and I-RLWE. We will also study between the one-dimensional LWE problem with structural noise and the hard one-dimensional LWE problem with non-structural noise [5].

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. Applebaum, B., Cash, D., Peikert, C., Sahai, A.: Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 595–618. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03356-8_35
2. Aggarwal, D., Joux, A., Prakash, A., Santha, M.: A new public-key cryptosystem via Mersenne numbers. Cryptology ePrint Archive, Report 2017/481 (2017). http://eprint.iacr.org/2017/481
3. Beunardeau, M., Connolly, A., Géraud, R., Naccache, D.: On the hardness of the Mersenne low hamming ratio assumption. Cryptology ePrint Archive, Report 2017/522 (2017). http://eprint.iacr.org/2017/522
4. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping. In: ICTS, pp. 309–325 (2012)
5. Brakerski, Z., Langlois, A., Peikert, C., Regev, O., Stehlè, D.: Classical hardness of learning with errors. In: STOC, pp. 575–584 (2013)
6. Brakerski, Z., Vaikuntanathan, V.: Fully homomorphic encryption from Ring-LWE and security for key dependent messages. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 505–524. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22792-9_29
7. Ducas, L., Durmus, A.: Ring-LWE in polynomial rings. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 34–51. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_3
8. Eisenträger, K., Hallgren, S., Lauter, K.: Weak instances of PLWE. In: Joux, A., Youssef, A. (eds.) SAC 2014. LNCS, vol. 8781, pp. 183–194. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-13051-4_11
9. Elias, Y., Lauter, K.E., Ozman, E., Stange, K.E.: Provably weak instances of Ring-LWE. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 63–92. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47989-6_4
10. von zur Gathen, J., Gerhard, J.: Modern Computer Algebra, 3rd edn. Cambridge University Press, Cambridge (2013)
11. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: a ring-based public key cryptosystem. In: Buhler, J.P. (ed.) ANTS 1998. LNCS, vol. 1423, pp. 267–288. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0054868

12. Lyubashevsky, V., Micciancio, D.: Generalized compact knapsacks are collision resistant. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4052, pp. 144–155. Springer, Heidelberg (2006). https://doi.org/10.1007/11787006_13
13. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 1–23. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_1
14. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Des. Codes Cryptogr. **75**(3), 565–599 (2015)
15. Lòpez-Alt, A., Tromer, E., Vaikuntanathan, V.: On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: STOC, pp. 1219–1234 (2012)
16. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on Gaussian measures. SIAM J. Comput. **37**(1), 267–302 (2007)
17. Micciancio, D., Regev, O.: Lattice-based cryptography. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.) Post Quantum Cryptography, pp. 147–191. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-540-88702-7_5
18. Peikert, C.: Public-key cryptosystems from the worst-case shortest vector problem. In: STOC, pp. 333–342 (2009)
19. Peikert, C.: How (Not) to instantiate Ring-LWE. In: Zikas, V., De Prisco, R. (eds.) SCN 2016. LNCS, vol. 9841, pp. 411–430. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-44618-9_22
20. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**(6), 1–40 (2009)
21. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
22. Stehlé, D., Steinfeld, R.: Making `NTRU` as secure as worst-case problems over ideal lattices. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 27–47. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4_4