An efficient key generation algorithm for GR-NTRU over dihedral group

Vikas Kumar[a], Ali Raya[b], Aditi Kar Gangopadhyay[a]

[a]*Department of Mathematics, IITR, 247667, Roorkee, India*
[b]*Department of Computer Science and Engineering, IITR, 247667, Roorkee, India*

Abstract

In this article, we focus on deriving an easily implementable and efficient method of constructing units of the group ring of dihedral group. We provide a necessary and sufficient condition that relates the units in the group ring of dihedral group with the units in the group ring of cyclic group. Using this relation and the methods available for inversion in the group ring of the cyclic group, we introduce an algorithm to construct units efficiently and check its performance experimentally.

Keywords: group ring, units of group ring, dihedral group, NTRU, GR-NTRU

1. Introduction

Group rings and their units receive attention from mathematicians for their close relation to algebra, number theory, and representation theory. For a detailed survey on units of group rings, one can refer to [1, 2]. The applications of units of group rings are not restricted to mathematics. Articles like [3–6] provide various applications of group rings and their units in cryptography.

One of the most famous examples where units are used to build a cryptosystem is NTRU [7], a post-quantum scheme built over a quotient ring of polynomials. Different NTRU-like variants can be built by changing the underlying ring. However, the key generation process involves sampling el-

Email addresses: v_kumar@ma.iitr.ac.in (Vikas Kumar), ali_r@cs.iitr.ac.in (Ali Raya), aditi.gangopadhyay@ma.iitr.ac.in (Aditi Kar Gangopadhyay)

ements from the ring such that one of them is a unit(i.e., an invertible element). Algorithm 1 outlines the key generation process for an NTRU-like scheme.

Algorithm 1: NTRU-like scheme key generation

Input: A parameter set N, p, q defining the cryptosystem
Output: h the public key

```
1 f ← Sampler /* Sampling an element from the ring        */
2 if f is not invertible then
3 |  go to step 1
4 g ← Sampler /* Sampling an element from the ring        */
5 h = g/f  mod q
6 return h
```

The most studied variants of NTRU are built over commutative rings of quotient polynomials where algorithms to invert elements are well-studied and optimized. Recently, Kim and Lee [8] demonstrated a polynomial-time attack on a relaxed version of NTRU problem called NTRU learning problem, which was considered to be as difficult as NTRU problem. A thorough analysis of their attack shows that the commutativity of the underlying structure helps construct linear equations whose solution contains information about the private key that can be recovered in polynomial time. Furthermore, when Coppersmith and Shamir [9] introduced lattice attack against NTRU, they suggested that considering a noncommutative group algebra could be another direction to provide better security against their attack. Therefore, exploring noncommutative variants of NTRU is an important direction of research.

Motivation: There are many noncommutative NTRU-like schemes in literature like [10–15]. However, none of these schemes provide a way to generate keys, which raises many questions about their practical implementation. Yasuda et al. [16] describe group ring NTRU (GR-NTRU) as a general structure to build different variants of NTRU-like schemes. In GR-NTRU, the group ring $\mathbb{Z}G$ corresponding to a finite group G is used to create an NTRU-like variant, where the group G can be abelian or nonabelian. One would need units to build GR-NTRU over dihedral group. Raya et al. [17] show that dihedral group is a good option for developing GR-NTRU by experimentally checking that the keyspace size for different key generation criteria is large enough. However, they have used the matrix inversion method to generate keys that becomes time-consuming in higher dimensions. They leave developing a fast inversion algorithm as future work. We put an end

to this task in this work.

Our Contribution: In this work, we focus on the construction of units in the group ring of dihedral group. There are works on the characterization of units in dihedral group rings [18] [19], [20]. However, all those classifications rely on group representation theory and are not easily implementable to serve the purpose of constructing units. Therefore, it becomes essential to look for alternative ways to check for units. In this paper, we first give some preliminary results on units in the group ring of the cyclic group. Then, as the main result, we find a necessary and sufficient condition for an element to be a unit in the group ring of dihedral group. We provide an explicit relation between units in dihedral group ring and the units in the group ring of cyclic group. Further, we check the efficiency of our approach experimentally.

2. Group ring of dihedral group

Consider a dihedral group D_N of order $2N$,

$$D_N = \left\langle x, y : x^N = y^2 = 1, xy = yx^{N-1} \right\rangle.$$

The group ring of diheral group over a commutative ring R is defined as:

$$RD_N = \{\alpha_0 1+\alpha_1 x+\cdots+\alpha_{N-1}x^{N-1}+\beta_0 y+\beta_1 yx+\cdots+\beta_{N-1}yx^{N-1} : \alpha_i, \beta_i \in R\}.$$

In this article, R is a commutative ring with unity. Suppose an element $a = \alpha_0 1+\alpha_1 x+\cdots+\alpha_{N-1}x^{N-1}+\beta_0 y+\beta_1 yx+\cdots+\beta_{N-1}yx^{N-1} \in RD_N$. Let $\alpha(x) = \alpha_0 1+\alpha_1 x+\cdots+\alpha_{N-1}x^{N-1}$ and $\beta(x) = \beta_0 1+\beta_1 x+\cdots+\beta_{N-1}x^{N-1}$. Then, we can think of $\alpha(x), \beta(x)$ as elements of the group ring RC_N, where C_N is the cyclic group of order N. In fact, RC_N is the subring of RD_N. By abuse of notation, we may write $a = \alpha(x) + y\beta(x)$. Thus, from now onwards

$$RD_N = \{\alpha(x) + y\beta(x) : \alpha(x), \beta(x) \in RC_N\}. \tag{1}$$

Consider the product

$$\begin{aligned}
\alpha(x)y &= \alpha_0 y + \alpha_1 xy + \alpha_2 x^2 y \cdots + \alpha_{N-1}x^{N-1}y \\
&= \alpha_0 y + \alpha_1 y(x^{N-1}) + \alpha_2 y(x^{N-1})^2 + \cdots + \alpha_{N-1}y(x^{N-1})^{N-1} \\
&= y(\alpha_0 + \alpha_1(x^{N-1}) + \alpha_2(x^{N-1})^2 + \cdots + \alpha_{N-1}(x^{N-1})^{N-1}) \\
&= y\alpha(x^{N-1}).
\end{aligned}$$

Therefore the product of two elements $w = u(x) + yv(x), a = \alpha(x) + y\beta(x) \in RD_N$ is given by

$$\begin{aligned} wa &= (u(x) + yv(x))(\alpha(x) + y\beta(x)) \\ &= u(x)\alpha(x) + yv(x)\alpha(x) + u(x)y\beta(x) + yv(x)y\beta(x) \\ &= u(x)\alpha(x) + yv(x)\alpha(x) + yu(x^{N-1})\beta(x) + v(x^{N-1})\beta(x) \\ &= u(x)\alpha(x) + v(x^{N-1})\beta(x) + y(v(x)\alpha(x) + u(x^{N-1})\beta(x)). \end{aligned}$$

In the following lemma, $(uv)(x^r)$ is an element in RC_N obtained by multiplying $u(x), v(x)$ and then replacing x with x^r in the product. While $u(x^r)v(x^r)$ is obtained by first replacing x with x^r in $u(x), v(x)$ and then multiplying them.

Lemma 1. *Let $u(x), v(x) \in RC_N$. Then $(uv)(x^r) = u(x^r)v(x^r)$, for all $r = 1, 2, \ldots, N-1$.*

Proof. Let $u(x) = \sum_{i=0}^{N-1} u_i x^i$ and $v(x) = \sum_{j=0}^{N-1} v_j x^j$. Then

$$u(x^r) = \sum_{k_1=0}^{N-1} \left(\sum_{\substack{ir \equiv k_1 (\mathrm{mod} N) \\ i \in \{0,1,\ldots,N-1\}}} a_i \right) x^{k_1} \quad \text{and} \quad v(x^r) = \sum_{k_2=0}^{N-1} \left(\sum_{\substack{jr \equiv k_2 (\mathrm{mod} N) \\ j \in \{0,1,\ldots,N-1\}}} b_j \right) x^{k_2}.$$

Now

$$\begin{aligned} u(x^r)v(x^r) &= \sum_{k_1=0}^{N-1} \left(\sum_{\substack{ir \equiv k_1 (\mathrm{mod} N) \\ i \in \{0,1,\ldots,N-1\}}} a_i \right) x^{k_1} \sum_{k_2=0}^{N-1} \left(\sum_{\substack{jr \equiv k_2 (\mathrm{mod} N) \\ j \in \{0,1,\ldots,N-1\}}} b_j \right) x^{k_2} \\ &= \sum_{k=0}^{N-1} \left[\sum_{k_1+k_2 \equiv k (\mathrm{mod} N)} \left(\sum_{\substack{ir \equiv k_1 (\mathrm{mod} N) \\ i \in \{0,1,\ldots,N-1\}}} a_i \right) \left(\sum_{\substack{jr \equiv k_2 (\mathrm{mod} N) \\ j \in \{0,1,\ldots,N-1\}}} b_j \right) \right] x^k \\ &= \sum_{k=0}^{N-1} \left[\sum_{k_1+k_2 \equiv k (\mathrm{mod} N)} \left(\sum_{\substack{ir, jr \equiv k_1, k_2 (\mathrm{mod} N) \\ i,j \in \{0,1,\ldots,N-1\}}} a_i b_j \right) \right] x^k \\ &= \sum_{k=0}^{N-1} \left(\sum_{\substack{(i+j)r \equiv k (\mathrm{mod} N) \\ i,j \in \{0,1,\ldots,N-1\}}} a_i b_j \right) x^k = (uv)(x^r). \end{aligned}$$

□

Corollary 1. *If $u(x) \in RC_N$ is a unit with inverse $v(x)$ then $u(x^r)$ is unit with inverse $v(x^r)$, for all $r \in \{1, 2, \ldots, N-1\}$.*

Proof. Suppose $u(x) \in RC_N$ is unit then there exists a $v(x) \in RC_N$ such that $(uv)(x) = u(x)v(x) = 1$. Then, by Lemma 1, for any positive integer $r \in \{1, 2, \ldots, N-1\}$, we have $u(x^r)v(x^r) = (uv)(x^r) = 1$. □

3. Constructing units in RD_N from units in RC_N

Corollary 2. *Let $u(x)$ be a unit in RC_N with inverse $v(x)$. Then $u(x^r)$ and $yu(x^r)$ are units in RD_N with inverses $v(x^r)$ and $yv(x^{(N-1)r})$, respectively, for all $r = 1, 2, \ldots, N-1$.*

Proof. Since, $u(x), v(x)$ are inverses of each other, therefore, $(uv)(x) = 1$. Using Lemma 1, we get

$$(yu(x^r))(yv(x^{(N-1)r})) = y^2u(x^{(N-1)r})v(x^{(N-1)r}) = (uv)(x^{(N-1)r}) = 1.$$

□

Theorem 1. *(Necessary and sufficient condition) Let $w = u(x) + yv(x) \in RD_N$. Then, w is a unit in RD_N if and only if the element $v(x)v(x^{N-1}) - u(x)u(x^{N-1})$ is a unit in RC_N. Moreover, if $h(x)$ denotes the inverse of $v(x)v(x^{N-1}) - u(x)u(x^{N-1})$ in RC_N then inverse of w is given by $a = \alpha(x) + y\beta(x)$ where $\alpha(x) = -u(x^{N-1})h(x)$ and $\beta(x) = v(x)h(x)$.*

Proof. Suppose $v(x)v(x^{N-1}) - u(x)u(x^{N-1})$ is a unit in RC_N with inverse $h(x)$ and $\alpha(x), \beta(x)$ be as in the statement of the theorem. Then

$$\begin{aligned} wa &= u(x)\alpha(x) + v(x^{N-1})\beta(x) + y(v(x)\alpha(x) + u(x^{N-1})\beta(x)) \\ &= -u(x)u(x^{N-1})h(x) + v(x^{N-1})v(x)h(x) \\ &\quad + y(-v(x)u(x^{N-1})h(x) + u(x^{N-1})v(x)h(x)) \\ &= h(x)(v(x)v(x^{N-1}) - u(x)u(x^{N-1})) = 1. \end{aligned}$$

Also, from Lemma 1, $h(x^{N-1})(v(x)v(x^{N-1}) - u(x)u(x^{N-1})) = 1$. Therefore,

by the uniqueness of the inverse, we get that $h(x) = h(x^{N-1})$. Consider

$$\begin{aligned} aw &= \alpha(x)u(x) + \beta(x^{N-1})v(x) + y(\beta(x)u(x) + \alpha(x^{N-1})v(x)) \\ &= -u(x)u(x^{N-1})h(x) + v(x^{N-1})v(x)h(x^{N-1}) \\ &\quad + y(v(x)u(x)h(x) - u(x)v(x)h(x^{N-1})) \\ &= h(x)(v(x)v(x^{N-1}) - u(x)u(x^{N-1})) \\ &\quad + y(v(x)u(x)h(x) - u(x)v(x)h(x)) \\ &= h(x)(v(x)v(x^{N-1}) - u(x)u(x^{N-1})) = 1. \end{aligned}$$

Conversely, suppose $w = u(x) + yv(x)$ is a unit in RD_N with inverse $a = \alpha(x) + y\beta(x)$. Then we have

$$u(x)\alpha(x) + v(x^{N-1})\beta(x) + y(v(x)\alpha(x) + u(x^{N-1})\beta(x)) = 1 + y0.$$

Comparing both sides gives

$$u(x)\alpha(x) + v(x^{N-1})\beta(x) = 1 \text{ and } v(x)\alpha(x) + u(x^{N-1})\beta(x) = 0.$$

Equivalently

$$\begin{pmatrix} u(x) & v(x^{N-1}) \\ v(x) & u(x^{N-1}) \end{pmatrix} \begin{pmatrix} \alpha(x) \\ \beta(x) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

The uniqueness of the inverse in a group ring guarantees that the matrix $\begin{pmatrix} u(x) & v(x^{N-1}) \\ v(x) & u(x^{N-1}) \end{pmatrix}$ is invertible. Therefore, $det \begin{pmatrix} u(x) & v(x^{N-1}) \\ v(x) & u(x^{N-1}) \end{pmatrix} = u(x)u(x^{N-1}) - v(x)v(x^{N-1})$ is unit in RC_N. Further,

$$\begin{aligned} \begin{pmatrix} \alpha(x) \\ \beta(x) \end{pmatrix} &= \begin{pmatrix} u(x) & v(x^{N-1}) \\ v(x) & u(x^{N-1}) \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \frac{1}{u(x)u(x^{N-1}) - v(x)v(x^{N-1})} \begin{pmatrix} u(x^{N-1}) & -v(x^{N-1}) \\ -v(x) & u(x) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \end{aligned}$$

This gives that $\alpha(x) = -h(x)u(x^{N-1})$ and $\beta(x) = h(x)v(x)$.

□

Corollary 3. *If $w = u(x)+yv(x)$ is a unit in RD_N then $w' = v(x)+yu(x)$ is also a unit in RD_N with inverse $a' = \alpha'(x)+y\beta'(x)$ where $\alpha' = v(x^{N-1})h(x)$, $\beta'(x) = -u(x)h(x)$ and $h(x)$ is the inverse of $v(x)v(x^{N-1}) - u(x)u(x^{N-1})$ in RC_N.*

Proof. Suppose $w = u(x) + yv(x)$ is a unit in RD_N then from Theorem 1, $v(x)v(x^{N-1}) - u(x)u(x^{N-1})$ is unit in RC_N. Let $\alpha'(x), \beta'(x)$ be as in statement of corollary. Consider

$$\begin{aligned} w'a' &= v(x)\alpha'(x) + u(x^{N-1})\beta'(x) + y(u(x)\alpha'(x) + v(x^{N-1})\beta'(x)) \\ &= v(x)v(x^{N-1})h(x) - u(x)u(x^{N-1})h(x) \\ &\quad + y(u(x)v(x^{N-1})h(x) - u(x)v(x^{N-1})h(x)) \\ &= h(x)(v(x)v(x^{N-1}) - u(x)u(x^{N-1})) = 1. \end{aligned}$$

And the other side $a'w' = 1$ can be proved similarly. □

Depending on the previous discussion, we provide Algorithm 2 to construct units in RD_N from units in RC_N.

Algorithm 2: Inversion in RD_N

Input: $w = u(x) + yv(x) \in RD_N$

Output: $w' = u'(x) + yv'(x) \in RD_N$ an inverse to w, or a failure

1 $mul_1 \leftarrow u(x)u(x^{N-1})$ `/* product in` RC_N `*/`
2 $mul_2 \leftarrow v(x)v(x^{N-1})$ `/* product in` RC_N `*/`
3 $c \leftarrow mul_2 - mul_1$ `/* Coefficient-wise subtraction in` R `*/`
4 $inv, found \leftarrow$ `find-inverse-in-`RC_N`(c)`
5 **if** *not found* **then**
6 **return** *failure*
7 $u'(x) \leftarrow -u(x^{N-1})inv$ `/* product in` RC_N `*/`
8 $v'(x) \leftarrow v(x)inv$ `/* product in` RC_N `*/`
9 **return** $u'(x) + yv'(x)$

Algorithm 2 relates the problem of finding the inverse of an element in RD_N into finding the inverse of an element in RC_N (Algorithm 2: line 4). In case $R = \mathbb{Z}_{q^r}$ for prime q and $r \geq 1$, one can use an efficient algorithm to find inverse for units in $\mathbb{Z}_{q^r}C_N$ as in [21], and therefore constructing units in $\mathbb{Z}_{q^r}D_N$ efficiently.

4. Experimental Results

In this section, we set our experiment to compare the efficiency of our algorithm (Algorithm 1) and the already existing approach to find inverses of elements in $\mathbb{Z}_{q^r}D_N$. We randomly generate invertible elements and check the

cost of finding the inverse using the conventional matrix-based method [20] versus our method. In the majority of NTRU-like schemes, units are sampled to be ternary, i.e., coefficients $\in \{0, 1, -1\}$, while some other schemes sample units as non-ternary elements to increase the entropy and make searching attacks on the key harder. Therefore, to notice the efficiency of the computations, we sample 100 random elements with different properties corresponding to different parameter sets as in Table 1. Table 1 and Figure 1 compare the average time to find the inverse of randomly sampled ternary, non-ternary elements in $\mathbb{Z}_{2^r}D_N$ for different values of N, r. The values of N, r are selected to sample elements similar to those used in cryptographic applications. The matrix approach involves building the matrix for group-ring elements in $\mathbb{Z}_{q^r}D_N$ and then finding the inverse of the corresponding matrix. For a particular value of N, the matrix representing an element in $\mathbb{Z}_{q^r}D_N$ has a dimension of $2N \times 2N$; therefore, finding the inverse of units involves inverting a matrix of size $2N \times 2N$. To calculate the inverse efficiently, we depend on the optimized implementation of SageMath [1] to invert matrices and compare the average running time for the matrix approach with our approach. Timed results have been executed on a system Linux (Ubuntu 22.04.2 LTS) with Intel(R) Xeon(R) CPU E3-1246 v3 @ 3.50GHz and 32 GB installed RAM. We can see from the results that finding the inverse according to the matrix approach is costly when N increases. For instance, inverting the matrices representing the non-ternary units for parameter sets $(N, r) = (677, 12), (821, 13)$ did not terminate in a reasonable time. Further, the average time to compute the inverse of a unit for $(N, r) = (509, 12)$ is 173.275 and 898.381 seconds for ternary, and random units, respectively. While using our approach takes, on average, just 1.395 and 14.511 seconds, respectively, for the same parameter set.

5. Conclusion

Although there are several characterizations of units in the group ring of dihedral group. However, we lack an efficient way to check and construct its units. In this paper, we provide a relation between units of the group ring of dihedral group and the group ring of the cyclic subgroup. This relation, together with existing work on finding units group ring of cyclic groups, proves

[1] https://www.sagemath.org/

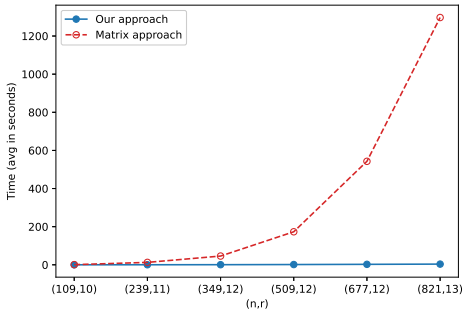
Table 1: Average time (seconds) to find inverse for units in $\mathbb{Z}_{2^r} D_N$

(a) Ternary units

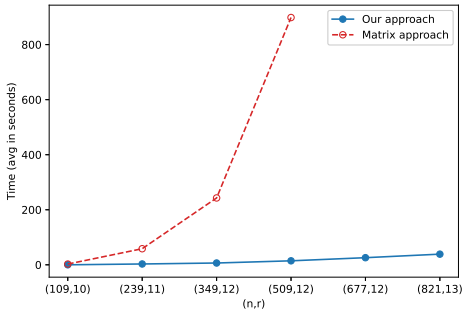
(N, r)	Matrix approach	Our approach
(109, 10)	0.8201	0.0618
(239,11)	12.730	0.287
(349,12)	45.909	0.631
(509,12)	173.275	1.395
(677,12)	542.823	2.480
(821,13)	1297.047	3.683

(b) Non-ternary units

(N, r)	Matrix approach	Our approach
(109, 10)	2.738	0.0628
(239,11)	58.457	3.0302
(349,12)	242.920	6.554
(509,12)	898.381	14.511
(677,12)	_	25.879
(821,13)	_	38.741



(a) Ternary units



(b) Non-ternary units

Figure 1: Average time (seconds) to find inverse for units in $\mathbb{Z}_{2^r} D_N$

of immense help for the efficient construction of units in the concerned group ring. Our method provides a huge benefit in time consumption for generating units and thus can be used in various cryptographic purposes.

Declaration of interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] C. Milies, S. Sehgal, An Introduction to Group Rings, 2002. doi:10.1007/978-94-010-0405-3.

[2] D. S. Passman, The algebraic structure of group rings, Wiley New York, 1977. URL: https://nla.gov.au/nla.cat-vn721538.

[3] T. Hurley, Group rings for communications, International Journal of Group Theory 4 (2015) 1–23. URL: https://ijgt.ui.ac.ir/article_5453_9f9342e7224465dd42f3537a6a7fe39a.pdf.

[4] B. Hurley, T. Hurley, Group ring cryptography, arXiv preprint arXiv:1104.1724 (2011). URL: https://doi.org/10.48550/arXiv.1104.1724.

[5] T. Hurley, Group ring cryptography: Cryptography, key exchange, public key, arXiv preprint arXiv:1305.4063 (2013). URL: https://doi.org/10.48550/arXiv.1305.4063.

[6] C. Carlet, Y. Tan, On group rings and some of their applications to combinatorics and symmetric cryptography, International Journal of Group Theory 4 (2015) 61–74. URL: https://ijgt.ui.ac.ir/article_5813_aae52578d139936ffc37b6d71a0be349.pdf.

[7] J. Hoffstein, J. Pipher, J. H. Silverman, NTRU: A ring-based public key cryptosystem, in: International algorithmic number theory symposium, Springer, Berlin, Heidelberg, 1998, pp. 267–288. doi:10.1007/BFb0054868.

[8] J. Kim, C. Lee, A polynomial time algorithm for breaking NTRU encryption with multiple keys, Designs, Codes and Cryptography 91 (2023) 2779–2789. URL: https://doi.org/10.1007/s10623-023-01233-5.

[9] D. Coppersmith, A. Shamir, Lattice Attacks on NTRU, in: Advances in Cryptology — EUROCRYPT '97, Springer Berlin Heidelberg, Berlin, Heidelberg, 1997, pp. 52–61. doi:10.1007/3-540-69053-0_5.

[10] J. Hoffstein, J. H. Silverman, A non-commutative version of the NTRU public key cryptosystem, unpublished paper, February (1997).

[11] A. Hassani Karbasi, S. Ebrahimi Atani, R. Ebrahimi Atani, Pairtru: Pairwise non-commutative extension of the NTRU public key cryptosystem, International Journal of Information Security Science 8 (2018) 1–10.

[12] K. Thakur, A variant of NTRU with split quaternions algebra, Palestine J. of Mathematics 6 (2017) 598–610. URL: https://pjm.ppu.edu/sites/default/files/papers/PJM_April_2017_28.pdf.

[13] E. Malekian, A. Zakerolhosseini, Otru: A non-associative and high speed public key cryptosystem, in: 2010 15th CSI International Symposium on Computer Architecture and Digital Systems, 2010, pp. 83–90. doi:10.1109/CADS.2010.5623536.

[14] E. Malekian, A. Zakerolhosseini, A. Mashatan, Qtru : a lattice attack resistant version of NTRU PKCS based on quaternion algebra, IACR Cryptology ePrint Archive 2009 (2009). URL: https://eprint.iacr.org/2009/386.

[15] K. Bagheri, M.-R. Sadeghi, D. Panario, A non-commutative cryptosystem based on quaternion algebras, Designs, Codes and Cryptography 86 (2018). doi:10.1007/s10623-017-0451-4.

[16] T. Yasuda, X. Dahan, K. Sakurai, Characterizing NTRU-variants using group ring and evaluating their lattice security, IACR Cryptol. ePrint Arch. (2015) 1170. URL: http://eprint.iacr.org/2015/1170.

[17] A. Raya, V. Kumar, S. Gangopadhyay, A. K. Gangopadhyay, Results on the key space of group-ring NTRU: The case of the dihedral group, in: Security, Privacy, and Applied Cryptography Engineering, Springer Nature Switzerland, Cham, 2024, pp. 1–19. doi:10.1007/978-3-031-51583-5_1.

[18] T. Miyata, On the units of the integral group ring of a dihedral group, Journal of the Mathematical Society Japan 32 (1980). URL: https://www.jstage.jst.go.jp/article/jmath1948/32/4/32_4_703/_article.

[19] N. Makhijani, R. Sharma, J. Srivastava, Units in finite dihedral and quaternion group algebras, Journal of the Egyptian Mathematical Society 24 (2016) 5–7. doi:https://doi.org/10.1016/j.joems.2014.08.001.

[20] T. Hurley, Group rings and rings of matrices, International Journal of Pure and Applied Mathematics 31 (2006) 319–335. URL: https://www.researchgate.net/publication/228928727_Group_rings_and_rings_of_matrices.

[21] J. H. , Silverman, Almost inverses and fast NTRU key creation, NTRU Cryptosystems Technical Report #14 (1999). URL: https://ntru.org/f/tr/tr014v1.pdf.