

# 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

Shor [20] described an efficient quantum algorithm that solves both discrete logarithms and factoring. As a result, many cryptographic schemes based on these problems are no longer secure once the quantum computer becomes a reality. Currently, the most promising quantum-safe works are those based on the hardness of lattice problems like LWE-based cryptosystems [19], Ring-LWE-based cryptosystems [12] and NTRU [11].

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 [12] defined a ring-based variant of LWE (RLWE) that uses algebraic structure, and described a polynomial time quantum 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 [4,6,13,14].

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 [8,18,9]. 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  $(\mathbf{a}_l, \mathbf{b}_l = \mathbf{a}_l s + \mathbf{e}_l) \in R_q^2$ , 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  $\chi$  rather than uniformly at random, the choice of other parameters remains unchanged. This variant becomes no easier to solve than the decisional LWE [16,1].

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  $\chi$ .

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  $\chi$ , 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  $\chi$ , 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  $\chi$  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  $\{1, 2, \dots, n\}$ . 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  $L = \{\mathbf{B}\mathbf{y} : \mathbf{y} \in \mathbb{Z}^n\}$ . We say that  $\mathbf{B}$  spans  $L$  if  $\mathbf{B}$  is a basis for  $L$ . Given a basis  $\mathbf{B}$  of  $L$ , we define  $P(\mathbf{B}) = \{\mathbf{B}\mathbf{y} | \mathbf{y} \in \mathbb{R}^n \text{ and } y_i \in [-1/2, 1/2]\}$  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  $Rot(g) = (g, x \cdot g, \dots, x^{n-1} \cdot g)$ .

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  $D_{L,\sigma,0}$  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 [15] 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  $\rho_{1/s}(L^* \setminus \{0\}) \leq \epsilon$ , where  $L^*$  is the dual lattice of  $L$ .

**Lemma 2.1 (Lemma 3.3 [15]).** 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 [15]).** 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 [12], 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 [16,1].

**Definition 2.3 (Ring-LWE Distribution).** Let  $\Psi$  be a Gaussian distribution with parameter  $\sigma$  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  $(\mathbf{a}, \mathbf{b} = \mathbf{a}\mathbf{s} + \mathbf{e}) \in R_q \times R_q$ .

**Definition 2.4 (Computational Ring-LWE).** The computational ring-LWE problem, denoted  $\text{RLWE}_{q, \sigma}$ , 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  $\text{DRLWE}_{q, \sigma}$ , is 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 [12].

**Lemma 2.6 (Theorem 3.6 [12]).** Let  $\mathbb{K}$  be the  $m$ th 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  $q \geq 2$ ,  $q \equiv 1 \pmod{m}$  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  $\text{DRLWE}_{q, \sigma}$ , 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,  $p = q^n + 1$ ,  $\chi$  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  $\text{I-DRLWE}_{q, \sigma}$ , 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  $f_i, i \in \{0, \dots, n-1\}$  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

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

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

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

for  $i = 0$ ,

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

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

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

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

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

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

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

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

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

Now we use the induction method to prove the result.

For induction basis, consider  $i = 0$ .

If  $\bar{h}_{n-1} = -1$ , 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,

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

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

If  $\bar{h}_{n-1} = 0$ , then  $0 \leq h_{n-1} \leq q/2$ . 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,  $f_{n-1} \geq 0$ . Hence,  $h_0 = [f]_q = [f_0]_q = [f_0 - \bar{h}_{n-1}]_q$ .

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

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  $\bar{h}_k = 1$  and  $f_k - \bar{h}_{k-1} < 0$ . 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  $h_{k+1} = [f_{k+1} - 1]_q = [f_{k+1} - \bar{h}_k]_q$ .

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

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

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

*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

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

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

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.  $\blacksquare$

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  $\mathbf{a} \leftarrow R_q, \mathbf{s} \leftarrow D_{\mathbb{Z}^n, \sigma}, \mathbf{b} = \mathbf{a}\mathbf{s} \in R_q$ , 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  $\mathbf{b} = \mathbf{a}\mathbf{s} \in R_q$ , 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

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

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

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

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

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

$$\bar{h}_{i-1} = \begin{cases} 0 & 0 \leq b_{i-1} + c_{b_{i-2}} - \bar{h}_{i-2} < q \\ 1 & b_{i-1} + c_{b_{i-2}} - \bar{h}_{i-2} < 0 \\ -1 & b_{i-1} + c_{b_{i-2}} - \bar{h}_{i-2} \geq q \end{cases};$$

for  $i = 0$ ,

$$\bar{h}_{-1} = \bar{h}_{n-1} = \begin{cases} 0 & 0 \leq b_{n-1} + c_{b_{n-2}} - \bar{h}_{n-2} < q \\ -1 & b_{n-1} + c_{b_{n-2}} - \bar{h}_{n-2} < 0 \\ 1 & b_{n-1} + c_{b_{n-2}} - \bar{h}_{n-2} \geq q \end{cases}.$$

Thus, we obtain

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

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

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

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

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

for  $i = 0$ ,

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

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

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  $(\mathbf{a}, \mathbf{b}') = \mathbf{a}\mathbf{s} + \mathbf{e} \in R_q \times R_q$ , 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

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

*Proof.* We denote  $\mathbf{b} = \mathbf{a}s \in R_q$ , and  $\mathbf{b}' = \mathbf{b} + \mathbf{e} \in R_q$ .

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

By Lemma 3.6,

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

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,  $b' = \sum_{i=0}^{n-1} b'_i q^i = \sum_{i=0}^{n-1} (b_i + e_i + d_i q) q^i$ .

Hence,

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

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

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

for  $i = 0$ ,

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

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

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

The proof is complete.  $\blacksquare$

**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  $(\mathbf{a}, \mathbf{b}' = \mathbf{a}s + \mathbf{e}') \in R_q \times R_q$ , such that

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

*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

$$\begin{aligned} \mathbf{a} &= (a_0, a_1, \dots, a_{n-1}), \\ \mathbf{b}' &= (b'_0, b'_1, \dots, b'_{n-1}). \end{aligned}$$

We denote  $\mathbf{b} = \mathbf{a}s \in R_q$ , 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,

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

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

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

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

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

for  $i = 0$ ,

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

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

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

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

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

The proof is complete.  $\blacksquare$

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  $\text{DRLWE}_{q,\sigma}$  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  $\text{DRLWE}_{q,O(n\sigma)}$ .

*Proof.* By Lemma 3.7, 3.8, the result directly follows from the transformation of samples between them.  $\blacksquare$

## 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:**  $(pk, sk) \leftarrow \text{KeyGen}(1^n)$ .

- (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:**  $(c_1, c_2) \leftarrow \text{Enc}(pk, \mathbf{m})$ .

- (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:**  $\mathbf{m} \leftarrow \text{Dec}(sk, (c_1, c_2))$ .

- (1) Given  $sk$  and a ciphertext  $(c_1, c_2)$ , compute  $t_0 = [c_2 - c_1 s]_p$ .
- (2) For  $i = 0, 1, \dots, n-1$ 
  - (2.1) Compute  $d_i = [t_i]_q$ .
  - (2.2) Compute  $t_{i+1} = [t_i/q]$ .
  - (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  $m_i = [d_i]_2, i \in \{0, 1, \dots, n-1\}$ .
- (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 [12], 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  $i$ th 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 [11,21] can be directly converted into an integer scheme of NTRU. For example, consider the NTRU scheme in [21]. 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

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

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

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

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

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

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

For  $i = 0$ , we have

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

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

Using Step (3), the algorithm Dec subtracts  $\bar{d}_{n-1}$  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  $m_i = [d_i]_2, i \in \{1, \dots, n-1\}$ .  $\blacksquare$

### 4.3 Security

Similar to [12], 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 Conclusions

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.

## 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, 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.
13. A Langlois and D Stehlé. Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography, 2015, 75(3), pp. 565-599.
14. A López-Alt, E Tromer, and V Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. STOC, 2012, pp. 1219-1234.
15. D Micciancio and O Regev. Worst-Case to Average-Case Reductions Based on Gaussian Measures, SIAM Journal on Computing, 37(1):267C302, 2007.
16. D Micciancio and O Regev. Lattice-based cryptography. Post Quantum Cryptography, pp. 147-191. Springer, February 2009.
17. C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem. STOC 2009, pp. 333-342.

18. C Peikert. How (Not) to Instantiate Ring-LWE. Security and Cryptography for Networks (SCN 2016), LNCS 9841, pp. 411-430.
19. O Regev. On lattices, learning with errors, random linear codes, and cryptography. Journal of ACM, 56(6), pp.1-40, 2009.
20. 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.
21. D Stehlé and R Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. EUROCRYPT 2011, LNCS 6632, pp. 27-47.