LWE from Non-commutative Group Rings

Qi Cheng[1] and Jincheng Zhuang[2]

[1] School of Computer Science, University of Oklahoma
Norman, OK 73019, USA.
Email: qcheng@ou.edu

[2] State Key Laboratory of Information Security, Institute of Information Engineering
Chinese Academy of Sciences, Beijing 100093, China
Email: zhuangjincheng@iie.ac.cn

Abstract. The Ring Learning-With-Errors (LWE) problem, whose security is based on hard ideal lattice problems, has proven to be a promising primitive with diverse applications in cryptography. There are however recent discoveries of faster algorithms for the principal ideal SVP problem, and attempts to generalize the attack to non-principal ideals. In this work, we study the LWE problem on group rings, and build cryptographic schemes based on this new primitive. One can regard the LWE on cyclotomic integers as a special case when the underlying group is cyclic, while our proposal utilizes non-commutative groups, which eliminates the weakness associated with the principal ideal lattices. In particular, we show how to build public key encryption schemes from dihedral group rings, which maintains the efficiency of the ring-LWE and improves its security. We also propose a simple modification of the Peikert-Vaikuntanathan-Waters cryptosystem, which is an amortized version of Regev's original proposal based on LWE. Our modification improves the encryption and decryption complexity per bit to sublinear in the security level, without affecting the security.

Keywords: Matrix-LWE, Non-commutative group ring, Dihedral group ring

1 Introduction

1.1 The LWE problem

Regev [31] introduced the learning with errors (LWE) problem as a generalization of the classic learning parity with noise (LPN) problem. To be precise, let q be a prime, $\mathbf{s} \in \mathbb{F}_q^n$ be a fixed private vector, $\mathbf{a_i} \in \mathbb{F}_q^n, 1 \leq i \leq m$ be randomly chosen, $e_i \in \mathbb{F}_q, 1 \leq i \leq m$ be chosen independently accordingly to the probability distribution $\chi : \mathbb{F}_q \mapsto \mathbb{R}^+$, which is a discrete Gaussian distribution that centers around 0 with width $qn^{-0.5-\epsilon}$, and $b_i = \langle \mathbf{a_i}, \mathbf{s} \rangle + e_i$. Given a list of pairs $(\mathbf{a}_i, b_i), 1 \leq i \leq m$, the LWE problem asks to solve for $\mathbf{s}$, and the LPN problem is the special case when $q = 2$.

Informally speaking, it is believed that LWE is hard in the sense that even though e_i tends to be small, when $\mathbf{s}$ is hidden, $(\mathbf{a_i}, b_i)$ can not be distinguished from a random vector in $\mathbb{F}_q^{n+1}$. In fact, Regev [31] proved the hardness for certain parameters q, χ by showing quantum reductions from approx-SVP and approx-SIVP problems for lattices. Later, Peikert [27] showed a classical reduction from approx-SVP to the LWE problem under more restrictive constraints.

Lyubashevsky, Peikert, and Regev [24] introduced an analogous version of standard LWE over rings, and coined it ring-LWE. Furthermore, they established the hardness of ring-LWE by showing the reduction from a certain ideal lattice problem to the ring-LWE problem. The cryptography systems based on ring-LWE are much more efficient in terms of key sizes and encryption and decryption complexity. However, the security of systems is based on conjecturally hard problems on ideal lattices rather than on general lattices.

The LWE problem and ring-LWE problem have proven to be versatile primitives for cryptographic purposes. Besides many other schemes, these applications include public key encryption schemes proposed by Regev [31], Peikert and Waters [30], Peikert [27], Lindner and Peikert [22], Stehlé and Steinfeld [34], Micciancio and Peikert [25]; identity-based encryption (IBE) schemes proposed by Gentry, Peikert, and Vaikuntanathan [19], Cash, Hofheinz, Kiltz, and Peikert [8], Agrawal, Boneh, and Boyen [2, 1]; fully homomorphic encryption (FHE) schemes proposed by Brakerski and Vaikuntanathan [6, 7], Brakerski, Gentry, and Vaikuntanathan [5], Fan and Vercauteren [17].

1.2 Our results

In this work, we first consider a matrix version of standard LWE in order to improve the efficiency via fast matrix multiplication. Our modification improves the encryption and decryption complexity per bit to sublinear in the security level. We note that there have been some matrix variants of original LWE, such as [18, 23, 14] or [4]. However, there are some differences with our work. In variants [18, 23, 14], the encrypted message is either a vector, or a matrix with binary alphabet. In [4], the application in concern is key establishment.

We then propose a general framework of generating LWE instances from group rings. In particular, we demonstrate our approach by generating LWE instances from dihedral group rings. Recall that given a finite group $G = \{g_1, \dots, g_n\}$ and a commutative ring R, the elements in group ring $R[G]$ are formal sums

$$\sum_{i=1}^{n} r_i g_i, r_i \in R.$$

If $R = \mathbb{Z}$, and we provide a $\mathbb{Z}$-module homomorphism from $\mathbb{Z}[G]$ to $\mathbb{R}^n$ (otherwise known as an embedding), then (one-side) ideals in group rings naturally correspond to integral lattices. We can generalize LWE to the group ring setting. In particular, let n be a power of two, D_{2n} be the dihedral group of order $2n$, and $r \in D_{2n}$ be an element that generates the cyclic subgroup of order n, then we should use the ring

$$\mathbb{Z}[D_{2n}]/((r^{n/2} + 1)\mathbb{Z}[D_{2n}]),$$

which is also a free $\mathbb{Z}$-module of rank n. Note that $(r^{n/2}+1)\mathbb{Z}[D_{2n}]$ is a two-sided ideal, thus the quotient ring is well defined.

In ring-LWE, there are two types of embeddings of rings of algebraic integers into Euclidean spaces: canonical embedding and coefficient embedding. If using canonical embedding, multiplication is component-wise. This is the main reason that the original ring-LWE paper preferred canonical embedding. Nevertheless, the whole ring is embedded as a lattice that is not self-dual, which complicates the implementation [28]. Note that the canonical embedding of cyclotomic integers is basically the combined map:

$$\mathbb{Z}[x]/(x^n+1) \hookrightarrow \mathbb{C}[x]/(x^n+1) \to \bigoplus_{0\leq k\leq n, 2\nmid k} \mathbb{C}[x]/(x - e^{2\pi\sqrt{-1}k/(2n)}),$$

where the first map is an inclusion, and the second one is an isomorphism. A component of the canonical embedding of $\mathbb{Z}[x]/(x^n+1)$ corresponds to a group representation of the cyclic group $\langle x\rangle$ of order $2n$:

$$\rho_k(x^j) = e^{2\pi\sqrt{-1}kj/(2n)}, 2 \nmid k.$$

If a group is not commutative, we can use irreducible group representations to find a canonical embedding of the group ring. However, some irreducible representations will have dimensions larger than one, thus multiplication in the group ring is not component-wise under these representations. We should use coefficient embedding to make implementation simpler.

There are recent discoveries of faster SVP algorithms for principal ideal lattices, and attempts to generalize the idea to non-principal ideal lattices. See [12, 13] and references therein. First observe that the ratio between two generators of a principal ideal is an integral unit. The main idea of the attacks comes from the Dirichlet unit theorem: the group of integral units in a number field is a direct product of a finite group with a free abelian group, whose generators are known as fundamental units. If taking logarithms of complex norms of their conjugates, the units are sent to the so-called log-unit lattice, whose SVP is not hard in many cases. Nevertheless, the ring-LWE cryptosystems are not under direct threat, since lattice problems in ideal lattices form lower bounds for their security, and the approximation factors in the attack are too large.

The principal ideals from non-commutative integral group rings do not appear to suffer from the weakness, since multiplications of units may not commute [32]. A few remarks are in order:

1. The group ring LWE includes LWE on cyclotomic integers as a special case, thus has security no less than the ring-LWE. Indeed, the ring $R = \mathbb{Z}[x]/(x^n+1)$, used in many ring-LWE cryptosystems, is a direct summand of a group ring from C_{2n} (the cyclic group of order $2n$):

$$\mathbb{Z}[C_{2n}] = \mathbb{Z}[x]/(x^{2n}-1) \equiv \mathbb{Z}[x]/(x^n+1) \oplus \mathbb{Z}[x]/(x^n-1)$$

   One should avoid using the ring $\mathbb{Z}[x]/(x^{2n}-1)$, as the map

$$\mathbb{Z}[x]/(x^{2n}-1) \to \mathbb{Z}[x]/(x-1)$$

may leak secret information.

2. The non-commutative group-ring LWE is broader than LWE based on commutative ring. For security and simplicity, many proposals of ring-LWE have lattice dimensions that are either powers of two, or (one less than) prime numbers. The group ring LWE provides us more choices, while keeping the simplicity. For example, if using dihedral group rings, the dimensions of the lattices can be $2(p-1)$ for primes p. Yet the efficiency, as well as the security, is as same as that of the ring-LWE of comparable dimensions.
3. We regard one-dimensional representations over finite fields as security risks that should be eliminated. Many attacks on the ring-LWE (implicitly) explores a one-dimensional representation that sends x to a small order element [9, 10, 15, 16], for example,
$$\mathbb{F}_q[x]/(f(x)) \to \mathbb{F}_q[x]/(x-1),$$
if $(x-1)|f(x)$ over $\mathbb{F}_q$.
4. Even though rings of algebraic integers in number fields may not be principal ideal domains (PID), their reductions modulo primes are always principal ideal rings. The group ring $\mathbb{F}_p[G]$, however, is not necessarily a principal ideal rings if G is non-commutative. We believe that this property provides an extra protection against attacks.

The proof of security is largely similar to the case of ring-LWE. There is, however, an important difference: unlike the ring of algebraic integers in a number field, group rings have ideals that are not invertible. The security of group-ring-LWE should be based on lattice problems of invertible ideals. A drawback of our approach is that we are unable to provide a search-to-decision reduction.

We note that there have been attempts to use non-commutative algebraic structures, especially the group structures, in designing cryptographical systems [26]. The approaches that relate closely to ours include using group rings to replace $(\mathbb{Z}/q\mathbb{Z})[x]/(x^n-1)$ in NTRU [36, 11, 35] and using the learning problem of non-commutative groups. The former approach has no security proof from lattice problems. The latter approach is not based on lattice problems.

1.3 Paper organization

The paper is organized as follows. In Section 2, we review the mathematical background. In Section 3 we briefly discuss previous works. In Section 4, we propose our variant version of the LWE-based scheme. In Section 5, we propose generating LWE instances from non-commutative group rings and establish public key cryptosystem from dihedral group rings. In Section 6 we analyse the security of the new approach. Section 7 concludes the paper. We will not try to optimize the parameters in this paper, leaving it to future work.

2 Mathematical preliminary

In the section, we review the mathematical background on lattices and group rings.

2.1 Efficiency of cryptographic schemes

To use a cryptography algorithm, one should first establish a security level n. It is expected that the cryptosystem cannot be broken in 2^n bit operations. In terms of efficiency, the most important parameters for an encryption algorithm are block size, public/secret key sizes, cipher-text expansion factor and time complexity per bit in encryption and decryption. Ideally these parameters should have sizes that grow slowly with the security level.

Let us first calculate the parameters for the popular public key cryptosystem RSA, whose security is based on the integer factorization problem. To factor a number of l bits, the best algorithm – Number Field Sieve – takes heuristic time at most $2^{l^{1/3+\epsilon}}$. Thus for security level n, the RSA-OAEP system, a practical implementation of RSA, should have key size $l = n^{3-\epsilon}$. To encrypt a block of $O(l)$ bits, it adds some padding into the message and computes an exponentiation modulo a number of l bits. Thus it has cipher-text expansion $O(1)$. The public exponent is small (e.g. $e = 65537$), but the private exponent has l bits. Therefore, encryption takes time $\tilde{O}(l)$ and decryption takes time $\tilde{O}(l^2)$, assuming that we use the fast multiplication algorithm for each modular multiplication. This results in bit complexity $n^{3-\epsilon}$ per ciphertext bit for decryption, and $(\log n)^{O(1)}$ per message bit for encryption if using small encryption exponent. Asymptotically the key size for RSA is not so good. However, the ϵ part has played an important role in its favor when n is small. To achieve a security level $n = 80$, one can use a public modulus of size 1000 bits rather than $80^3 = 512000$ bits, although a public modulus of 2000-bits is recommended now.

2.2 Lattices and ring-LWE

Given a list of linearly independent column vectors $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n) \in \mathbb{R}^{n\times n}$, the (full rank) lattice $\mathcal{L}(\mathbf{B})$ is the set

$$\mathcal{L}(\mathbf{B}) = \{\sum_{i=1}^{n} x_i \mathbf{b}_i, x_i \in \mathbb{Z}\}.$$

The determinant of the lattice is

$$\det(\mathcal{L}) := |\det(\mathbf{B})|.$$

The minimum distance of the lattice is

$$\lambda_1(\mathcal{L}) := \min_{0\neq v\in\mathcal{L}} |v|$$

where $|\cdot|$ is the Euclidean norm. The dual lattice is

$$\mathcal{L}^* := \{u \in \mathbb{R}^n | \forall v \in \mathcal{L}, \langle u, v\rangle \in \mathbb{Z}\}.$$

Definition 1. *Let $\mathcal{L} \in \mathbb{R}^n$ be a full rank lattice. The Shortest Vector Problem (SVP) is to find a vector $v \in \mathcal{L}$ such that*

$$|v| = \lambda_1.$$

Given a target vector $t \in \mathbb{R}^n$, the Closest Vector Problem (CVP) is to find a vector $v \in \mathcal{L}$ such that

$$|v - t| \le |v' - t|, \forall v' \in \mathcal{L}.$$

Definition 2. *Let $0 < \beta < 1/2$ be a constant, and $\mathcal{L}$ be a lattice. Let $y = x + e$ where $x \in \mathcal{L}$, and $|e| < \beta\lambda_1(\mathcal{L})$. Given y, the β-BDD problem is to find x.*

Definition 3. *Let $0 < \beta < 1/2$ be a constant, and $\mathcal{L}$ be a lattice. Let $y = x + e$ where $x \in \mathcal{L}$, and $|e| < \beta\lambda_1(\mathcal{L})$. Given y, the (q, β)-BDD problem is to find any x' such that $x \equiv x' \pmod{q\mathcal{L}}$.*

The β-BDD problem can be reduced to (q, β)-BDD problem. In fact, if $x - x' \in q\mathcal{L}$, then $(x - x')/q \in \mathcal{L}$. The distance between $(y - x')/q$ and $(x - x')/q$ is $|e/q|$. So we have a new BDD problem on the same lattice but with smaller error. Repeating the procedure will give us a BDD problem that can be solved by lattice reduction algorithms such as LLL.

2.3 Dihedral groups and group rings

Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group of order n. The elements in group ring $R[G]$ are formal sums

$$\sum_{i=1}^{n} r_i g_i, r_i \in R.$$

Addition is defined by

$$\sum_{i=1}^{n} a_i g_i + \sum_{i=1}^{n} b_i g_i = \sum_{i=1}^{n} (a_i + b_i) g_i.$$

Multiplication is defined by

$$(\sum_{i=1}^{n} a_i g_i)(\sum_{i=1}^{n} b_i g_i) = \sum_{l=1}^{n} (\sum_{g_i g_j = g_l} a_i b_j) g_l. \tag{1}$$

If $R = \mathbb{Z}$, a (one-side) ideal of $\mathbb{Z}[G]$ is mapped to a lattice, under an embedding of $\mathbb{Z}[G]$ to $\mathbb{R}^n$. Here we use coefficient embedding, i.e. a group element is sent to a unit vector in $\mathbb{Z}^n$. The whole group ring $\mathbb{Z}[G]$ corresponds to $\mathbb{Z}^n$. Denote the length of a group ring element X in the Euclidean norm under the embedding by $|X|$. The following lemma shows that lengths of group ring elements behave nicely under multiplication.

Lemma 1. *Let $X, Y \in \mathbb{R}[G]$ be two elements. Then*

$$|XY| \le \sqrt{n}|X||Y|$$

Proof. From Equation (1), the l_∞ norm of XY is less than $|X||Y|$ by the Cauchy-Schwarz inequality.

Let I be a right ideal, the left dual of I is defined as

$$I^{-1} = \{x \in \mathbb{Q}[G] \mid \forall y \in I, xy \in \mathbb{Z}[G]\}$$

It can be verified that the left dual is a left $\mathbb{Z}[G]$ module, and

$$I \subseteq \mathbb{Z}[G] \subseteq I^{-1}.$$

We call an ideal invertible if $I^{-1}I = \mathbb{Z}[G]$. If I is invertible, then I^{-1} is a left fractional ideal, namely, there is an integer t such that $tI^{-1} \subseteq \mathbb{Z}[G]$.

A dihedral group of order $2n$, denoted by D_{2n}, is the set

$$\{r^i s^j \mid 0 \leq i \leq n-1, 0 \leq j \leq 1\}$$

satisfying the relations

$$r^n = s^2 = 1, srs = r^{-1}.$$

In some sense, the dihedral group is the non-commutative group that is the closest to the commutative one, since the dimension of any irreducible representation is bounded by 2, while commutative groups only have one-dimensional irreducible representations.

If n is odd, there are $(n+1)/2$ irreducible representations for D_{2n}. Two of them are one-dimensional:

$$\rho_0(r^i) = 1, \rho_0(sr^j) = 1$$

and

$$\rho_1(r^i) = 1, \rho_1(sr^j) = -1.$$

The rest are two-dimensional: for $2 \leq k \leq (n+1)/2$,

$$\rho_k(r^i) = \begin{pmatrix} e^{2\pi\sqrt{-1}i(k-1)/n} & 0 \\ 0 & e^{-2\pi\sqrt{-1}i(k-1)/n} \end{pmatrix},$$

$$\rho_k(sr^i) = \begin{pmatrix} 0 & e^{2\pi\sqrt{-1}i(k-1)/n} \\ e^{-2\pi\sqrt{-1}i(k-1)/n} & 0 \end{pmatrix}.$$

By the Wedderburn theorem, the group ring $\mathbb{C}[D_{2n}]$ can be decomposed into

$$\mathbb{C}[D_{2n}] \equiv \mathbb{C} \oplus \mathbb{C} \oplus \bigoplus_{i=2}^{(n+1)/2} \mathbb{C}^{2\times 2},$$

where the first two copies of $\mathbb{C}$ correspond to ρ_0 and ρ_1, the last $(n-1)/2$ copies of 2×2 matrix algebras corresponds to the two-dimensional representations ρ_i ($2 \leq k \leq (n+1)/2$). To eliminate the influence of one-dimensional representations, one can let n be a prime, and use the direct summand of the ring $\mathbb{Z}[D_{2n}]$:

$$\mathbb{Z}[D_{2n}]/((r^{n-1} + r^{n-2} + \cdots + 1)\mathbb{Z}[D_{2n}]).$$

Note that $(r^{n-1}+r^{n-2}+\cdots+1)\mathbb{Z}[D_{2n}]$ is a two-sided ideal, so the above ring is well defined, and it can be regarded as a projection of $\mathbb{Z}[D_{2n}]$ to $\bigoplus_{i=2}^{(n+1)/2}\mathbb{C}^{2\times 2}$. In this paper we assume that n is a power of two, and let

$$\mathbf{R}=\mathbb{Z}[D_{2n}]/((r^{n/2}+1)\mathbb{Z}[D_{2n}]),$$

which is also without one-dimensional component. Let q be a prime such that $\gcd(q,2n)=1$. Define

$$\mathbf{R}_q=\mathbb{F}_q[D_{2n}]/((r^{n/2}+1)\mathbb{F}_q[D_{2n}]).$$

Definition 4. *Let n be a power of two, let q be a prime such that $\gcd(q,2n)=1$, and $q\in[n^2,2n^2]$. Let the error distribution χ on $\mathbf{R}_q$ be selection of coefficients independently according to a Gaussian of width $n^{1.5-\epsilon}$. The $\mathbf{R}_q$-LWE problem is to find the secret s, given a sequence of (a_i,b_i), where a_i is selected uniformly and independently from $\mathbf{R}_q$, $b_i=a_is+e_i$, e_i is selected independently according to χ.*

Remark 1. Not every ideal is invertible. For example, $1+s\in\mathbf{R}$ generates an ideal that is not invertible. It is very important to have an ideal that is invertible in order to have hard lattice problems. In the later proof, we need an onto $\mathbf{R}$-module morphism $I\to\mathbf{R}_q$, which requires I to be invertible.

Lemma 2. *The element $\sum_{0\le i\le(n/2)-1}a_ir^i+\sum_{0\le i\le(n/2)-1}b_isr^i\in\mathbf{R}$ is invertible in $\mathbf{R}\otimes\mathbb{Q}$ iff for all odd $1\le k\le n/2$,*

$$|\sum_{0\le i\le(n/2)-1}a_ie^{2\pi\sqrt{-1}ki/n}|-|\sum_{0\le i\le(n/2)-1}b_ie^{2\pi\sqrt{-1}ki/n}|\neq 0,$$

where $|*|$ is the complex norm.

3 Previous works

Lattice-based cryptography has attracted much attention recently. It has a few advantages over classical number theoretic cryptosystems such as RSA or Diffie-Hellman. First, it resists quantum attacks, in contrast to the traditional hard problems such as integer factorization, or discrete logarithms [33]. Second, it enjoys the worst case to the average case reduction, shown in the pioneering work of Ajtai [3]. Third, computation can be done on small numbers. No large number exponentiations are needed, which tend to slow down the other public key cryptosystems. It does have a major drawback in key sizes. The NTRU cryptosystem [20] is the first successful cryptosystem based on lattices.

3.1 Regev's scheme

Regev [31] introduced the Learning With Errors (LWE) problem as a generalization of the classic learning parity with noise (LPN) problem to higher moduli and proposed a public key encryption system based on the LWE problem. In the following description of Regev's scheme, n is the security parameter, $q \in [n^2, 2n^2]$ is a prime number and $m = O(n \log q), \alpha = o(\frac{1}{\sqrt{n} \log n})$.

The distribution Ψ_α is defined to be a normal distribution of $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ with mean 0 and standard deviation $\frac{\alpha}{\sqrt{2\pi}}$. And $\bar{\Psi}_\alpha$ is the discrete distribution of the random variable $\lfloor q \cdot \mathbf{X} \rceil \mod q$ over $\mathbb{F}_q$, where $a \mod b = a - \lfloor a/b \rfloor b$ and $\mathbf{X}$ is from the distribution Ψ_α.

- **Private key:** Choose a random $\mathbf{s} \in (\mathbb{Z}/q\mathbb{Z})^n$ uniformly.
- **Public key:** Choose a random matrix $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{n \times m}$ uniformly. Choose an error vector $\mathbf{x}$ from $(\mathbb{Z}/q\mathbb{Z})^m$, where each component of $\mathbf{x}$ is chosen according to the distribution $\chi = \bar{\Psi}_\alpha$. Announce the public key $(\mathbf{A}, \mathbf{P})$ where $\mathbf{P} \in (\mathbb{Z}/q\mathbb{Z})^m$ should be calculated as $\mathbf{sA} + \mathbf{x}$.
- **Encryption:** First select a random vector $\mathbf{e}^T \in \{0,1\}^m$. For a message bit $v \in \{0,1\}$, the encryption is $(\mathbf{Ae}, v\lfloor \frac{q}{2} \rfloor + \mathbf{Pe})$.
- **Decryption:** For the cipher-text $(\mathbf{a}, b)$, output 0 if $b - \langle \mathbf{a}, \mathbf{s} \rangle$ is closer to 0 than to $q/2$; Otherwise de-crypt to 1.

For security level n, the private key has $\tilde{O}(n)$ bits. The public key has $\tilde{O}(n^2)$ bits, and can be reduced to $\tilde{O}(n)$. The cipher-text expansion is $\tilde{O}(n)$. The encoding and decoding complexity is $\tilde{O}(n^2)$ per bit. Hence this system is not efficient, especially in terms of cipher-text expansion and encryption/decryption complexity.

To find the private key from the public key, one can solve a CVP problem in the lattice $\mathcal{L} = \{v\mathbf{A} \mid v \in (\mathbb{Z}/q\mathbb{Z})^n\}$, which is a sub-lattice of $q\mathbb{Z}^m$. Note that $q^{m-n} \mid \det(\mathcal{L})$. The shortest vector of $\mathcal{L}$ has length $\tilde{O}(q\sqrt{m})$. This means that the secret key is likely unique.

3.2 PVW improvement

Peikert, Vaikuntanathan, and Waters [29] proposed a more efficient system based on LWE. They made two important changes: first the secret and the error in the public key are matrices, and the message space consists of vectors; secondly the alphabet of the message is $\mathbb{Z}/p\mathbb{Z}$ for some p that may be greater than 2. The latter idea has also been utilized by Kawachi, Tanaka, and Xagawa [21] to improve the efficiency of several single-bit cryptosystems based on lattice problems.

Suppose that $p = poly(n)$, $l = poly(n)$, $m = O(n \log n)$, $\alpha = 1/(p\sqrt{m} \log n)$ and $q > p$ is a prime. Let t be a function from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}/q\mathbb{Z}$ defined by $t(x) = [x \times \frac{q}{p}]$ and extended to act component-wise on vector spaces over $\mathbb{Z}/p\mathbb{Z}$.

- **Private key:** Choose a random matrix $\mathbf{S} \in (\mathbb{Z}/q\mathbb{Z})^{n \times l}$ uniformly.
- **Public key:** Choose a random matrix $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{n \times m}$ uniformly. Find an error matrix $\mathbf{X} \in (\mathbb{Z}/q\mathbb{Z})^{l \times m}$ where each entry is chosen independently according to the error distribution $\chi = \bar{\Psi}_\alpha$. The public key is $(\mathbf{A}, \mathbf{P})$ where $\mathbf{P} = \mathbf{S}^T\mathbf{A} + \mathbf{X} \in (\mathbb{Z}/q\mathbb{Z})^{l \times m}$.

- **Encryption:** The message is assumed to be a vector $\mathbf{v} \in (\mathbb{Z}/p\mathbb{Z})^l$. First convert it to a vector $t(\mathbf{v})$ in $(\mathbb{Z}/q\mathbb{Z})^l$. Then select $\mathbf{e}^T \in \{0,1\}^m$ uniformly at random. The encryption is $(\mathbf{Ae}, \mathbf{Pe} + t(\mathbf{v})) \in (\mathbb{Z}/q\mathbb{Z})^n \times (\mathbb{Z}/q\mathbb{Z})^l$.
- **Decryption:** For the cipher-text $(\mathbf{u}, \mathbf{c})$, compute $\mathbf{d} = \mathbf{c} - \mathbf{S}^T\mathbf{u}$, and output $\mathbf{v} \in (\mathbb{Z}/p\mathbb{Z})^l$, where v_i is the element in $\mathbb{Z}/p\mathbb{Z}$ that makes $d_i - t(v_i)$ closest to $0 \pmod q$.

Note that one may set $l = n$ in the cryptosystem. In this case, the public key size and secure key size are $\tilde{O}(n^2)$. The algorithm has cipher-text expansion $O(1)$. The encryption and decryption complexity is $\tilde{O}(n)$ per bit.

The security of the cryptosystem comes from the fact that if $\mathbf{S}$ is hidden, the public key $(\mathbf{A}, \mathbf{P})$ is computationally indistinguishable from uniform distribution over $(\mathbb{Z}/q\mathbb{Z})^{n\times m} \times (\mathbb{Z}/q\mathbb{Z})^{l\times m}$, for suitable parameters, under the hypothesis that LWE is hard.

3.3 PKC based on ideal lattices

To improve the efficiency of the LWE-based system, Lyubashevsky, Peikert, and Regev [24] proposed the primitive of ring-LWE. Let $R = \mathbb{Z}[x]/(x^n + 1)$, where n is a power of two. Let $R_q = (\mathbb{Z}/q\mathbb{Z})[x]/(x^n + 1)$.

- **Private key:** The private key is $s, e \in R_q$ from an error distribution.
- **Public key:** Select a random $a \in R_q$ uniformly. Output $(a, b) \in R_q^2$, where $b = as + e$.
- **Encryption:** To encrypt a bit string z of length n, we view it as an element in R_q so that bits in z become coefficients of a polynomial. The cipher-text is (u, v) obtained by

  $$u = ar + e_1, v = br + e_2 + \lfloor q/2 \rfloor z,$$

  where r, e_1, e_2 are chosen from an error distribution.
- **Decryption:** For cipher-text (u, v), computes $v - us$, which equals

  $$(re - se_1 - e_2) + \lfloor q/2 \rfloor z.$$

  One can read z from $v - us$, since r, e, e_1 and e_2 have small coefficients.

The algorithm is very efficient. Public and private key size is $\tilde{O}(n)$. Cipher-text expansion is $O(1)$, and encryption/decryption complexity per bit is $(\log n)^{O(1)}$, assuming that we use the fast multiplication algorithm. The parameters are optimal asymptotically, however, the security is based on approx-SVP of ideal lattices, rather than general lattices.

4 The matrix-LWE

Our first proposal would be a modification of PVW, which is a matrix version of the standard LWE.

- **Private key:** Choose a random matrix $\mathbf{S} \in (\mathbb{Z}/q\mathbb{Z})^{n\times l}$ uniformly.
- **Public key:** Choose a random matrix $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{n\times m}$ uniformly. Find an error matrix $\mathbf{X} \in (\mathbb{Z}/q\mathbb{Z})^{l\times m}$ where each entry is chosen independently according to the error distribution χ. The public key is $(\mathbf{A}, \mathbf{P})$ where $\mathbf{P} = \mathbf{S}^T\mathbf{A} + \mathbf{X} \in (\mathbb{Z}/q\mathbb{Z})^{l\times m}$.
- **Encryption:** The message is assumed to be a matrix $\mathbf{V} \in (\mathbb{Z}/p\mathbb{Z})^{l\times k}$. First convert it to a matrix in $t(\mathbf{V}) \in (\mathbb{Z}/q\mathbb{Z})^{l\times k}$. Then select $\mathbf{E} \in \{0,1\}^{m\times k}$ uniformly at random. The encryption is $(\mathbf{AE}, \mathbf{PE} + t(\mathbf{V})) \in (\mathbb{Z}/q\mathbb{Z})^{n\times k} \times (\mathbb{Z}/q\mathbb{Z})^{l\times k}$.
- **Decryption:** For the cipher-text $(\mathbf{U}, \mathbf{C})$, compute $\mathbf{D} = \mathbf{C} - \mathbf{S}^T\mathbf{U}$, and output $\mathbf{V} \in (\mathbb{Z}/p\mathbb{Z})^{l\times k}$, where v_{ij} is the element in $\mathbb{Z}/p\mathbb{Z}$ that makes $\mathbf{D}_{ij} - t(\mathbf{V}_{ij})$ closest to $0 \pmod q$.

As a general principle, there is a tradeoff between the efficiency and security of the scheme using different parameters. For an instantiation that offers both efficiency and security, we follow PVW's concrete parameters. In detail, we express parameters as functions of n. Let $p = n^c$ for some positive constant c and $l = n = k$. Let $m = (12 + 6c) \cdot n \log n$ and q be a prime in $[10, 20] \cdot pm \log n$. The error distribution is $\chi = \bar{\Psi}_\alpha$, where $\alpha = \frac{1}{p\sqrt{m}\log n}$. Note that if $p = 2$ $(c = 0)$, we have the binary case.

Following a similar argument as PVW's, we can firstly show the correctness of our scheme.

Proposition 1. *With the parameters fixed as above, the encryption procedure fails with negligible probability, where the probability is taken over the random choice of* $\mathbf{X}$.

Following a similar proof of security as PVW's, we have the following theorem which implies that the matrix LWE is secure under chosen plaintext attack.

Proposition 2. *With the given parameters, the matrix version of LWE scheme is provably semantic secure, under the assumption that approx-SIVP and approx-SVP to within some $\tilde{O}(n^{c+3/2})$ factor is hard for quantum algorithms.*

The efficiency is improved since we can use the fast matrix multiplication. More precisely, we can set $l = n$, and $m = \Theta(n \log n)$. The matrix is almost square. Then we use the fast square matrix multiplication to optimize the performance. The block size, public key and private key sizes are $\tilde{O}(n^2)$, and cipher-text expansion is $\tilde{O}_n(1)$. Most importantly, encryption and decryption complexity is $\tilde{O}(n^{\omega-2})$ per bit, which is sublinear. Here $\omega < 2.38$ is the matrix multiplication exponent. For practical purpose, using the Strassen's matrix multiplication method should be a better choice, which also results in a sublinear encryption/decryption complexity per bit.

5 PKC from dihedral group rings

In this section, we describe a cryptosystem based on the dihedral group ring. The protocol is identical to one based on the ideal lattice, except that since multiplication is not commutative, one needs to pay attention to the order of multiplication. Let n be a power of two, let q be a prime such that $\gcd(q, 2n) = 1$, and $q \in [n^2, 2n^2]$. Recall

$$\mathbf{R} = \mathbb{Z}[D_{2n}]/((r^{n/2} + 1)\mathbb{Z}[D_{2n}]),$$

$$\mathbf{R}_q = \mathbb{F}_q[D_{2n}]/((r^{n/2} + 1)\mathbb{F}_q[D_{2n}]),$$

and the error distribution χ on $\mathbf{R}_q$ is to select coefficients independently according to a Guassian of width $n^{1.5-\epsilon}$.

- **Private key:** The private key is $s, e \in \mathbf{R}_q$ from the error distribution.
- **Public key:** Select a random $a \in \mathbf{R}_q$ uniformly. Output $(a, b) \in \mathbf{R}_q^2$, where $b = sa + e$.
- **Encryption:** To encrypt a bit string z of length n, we view it as an element in $\mathbf{R}_q$ so that bits in z become coefficients of a polynomial. The cipher-text is (u, v) obtained by

  $$u = ar + e_1, v = br + e_2 + \lfloor q/2 \rfloor z,$$

  where r, e_1, e_2 are chosen from an error distribution.
- **Decryption:** For cipher-text (u, v), one computes $v - su$, which equals

  $$(re - se_1 - e_2) + \lfloor q/2 \rfloor z.$$

  One can read z from $v - us$, since r, e, e_1 and e_2 have small coefficients.

One can verify that the public and private key sizes are linear in the security level, and the ciphertext expansion is almost a constant. The following theorem shows that the encryption/decryption complexity is logarithmic per bit.

Theorem 1. *The multiplication in $\mathbb{Z}[D_{2n}]$ can be done in $\tilde{O}(n \log q)$ time.*

In this theorem, we use the whole group ring for generality. One can check that it applies to $\mathbf{R}$ as well.

Proof. The main idea is to separate the terms in $(\mathbb{Z}/q\mathbb{Z})[D_{2n}]$ into two parts. Let $f_1 + sf_2$ and $f_3 + sf_4$ be two elements where f_1, f_2, f_3 and f_4 are polynomials in r. We have

$$\begin{aligned} &(f_1 + sf_2)(f_3 + sf_4) \\ =&f_1f_3 + sf_2f_3 + f_1sf_4 + sf_2sf_4 \\ =&f_1f_3 + sf_2f_3 + s(sf_1s)f_4 + (sf_2s)f_4 \\ =&(f_1f_3 + (sf_2s)f_4) + s(f_2f_3 + (sf_1s)f_4) \end{aligned}$$

where sf_1s and sf_2s are polynomials in r that can be calculated in linear time. To find the product, we need to compute four polynomial multiplications in $(\mathbb{Z}/q\mathbb{Z})[r]$, that can be done in time $\tilde{O}(n \log q)$.

In the normal version of group ring LWE, s and e are selected according to error distribution, while in the regular version, only e is selected according to error distribution. The following theorem shows that these two versions are equivalent.

Theorem 2. *The regular version of dihedral GR-LWE can be reduced to the normal version of dihedral GR-LWE.*

Proof. (Sketch) Suppose that the input of the LWE problem is (a_1, b_1) and (a_2, b_2). With high probability, a_1 is invertible, we construct the input for normal version of LWE as

$$(a_2a_1^{-1}, a_2a_1^{-1}b_1 - b_2).$$

Note that

$$a_2a_1^{-1}b_1 - b_2 = a_2a_1^{-1}(a_1s + e_1) - (a_2s + e_2) = a_2a_1^{-1}e_1 - e_2.$$

6 Security analysis of the new approach

In this section, we prove the main theorem

Theorem 3. *Given an average case of search version of dihedral GR-LWE oracle, there is a quantum polynomial time algorithm that solves the search version of the SVP problem for any invertible ideal of* $\mathbf{R}$ *with approximate factor* $O(n^{1.5})$.

Let us first review the main ideas in Regev's reduction from approx-SVP to LWE, which inspires our proof. The reduction can be divided into iterative steps. We will solve the *Discrete Gaussian Sampling* problem (DGS) for a lattice, that has a comparable hardness as approx-SVP. The $\mathrm{DGS}_{\mathcal{L},r}$ problem is to sample lattice points of a lattice $\mathcal{L}$ according to a Gaussian centering at O with width r. For precise definition, see [31]. The DGS will be reduced, by a quantum algorithm, to a β-BDD problem on its dual lattice $\mathcal{L}^*$, which will then be reduced to a (q, β)-BDD problem. The (q, β)-BDD will be reduced to a DGS problem of larger width. This step needs help from the search LWE oracle. After a few iterations, we arrive at DGS with a width that allows a polynomial time algorithm.

The only step that needs an LWE oracle is the reduction from (q, β)-BDD to DGS. Suppose we have a (q, β)-BDD instance $y(= x + e)$, where $x \in \mathcal{L}^*$ and $|e| \leq \lambda_1(\mathcal{L}^*)\beta$. We wish to find $x \pmod{q\mathcal{L}^*}$. We are able to sample a random element $z \in \mathcal{L}$ by the DGS algorithm, such that $|z| \leq m/\lambda_1(\mathcal{L}^*)$, where $m \geq q\sqrt{n}$. So we have

$$m/\lambda_1(\mathcal{L}^*) \geq q\sqrt{n}/\lambda_1(\mathcal{L}^*) \approx q\eta(\mathcal{L}) = \eta(q\mathcal{L}),$$

where $\eta(*)$ is the smoothing parameter of a lattice. Let a be $z \mod q\mathcal{L}$. Then a is a random element in $\mathbb{F}_q^n$ by the definition of a smoothing parameter. We compute a by writing down the coefficients of z in the base B and modulo them by q. There is a map from $\mathbb{F}_q^n$ to $\mathcal{L} \pmod{q\mathcal{L}}$ given by the base matrix $\mathbf{B}$, such that $\psi\mathbf{B} = 1$, where ψ is a map in the $\mathbb{Z}$-module exact sequence:

$$0 \to q\mathcal{L} \to \mathcal{L} \xrightarrow{\psi} \mathbb{F}_q^n \to 0$$

Note that the map given by $\mathbf{B}$ is not a $\mathbb{Z}$-module homomorphism, since the exact sequence is not splitting. Let $b = z(x+e)^T = zx^T + ze^T \pmod{q\mathbb{Z}}$, and $s = x\mathbf{B}^T$. Note that $|ze^T|_\infty \leq m\beta$, and $zx^T = a\mathbf{B}x^T = a\mathbf{B}(s(\mathbf{B}^{-1})^T)^T = as$. Call the search LWE oracle, we will get s, which gives us $x \pmod{q\mathcal{L}^*}$, and completes the reduction. We can see that working with the dual lattice is very important.

Remark 2. Here the transformation by $\mathbf{B}$ is important. We can not just mod z by $q\mathbb{Z}^n$, since it may be the case that $\mathcal{L} \subseteq q\mathbb{Z}^n$, or $\mathcal{L}$ is not even an integral lattice.

For LWE on the ring $R = \mathbb{Z}[x]/(x^n+1)$, the idea is similar. Any ideal in the number field $\mathbb{Q}[x]/(x^n+1)$ is a $\mathbb{Z}$-module thus corresponds to a lattice if we provide an embedding. There are two ways of embedding: canonical and coefficient. If we use canonical embedding, then the dual is $I^\vee$ [24], instead of I^{-1}. To keep the multiplicative structure of the ring, we need a R-module isomorphism from $I/(qI)$ to $R/(qR) = \mathbb{F}_q[x]/(f(x))$, and from $I^\vee/(qI^\vee)$ to $R^\vee/(qR^\vee) = \mathbb{F}_q[x]/(f(x))$, so we can recover $I^\vee/(qI^\vee)$ from a polynomial in $R/(qR)$. As pointed out in [24], it is important to clear ideals while preserving the R-module structure.

Example 1. Let $R = \mathbb{Z}$, $q = 5$ and $I = (3)$. Suppose that $z = 24 \in I$, $z \pmod{qI}$ should be 9 in the parallelepiped $[0, 15)$. Dividing by $t = 3$, we send z to 3 in $\mathbb{Z}/q\mathbb{Z}$. Hence multiplying by 3 is a $\mathbb{Z}$-module isomorphism from $\mathbb{Z}/5\mathbb{Z}$ to $I/5I$.

On the other hand, $\mathbb{Z}$-module isomorphism is not unique. If we can just use the inclusion $I \hookrightarrow R$, we have $z = 4 \pmod 5$. This is another $\mathbb{Z}$-module isomorphism. If $\psi : I \to R$ is a R-module isomorphism, so is $t\psi$ for any $t \in R$.

To complete the reduction, one needs to send an element in $\mathbb{Z}/5\mathbb{Z}$ back to $I^{-1}/5I^{-1}$. Here $I^{-1} = (1/3)\mathbb{Z}$. One can see that the inclusion $\mathbb{Z} \subseteq I^{-1}$ induces an isomorphism $\mathbb{Z}/5\mathbb{Z} \to I^{-1}/5I^{-1}$.

Now we will extend the idea to non-commutative group ring LWE. We should use coefficient embedding to map ideals to lattices. In the following discussion, we will use the same symbol for an ideal and its corresponding lattice under coefficient embedding. All of the steps in the work of [31, 24] can be adopted in a straightforward manner, except for the step from (q, β)-BDD to DGS using the GR-LWE oracle. Thus we only need to show

Lemma 3. *With help from a search dihedral GR-LWE oracle, we can reduce the (q, β)-BDD problem for I^{-1}, where I is any invertible left ideal of $\mathbf{R}$, to the DGS on I with width $m/\lambda_1(I^{-1})$, as long as $m\beta \leq n^{1.5-\epsilon}$, $q > n^2$, $gcd(q, 2n) = 1$ and $q \nmid det(I)$.*

Proof. (Sketch) Suppose that we have a BDD problem $y = x + e$ in I^{-1}. We find a short $z \in I$ using DGS algorithm, and let $a = \phi_1(z) \pmod{q\mathbf{R}} \in \mathbf{R}/(q\mathbf{R})$, where ϕ_1 is the inclusion $I \to \mathbf{R}$, which is also a left $\mathbf{R}$-module homomorphism. Note that $q\mathbf{R}$ is a two-sided ideal, $\mathbf{R}/q\mathbf{R}$ is a direct summand of the ring $\mathbb{F}_q[D_{2n}]$. Since $det(I)$ is not divisible by q, ϕ_1 induces a natural left $\mathbf{R}$-module surjective homomorphism $I \to \mathbf{R}/(q\mathbf{R})$. We then calculate zy (in $\mathbb{R} \otimes_{\mathbb{Z}} \mathbf{R}$), discretize it to $\mathbf{R}$, and modulo $q\mathbf{R}$. The discretization is easy, since $\mathbf{R} = \mathbb{Z}^n$ by coefficient embedding. Let b be the result. We have $b \equiv zy = zx + ze \pmod{q\mathbf{R}}$, where $zx \in \mathbf{R}$ and ze is short. In order to uniquely determine $x \pmod{qI^{-1}}$, we generate several instances of (a, b), and send them to the LWE oracle. Assume that the oracle answers s in $\mathbf{R}/q\mathbf{R}$. Let ϕ_2 be the inclusion $\mathbf{R} \to I^{-1}$, which is also a right $\mathbf{R}$-module homomorphism. It induces a natural right module homomorphism $I^{-1} \to \mathbf{R}/(q\mathbf{R})$, since $q \nmid det(I)$. So pulling s back along the homomorphism gives us the residue class of $x \pmod{qI^{-1}}$.

7 Conclusion

In this work, we first propose a matrix version of the standard LWE problem which improves the efficiency of the public key cryptosystem, while maintaining its security. We then propose generating LWE instances from non-commutative group rings and illustrate the approach by presenting a public key scheme based on dihedral group rings. We believe that LWE on dihedral group rings achieves the right trade-off between security and efficiency. As with the original LWE and ring-LWE, we hope that the new approach is a versatile primitive, so we can build various cryptographic schemes based on this primitive besides public-key encryption. There are two open problems that we find very interesting: Can we generalize the approach to other non-commutative groups and keep the efficiency of ring-LWE? Can we have LWE on non-commutative group rings that is CCA secure?

References

1. Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient lattice (H)IBE in the standard model. In *Advances in Cryptology - EUROCRYPT 2010*, pages 553–572, 2010.
2. Shweta Agrawal, Dan Boneh, and Xavier Boyen. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In *Advances in Cryptology - CRYPTO 2010*, pages 98–115, 2010.
3. Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing - STOC*, pages 99–108, 1996.
4. Joppe W. Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from LWE. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1006–1018, 2016.

5. Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. In *Innovations in Theoretical Computer Science - ICTS*, pages 309–325, 2012.
6. Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS*, pages 97–106, 2011.
7. Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-lwe and security for key dependent messages. In *Advances in Cryptology - CRYPTO 2011*, pages 505–524, 2011.
8. David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. In *Advances in Cryptology - EUROCRYPT 2010*, pages 523–552, 2010.
9. Hao Chen, Kristin E. Lauter, and Katherine E. Stange. Attacks on search RLWE. Cryptology ePrint Archive, Report 2015/971, 2015.
10. Hao Chen, Kristin E. Lauter, and Katherine E. Stange. Vulnerable galois RLWE families and improved attacks. Cryptology ePrint Archive, Report 2016/193, 2016.
11. D. Coppersmith. Attacking non-commutative ntru. IBM Research Report, 1997.
12. Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In *Advances in Cryptology - EUROCRYPT 2016*, pages 559–585, 2016.
13. Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short stickelberger class relations and application to ideal-svp. Cryptology ePrint Archive, Report 2016/885, 2016.
14. Jintai Ding. New cryptographic constructions using generalized learning with errors problem. Cryptology ePrint Archive, Report 2012/387, 2012.
15. Kirsten Eisenträger, Sean Hallgren, and Kristin E. Lauter. Weak instances of PLWE. In *Selected Areas in Cryptography - SAC 2014*, pages 183–194, 2014.
16. Yara Elias, Kristin E. Lauter, Ekin Ozman, and Katherine E. Stange. Provably weak instances of ring-lwe. In *Advances in Cryptology - CRYPTO 2015*, pages 63–92, 2015.
17. Junfeng Fan and Frederik Vercauteren. Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive, Report 2012/144, 2012.
18. Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. A simple bgn-type cryptosystem from LWE. In *Advances in Cryptology - EUROCRYPT 2010*, pages 506–522, 2010.
19. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 197–206, 2008.
20. Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In *Algorithmic Number Theory, Third International Symposium, ANTS-III*, pages 267–288, 1998.
21. Akinori Kawachi, Keisuke Tanaka, and Keita Xagawa. Multi-bit cryptosystems based on lattice problems. In *Public Key Cryptography - PKC*, volume 4450 of *Lecture Notes in Computer Science*, pages 315–329. Springer, 2007.
22. Richard Lindner and Chris Peikert. Better key sizes (and attacks) for lwe-based encryption. In *Topics in Cryptology - CT-RSA 2011*, pages 319–339, 2011.
23. Richard Lindner and Chris Peikert. Better key sizes (and attacks) for lwe-based encryption. In *Topics in Cryptology - CT-RSA 2011*, pages 319–339, 2011.
24. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Advances in Cryptology - EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23. Springer, 2010.

25. Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Advances in Cryptology - EUROCRYPT 2012*, pages 700–718, 2012.
26. Alexei G. Myasnikov, Vladimir Shpilrain, and Alexander Ushakov. *Non-commutative Cryptography and Complexity of Group-theoretic Problems*. American Mathematical Society, 2011.
27. Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009*, pages 333–342. ACM, 2009.
28. Chris Peikert. How (not) to instantiate ring-lwe. In *Security and Cryptography for Networks - 10th International Conference, SCN 2016*, pages 411–430, 2016.
29. Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A framework for efficient and composable oblivious transfer. In *Advances in Cryptology - CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 554–571. Springer, 2008.
30. Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 187–196, 2008.
31. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):34, 2009. Preliminary version in STOC'05.
32. Sudarshan K Sehgal. *Units in integral group rings*. Longman, 1993.
33. Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science - FOCS*, pages 124–134, 1994.
34. Damien Stehlé and Ron Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. In *Advances in Cryptology - EUROCRYPT 2011*, pages 27–47, 2011.
35. K. R. Truman. *Analysis and extension of non-commutative NTRU*. PhD thesis, University of Maryland, 2007.
36. Takanori Yasuda, Xavier Dahan, and Kouichi Sakurai. Characterizing ntru-variants using group ring and evaluating their lattice security. Cryptology ePrint Archive, Report 2015/1170, 2015.