An Efficient Noncommutative NTRU from Semidirect Product

__Vikas Kumar__[1], Ali Raya[2], Aditi Kar Gangopadhyay[1], Sugata Gangopadhyay[2], and Md. Tarique Hussain[3]

[1]Department of Mathematics, IIT Roorkee

[2]Department of Computer Science and Engineering, IIT Roorkee

[3]Department of Information Technology, IIEST Shibpur

Table of contents

Table of contents

Introduction

- With the possibility of the development of large-scale quantum computers in the near future, there comes a threat to the security of cryptographic schemes based on hard mathematical problems that can not resist quantum attacks.

- The goal of Post Quantum Cryptography (PQC) is to design cryptographic systems that are secure against both classical as well as quantum attacks.

- The National Institute of Standards and Technology (NIST), US, started a competition in 2016 with a motive to update their standards to include post-quantum cryptography.

Introduction

- All the submissions to the NIST PQC competition belong to one of the families:
  - Lattice-based cryptography
  - Code-based cryptography
  - Isogeny-based cryptography
  - Hash-based cryptography
  - Multivariate cryptography

Introduction

NTRU

- NTRU is a post-quantum lattice-based cryptosystem that made its way to the third round of the NIST competition.
- The first version of NTRU[HPS96] as introduced in Crypto 1996.
- NTRU is now recognized as a hard problem in cryptography rather than a unique cryptosystem that can be extended to different algebraic structures.

[HPS96] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: International Algorithmic Number Theory Symposium, Berlin, Heidelberg, pp. 267–288 (1996).

Introduction

NTRU Problem

Definition: Let N be a prime, q be a positive integer, and $f, g \in \frac{\mathbb{Z}[x]}{\langle x^N - 1 \rangle}$ be two polynomials with small coefficients (mostly ternary) such that f is invertible modulo q.

Private key. The pair (f, g) forms the secret key.

Public Key. The element $h = f^{-1} * g (mod\ q) \in \frac{\mathbb{Z}_q[x]}{\langle x^N - 1 \rangle}$ is the public key.

NTRU Problem. Given the public parameters and the public key h, the NTRU problem asks to find the private key or its rotations $(x^i * f, x^i * g)$ for $i \in \{0, 1, \dots, N-1\}$.

Introduction

Context

- The design flexibility in NTRU has resulted in many variants of NTRU in literature.
- Some of them are introduced with a motivation to improve the performance and others to strengthen the cryptosystem against possible attacks.
- Although the majority of practical NTRU-like cryptosystems are built over commutative algebras, the use of noncommutative algebraic structure has been endorsed as a promising direction to generalize NTRU in order to avoid certain attacks.

Introduction

Context

Why noncommutativity?

- When Coppersmith and Shamir[CS97] introduced their lattice attack on NTRU, they suggested that noncommutative structures may avoid their attacks and some other attacks that might take benefit of the underlying commutative algebra.

[CS97] Coppersmith, D., Shamir, A.: Lattice Attacks on NTRU. In: Advances in Cryptology — EUROCRYPT ’97. pp. 52–61. Springer Berlin Heidelberg, Berlin, Heidelberg (1997).

Introduction

Context

Why noncommutativity?

NTRU-learning problem: Given NTRU public keys $h_i = f^{-1} * g_i \ (mod\ q)$, for a fixed f and a number of independently sampled g_i, find f.

- This problem was believed to be as hard as NTRU problem until recently, Kim and Lee[KL23] demonstrated that leveraging the commutativity of the underlying ring of polynomials, one can formulate a system of equations that can reveal the private key.

[KL23] Kim, J., Lee, C.: A polynomial time algorithm for breaking NTRU encryption with multiple keys. Designs, Codes and Cryptography 91, 2779–2789 (2023).

Introduction

Context

Noncommutative NTRU-like designs

- There are many noncommutative NTRU-like cryptosystems in literature. But most of them are impractical and have issues related to security due to lack of analysis.

- BQTRU[BSP18] was claimed to be the fastest noncommutative variant of NTRU. However, we[RKGG24] broke BQTRU and hence it no longer is practically secure to be used.

[BSP18] Bagheri, K., Sadeghi, M.R., Panario, D.: A non-commutative cryptosystem based on quaternion algebras. Designs, Codes and Cryptography 86, 2345–2377 (2018).
[RKGG24] Raya A, Kumar V, Gangopadhyay AK, Gangopadhyay S. Giant Does NOT Mean Strong: Cryptanalysis of BQTRU. Cryptology ePrint Archive,Paper 2024/1853; (2024).

Introduction

Context

Noncommutative NTRU-like designs

- DiTRU[RKG24] built over the dihedral group ring is the only practical noncommutative alternative of NTRU.

- However, DiTRU is susceptible to dimension reduction attacks that reduces the dimension of lattices to be attacked by a factor of 2. Consequently, DiTRU is two times slower that NTRU for equivalent security levels.

[RKG24] Raya, A., Kumar, V., Gangopadhyay, S.: DiTRU: A Resurrection of NTRU over Dihedral Group. In: Vaudenay, S., Petit, C. (eds.) Progress in Cryptology - AFRICACRYPT 2024. pp. 349–375. Springer Nature Switzerland, Cham (2024).

Introduction

Our contribution

- The absence of a practical efficient and secure noncommutative version of NTRU motivated us for this work.

- We designed a noncommutative variant of NTRU in the GR-NTRU framework emphasizing on the following practical and security aspects:

  - Inversion algorithm
  - Analysis of lattice and other attacks
  - Concrete parameter selection
  - Reference implementation

Table of contents

- Introduction
- Group Ring
- GR-NTRU and lattice attacks
- Our design

Group Ring

Definition: Let $G = \{g_i : i = 1,2,\dots,N\}$ be a finite group and R be a ring. The set of formal sums

$$RG = \{\sum_{i=1}^{n} \alpha_i g_i : \alpha_i \in R\}$$

with the component-wise addition and convolution multiplication defines the group ring of G over R.

Definition: Each group ring element $a = \sum_{i=1}^{n} \alpha_i g_i \in RG$ can be associated to its unique coefficient vector $(\alpha_1, \alpha_2, \dots, \alpha_n) \in R^n$.

Group Ring

Definition: The RG-matrix[Hur06] of an element $a = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in RG$ is defined as:

$$M_{RG}(a) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \ldots & \alpha_{g_n^{-1}g_n} \end{pmatrix}.$$

Note: The RG**-**matrix of an element belonging to the cyclic group ring is a circulant matrix.

[Hur06] T. Hurley, Group rings and rings of matrices, International Journal of Pure and Applied Mathematics 31 (2006) 319–335.

Group Ring

Remark: The standard NTRU operates over the truncated ring of polynomials $\frac{\mathbb{Z}[x]}{\langle x^N - 1\rangle}$. If we let $C_N = \langle x : x^N = 1\rangle$ to be the cyclic group of order N, then $\frac{\mathbb{Z}[x]}{\langle x^N - 1\rangle}$ can be viewed as a group ring of C_N over $\mathbb{Z}$, i.e.,

$$\frac{\mathbb{Z}[x]}{\langle x^N - 1\rangle} \approx \mathbb{Z}C_N.$$

In other words, NTRU can be realized as a cryptosystem built over the group ring of cyclic group.

Table of contents

GR-NTRU and lattice attacks

Definition: The GR-NTRU/Group Ring NTRU generalizes NTRU by replacing the cyclic group ring $\mathbb{Z}\boldsymbol{C_N}$ in NTRU with any group ring $\mathbb{Z}\boldsymbol{G}$ of a finite group $\boldsymbol{G}$ and keeping all other procedures the same with a little modification depending on the requirements.

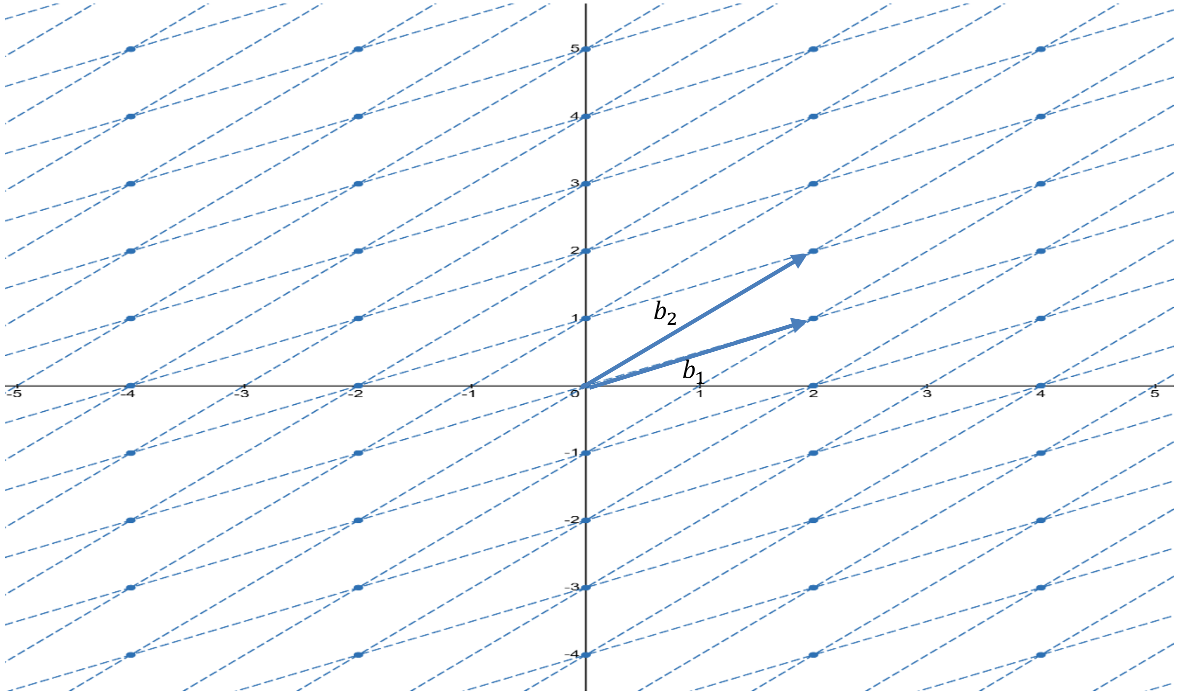
Note: In fact, the ring R can be chosen to be a Euclidean domain as taken in few NTRU-like designs, for example ETRU[JN15].

[JN15] Jarvis, K., Nevins, M.: ETRU: NTRU over the Eisenstein integers. Des. Codes Cryptogr. 74, 219–242 (2015).

GR-NTRU and lattice attacks

Lattices and hard problem

Definition: For $m \leq n$, let $B = [b_1, b_2, \ldots, b_m] \in \mathbb{R}^{m \times n}$ be a matrix whose rows $b_i \in \mathbb{R}^n$ are linearly independent vectors. Then, the lattice defined by the basis B is defined as



$$L_B = \{xB = \sum_{i=1}^{m} x_i b_i : x = (x_1, x_2, \ldots, x_m) \in \mathbb{Z}^m\}.$$

GR-NTRU and lattice attacks

Lattices and hard problem

Definition: A vector $v \in L_B - \{0\}$ is called the shortest nonzero vector if

$$\|v\| = \min_{w \in L_B - \{0\}} \|w\|.$$

The problem of finding such a vector v in a lattice is called the Shortest Vector Problem (SVP).

GR-NTRU and lattice attacks

- The coefficient vector of the private key (f, g) or its rotations is one of the shortest vector of the lattice L_h generated by the basis matrix

$$M_h = \begin{pmatrix} I_N & M_{RG}(h) \\ 0_N & qI_N \end{pmatrix}$$

$|G| \times |G|$ RG-matrix of the public key h.

with high probability.

- Therefore, attacking the private key is equivalent to solving SVP in a $2|G|$-dimensional lattice.

Table of contents

Our design

- We have designed our variant over the group ring

$$RG = \mathbb{Z}[\omega](C_N \rtimes C_3) \text{ where}$$

Definition: Let ω be the primitive cube root of unity, i.e., $\omega^3 = 1$ and $\omega \neq 1$. The ring

$$\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$$

is called the ring of Eisenstein integers.

Definition: Let N and t be positive integers such that $3|N - 1, t^3 = 1\ (mod\ N), t \neq 1\ (mod\ N)$.

$$C_N \rtimes C_3 = \langle x, y : x^N = y^3 = 1, xy = yx^t \rangle$$

is the semidirect product (noncommutative) of cyclic groups C_N and C_3 of order N and 3, respectively.

Our design

Ring of Eisenstein integers

- Fast multiplication: $(a + b\omega) * (c + d\omega) = ac - bd + \big(ac + (a - b)(d - c)\big)\omega$ needs 3 integer multiplications. Therefore,

$-$ $f * g$ needs $3n^2$ multiplication for $f, g \in \mathbb{Z}[\omega]^n$.
$-$ $f * g$ needs $4n^2$ multiplication for $f, g \in \mathbb{Z}^{2n}$.

➡ gain in efficiency by 4/3.

Our design

Group ring $R(C_N \rtimes C_3)$

- $R(C_N \rtimes C_3) = \{\alpha(x) + y\beta(x) + y^2\gamma(x) : \alpha, \beta, \gamma \in RC_N\}$.

- Matrix representation: The RG-matrix of an element $z \in R(C_N \rtimes C_3)$ has the form

$$M_{RG}(z) = \begin{pmatrix} M_0 & M_1 & M_2 \\ M_2 & M_0 & M_1 \\ M_1 & M_2 & M_0 \end{pmatrix} \in R^{3N \times 3N}.$$

special 3×3 block Circulant structure.

Our design

Group ring $\boldsymbol{R(C_N \rtimes C_3)}$

- Units: An element $z = u(x) + yv(x) + y^2w(x)$ is invertible in $R(C_N \rtimes C_3)$ iff

$$\det(u, v, w) = \det\begin{pmatrix} u(x) & w(x^t) & v(x^{t^2}) \\ v(x) & u(x^t) & w(x^{t^2}) \\ w(x) & v(x^t) & u(x^{t^2}) \end{pmatrix}$$

is a unit in RC_N.

Note: There already exist algorithms to check and find inverses in the group RC_N for $R = \mathbb{Z}_q$ where q is a prime or prime power.

Our design

More details

- N: primes number.
  $p, q \in \mathbb{Z}[\omega]$: prime elements in $\mathbb{Z}[\omega]$.
  $|p| \ll |q|$, $p = 2$ is fixed for our design.

- Private key $f, g \in \mathbb{Z}[\omega](C_N \rtimes C_3)$ are elements with 2/3rd coefficients from the set $\{0, \pm 1, \pm\omega, \pm\omega^2\}$ such that f is invertible modulo q.

- The message space consists of elements from $\mathbb{Z}[\omega](C_N \rtimes C_3)$ with coefficients from the set $\{0, \pm 1, \pm\omega, \pm\omega^2\}$.

- The encryption and decryption are exactly same as NTRU with the modification that operations are now performed over the ring $\mathbb{Z}[\omega](C_N \rtimes C_3)$.

Note: The process is entirely free from decryption failure if $|q| > 8N|p| + 2$.

Our design

Key generation

- The key generation involves inverting the elements in the group ring $\mathbb{Z}[\omega](C_N \rtimes C_3)$.

- Modifying the inversion algorithms for $\mathbb{Z}_q C_N$, we proposed an efficient constant time inversion algorithm for $\frac{\mathbb{Z}[\omega]}{\langle q \rangle} C_N$. That can be used to calculate inverses in $\mathbb{Z}[\omega](C_N \rtimes C_3)$.

Input: $z = u(x) + yv(x) + y^2 w(x) \in R_q^\omega$

Output: $z^{-1} = \alpha(x) + y\beta(x) + y^2\gamma(x) \in R_q^\omega$ as inverse of f, or a failure

$d(x) \leftarrow det(u, v, w)$

$inv(x), found \leftarrow$ `find-inverse-of-d(x)-in-`$\frac{\mathbb{Z}[\omega]}{<q>} C_N$

if *not found* **then** **return** *failure*

$\alpha(x) \leftarrow inv(x) * (u(x^t)u(x^{t^2}) - v(x^t)w(x^{t^2}))$ `/* product in` $\frac{\mathbb{Z}[\omega]}{<q>} C_N$ `*/`

$\beta(x) \leftarrow inv(x) * (w(x)w(x^{t^2}) - v(x)u(x^{t^2}))$ `/* product in` $\frac{\mathbb{Z}[\omega]}{<q>} C_N$ `*/`

$\gamma(x) \leftarrow inv(x) * (v(x)v(x^t) - w(x)u(x^t))$ `/* product in` $\frac{\mathbb{Z}[\omega]}{<q>} C_N$ `*/`

return $z^{-1} = \alpha(x) + y\beta(x) + y^2\gamma(x)$

Algorithm to find inverse in $\mathbb{Z}[\omega](C_N \rtimes C_3)$

Inversion in $\frac{\mathbb{Z}[\omega]}{\langle q \rangle} C_N$ needs to perform division in $\mathbb{Z}[\omega]$ by q. We have proposed an efficient division method for the same.

Input: $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, and an element $q = q + 0\omega \in \mathbb{Z}[\omega]$.

Output: $\beta \in \mathbb{Z}[\omega]$ such that $\alpha = rq + \beta$ where $r \in \mathbb{Z}[\omega]$ is nearest to $q^{-1}\alpha$.

$x = a \pmod q,\ y = b \pmod q,\ X = 2x,\ Y = 2y$

if $x + y > q,\ X > y,\ Y \geq x$ **then** **return** $\beta = (x - q) + (y - q)\omega$

if $X - y > q,\ Y < x$ **then** **return** $\beta = (x - q) + y\omega$

if $Y - x \geq q,\ X \leq y$ **then** **return** $\beta = x + (y - q)\omega$

else **return** $\beta = x + y\omega$

Division in $\mathbb{Z}[\omega]$

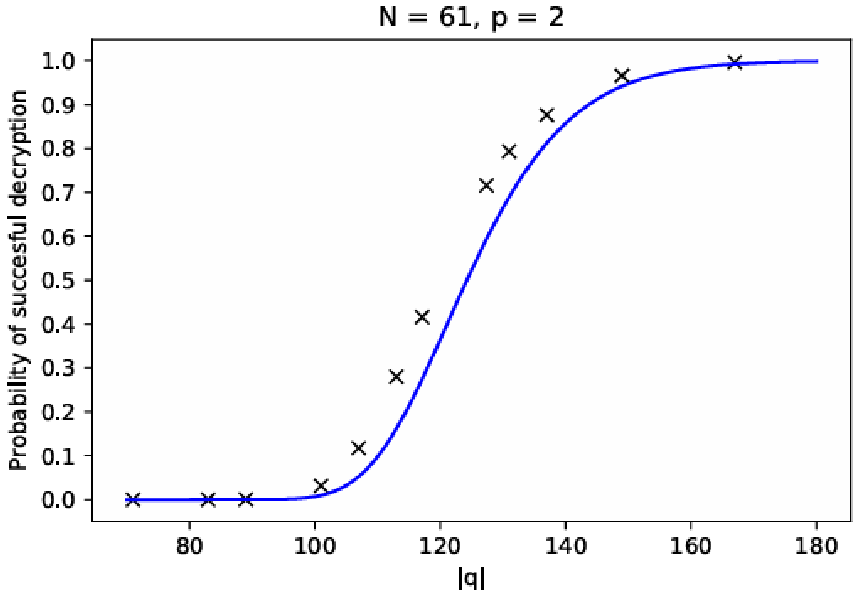
Our design

Probability of successful decryption

- Allowing negligible decryption failure can help reduce the key sizes.

- We model the probability of successful decryption as

$$P(N,q) = \left(1 - \exp\left(-\frac{|q|^2}{8\sigma^2}\right)\right)^{3N} \text{ where } \sigma^2 = \frac{17N}{3} + \frac{3}{8}.$$



The probability of successful decryption as a function of $|q|$ for $N = 61$, $p = 2$. The curve represents $P(N,q)$, and the crosses represent the ratio of the successful decryption out of 10,000 randomly generated messages for each prime q.

Our design

Security analysis

- Combinatorial search: Secure against combinatorial search attack that cost approximately $\sqrt{\frac{1}{3N}\binom{6N}{3N}6^{2N}}$ operations.

- Overstreched NTRU attack: These attacks exploits the special algebraic structures present in NTRU-like lattices with a very large modulus q referred to as overstretched.

Note: Ducas and Woerdon[DW21] estimated that *fatigue point* (that separates the over stretched regime from the standard regime) for an NTRU lattice of dimension $2n$ with modulus q, the fatigue point is $q \approx 0.004 \cdot n^{2.484}$.

The parameter selected for our design satisfy $|q| \ll 0.004 \cdot n^{2.484}$.

[DW21] Ducas, L., van Woerden, W.: NTRU Fatigue: How Stretched is Overstretched? In: Advances in Cryptology– ASIACRYPT 2021. pp. 3–32. Springer International Publishing (2021)

Our design

Security analysis

- Lattice attacks: Recovering the private key is equivalent to solving SVP in a $12N$-dimensional lattice L_H generated by the basis matrix

$$M_H = \begin{pmatrix} I_{6N} & \boxed{\mathbf{H}} \\ 0_{6N} & qI_N \end{pmatrix} \xrightarrow[\text{Circulant matrix}]{3 \times 3 \text{ block}} \begin{pmatrix} \mathbf{H}_0 & \mathbf{H}_1 & \mathbf{H}_2 \\ \mathbf{H}_2 & \mathbf{H}_0 & \mathbf{H}_1 \\ \mathbf{H}_1 & \mathbf{H}_2 & \mathbf{H}_0 \end{pmatrix}$$

For the public key h, the $\mathbb{Z}[\omega](C_N \rtimes C_3)$-matrix is a $3N \times 3N$ matrix H with entries from $\mathbb{Z}[\omega]$. For converting it to an integral matrix $\mathbf{H} \in \mathbb{Z}^{6N\times 6N}$ in a such a way that the public key equation $f * h = g\ (mod\ q)$ is preserved, we used that fact that every element $a + b\omega$ can be mapped to its unique vector $(a, b) \in \mathbb{Z}^2$ and 2×2 integer matrix $\begin{pmatrix} a & b \\ -b & a-b \end{pmatrix}$ such that $(a + b\omega) * (c + d\omega)$ can be identified by $(a, b) * \begin{pmatrix} c & d \\ -d & c-d \end{pmatrix}$.

Our design

Security analysis

- Lattice attacks:

Similarly to DiTRU, the special structure of the basis matrix allows lattice dimension reduction attack.

We have shown that it is possible (although with rare probability) to decipher the private key by searching for its images in three $8N$-dimensional lattices.

Note: Theoretically lattice security of our construction is equivalent to standard NTRU over $\mathbb{Z}C_{N'}$ where $N' \approx 4N$. For $N' \approx 4N$, our scheme is only 1.125 times slower than NTRU for equivalent lattice dimensions

Our design

Security analysis

- Lattice attacks:

  Benefits over DiTRU

  – DiTRU over dihedral group ring suffers a dimension loss by a factor of 2. But in our case, the dimension is reduced only factor of 1.5

  – This provides a speed up over DiTRU by a factor of 1.7 . The ring of Eisenstein integers further improves the performance.

  – Further, our scheme is more compact to DiTRU with less memory requirements.

Our design

Parameters and performance

	No decryption failure			Neglible decryption failure		
Security level	I	III	V	I	III	V
(N, q, p)	(127, 2039, 2)	(181, 2903, 2)	(241, 3863, 2)	(109, 701, 2)	(157, 1013, 2)	(211, 1361, 2)
sk (bytes)	153	218	290	131	189	254
pk (bytes)	1143	1629	2350	818	1296	1741
β	461	664	890	464	663	886
BKZ(S) [classical]	134	193	259	135	193	258
BKZ(S) [quantum]	122	175	235	122	175	234
Comb	505	719	957	433	624	838
Dec failure	–	–	–	2^{-135}	2^{-199}	2^{-269}
CPU cycles $\times 10^3$						
KeyGen	38 163	72 545	131 162	27 498	58 308	103 094
Enc	6 692	11 442	20 452	4 907	9 878	16 313
Dec	12 125	21 308	38 147	8 712	18 109	30 619

β is the blocksize needed by the algorithm BKZ to find the shortest vector in the underlying lattices estimated using 2016-estimation.

Parameters for $\mathbb{Z}[\omega](CN \rtimes C3)$ –NTRU with no decryption failure and negligible decryption failure

Our design

Comparison with NTRU and DiTRU

	NTRU HPS $(N, q, p = 3)$			This work $(N, q, p = 2)$			Ratio
	$(587, 2048)$	$(863, 2048)$	$(1109, 4096)$	$(109, 701)$	$(157, 1013)$	$(211, 1361)$	(r_1, r_2, r_3)
Gen:	62 311	146 706	224 363	27 498	58 308	103 094	$(2.27, 2.52, 2.18)$
Enc:	3 132 799	9 105 932	19 790 178	2 772 310	7 569 493	16 294 397	$(1.13, 1.20, 1.21)$
Dec:	5 800 643	17 201 618	37 829 256	4 988 320	13 965 567	30 569 442	$(1.16, 1.23, 1.24)$
	DiTRU $(N, q, p = 3)$						
	$(541, 2048)$	$(797, 4096)$	$(1039, 4096)$	$(109, 701)$	$(157, 1013)$	$(211, 1361)$	(r_1, r_2, r_3)
Gen:	84 756	189 770	308 543	27 498	58 308	103 094	$(3.08, 3.05, 2.99)$
Enc:	9 777 811	29 658 528	66 558 364	5 092 057	14 373 555	30 551 756	$(1.92, 2.06, 2.19)$
Dec:	18 682 243	57 329 287	129 664 570	9 180 125	26 540 407	57 287 299	$(2.04, 2.16, 2.26)$

Performance benchmark (CPUcycles$\times 10^3$) of this work vs. NTRU and DiTRU for Key generation, Encryption, and Decryption
For messages of equal lengths.

For $N' \approx 4N$, our design is 1.125 times slower than NTRU for equal security levels. However, for the selected parameters $N < N'/4$. Consequently, we can see that our design shows an improvement in performance over NTRU.

Our design

Comparison with NTRU and DiTRU

	NTRU HPS		DiTRU		Our design	
Level	sk	pk	sk	pk	sk	pk
I	118	808	217	1488	131	818
III	173	1187	319	2391	189	1296
V	221	1664	416	3116	254	1741

Memory requirements of the considered NTRU variants.

This demonstrates the memory benefits of the proposed scheme as the size of the private (**sk**) and public key (**pk**) (in bytes) of parameters allowing negligible decryption failure for our design are less than DiTRU, while are approximately equal to NTRU HPS.

References

[HPS96] Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: International Algorithmic Number Theory Symposium, Berlin, Heidelberg, pp. 267–288 (1996).

[Gen01] C. Gentry, Key Recovery and Message Attacks on NTRU-Composite, in: B. Pfitzmann (Ed.), Advances in Cryptology — EUROCRYPT 2001, Springer Berlin Heidelberg, Berlin, Heidelberg, 2001, pp. 182–194.

[RKG24] A. Raya, V. Kumar, S. Gangopadhyay, DiTRU: A resurrection of NTRU over dihedral group, in: S. Vaudenay, C. Petit (Eds.), Progress in Cryptology - AFRICACRYPT 2024, Springer Nature Switzerland, 2024,pp. 349–375.

[YDS15] T. Yasuda, X. Dahan, K. Sakurai, Characterizing NTRU-variants using group ring and evaluating their lattice security, IACR Cryptol. ePrint Arch. (2015).

[Hur06] T. Hurley, Group rings and rings of matrices, International Journal of Pure and Applied Mathematics 31 (2006) 319–335.

[JN15] Jarvis, K., Nevins, M.: ETRU: NTRU over the Eisenstein integers. Des. Codes Cryptogr. 74, 219–242 (2015).

[KRGG23] V. Kumar, A. Raya, S. Gangopadhyay, A. K. Gangopadhyay, Lattice attack on group ring NTRU: The case of the dihedral group, https://doi.org/10.48550/arXiv.2309.08304 (2023).

[KL23] Kim, J., Lee, C.: A polynomial time algorithm for breaking NTRU encryption with multiple keys. Designs, Codes and Cryptography 91, 2779–2789 (2023).

[BSP18] Bagheri, K., Sadeghi, M.R., Panario, D.: A non-commutative cryptosystem based on quaternion algebras. Designs, Codes and Cryptography 86, 2345–2377 (2018).

[RKGG] Raya A, Kumar V, Gangopadhyay AK, Gangopadhyay S. Giant Does NOT Mean Strong: Cryptanalysis of BQTRU. Cryptology ePrint Archive,Paper 2024/1853; (2024).

[CS97] Coppersmith, D., Shamir, A.: Lattice Attacks on NTRU. In: Advances in Cryptology — EUROCRYPT ’97. pp. 52–61. Springer Berlin Heidelberg, Berlin, Heidelberg (1997).

Questions?