CoNAN: A Structure-Aware Framework for Lattice Cryptanalysis

Ali Raya[1], Vikas Kumar[2], Kushal Dey[1], and Sugata Gangopadhyay[1]

[1] Department of Computer Science and Engineering
Indian Institute of Technology Roorkee, 247667, Uttarakhand, India
{ali_r, kushal_d, sugata.gangopadhyay}@cs.iitr.ac.in
[2] Department of Computer Science
University of Calgary, Canada
vikas.kumar1@ucalgary.ca

Abstract. The security of structured lattice-based schemes is typically evaluated through the estimated cost of the best known lattice attacks, which in turn guides practical parameter selection.
However, existing lattice security estimators typically evaluate different algebraic structures in a largely uniform manner, without fully accounting for the additional structure introduced by the underlying algebra. In this work, we show that such structure can, in certain instances, be exploited through algebra-induced homomorphisms to derive lower-dimensional lattice representations, thereby enabling more efficient attacks and yielding more realistic—and in some cases significantly lower—security estimates.
To this end, we introduce CoNAN, a framework for incorporating algebraic structure into the security estimation of lattice-based constructions. We develop our main analysis in the context of NTRU-like constructions and further show that the framework naturally extends to several structured LWE-based schemes. Our framework reproduces known algebraic attacks against lattice-based constructions such as NTRU Composite (EUROCRYPT 2001), BQTRU (PQCrypto 2024), and multivariate LWE (ANTS 2020). Furthermore, it highlights specific schemes, such as LWE over noncommutative group rings and semidirect products (DCC 2022, DCC 2026), where the underlying algebraic structure degrades concrete security by at least 60 bits relative to standard lattice estimator predictions. Beyond cryptanalysis, our work provides practical guidance for the secure design of future lattice-based schemes, particularly those instantiated over structured or noncommutative algebras.

Keywords: Lattice-estimator · NTRU · LWE · Noncommutative.

1 Introduction

Post-quantum cryptography (PQC) has emerged to describe cryptographic schemes built on mathematical problems believed to be resistant against both classical and quantum adversaries. Several standardization bodies have initiated the

study and analysis of various mathematical problems that can serve as potential candidates for constructing such quantum-safe schemes. Lattice-based schemes account for the majority of submissions, with the largest number of algorithms selected for standardization belonging to this category [48,17,9,14,30]. Furthermore, several recent proposals for lattice-based cryptographic constructions [10,36,35,21] built over noncommutative algebras have been introduced with the aim of mitigating *potential* attacks arising from polynomial-time quantum algorithms for solving the SVP/SIVP problems in certain classes of ideal lattices.

In lattice-based cryptography, parameter selection is guided by the best currently known attacks. Consequently, the concrete security level achieved by a scheme depends critically on the depth and rigor of the underlying security analysis.

Lattice estimators. To support concrete security estimation for lattice-based constructions, several lattice estimators have been developed to evaluate the hardness of lattice reduction under different cost models and across a variety of effective lattice-based attacks. The *Lattice Estimator* [2] by Albrecht et al. is one of the most widely used tools for assessing the hardness of the LWE problem under multiple attack models, assuming that the adversary has access to an optimal number of LWE samples. This estimator was later extended by Bindel et al. [7] to provide more accurate security estimates in scenarios where only a limited number of LWE samples are available. Other estimators address more specialized settings. For example, the *leaky-LWE estimator* [12] incorporates security analysis in the presence of side information or hints about the secret key and/or the noise of LWE instances. Similarly, estimators tailored to NTRU—such as the *fatigue-estimator* [15]—focus on analyzing the hardness of NTRU lattices and the behaviour of lattice reduction algorithms, particularly in regimes where the modulus q in the public-key equation is relatively large. Recent works on Module-BKZ [13,44] have investigated the potential gain or loss in the effective blocksize when applying Module-BKZ lattice reduction to constructions defined over certain number fields.

Nevertheless, most existing security estimators do not explicitly examine the internal algebraic structure of the underlying algebra. Such a structure may substantially simplify lattice attacks by enabling homomorphic reductions to lower-dimensional instances, where lattice reduction algorithms become significantly more efficient.

Weak instantiations. Different instantiations of lattice-based constructions over algebraic rings have been introduced, leading to weaker instances and, hence, reduced security estimates arising from the underlying lattice structure. The resulting security losses are non-trivial and cannot be directly captured by current lattice estimators.

– **Attack against Composite NTRU [20]:** The original attack by Gentry against Composite NTRU focused on a homomorphism of the form

$\theta : \mathbb{Z}[x]/(x^N - 1) \longrightarrow \mathbb{Z}[x]/(x^d - 1)$, which sends short polynomials (in Euclidean norm) to short polynomials, in general, for $\sqrt{N} < d < N$. Therefore, lattice attacks can transform the problem of solving the Shortest Vector Problem from lattices of dimension $n = 2N$ to lattices of dimension $2d$, thereby rendering the lattice problems much easier for lattice reduction algorithms.

– **Attack against BQTRU [4]:** The attack against the BQTRU cryptosystem extends the folding techniques introduced by Gentry to the noncommutative ring of the quaternion algebra over the bivariate polynomial ring. The attack exploits the fact that any element from the underlying ring of BQTRU has a corresponding matrix representation that can be homomorphically mapped to a matrix of half the dimension as

$$\begin{pmatrix} \mathbf{S}_0 & \mathbf{S}_1 & \mathbf{S}_2 & \mathbf{S}_3 \\ \mathbf{S}_1 & \mathbf{S}_0 & \mathbf{S}_3 & \mathbf{S}_2 \\ \mathbf{S}_2 & -\mathbf{S}_3 & \mathbf{S}_0 & -\mathbf{S}_1 \\ -\mathbf{S}_3 & \mathbf{S}_2 & -\mathbf{S}_1 & \mathbf{S}_0 \end{pmatrix} \longrightarrow \begin{pmatrix} \mathbf{S}_0 + \mathbf{S}_1 & \mathbf{S}_2 + \mathbf{S}_3 \\ \mathbf{S}_2 - \mathbf{S}_3 & \mathbf{S}_0 - \mathbf{S}_1 \end{pmatrix}. \tag{1}$$

As a result, lattice reduction attacks can be mapped to lattices of half the dimension of the original lattice. The proposed attack shows that the new lattice estimate reduces the security by at least 55 and 130 bits for the moderate and highest parameter sets, respectively.

– **Attack against multivariate LWE [8]:** The attack was introduced against multivariate LWE, which has been proposed in a series of works [41,42,43] in order to construct a structured Module LWE (an analog of RLWE compared to LWE). For the two-variable case, the problem is defined over the ring $Z_q[x, y]/(f(x), g(y))$. The attack of [8] shows that retrieving the secret/error of multivariate LWE is equivalent to solving Ring LWE in a dimension corresponding to the maximum degree of the multivariate ring rather than the product dimension. For some parameter sets, the introduced attack can solve instances that were estimated to achieve 2 500 bits of security, even with only BKZ with blocksize 10, highlighting a severe overestimation of security.

The existence of different attempts over structured rings that were found vulnerable to homomorphically dimension-reduction attacks, which would not be directly caught while estimating the security, however, result in attacks that immensely reduce the claimed security levels, motivated us to ask the following questions:

Is it possible to introduce an automated framework that can account for the algebraic structure while estimating the security of lattice-based constructions?
Can this framework understand the structure of the underlying algebraic ring and search for more effective attacks, especially while operating over noncommutative rings where the process of decomposing the algebra seems a little more non-trivial?

1.1 Contributions

In this work, we introduce **CoNAN**, an automated framework for constructing and analyzing lattice-based constructions that accounts for the underlying lattice structure induced by the algebraic ring. In particular, the framework (see Figure 1) estimates security by considering possible homomorphic dimension reductions that may lead to more effective attacks when deriving concrete security estimates.

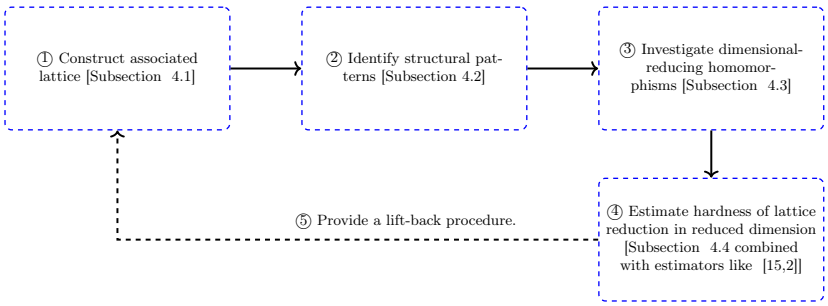


Fig. 1. General architecture of CoNAN for identifying homomorphic dimension reductions in structured lattice-based constructions.

We provide our main analysis in the context of NTRU-like constructions and then show its natural extension to some structured LWE schemes. In particular, we consider cryptographic schemes that can be represented as associative R-algebras, which is the case for the majority of related lattice-based constructions.

Our contributions are summarized as follows:

- **Unified representation.** We provide a general mathematical framework that serves as a unifying umbrella for different NTRU variants. We begin by revisiting the representations of Group-ring NTRU and twisted group-ring NTRU, and demonstrate that most existing NTRU proposals can be expressed within this formulation. We then extend the framework to generalized NTRU (Gen-NTRU), providing a more general representation that captures NTRU variants defined over a wider class of rings and associative algebras. The proposed representation extends naturally to the context of structured LWE constructions.
- **Automated structural analysis.** Unlike conventional lattice estimators, our framework integrates structural information directly into the security evaluation. Given a specification of the multiplication rules of the underlying algebraic structure, CoNAN automatically constructs the corresponding lattice, detects structural patterns, and derives potential dimension-reduction homomorphisms. It further evaluates whether these homomorphisms can translate into more efficient attacks and adjusts the security estimation accordingly. Our framework enables the analysis of structural properties of

algebras beyond commutative univariate ring settings, extending naturally to multivariate and noncommutative algebras. This facilitates cryptanalysis, particularly for constructions where CRT-style decompositions are not straightforward. In this regard, we highlight that CoNAN can detect a broad range of useful homomorphisms that enable more effective attacks. Any homomorphism found by CoNAN is guaranteed to exist. However, the inability of our framework to find suitable homomorphisms does not imply that the studied structure is resistant to all possible related lines of attack.

– **Proof-of-concept implementation.** We provide a proof-of-concept implementation to validate the framework. We test CoNAN against various constructions from the literature and evaluate its ability to detect structural homomorphisms that lead to reduced security estimates. Our framework reproduces known attacks against lattice-based constructions and identifies additional structural vulnerabilities in other proposals, as discussed in detail in the next subsection. The artifact and analysis code are available at `https://github.com/lattice-analyzer/CoNAN`.

1.2 Our Results

We apply CoNAN to a broad class of structured lattice constructions in order to account for the additional lattice structure induced by the underlying ring during security estimation. Our framework successfully reproduces several known attacks against lattice-based schemes, including NTRU Composite [20], BQTRU [45], and some instances of multivariate LWE [8]. Beyond reproducing existing results, we obtain both practical and asymptotic improvements in the cost of recovering either a candidate decryption key or the encrypted message for several constructions, including [10,33,36].

Notably, all newly identified vulnerabilities arise in designs over noncommutative rings. These results highlight the difficulty of reasoning about homomorphic decompositions in such settings, even though the designers of [4,10,36] explicitly considered and attempted to mitigate decomposition-based attacks arising from [20]. This is precisely where CoNAN demonstrates its utility as a cryptanalytic assistant for the design and evaluation of structured lattice-based constructions. Concretely, Table 1 summarizes both the reproduced and newly identified homomorphic dimension-reduction attacks, together with the corresponding security estimates obtained with and without exploiting the induced algebraic structure. The security estimation is computed according to the sieving model as (0.292β), where β is the blocksize required to retrieve a decryption key/message, and the parameters shown for each scheme are selected to target the first level of security compared to NTRU/Kyber.

We further emphasize that our attack on [10,36] differs fundamentally from the approach proposed in [40]. In particular, CoNAN provides a simpler methodology for detecting the structural weaknesses; it further identifies attacks against both the families introduced in [36]. From Table 1, we observe that estimates that do not account for exploitable algebra-induced homomorphisms may significantly overestimate the security achieved by a given parameter set. For example,

Table 1. Comparison of security estimates obtained using the lattice estimator [2] and CoNAN. The notation $(\mathsf{dim}, \mathsf{sec})$ denotes the lattice dimension and the corresponding estimated bit-security (0.292β) across different schemes.

Scheme	**Param.**	**Lattice Est.** $(\mathsf{dim}, \mathsf{sec})$	**CoNAN** $(\mathsf{dim}, \mathsf{sec})$	**Remarks**
NTRU Composite [49]	P_1	$(1024, 103)$	$(512, 45)$	Reproduced [20]
BQTRU [4]	P_2	$(968, 131)$	$(484, 66)$	Reproduced [45]
Multivariate LWE [41,42,43]	P_3	$(1024, 115)$	$(512, 54)$	Reproduced [8]
Noncommutative NTRU [33]	P_4	$(1668, 214)$	$(1112, 147)$	Improved attack[†]
Noncommutative LWE [10]	P_5	$(1024, 118)$	$(512, 54)$	New[$]
LWE from SDP [♣] (Type 1) [36]	P_6	$(1024, 118)$	$(512, 54)$	New
LWE from SDP (Type 2) [36]	P_7	$(1024, 118)$	$(512, 54)$	New
NTRU over Split Quaternion Algebra [50]	P_8	$(1048, 115)$	$(524, 53)$	New

$P_1 : (N = 512, q = 7601, \sigma^2 = 4/3)$ $P_2 : (N = 11, q = 191, \sigma^2 = 2/7)$
$P_3 : (n_1 = 128, n_2 = 4, q = 3329, \sigma^2 = 1.49)$ $P_4 : (N = 139, q = 2237, \sigma^2 = 1.1)$
$P_5 : (N = 256, q = 3329, \sigma^2 = 1.49)$ $P_6 : (n = 128, m = 4, q = 3329, \sigma^2 = 1.49)$
$P_7 : (n = 512, q = 3329, \sigma^2 = 1.49)$ $P_8 : (N = 131, q = 2048, \sigma^2 = 2/3)$

[†] Improves the practical attack without changing the asymptotic security estimate. Unlike [33], which requires three lattice reductions (two of dimension $8N$ and one of dimension $4N$), CoNAN achieves a similar attack using only two reductions (of dimensions $8N$ and $4N$).
[$] The attack found by CoNAN is different and much simpler from the one discussed in [10].
[♣] SDP: Semidirect Product.

for both types of constructions proposed in [36], parameter sets instantiated according to the security analysis of [36] and targeting approximately 118 bits of Core-SVP security achieve no more than 55 bits of security as per CoNAN.

1.3 Technical Overview

Gentry's [20] standard dimension-reduction attack on composite NTRU exploits the Chinese Remainder Theorem (CRT) decomposition of the underlying ring. For composite N, the isomorphism $\mathbb{Z}[x]/(x^N - 1) \cong \prod_{d|N} \mathbb{Z}[x]/(\Phi_d(x))$ splits the ambient space of the corresponding lattices into independent lower-dimensional lattices, each of which can be attacked separately. This work studies the analogous question beyond the commutative setting, namely for a general associative R-algebra, $\mathcal{A}$, where the decomposition process is considerably more subtle than in the classical commutative CRT setting.

To simplify this analysis, we embed $\mathcal{A}$ into a matrix algebra via a representation $\tau : \mathcal{A} \to M_n(R)$, and study the decomposition at the level of the matrix image. The key observation is that a CRT-style splitting of $\tau(\mathcal{A})$ can be obtained from a family of orthogonal central idempotents in the commutant $\mathcal{C}$ of the structure matrices, yielding $\tau(\mathcal{A}) \cong \prod_j \phi_j(\mathcal{A})$ as a direct product of lower-dimensional R-algebras. Hence, the decomposition is performed at the level of the matrix representation rather than directly within $\mathcal{A}$ itself.

In many structured cryptosystems, we further show that the matrix representation admits additional algebraic structure that allows the decomposition process to be carried out directly on the symbolic representation matrix, rather than on a concrete matrix instance $\mathbf{M} = \tau(a)$ for some $a \in \mathcal{A}$.

Algorithm 1 summarizes our main decomposition procedure. In particular, the two most expensive steps of the algorithm are the ones related to finding a basis for the commutant $\mathcal{C}$ and then finding idempotents in this commutant. In Proposition 3, we show that one can efficiently compute a basis for the commutant for any associative R-algebra with unity (which is the case for the majority of cryptographic proposals over lattices) without the need to solve $\mathcal{C} \leftarrow \{\mathbf{X} \mid \mathbf{X} \cdot \mathbf{A}_i = \mathbf{A}_i \cdot \mathbf{X},\ \forall i\}$, where the $\mathbf{A}_i$s are the basis of the matrix $\mathbf{M}$.

Further, Proposition 4 shows that constructing a non-trivial central idempotent can be reduced to factoring characteristic polynomials of elements in the commutant $\mathcal{C}$, thereby avoiding the direct solution of $\mathbf{X}^2 = \mathbf{X}$ inside $\mathcal{C}$. Each resulting idempotent induces a block-diagonalization of the matrix representation and gives rise to a corresponding homomorphic projection. In other words, our analysis demonstrates that, even in the setting of multivariate or noncommutative rings, one may search for homomorphisms that yield more effective attacks by studying the irreducibility of the univariate polynomials arising as characteristic polynomials of elements in the commutant $\mathcal{C}$ of the algebra.

This decomposition procedure can be applied recursively up to k times, which we refer to as the *folding factor*, whenever such a decomposition exists. Among the resulting central idempotents, particular attention is given to those inducing "smallness-preserving" homomorphisms, as these lead to more efficient lattice attacks. We derive upper bounds on the folding factor and analyze the conditions under which such decompositions improve lattice attacks in NTRU-like constructions, before extending the discussion to structured LWE-based schemes.

1.4 Road map

The structure of this paper is outlined as follows. Section 2 defines the necessary notations and prerequisites for the work. Section 3 provides a formal description of the NTRU framework and discusses the attack landscape. Section 4 contains the main contribution of the paper, where we introduce a more general representation for representing NTRU-like schemes, called Gen-NTRU. Then, we present the underlying algorithm for CoNAN, which identifies and analyzes dimension-reducing homomorphisms. In Section 5, we extend the CoNAN framework to structured Learning with Errors (LWE) constructions. Finally, in Section 6, we

analyze new findings from CoNAN that demonstrate practical dimension reduction against certain NTRU and structured LWE-based designs.

2 Notations and Definitions

$\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$ denote the rings of integers, real numbers, and complex numbers, respectively. For an integer $q > 1$, $\mathbb{Z}_q$ denotes the ring of integers modulo q. Bold lowercase letters, such as $\boldsymbol{v}$, denote vectors, while bold uppercase letters, such as $\mathbf{A}$, denote matrices. For a vector $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{R}^n$, the Euclidean norm (or ℓ_2-norm) is defined by $\|\boldsymbol{v}\| = \sqrt{\sum_{i=1}^{n} v_i^2}$, the ℓ_∞-norm by $\|\boldsymbol{v}\|_\infty = \max_{1 \le i \le n} |v_i|$, and the ℓ_1-norm by $\|\boldsymbol{v}\|_1 = \sum_{i=1}^{n} |v_i|$. For a ring R and either a group ring over R or an R-module $\mathcal{A}$, the multiplication of two elements $r, s \in R$ and the scalar multiplication of $r \in R$ with $a \in \mathcal{A}$ are denoted simply by rs and ra, respectively, and, the multiplication of two elements $a, b \in \mathcal{A}$ is denoted by $a * b$. For vectors $\boldsymbol{v}$ and matrices $\mathbf{A}, \mathbf{B}$, matrix products are denoted by $\mathbf{A} \cdot \mathbf{B}$ and $\mathbf{A} \cdot \boldsymbol{v}$ or $\boldsymbol{v} \cdot \mathbf{A}$, whenever the operations are well-defined. For a matrix $\mathbf{A}$ and vector $\boldsymbol{a}$, $\mathbf{A}^{Tr}$ and $\boldsymbol{a}^{Tr}$ denote their transposes. For a ring R, $M_n(R)$ denotes the ring of $n \times n$ matrices with entries in R. The symbols $\mathbf{I}_n$ and $\mathbf{0}_n$ denote the identity matrix and the zero matrix of order n, respectively. The notation $\cong$ denotes an isomorphism between two algebraic structures. For matrix $\mathbf{A}$, we denote the characteristic polynomial of $\mathbf{A}$ by $p_{\mathbf{A}}(x) = \det(x\mathbf{I} - \mathbf{A})$.

2.1 Lattices

Definition 1 (Lattice). *Let $\mathbf{B} \in \mathbb{R}^{n \times m}$ with independent rows $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n \in \mathbb{R}^m$. A lattice $\mathcal{L}(\mathbf{B})$ generated by the matrix $\mathbf{B}$ is the set of integer linear combination of rows of $\mathbf{B}$, i.e.,*

$$\mathcal{L}(\mathbf{B}) = \sum_{i=1}^{n} \mathbb{Z}\boldsymbol{b}_i = \left\{ \sum_{i=1}^{n} z_i \boldsymbol{b}_i, \text{ where } z_i \in \mathbb{Z} \right\}. \tag{2}$$

We call $\mathbf{B}$ a basis matrix of the lattice. If $\boldsymbol{b}_i \in \mathbb{Z}^n$, we call the lattice an integral lattice. In the scope of this paper, we consider only full-rank integral lattices, i.e., $n = m$.

We refer to the volume of the parallelepiped spanned by the basis $\boldsymbol{b}_i$'s as the volume of the lattice and is denoted as $det(\mathcal{L}(\mathbf{B}))$:

$$det(\mathcal{L}(\mathbf{B})) = \sqrt{\left| det\left(\mathbf{B}\mathbf{B}^{Tr}\right) \right|}. \tag{3}$$

Definition 2 (SVP). *Given a lattice $\mathcal{L}(\mathbf{B}) \subset \mathbb{R}^n$, the Shortest Vector Problem (SVP) asks to find a non-zero vector $\boldsymbol{v} \in \mathcal{L}(\mathbf{B})$ such that $\|\boldsymbol{v}\| \le \|\boldsymbol{w}\|$ for all non-zero vectors $\boldsymbol{w} \in \mathcal{L}(\mathbf{B})$; the length of the shortest vector in the lattice is denoted as $\lambda_1(\mathcal{L}(\mathbf{B}))$.*

A relaxed variant of the SVP asks to find a short nonzero vector $\boldsymbol{x} \in \mathcal{L}(\mathbf{B})$ with length related to the norm of the shortest vector with an approximation factor $\gamma(n)$, i.e., $\|\boldsymbol{x}\| \le \gamma(n)\lambda_1(\mathcal{L}(\mathbf{B}))$, where $\gamma(n) \ge 1$. We refer to this problem as γ-SVP.

Definition 3 (Gaussian heuristic). *For a full rank lattice $\mathcal{L}(\mathbf{B})$ of dimension n, the estimation of the norm of the shortest vector according to the Gaussian heuristic is denoted as $gh(\mathcal{L}(\mathbf{B}))$, and calculated as*

$$gh(\mathcal{L}(\mathbf{B})) = \sqrt{n/2\pi e} \cdot \quad det(\mathcal{L}(\mathbf{B}))^{1/n}. \tag{4}$$

2.2 Algebra

Definition 4 (Group ring). *Let R be a ring and let $G = \{g_1, \ldots, g_N\}$ be a finite group of order N. The* group ring *of G over R, denoted by RG, consists of all formal linear combinations*

$$RG \;=\; \left\{ a = \sum_{i=1}^{N} \alpha_{g_i} g_i \;\middle|\; \alpha_{g_i} \in R \text{ for } i = 1, \ldots, N \right\}. \tag{5}$$

The set RG is equipped with a ring structure induced by the following operations. Let $a = \sum_{i=1}^{N} \alpha_{g_i} g_i$ and $b = \sum_{i=1}^{N} \beta_{g_i} g_i$ be elements of RG.

- Addition: $a + b \;=\; \sum_{i=1}^{N} (\alpha_{g_i} + \beta_{g_i})\, g_i$
- Multiplication: $a * b \;=\; \left(\sum_{i=1}^{N} \alpha_{g_i} g_i\right) * \left(\sum_{i=1}^{N} \beta_{g_i} g_i\right) \;=\; \sum_{k=1}^{N} \gamma_{g_k} g_k$ *where the coefficients γ_{g_k} are computed as*

$$\gamma_{g_k} \;=\; \sum_{g_i g_j = g_k} \alpha_{g_i} \beta_{g_j} \;=\; \sum_{i=1}^{N} \alpha_{g_i} \beta_{g_i^{-1} g_k} \;=\; \sum_{i=1}^{N} \alpha_{g_k g_i^{-1}} \beta_{g_i}.$$

For each $a = \sum_{i=1}^{N} \alpha_{g_i} g_i \in RG$, the group ring matrix of a is given by

$$\tau(a) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots\cdots & \alpha_{g_1^{-1}g_N} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots\cdots & \alpha_{g_2^{-1}g_N} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{g_N^{-1}g_1} & \alpha_{g_N^{-1}g_2} & \cdots\cdots & \alpha_{g_N^{-1}g_N} \end{pmatrix}. \tag{6}$$

As shown in [27, Theorem 1], the map $\tau\colon RG \to M_N(R)$ is a ring homomorphism. In particular, it preserves both addition and multiplication, that is,

$$\tau(a+b) = \tau(a) + \tau(b) \quad \text{and} \quad \tau(a * b) = \tau(a) \cdot \tau(b), \tag{7}$$

where $+$ denotes matrix addition and $\cdot$ denotes matrix multiplication. We also associate a unique vector $\boldsymbol{a} = (\alpha_{g_1}, \alpha_{g_2}, \ldots, \alpha_{g_N}) \in R^N$ with a.

Lemma 1. *Let $\boldsymbol{a}$ and $\boldsymbol{b}$ denote the unique vectors associated with the elements $a, b \in RG$, respectively. Then, the vector representation of the sum $a+b$ and the multiplication $a * b$ is given by $\boldsymbol{a} + \boldsymbol{b}$ and $\boldsymbol{a} * \boldsymbol{b} = \boldsymbol{a} \cdot \tau(b)$, respectively.*

Proof. Noticing that for an element $a \in RG$, its vector $\boldsymbol{a}$ is the first row of the matrix representation $\tau(a)$, the first identity follows from the additivity of the ring homomorphism τ. The second follows directly from the definition of τ and the group-ring multiplication in (4), which implies that the first row of $\tau(a * b)$ equals $\boldsymbol{a} \cdot \tau(b)$. □

Definition 5 (Module). *Let R be a ring. A* (left) R-module *is an abelian group $(\mathcal{M}, +)$ equipped with a scalar multiplication*

$$R \times \mathcal{M} \to \mathcal{M}, \quad (r, m) \mapsto rm,$$

such that for all $r, s \in R$ and $m, n \in \mathcal{M}$,

$$r(m+n) = rm + rn, \qquad (r+s)m = rm + sm, \qquad (rs)m = r(sm),$$

and, if R has identity 1_R, then $1_R m = m$. If the action is $\mathcal{M} \times R \to \mathcal{M}$, $(m, r) \mapsto mr$, then $\mathcal{M}$ is called a right R-module.

Definition 6 (Free module). *An R-module $\mathcal{M}$ is called* free *if it admits a linearly independent subset $B \subseteq \mathcal{M}$ that spans $\mathcal{M}$. The set B is called a basis of $\mathcal{M}$.*

Definition 7 (R-Algebra). *An R-*algebra *$\mathcal{A}$ is an R-module equipped with a bilinear multiplication $* : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ such that for all $a \in R$ and $u, v, w \in \mathcal{A}$,*

$$(u+v) * w = u * w + v * w, \quad u * (v+w) = u * v + u * w, \quad (au) * v = a(u * v) = u * (av)$$

Unless otherwise stated, all algebras are treated as free R-modules with a finite basis, and the base ring R is assumed to be a unital ring, typically a subring of the integers.

Definition 8 (Associative $R-$algebra). *An R-algebra $\mathcal{A}$ is called* associative *if its multiplication $* : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ is bilinear and satisfies*

$$(u * v) * w = u * (v * w) \quad \text{for all } u, v, w \in \mathcal{A}.$$

If there exists $1_{\mathcal{A}} \in \mathcal{A}$ such that $1_{\mathcal{A}} * u = u * 1_{\mathcal{A}} = u$ for all $u \in \mathcal{A}$, then $\mathcal{A}$ is called a unital associative algebra. For the remainder of this paper, all algebras are assumed to be unital and associative unless explicitly stated otherwise.

Definition 9 (Idempotent). *Let R be a ring with identity. An element $e \in R$ is called an* idempotent *if $e^2 = e$. An idempotent e is called* nontrivial *if $e \neq 0$ and $e \neq 1$.*

Proposition 1 (Idempotents induce projections). *Let R be a ring and let $e \in R$ be an idempotent. Define the map*

$$\pi_e : R \to R, \qquad \pi_e(r) = er.$$

Then π_e is a projection in the sense that $\pi_e^2 = \pi_e$.

Proof. For any $r \in R$ we have $\pi_e^2(r) = \pi_e(\pi_e(r)) = \pi_e(er) = e(er) = e^2 r$. Since e is idempotent, $e^2 = e$, hence $\pi_e^2(r) = er = \pi_e(r)$. Therefore, π_e is a projection operator.

Definition 10 (Central idempotent). *An idempotent $e \in R$ is called* central *if $er = re, \forall r \in R$. Equivalently, e lies in the center of the ring.*

3 NTRU framework

The original NTRU construction [23], introduced by Hoffstein, Pipher, and Silverman, is defined over a ring of truncated polynomials. We briefly recall the overall setup and outline the key generation, encryption, and decryption procedures.

Setup.

- Let (N, p, q) be public parameters, where N is a prime determining the ring dimension, p is a small prime modulus, and q is a power-of-two modulus satisfying $p \ll q$. The scheme is defined over the following rings:

$$\mathcal{R} = \mathbb{Z}[x]/(x^N - 1), \quad \mathcal{R}_p = \mathbb{Z}_p[x]/(x^N - 1), \quad \mathcal{R}_q = \mathbb{Z}_q[x]/(x^N - 1). \tag{8}$$

- Let $\mathcal{T}_N$ denote the set of polynomials of degree at most $N-1$ with coefficients in $\{-1, 0, 1\}$. For integers d_1, d_2, we denote by $\mathcal{T}(d_1, d_2) \subset \mathcal{T}_N$ the subset of ternary polynomials having exactly d_1 coefficients equal to 1, d_2 coefficients equal to -1, and all remaining coefficients equal to 0.
- For $d = \lfloor N/3 \rfloor$, define the sampling spaces

$$\mathcal{L}_g = \mathcal{L}_r = \mathcal{T}(d, d), \qquad \mathcal{L}_f = \mathcal{T}(d+1, d).$$

- The procedure $\mathsf{Centerlift}(f, q)$ maps a polynomial $f \in \mathcal{R}_q$ to its unique representative $f' \in \mathcal{R}$ whose coefficients lie in the interval $(-q/2, q/2]$ and satisfy $f' \bmod q = f$.
- A Sampler, initialized with a seed and a specified sampling space, deterministically outputs a polynomial from that space according to the given seed.

Given the above setup, the key generation, encryption, and decryption algorithms of NTRU can be described as summarized in Figure 2.

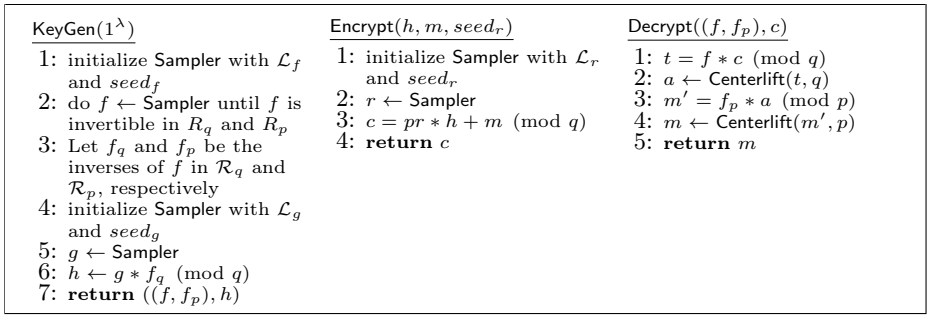


Fig. 2. Key Generation, Encryption, and Decryption procedures for NTRU as introduced in [23].

Apart from the ring $\mathbb{Z}[x]/(x^N-1)$, many other NTRU variants [6,17,30,28,46,47,33] [38,4,50] have been introduced in the literature motivated by faster computation

or higher security against attacks. Figure 3 and Appendix B list some of the most prominent NTRU variants introduced over different algebraic rings. There exist several approaches to attack the secret key and the message in NTRU constructions. The most direct (and also the most expensive) method is a brute-force search for a short pair (f', g') with small Euclidean norm satisfying the NTRU public key equation

$$f' * h = g' \pmod{q}.$$

Although such search attacks can be optimized using techniques such as Meet-in-the-Middle attacks [24] and related combinatorial methods [39,16], lattice-based attacks remain by far the most effective against NTRU. In the following, we sketch the primal attack and mention other related attacks.

3.1 Lattice attacks on NTRU

Primal attack: A key-recovery attack proceeds by embedding the public key into the Coppersmith–Shamir lattice $\mathcal{L}_{CS}$ of dimension $n = 2N$. A basis of $\mathcal{L}_{CS}$ is given by

$$\mathbf{B}_{CS} = \begin{pmatrix} \mathbf{I}_N & \mathbf{H} \\ \mathbf{0}_N & q\mathbf{I}_N \end{pmatrix}, \tag{9}$$

where $\mathbf{H}$ denotes the right-circulant matrix associated with the ring $\mathcal{R} = \mathbb{Z}[x]/(x^N - 1)$, whose first row is the coefficient vector of the public key h. Explicitly,

$$\mathbf{H} = \begin{pmatrix} h_0 & h_1 & \dots & h_{N-1} \\ h_{N-1} & h_0 & \dots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \dots & h_0 \end{pmatrix}. \tag{10}$$

The goal of the attack is to reduce $\mathbf{B}_{CS}$ until a sufficiently short vector $(\boldsymbol{f}', \boldsymbol{g}')$ is found, which can be interpreted as a valid secret key. The attack cost is therefore governed by the blocksize β required for BKZ to reveal such a vector. The cost of BKZ-β with sieving is commonly approximated by $2^{0.292\beta + o(\beta)}$ in the classical setting [5] and $2^{0.265\beta + o(\beta)}$ against quantum adversaries [34].

Hybrid attack: Combining lattice reduction with exhaustive search techniques yields significantly more efficient attacks, particularly against instances with sparse secret keys. Such methods are commonly referred to as *hybrid attacks* [25]. Consider the Coppersmith–Shamir lattice $\mathcal{L}_{CS}$ with reordered basis

$$\mathbf{B}_{CS} = \left(\begin{array}{c|c} q\mathbf{I}_N & \mathbf{0}_N \\ \hline \mathbf{H} & \mathbf{I}_N \end{array}\right) = \left(\begin{array}{c|c|c} q\mathbf{I}_{r_1} & 0 & 0 \\ \hline * & \mathbf{L}' & 0 \\ \hline * & * & \mathbf{I}_{2N-r_2} \end{array}\right), \tag{11}$$

where $\mathbf{L}'$ denotes a sublattice of dimension $r_2 - r_1$.

A hybrid attack applies lattice reduction to the block $\mathbf{L}'$ while exhaustively enumerating the remaining $K = 2N - r_2$ coefficients of the secret key. Following the analysis of [11], the complete private key can be recovered provided that the final K coefficients are guessed correctly and that $\mathbf{L}'$ is reduced with blocksize β satisfying

$$q^{\alpha_{r_2}} \geq 2\|(\mathbf{g}, \mathbf{f})\|_\infty, \tag{12}$$

where

$$\alpha_{r_2} = \frac{N - r_1}{r_2 - r_1} - (r_2 - r_1)\log_q(\delta_\beta), \tag{13}$$

and δ_β denotes the root-Hermite factor given by $\delta_\beta = \left(\frac{\beta}{2\pi e}(\pi\beta)^{\frac{1}{\beta}}\right)^{\frac{1}{2(\beta-1)}}$.

The attacker therefore chooses parameters (r_1, r_2) to balance the cost of lattice reduction in dimension $r_2 - r_1$ against the exhaustive search over the remaining $2N - r_2$ secret coefficients. Hence, the overall complexity of the hybrid attack is determined by the larger of these two costs (see Appendix G for a detailed description).

Other attacks: Apart from the aforementioned attacks, several additional lines of cryptanalysis have been investigated for NTRU-like constructions. In particular, *decryption-failure attacks* exploit non-negligible decryption failure rates arising from certain parameter choices [26]. Another important class of attacks relies on *dense sublattice discovery (DSD)*, which enables a more efficient recovery of the secret key by solving the shortest vector problem (SVP) in a suitably identified dense sublattice rather than in the full lattice associated with the construction. Such attacks have been studied extensively in [31,15].

Finally, a distinct line of attacks [20,45] exploits the *algebraic structure* of the underlying ring used in the construction. Understanding and assessing the security implications arising from such structural properties constitutes the primary focus of this work.

4 CoNAN

Figure 1 summarizes the overall workflow and design logic of CONAN. In the following, we describe the corresponding design specifications.

4.1 Towards Generalization

We study NTRU variants instantiated over a sequence of increasingly expressive algebraic platforms: group rings, twisted group rings, and module-based representations, with each class subsuming the previous as a special case. Yasuda *et al.* [51] proposed *GR-NTRU* as a unifying abstraction for NTRU-type constructions, formulated over group rings. This framework subsumes a wide range of previously proposed NTRU variants by expressing them within a common algebraic setting. In the following, we briefly recall the group-ring definition underlying GR-NTRU and explain how most known NTRU-style schemes can be realized as concrete instantiations of GR-NTRU or its extension, referred to as *(twisted)* GR-NTRU. We further extend this representation to *generalized* NTRU or Gen-NTRU, which can describe all algebraic NTRU instantiations over an associative algebra. Adopting this viewpoint yields a systematic method for deriving the lattice representation associated with a given construction.

Group-Ring NTRU. We view the NTRU public key relation $h = f^{-1} * g \pmod q$ as an instantiation of the Group-Ring NTRU (GR-NTRU) framework. By definition, this implies that

$$\begin{aligned} & f * h = g + qu \quad \text{for some } u \in RG, \\ \implies \quad & \boldsymbol{f} * \boldsymbol{h} = \boldsymbol{g} + q\boldsymbol{u}. \ \text{Equivalently, } \ \boldsymbol{f} \cdot \tau(h) = \boldsymbol{g} + q\boldsymbol{u}, \end{aligned} \tag{14}$$

where the last equivalence follows from Lemma 1.

Consequently, the private vector $(\boldsymbol{f}, \boldsymbol{g})$ corresponds to a short vector in the lattice generated by the basis

$$\mathbf{B}_{CS}^{\mathrm{GR}} = \begin{pmatrix} \mathbf{I}_{|G|} & \tau(h) \\ \mathbf{0}_{|G|} & q\mathbf{I}_{|G|} \end{pmatrix}.$$

The basis $\mathbf{B}_{CS}^{\mathrm{GR}}$ can be seen as a natural generalization of the classical Coppersmith–Shamir lattice basis given in Equation (9), obtained by replacing the circulant structure with the group-ring embedding $\tau(\cdot)$.

Twisted Group-Ring. While GR-NTRU provides a generalization for many of the NTRU constructions, other constructions still can not be directly viewed as GR-NTRU. Twisted GR-NTRU further provides a step towards a general abstraction for representing other rings.

Definition 11 (Twisted group ring). *Let R be a ring and let $G = \{g_1, \ldots, g_N\}$ be a finite group of order N with identity element 1_G. Let $\lambda : G \times G \to R$ be a map satisfying the following conditions:*

- $\lambda(1_G, 1_G) = 1_R$, *and*
- *for all $g_1, g_2, g_3 \in G$, $\lambda(g_1 g_2, g_3)\,\lambda(g_1, g_2) = \lambda(g_1, g_2 g_3)\,\lambda(g_2, g_3)$.*

The twisted group ring *of G over R with respect to λ, denoted by RG^λ, is defined as the R-module*

$$RG^\lambda = \left\{ \sum_{i=1}^{N} \alpha_{g_i} g_i \ : \ \alpha_{g_i} \in R \right\},$$

equipped with addition as in Definition 4, and multiplication given by

$$\left(\sum_{i=1}^{N} \alpha_{g_i} g_i \right) * \left(\sum_{i=1}^{N} \beta_{g_i} g_i \right) = \sum_{i=1}^{N} \left(\sum_{g_h g_k = g_i} \alpha_{g_h} \beta_{g_k} \lambda(g_h, g_k) \right) g_i. \tag{15}$$

Further, for any $a \in RG^\lambda$, the associated twisted group ring matrix is given by

$$\tau^\lambda(a) = \begin{pmatrix} \lambda(g_1, g_1^{-1}g_1)\alpha_{g_1^{-1}g_1} & \lambda(g_1, g_1^{-1}g_2)\alpha_{g_1^{-1}g_2} & \ldots & \lambda(g_1, g_1^{-1}g_N)\alpha_{g_1^{-1}g_N} \\ \lambda(g_2, g_2^{-1}g_1)\alpha_{g_2^{-1}g_1} & \lambda(g_2, g_2^{-1}g_2)\alpha_{g_2^{-1}g_2} & \ldots & \lambda(g_2, g_2^{-1}g_N)\alpha_{g_2^{-1}g_N} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda(g_N, g_N^{-1}g_1)\alpha_{g_N^{-1}g_1} & \lambda(g_N, g_N^{-1}g_2)\alpha_{g_N^{-1}g_2} & \ldots & \lambda(g_N, g_N^{-1}g_n)\alpha_{g_N^{-1}g_N} \end{pmatrix}. \tag{16}$$

Hence, twisted GR-NTRU provides a unified framework for modeling a broader class of underlying rings. In this setting, the lattice associated with the construction is generated by the basis $\mathbf{B}_{CS}^{GR^\lambda}$, which further generalizes $\mathbf{B}_{CS}^{GR}$ by replacing

$\tau(h)$ with its twisted counterpart $\tau^{\lambda}(h)$. In particular, GR-NTRU arises as the special case of twisted GR-NTRU for which $\lambda(g_1, g_2) = 1$ for all $g_1, g_2 \in G$.

Figure 3 demonstrates that the majority of known NTRU variants admit an interpretation as instances of (twisted) GR-NTRU.

A More General Abstraction: Generalized-NTRU. While the twisted group-ring framework captures a broad class of NTRU variants, it does not encompass certain constructions such as NTRUPrime [6] and NTRU+ [30]. To address this limitation, we introduce a further and more general abstraction, termed *Gen-NTRU*, which serves as a more general algebraic framework in our hierarchy for representing associative NTRU-type constructions.

Lemma 2. *Let $\mathcal{A}$ be an R-algebra with finite basis $B = \{b_1, \ldots, b_n\}$ such that basis multiplication decomposition is given by*

$$b_i * b_j = \sum_{k=1}^{n} c_{ijk} b_k, \qquad c_{ijk} \in R.$$

Then:

(a) For $f = \sum_{i=1}^{n} f_i b_i$ and $g = \sum_{j=1}^{n} g_j b_j$ with $f_i, g_j \in R$,

$$f * g = \sum_{k=1}^{n} \left(\sum_{i=1}^{n} \sum_{j=1}^{n} f_i g_j c_{ijk} \right) b_k.$$

(b) The multiplication of $\mathcal{A}$ is associative iff for all $1 \le i, j, k, s \le n$,

$$\sum_{r=1}^{n} c_{ijr} c_{rks} = \sum_{r=1}^{n} c_{jkr} c_{irs}.$$

Proof. (a) By bilinearity,

$$f * g = \left(\sum_i f_i b_i \right) * \left(\sum_j g_j b_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{n} f_i g_j (b_i * b_j),$$

and substituting the basis decomposition yields the result.

(b) By bilinearity, it suffices to verify associativity on basis elements:

$$(b_i * b_j) * b_k = b_i * (b_j * b_k).$$

By substituting the basis decomposition,

$$(b_i * b_j) * b_k = \left(\sum_r c_{ijr} b_r \right) * b_k = \sum_s \sum_r c_{ijr} c_{rks} b_s,$$

and

$$b_i * (b_j * b_k) = b_i * \left(\sum_r c_{jkr} b_r \right) = \sum_s \sum_r c_{jkr} c_{irs} b_s.$$

Since $\{b_s\}$ is a basis, equality holds iff the coefficients of each b_s match, which gives the stated condition.

□

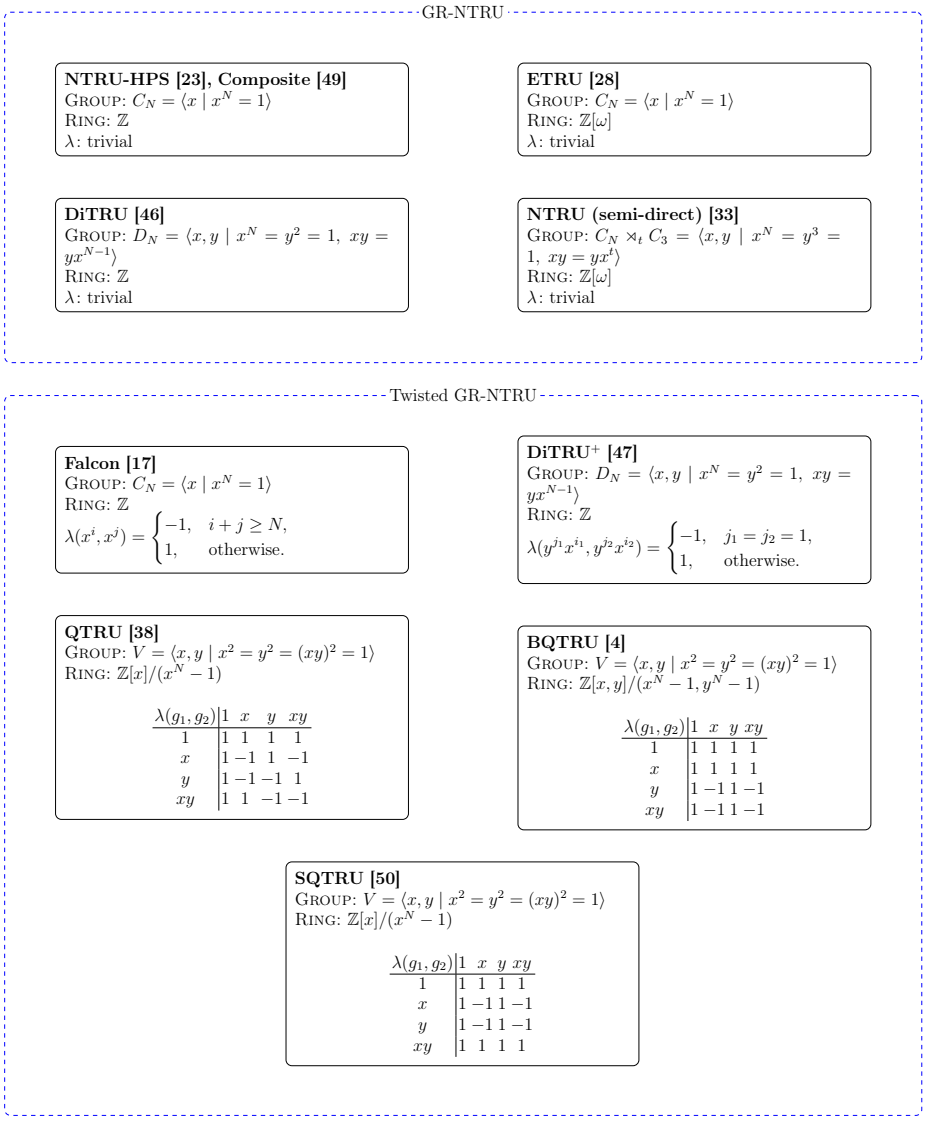


Fig. 3. A unified interpretation of NTRU variants as instances of (twisted) GR-NTRU, where the underlying ring of each scheme corresponds (up to isomorphism) to RG for some ring R and group G. The notation λ: trivial specifies that $\lambda(g_1, g_2) = 1$ for all $g_1, g_2 \in G$.

Further, for any $f \in \mathcal{A} \cong R^B$, where $f = \sum_{i=1}^{n} f_i b_i$ and $f_i \in R$, the coordinate vector of f with respect to the basis B is

$$\boldsymbol{f} = (f_1, f_2, \ldots, f_n) \in R^n,$$

where each f_i is the coefficient corresponding to the basis element b_i. The left and the right matrix representation of f, denoted by $\tau(f)$ and $\tau'(f)$, which are embeddings from $\mathcal{A}$ to $M_n(R)$, respectively is defined as

$$\tau(f) = \begin{pmatrix} \sum_{r=1}^{n} c_{1r1} f_r & \sum_{r=1}^{n} c_{1r2} f_r & \cdots & \sum_{r=1}^{n} c_{1rn} f_r \\ \sum_{r=1}^{n} c_{2r1} f_r & \sum_{r=1}^{n} c_{2r2} f_r & \cdots & \sum_{r=1}^{n} c_{2rn} f_r \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{r=1}^{n} c_{nr1} f_r & \sum_{r=1}^{n} c_{nr2} f_r & \cdots & \sum_{r=1}^{n} c_{nrn} f_r \end{pmatrix}, \; \tau'(f) = \begin{pmatrix} \sum_{r=1}^{n} c_{r11} f_r & \sum_{r=1}^{n} c_{r21} f_r & \cdots & \sum_{r=1}^{n} c_{rn1} f_r \\ \sum_{r=1}^{n} c_{r12} f_r & \sum_{r=1}^{n} c_{r22} f_r & \cdots & \sum_{r=1}^{n} c_{rn2} f_r \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{r=1}^{n} c_{r1n} f_r & \sum_{r=1}^{n} c_{r2n} f_r & \cdots & \sum_{r=1}^{n} c_{rnn} f_r \end{pmatrix}$$

Lemma 3. *Let $\boldsymbol{f}$, $\boldsymbol{h}$, and $\boldsymbol{f} * \boldsymbol{h}$ denote the coordinate vectors of f, h, and $f * h$, respectively. Then*

$$\boldsymbol{f} * \boldsymbol{h} = \boldsymbol{f} \cdot \tau(h), \qquad (\boldsymbol{f} * \boldsymbol{h})^{Tr} = \tau'(f) \cdot \boldsymbol{h}^{Tr}.$$

Furthermore, $\tau(f) \cdot \tau(h) = \tau(f * h), \qquad \tau'(f) \cdot \tau'(h) = \tau'(f * h).$

Proof. Recall that

$$f * h = \sum_{k=1}^{n} \left(\sum_{i=1}^{n} \sum_{j=1}^{n} c_{ijk} f_i h_j \right) b_k.$$

Let

$$\boldsymbol{t} = \left(\sum_{i=1}^{n} \sum_{j=1}^{n} c_{ij1} f_i h_j, \; \sum_{i=1}^{n} \sum_{j=1}^{n} c_{ij2} f_i h_j, \; \ldots, \; \sum_{i=1}^{n} \sum_{j=1}^{n} c_{ijn} f_i h_j \right).$$

Then $\boldsymbol{t}$ is precisely the coordinate vector of $f * h$. By the definitions of $\tau(h)$ and $\tau'(f)$,

$$\boldsymbol{f} \cdot \tau(h) = \boldsymbol{t}, \qquad \tau'(f) \cdot \boldsymbol{h}^{Tr} = \boldsymbol{t}^{Tr}.$$

The remaining identities follow directly from the definitions of $\tau(\cdot)$ and $\tau'(\cdot)$ together with associativity of multiplication in $\mathcal{A}$.

Remark 1. An R-algebra naturally forms a ring under coordinate-wise addition and its bilinear multiplication.

Remark 2. The maps τ and τ' are ring isomorphisms from the R-algebra $\mathcal{A}$ onto the subrings $\tau(\mathcal{A})$ and $\tau'(\mathcal{A})$ of $M_n(R)$, respectively.

NTRU-variants as Gen-NTRU. Naturally, the generalized NTRU (Gen-NTRU) provides a unified, more general framework that encompasses various NTRU variants. In particular, the twisted group ring representation (Twisted GR-NTRU) can be viewed as a special case of Gen-NTRU.

Let R be the base ring, $G = \{g_1, \ldots, g_n\}$ be a finite group, and let $\lambda : G \times G \to R^\times$ be a 2-cocycle defining a twisted group ring structure. Let $\mathcal{A}$ be an R-algebra with basis $B = \{b_1, \ldots, b_n\}$, where each b_i corresponds bijectively to g_i. Then the multiplication in $\mathcal{A}$ as follows:

$$\forall i, j, \quad b_i * b_j = \lambda(g_i, g_j) b_r, \quad \text{where } g_i * g_j = g_r.$$

Equivalently, in terms of the structure constants,

$$c_{ijk} = \begin{cases} \lambda(g_i, g_j), & \text{if } g_i * g_j = g_k, \\ 0, & \text{otherwise.} \end{cases}$$

See Appendix C for examples about how NTRU Prime and NTTRU/NTRU+ can be represented as Gen-NTRU instances.

4.2 Structured Symbolic Matrix Representations

Via the embedding $\tau : \mathcal{R} \to M_n(R)$, each element $h \in \mathcal{R}$ admits a matrix representation $\tau(h)$. Rather than treating $\tau(h)$ as a generic dense matrix, we exploit its internal block structure. By identifying repeating submatrices, we can partition $\tau(h)$ into a set of distinct blocks $\{H_0, H_1, \ldots, H_{k-1}\}$. Replacing these repeated blocks with symbolic representatives yields a smaller symbolic matrix $M(H_0, H_1, \ldots, H_{k-1})$. This symbolic matrix simplifies decomposition analysis by capturing structural symmetries while preserving the original algebraic interactions.

For instance, in both dihedral group-ring constructions and cyclic-group-ring constructions (e.g., Composite-NTRU), left multiplication matrices naturally admit the form:

$$\tau(h) = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B} & \mathbf{A} \end{pmatrix} \implies M(H_0, H_1) = \begin{pmatrix} H_0 & H_1 \\ H_1 & H_0 \end{pmatrix}.$$

Here, H_0 and H_1 symbolically represent the blocks $\mathbf{A}$ and $\mathbf{B}$. While the symbolic matrix $M(H_0, H_1)$ is identical in both settings, the internal algebraic structures of $\mathbf{A}$ and $\mathbf{B}$ differ based on the underlying ring (e.g., right and left circulant matrices for dihedral versus composite cyclic structures).

Finally, in cases where no repeated submatrices exist, the symbolic representation trivially reduces to the original matrix itself.

4.3 Homomorphism induced by a central idempotent.

For the ring under analysis, we investigate the existence of "smallness-preserving" homomorphisms that reduce the underlying lattice problem to lower-dimensional instances, where lattice attacks can be carried out more efficiently.

Proposition 2. *Let R be a ring and let e be a central idempotent. Define $\phi_e : R \to eR$ by $\phi_e(r) = er$. Then ϕ_e is a ring homomorphism.*

Proof. Let $a, b \in R$. Then $\phi_e(ab) = eab$, while $\phi_e(a)\phi_e(b) = (ea)(eb) = eabe = eab$, where we used that e is central and $e^2 = e$. Hence $\phi_e(ab) = \phi_e(a)\phi_e(b)$. Additivity is immediate, so ϕ_e is a ring homomorphism.

Therefore, central idempotents yield a canonical decomposition of rings.

Corollary 1 (Ring decomposition via central idempotents). *Let R be a ring with unity and let $e \in R$ be a central idempotent. Then $R \cong eR \times (1-e)R$ via the ring isomorphism $r \mapsto (er, (1-e)r)$.*

Computing algebraic central idempotents is typically challenging. Instead, we search for nontrivial idempotents within the commutant of the symbolic matrix algebra generated by $M(H_0, \ldots, H_{k-1})$. These idempotents block-diagonalize the symbolic representation by inducing invariant submodule decompositions, though they need not correspond to central idempotents in the original ring. This procedure is formalized in Algorithm 1. The steps listed in the body of the algorithm work according to the following logic: Let $E_0 = \ker(\mathbf{P})$ and $E_1 = \mathrm{Im}(\mathbf{P})$ be the eigenspaces of the idempotent $\mathbf{P}$, with respective bases $U = \{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\ell\}$ and $V = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{k-\ell}\}$. We construct the change-of-basis matrix $\mathbf{T}$ by concatenating these column vectors:

$$\mathbf{T} = [\mathbf{U} \mid \mathbf{V}].$$

Because $\mathbf{M}$ and $\mathbf{P}$ commute ($\mathbf{P} \cdot \mathbf{M} = \mathbf{M} \cdot \mathbf{P}$), the eigenspaces E_0 and E_1 are invariant under the action of $\mathbf{M}$. Specifically, for any $\boldsymbol{u} \in E_0$ and $\boldsymbol{v} \in E_1$, we observe:

$$\mathbf{P} \cdot (\mathbf{M} \cdot \boldsymbol{u}) = \mathbf{M}(\mathbf{P} \cdot \boldsymbol{u}) = \mathbf{M}(0) = 0 \implies \mathbf{M} \cdot \boldsymbol{u} \in E_0,$$
$$\mathbf{P} \cdot (\mathbf{M} \cdot \boldsymbol{v}) = \mathbf{M} \cdot (\mathbf{P} \cdot \boldsymbol{v}) = \mathbf{M} \cdot \boldsymbol{v} \implies \mathbf{M} \cdot \boldsymbol{v} \in E_1.$$

This invariance ensures that $\mathbf{M}$ maps the basis U strictly to linear combinations within U (represented by an $\ell \times \ell$ matrix $\mathbf{M}_0$), and $\mathbf{V}$ strictly to linear combinations within $\mathbf{V}$ (represented by a $(k-\ell) \times (k-\ell)$ matrix $\mathbf{M}_1$). Consequently, the matrix multiplication $\mathbf{M} \cdot \mathbf{T}$ simplifies as follows:

$$\mathbf{M} \cdot \mathbf{T} = \mathbf{M} \cdot [\mathbf{U} \mid \mathbf{V}] = [\mathbf{M} \cdot \mathbf{U} \mid \mathbf{M} \cdot \mathbf{V}] = [\mathbf{U} \cdot \mathbf{M}_0 \mid \mathbf{V} \cdot \mathbf{M}_1].$$

Factoring out the transformation matrix $\mathbf{T} = [\mathbf{U} \mid \mathbf{V}]$ yields the block structure:

$$\mathbf{M} \cdot \mathbf{T} = \mathbf{T} \cdot \begin{pmatrix} \mathbf{M}_0 & \mathbf{0} \\ \mathbf{0} & \mathbf{M}_1 \end{pmatrix}.$$

Left-multiplying by $\mathbf{T}^{-1}$ produces the desired block-diagonal decomposition. Since matrix conjugation by an invertible matrix $\mathbf{T}$ is a ring automorphism, the map $\mathbf{M} \mapsto \mathbf{T}^{-1} \cdot \mathbf{M} \cdot \mathbf{T} = \begin{pmatrix} \mathbf{M}_0 & \mathbf{0} \\ \mathbf{0} & \mathbf{M}_1 \end{pmatrix}$ preserves the ring structure. This is verified by the identities $\mathbf{T}^{-1} \cdot (\mathbf{M} + \mathbf{N}) \cdot \mathbf{T} = \mathbf{T}^{-1} \cdot \mathbf{M} \cdot \mathbf{T} + \mathbf{T}^{-1} \cdot \mathbf{N} \cdot \mathbf{T}$ and $\mathbf{T}^{-1} \cdot (\mathbf{M} \cdot \mathbf{N}) \cdot \mathbf{T} = (\mathbf{T}^{-1} \cdot \mathbf{M} \cdot \mathbf{T})(\mathbf{T}^{-1} \cdot \mathbf{N} \cdot \mathbf{T})$.

Because the ring operations on block-diagonal matrices are defined componentwise, it follows that the maps

$$\phi_0 : M_k(R) \to M_\ell(R) \text{ as } \phi_0(\mathbf{M}) = \mathbf{M}_0 \text{ and } \phi_1 : M_k(R) \to M_{k-\ell}(R) \text{ as } \phi_1(\mathbf{M}) = \mathbf{M}_1$$

are also ring homomorphisms. In the context of NTRU-like schemes, the public equation takes the form $f * h = g \pmod q$, where the secret elements $f, g \in$

$\mathcal{R} \cong R^n$ have small coefficients. This equation admits an equivalent matrix representation $\mathbf{F} \cdot \mathbf{H} = \mathbf{G} \pmod{q}$.

Suppose the matrix representations of elements in $\mathcal{R}$ admit a symbolic representation generated by structural matrices $\mathbf{A}_i \in R^{k \times k}$ for $i = 0, 1, \ldots, k-1$, where $k \mid n$. For an input matrix $\mathbf{H}$ with symbolic representation

$$\mathbf{H} = M(H_0, H_1, \ldots, H_{k-1}) = \sum_{i=0}^{k-1} H_i \mathbf{A}_i,$$

Algorithm 1 computes a transformation matrix $\mathbf{T}$ such that

$$\mathbf{T}^{-1} \cdot \mathbf{H} \cdot \mathbf{T} = \begin{pmatrix} \mathbf{H}_0 & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_1 \end{pmatrix},$$

where $\mathbf{H}_0 \in R^{\ell \times \ell}$ and $\mathbf{H}_1 \in R^{(k-\ell)\times(k-\ell)}$. Applying the induced homomorphisms ϕ_0 and ϕ_1 to the public equation yields

$$\mathbf{F}_i \cdot \mathbf{H}_i = \mathbf{G}_i \pmod{q}, \quad \text{for } i = 0, 1.$$

Crucially, if the transformation $\mathbf{T}$ preserves the smallness of coefficients—that is, for any matrix $\mathbf{S}$ with small entries, the blocks $\mathbf{S}_0$ and $\mathbf{S}_1$ of its conjugate $\mathbf{T}^{-1} \cdot \mathbf{S} \cdot \mathbf{T}$ also have correspondingly small entries—this decomposition directly breaks the cryptanalysis problem into two independent problems. It reduces the problem of recovering the private key from solving the Shortest Vector Problem (SVP) in a single lattice of dimension n to solving two independent SVP instances in lower-dimensional sublattices corresponding to the structural dimensions ℓ and $k - \ell$. This dimensional reduction can be applied recursively as long as further non-trivial idempotents exist and the small-entry condition is preserved.

Steps 5 and 6 of the Algorithm corresponding to finding a basis for the commutant can be computed efficiently as per the Proposition 3, especially when the matrix representation does not accept symbolic representation.

Step 7 of Algorithm 1, which constructs an idempotent in the commutant, is realized through steps **(a)**–**(i)**. This approach is more efficient than directly solving the quadratic equation $\mathbf{X}^2 = \mathbf{X}$ for $\mathbf{X} \in \mathcal{C}$ and follows from the correctness of Proposition 4. Hence, the algorithm 1 requires polynomial-time computation to convert the problem of finding dimension-reduction homomorphisms into checking the irreducibility of univariate polynomials arising from the characteristic polynomials.

Proposition 3. *Let $\mathcal{A}$ be an associative R-algebra with unity $1_{\mathcal{A}}$ and with finite basis $B = \{b_1, \ldots, b_n\}$. The commutant of $\tau(\mathcal{A})$ satisfies $\mathcal{C}(\tau(\mathcal{A})) = {\tau'}^{Tr}(\mathcal{A})$ and $\mathcal{C}(\tau'(\mathcal{A})) = \tau^{Tr}(\mathcal{A})$ (see Figure 4).*

Proof. Let $\mathbf{X} \in M_n(R)$ satisfy $\mathbf{X} \cdot \tau(y) = \tau(y) \cdot \mathbf{X}$ for all $y \in \mathcal{A}$. Let $\mathbf{1}_{\mathcal{A}}$ and $\mathbf{b}_i$ denote the coordinate row vectors for $1_{\mathcal{A}}$ and b_i, respectively, and define $\boldsymbol{x} = \mathbf{1}_{\mathcal{A}} \cdot \mathbf{X}$. The (i, j)-th entry of $\mathbf{X}$ evaluates to:

$$\mathbf{X}_{ij} = \boldsymbol{b}_i \cdot \mathbf{X} \cdot \boldsymbol{b}_j^{Tr} = (\mathbf{1}_{\mathcal{A}} \cdot \tau(b_i)) \cdot \mathbf{X} \cdot \boldsymbol{b}_j^{Tr} = \mathbf{1}_{\mathcal{A}} \cdot \mathbf{X} \cdot \tau(b_i) \cdot \boldsymbol{b}_j^{Tr} = \boldsymbol{x} \cdot \tau(b_i) \cdot \boldsymbol{b}_j^{Tr}.$$

Algorithm 1 Detection of Dimension-Reducing Homomorphisms

Input: Symbolic matrix $M(H_0, \ldots, H_{k-1})$, maximum folding factor k, current block count b (default $b = 1$)

Output: Set of change-of-basis matrices $\mathcal{T}$

if $b \geq k$ **then**
    return $\emptyset$
end if

Write

$$\mathbf{M} = \sum_{i=0}^{k-1} H_i \mathbf{A}_i$$

Compute the commutant

$$\mathcal{C} \leftarrow \{\mathbf{X} \mid \mathbf{X} \cdot \mathbf{A}_i = \mathbf{A}_i \cdot \mathbf{X},\ \forall i\}$$

▷ Proposition 3 $O(n^3)$

Compute a basis $\{\mathbf{C}_1, \ldots, \mathbf{C}_m\}$ of $\mathcal{C}$

Construct an idempotent projector from the basis:

Idempotent Search Over Basis: ▷ Proposition 4

(a) **For** each basis element $\mathbf{C}_j \in \{\mathbf{C}_1, \ldots, \mathbf{C}_m\}$ **do**:
(b) **If** $\mathbf{C}_j$ is a scalar matrix, **continue** to the next element.
(c) Compute the characteristic polynomial $p(x) = \det(x\mathbf{I} - \mathbf{C}_j)$.
(d) **If** $p(x)$ is a power of an irreducible polynomial, **continue** to the next element.
(e) Factor $p(x) = p_1(x)p_2(x)$ such that $\gcd(p_1, p_2) = 1$.
(f) Compute $s(x), t(x) \in \mathbb{F}[x]$ satisfying $s(x)p_1(x) + t(x)p_2(x) = 1$.
(g) Construct the idempotent projector $\mathbf{P} = t(\mathbf{C}_j) \cdot p_2(\mathbf{C}_j)$.
(h) **Break** the loop.
(i) **If** no projector $\mathbf{P}$ was constructed, **Return** $\emptyset$ (irreducible).

Compute a basis of $\mathrm{Im}(\mathbf{P})$

Extend it to a basis of the full space and construct the change-of-basis matrix $\mathbf{T}$

Compute the block decomposition

$$\mathbf{T}^{-1} \cdot \mathbf{M} \cdot \mathbf{T} = \begin{pmatrix} \mathbf{M}_0 & \mathbf{0} \\ \mathbf{0} & \mathbf{M}_1 \end{pmatrix}$$

$b \leftarrow b + 1$

$\mathcal{T}_0 \leftarrow$ Algorithm 1 applied to $(\mathbf{M}_0, k, b)$

$b \leftarrow b + |\mathcal{T}_0|$ ▷ Update total block count from the first recursive branch

$\mathcal{T}_1 \leftarrow$ Algorithm 1 applied to $(\mathbf{M}_1, k, b)$

return $\{\mathbf{T}\} \cup \mathcal{T}_0 \cup \mathcal{T}_1$

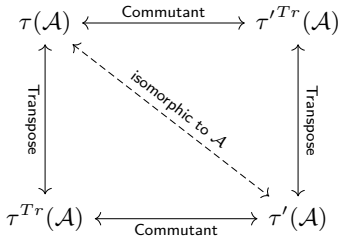


Fig. 4. Commutant for Associative R-algebra with unity.

Expanding $\boldsymbol{x}$ as $\sum_k x_k \boldsymbol{b}_k$ over the basis yields:

$$\mathbf{X}_{ij} = \sum_k x_k \boldsymbol{b}_k \cdot \tau(b_i) \cdot \boldsymbol{b}_j^{Tr} = \sum_k x_k c_{kij}.$$

Therefore, $\mathbf{X} = [\mathbf{X}_{ij}] = [\sum_k x_k c_{kij}] = [\sum_k x_k c_{kji}]^{Tr} = \tau'(x)^{Tr}$ for some $x \in \mathcal{A}$, establishing $\mathcal{C}(\tau(\mathcal{A})) = \tau'^{Tr}(\mathcal{A})$. The identity $\mathcal{C}(\tau'^{Tr}(\mathcal{A})) = \tau^{Tr}(\mathcal{A})$ follows symmetrically.

Proposition 4. *Let $\mathcal{C}$ be a matrix algebra over a field $\mathbb{F}$ and $\boldsymbol{C} \in \mathcal{C}$. Let $p(x) = \det(x\boldsymbol{I} - \boldsymbol{C})$ be the characteristic polynomial of $\boldsymbol{C}$. Suppose $p(x)$ factors into two non-constant, coprime polynomials $p_1(x), p_2(x) \in \mathbb{F}[x]$ such that $p(x) = p_1(x)p_2(x)$. Let $s(x), t(x) \in \mathbb{F}[x]$ satisfy Bézout's identity $s(x)p_1(x)+t(x)p_2(x) = 1$. Then, the matrix $\boldsymbol{P} = t(\boldsymbol{C}) \cdot p_2(\boldsymbol{C})$ is a non-trivial idempotent ($\boldsymbol{P}^2 = \boldsymbol{P}$, $\boldsymbol{P} \neq 0, \boldsymbol{I}$) that belongs to the commutant algebra $\mathcal{C}$.*

Proof. By the Cayley–Hamilton theorem, $p(\mathbf{C}) = 0$. Evaluating Bézout's identity at $\mathbf{C}$ yields $s(\mathbf{C}) \cdot p_1(\mathbf{C}) + t(\mathbf{C}) \cdot p_2(\mathbf{C}) = \mathbf{I}$. Define $\mathbf{P} = t(\mathbf{C}) \cdot p_2(\mathbf{C})$ and $\mathbf{Q} = s(\mathbf{C}) \cdot p_1(\mathbf{C})$, so that $\mathbf{P} + \mathbf{Q} = \mathbf{I}$. Moreover,

$$\mathbf{P} \cdot \mathbf{Q} = t(\mathbf{C}) \cdot s(\mathbf{C}) \cdot p_1(\mathbf{C}) \cdot p_2(\mathbf{C}) = t(\mathbf{C}) \cdot s(\mathbf{C}) \cdot p(\mathbf{C}) = 0.$$

Hence, $\mathbf{P}^2 = \mathbf{P} \cdot (\mathbf{I} - \mathbf{Q}) = \mathbf{P} - \mathbf{P} \cdot \mathbf{Q} = \mathbf{P}$, establishing that $\mathbf{P}$ is idempotent. Since $\mathbf{P}$ is a polynomial in $\mathbf{C}$ and $\mathcal{C}$ is closed under addition and multiplication, it follows that $\mathbf{P} \in \mathcal{C}$.

Suppose, for contradiction, that $\mathbf{P} = 0$. Then $\mathbf{Q} = s(\mathbf{C}) \cdot p_1(\mathbf{C}) = \mathbf{I}$, implying that $p_1(\mathbf{C})$ is invertible. Let λ be a root of $p_1(x)$. Since $p_1(x) \mid p(x)$, we have $p(\lambda) = 0$, and therefore λ is an eigenvalue of $\mathbf{C}$. If $\mathbf{C} \cdot \boldsymbol{v} = \lambda \boldsymbol{v}$ for some $\boldsymbol{v} \neq 0$, then $p_1(\mathbf{C}) \cdot \boldsymbol{v} = p_1(\lambda)\boldsymbol{v} = 0$, showing that $p_1(\mathbf{C})$ has a non-trivial kernel, contradicting invertibility. Hence, $\mathbf{P} \neq 0$. By an analogous argument, we also obtain $\mathbf{P} \neq \mathbf{I}$. Therefore, $\mathbf{P}$ is a nontrivial idempotent element of $\mathcal{C}$.

In our setting, factorization is performed preferentially over the rational numbers $\mathbb{Q}$, and only when necessary over the Gaussian rationals $\mathbb{Q}(i)$, in order to identify potential homomorphisms that may lead, in practice, to more effective attacks (See Appendix A for a step-by-step execution of Algorithm 1.)

4.4 Cost of Reduced-Dimension Lattice Attacks.

Homomorphically mapping the short vector corresponding to the private key from the original lattice to lower-dimensional lattices does not necessarily improve the efficiency of lattice-reduction attacks. In the following, we highlight the factors that affect the cost of the reduction in lower dimensions.

For *primal attacks*, and as indicated by (40), the blocksize required to recover a target vector $\boldsymbol{v}$ depends on (i) the norm of $\boldsymbol{v}$, (ii) the lattice dimension, and (iii) the determinant of the lattice. Equivalently, the larger the lattice dimension and the lattice gap $\frac{\|\boldsymbol{v}\|}{gh(\mathcal{L}(\mathbf{B}))}$, the larger the blocksize required for reduction.

Consider a dimension-reducing homomorphism that decreases the lattice dimension by a factor k_1, decreases the lattice volume by a factor k_2, and increases the norm of the target vector by a factor k_3. Such a transformation yields a more efficient attack, according to the 2016 estimation, only if the resulting blocksize β that satisfies

$$\sqrt{k_1\beta/n}\, k_3\|\boldsymbol{v}\| \;\leq\; \delta_\beta^{2\beta-n/k_1-1} \cdot \left(\frac{\det(\mathcal{L}_{CS})}{k_2}\right)^{k_1/n} \tag{17}$$

is smaller than the blocksize obtained from (40).

Example. For NTRU lattices of dimension $n = 2N$, assume the vector corresponding to the private key $\boldsymbol{v} = (\boldsymbol{f}, \boldsymbol{g})$ is distributed as a discrete Gaussian with mean 0 and variance σ^2. Then $\|\boldsymbol{v}\| \approx \sqrt{n\,\sigma^2}$.

Further, let us consider the homomorphism that folds the secret by summing k_1 independent parts of $\boldsymbol{v}$. Since the sum of k_1 i.i.d. discrete Gaussian variables with variance σ^2 is itself discrete Gaussian with variance $k_1\sigma^2$, it follows that for the folded key $\phi^{(k_1)}(\boldsymbol{v})$,

$$\|\phi^{(k_1)}(\boldsymbol{v})\| \approx \sqrt{\left(\frac{n}{k_1}\right) \cdot k_1\sigma^2} = \sqrt{n\,\sigma^2}.$$

Hence, folding does not approximately increase, on average, the expected norm of the secret. Moreover, if reducing the dimension by a factor k_1 decreases the lattice volume from q^N to some integer value in the range $[1,\, q^{N/k_1}]$, i.e., if k_2 is an integer in the range $[q^{N-N/k_1},\, q^N]$, then Figure 5 illustrates how the blocksize required to retrieve the vector $\phi^{k_1}(\boldsymbol{v})$ varies for $k_1 = 2$, and shows the range of homomorphisms that can lead to more efficient attacks.

For hybrid attack, homomorphically reducing the dimension of the lattice naturally leads to $\|\phi^{k1}(\boldsymbol{v})\|_\infty \geq \|\boldsymbol{v}\|_\infty$ and hence increase the cost of the hybrid attack. As stated in Subsection 3.1, the cost of the hybrid attack is the maximum between search and reduction cost. For the reduction part, in order to succeed in the reduction, Equations (12) and (13) indicate that

$$\log_2(\delta_\beta) \leq \frac{N - r_1}{(r_2 - r_1)^2}\log_2(q) - \frac{\log_2\left(2 \cdot \|\phi^{k1}(\boldsymbol{v}))\|_\infty\right)}{(r_2 - r_1)} \tag{18}$$

Therefore, larger values of $\|\phi^{k_1}(\boldsymbol{v})\|_\infty$ leads to smaller δ_β (which in its turn lead to greater value of β; refer to Equation (39)) and hence more costly lattice reduction.

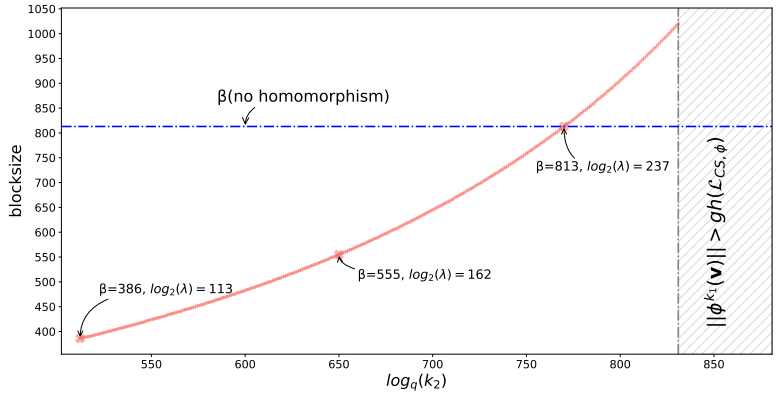


Fig. 5. Blocksize required to recover the image of the short vector $\phi^{k_1}(\boldsymbol{v})$ for $(N = 1024, q = 4096)$ with secret key sampled from $\mathcal{N}(0, 2/3)$, evaluated over candidate homomorphisms inducing a dimension reduction factor of 2 under varying lattice volumes. The figure illustrates that certain admissible homomorphisms can substantially decrease the estimated security level λ relative to the baseline setting without homomorphisms. Security estimates are computed under the sieving cost model (0.292β). The hatched region on the right indicates the parameter range for which $\phi^{k_1=2}(\boldsymbol{v})$ is unlikely to be the shortest vector in the dimensionally reduced lattice $\mathcal{L}_{CS,\phi}$ under the chosen homomorphism.

As the attacker needs to correctly enumerate the last $2N - r_2$ coefficients of the vector $\boldsymbol{v}$, the search cost of the hybrid attack increases with the growth of $\|\phi^{k_1}(\boldsymbol{v})\|_\infty$. To estimate the search cost, the hybrid attack [22] introduces the projection map $\pi : \mathbb{Z}^N \to \mathbb{Z}^{2N-r_2}$ which selects the last $2N - r_2$ coefficients, and defines $\mathcal{F}_\pi = \{\pi(\boldsymbol{v}) : \boldsymbol{v} \in \mathsf{Key\,Space}\}$. Hence, $|\mathcal{F}_\pi|$ increases when larger coefficients appear in the key space, and therefore the search cost of the hybrid attack increases. Consequently, it is highly unlikely for the hybrid attack to outperform the primal attack for homomorphisms that increase the coefficient sizes, unless the original private key is extremely sparse, which is not the case for the majority of schemes in the literature.

Folding factor. Let $\mathcal{L}_{CS}$ be an n-dimensional NTRU-like lattice generated by a basis matrix $\mathbf{B}_{CS}$. Dimension-reduction attacks may reduce this lattice dimension by a factor k, yielding a *folded* lattice of dimension n/k. The adversary's challenge shifts from finding the private key (a shortest vector in $\mathcal{L}_{CS}$) to finding its k homomorphic images in the reduced lattices (see Figure 6).

Because these reduced vectors may not directly reveal the key, the attacker must perform a *lift-back* (or *pull-back*) to reconstruct a short vector in the original n-dimensional lattice. A lifted-back vector $(\boldsymbol{f}', \boldsymbol{g}')$ successfully serves as a decryption key if $\|p\boldsymbol{g}' * \boldsymbol{r} + \boldsymbol{f}' * \boldsymbol{m}\|_\infty < q/2$.

Assume the coefficients of the k folded short vectors $\boldsymbol{v}_i = (\boldsymbol{f}_i, \boldsymbol{g}_i)$ are i.i.d. following $\mathcal{N}(0, \sigma^2_{\text{fold}})$. The lift-back vector is $\boldsymbol{v}_{\text{lift}} = \sum_{i=1}^{k} \alpha_i \boldsymbol{v}_i = (\boldsymbol{f}', \boldsymbol{g}')$, where α_i

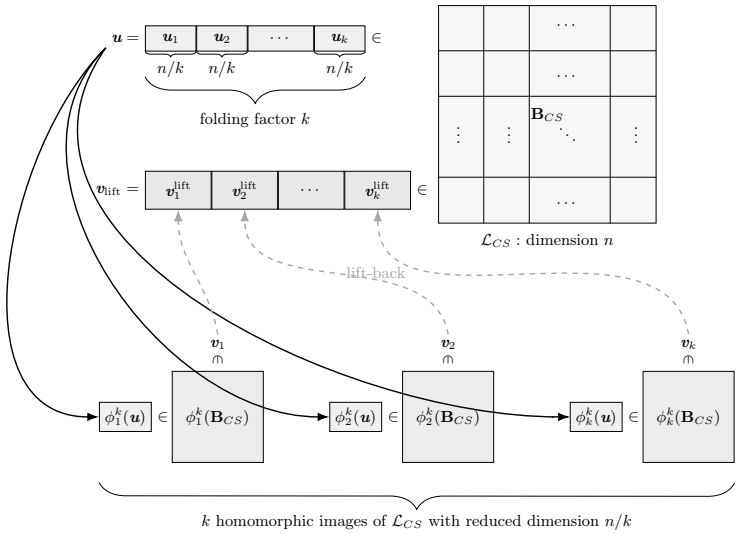


Fig. 6. Illustration of homomorphically *folding* the private key vector into lower-dimensional lattices.

are small constants (typically $|\alpha_i| = 1$). The coefficients of $\boldsymbol{v}_{\text{lift}}$ follow $\mathcal{N}(0, \sigma_{\text{lift}}^2)$, where $\sigma_{\text{lift}}^2 = (\sum_{i=1}^{k} |\alpha_i|^2)\sigma_{\text{fold}}^2$. Since $\boldsymbol{m} \in \mathcal{T}(d_m, d_m)$ takes exactly $2d_m$ nonzero values (± 1), the coefficients of $\boldsymbol{f}' * \boldsymbol{m}$ follow $\mathcal{N}(0, 2d_m\sigma_{\text{lift}}^2)$. Extending this to $\boldsymbol{g}' * \boldsymbol{r}$, the coefficients of $p\boldsymbol{g}' * \boldsymbol{r} + \boldsymbol{f}' * \boldsymbol{m}$ follow $\mathcal{N}(0, \sigma_{\text{dec}}^2)$, where $\sigma_{\text{dec}}^2 = 2\sigma_{\text{lift}}^2(p^2 d_r + d_m)$.

For the private key $\boldsymbol{u} = (\boldsymbol{f}, \boldsymbol{g})$, the coefficients of a k-folded key $\phi^k(\boldsymbol{u}) = \sum_{i=1}^{k} \gamma_i \boldsymbol{u}_i$ follow $\mathcal{N}(0, \sigma_{\text{key}}^2 \sum_{i=1}^{k} |\gamma_i|^2)$, with $\sigma_{\text{key}}^2 = \frac{2(d_f + d_g)}{n}$. We assume small constants $|\gamma_i| \lessapprox \xi_{\text{fold}}$ and $|\alpha_i| \lessapprox \xi_{\text{lift}}$ (typically equal to 1). Because lattice reduction yields vectors roughly bounded by the k-folded key, we approximate $\sigma_{\text{fold}}^2 \approx k\xi_{\text{fold}}^2\sigma_{\text{key}}^2$. Setting $d_f \approx d_g \approx d_m \approx d_r = \frac{n}{6}$, we obtain $\sigma_{\text{lift}}^2 = \frac{2}{3}k^2\xi_{\text{lift}}^2\xi_{\text{fold}}^2$, yielding $\sigma_{\text{dec}}^2 = \frac{2n}{9}k^2(p^2+1)\xi_{\text{lift}}^2\xi_{\text{fold}}^2$. Assuming these coefficients are i.i.d., the probability that the lifted-back vector successfully decrypts is:

$$\begin{aligned}\Pr[\|p\boldsymbol{g}' * \boldsymbol{r} + \boldsymbol{f}' * \boldsymbol{m}\|_\infty < q/2] &= \left(2\Phi\left(\frac{q}{2\sigma_{\text{dec}}}\right) - 1\right)^n \\ &= \left(1 - \mathsf{erfc}\left(\frac{3q}{2\sqrt{4n(p^2+1)}k\xi_{\text{lift}}\xi_{\text{fold}}}\right)\right)^n.\end{aligned}$$

Because erfc [3] is strictly decreasing, successful decryption with a probability $> 1/2$ requires:

$$k < \frac{3q}{2\sqrt{4n(p^2+1)}\,\xi_{\text{lift}}\xi_{\text{fold}}\,\mathsf{erfc}^{-1}(1 - 2^{-1/n})}. \tag{19}$$

[3] erfc refers to the complementary error function

For example, consider NTRU over $\mathbb{Z}_{2048}[x]/(x^{512}-1)$ where $n = 1024, q = 2048$, and $p = 3$. If $\xi_{\text{lift}} = \xi_{\text{fold}} = 1$, then $k \leq 6$. If either ξ_{lift} or ξ_{fold} is 2 while the other is 1, then $k \leq 3$. If both are 2, then $k = 1$.

5 Extension towards structured LWE

It is natural to extend the CoNAN framework to structured LWE constructions.

Let $\mathcal{R}_q$ be an algebraic ring whose elements admit a coefficient embedding of dimension N, and consider a structured (ℓ-rank module) LWE instance with m samples of the form

$$\bar{\boldsymbol{b}} = \bar{\mathbf{A}} \cdot \bar{\boldsymbol{s}} + \bar{\boldsymbol{e}} \pmod{q},$$

where $\bar{\mathbf{A}} \in \mathcal{R}_q^{m \times \ell}$, $\bar{\boldsymbol{s}} \in \chi_s^{\ell}$, and $\bar{\boldsymbol{e}} \in \chi_e^{m}$, for sufficiently small distributions χ_s, χ_e over $\mathcal{R}_q$.

Recovering the secret/error pair $(-\boldsymbol{s}, \boldsymbol{e}) \in \mathbb{Z}^{(m+\ell)N}$ is equivalent to solving a BDD instance in the $(m+\ell)N$-dimensional lattice generated by $\begin{pmatrix} q\mathbf{I} & \mathbf{A} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}$, with target $(\boldsymbol{b}, \mathbf{0})$, where $\mathbf{A} \in \mathbb{Z}^{mN \times \ell N}$ denotes the coefficient embedding of $\bar{\mathbf{A}}$ and $\boldsymbol{s}, \boldsymbol{e}, \boldsymbol{b}$ denote the coefficient embeddings of $\bar{\boldsymbol{s}}, \bar{\boldsymbol{e}}, \bar{\boldsymbol{b}}$, respectively.

Restricting to the common setting $\ell = m$, if $\mathbf{A}$ admits dimension-reducing homomorphisms yielding a folding factor k, then this BDD instance decomposes into k independent lower-dimensional BDD instances over lattices of the form

$$\begin{pmatrix} q\mathbf{I} & \phi_i^{(k)}(\mathbf{A}) \\ \mathbf{0} & \mathbf{I} \end{pmatrix}, \qquad i \in \{1, \ldots, k\},$$

each in dimension reduced by a factor of k.

Applying Kannan's embedding [29] converts each reduced BDD instance into an SVP instance in one additional dimension. Consequently, the resulting blocksize savings admit an analysis directly analogous to that of the reduced-dimension attacks on NTRU lattices discussed above.

For the case where $m = \ell = 1$, we deal with ring-LWE instances. Our analysis using CoNAN led to the conclusion that some of the proposals in the literature, such as LWE from non-commutative group rings [10] and [36], are vulnerable to such attacks.

6 Analysis of Some Attacks Identified by CoNAN

GR-LWE over dihedral group: Cheng *et al.* [10] introduced a variant of the Learning With Errors (LWE) problem over the quotient dihedral group ring

$$\mathcal{R}_q = \frac{\mathbb{Z}D_n}{(x^{n/2}+1)\mathbb{Z}D_n},$$

where D_n is the dihedral group of order $2n$, n is a power of 2, and q is an odd prime. We focus on the dimension-reducing homomorphisms for GR-LWE over

$\mathcal{R}_q$ (details are deferred to Appendix E). Any element $a = a_0(x) + ya_1(x) \in \mathcal{R}_q$ admits a structured matrix representation

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_0 & \mathbf{A}_1 \\ \mathbf{A}_1 & \mathbf{A}_0 \end{pmatrix},$$

where $\mathbf{A}_0, \mathbf{A}_1$ are skew-circulant matrices of size $n/2$. Therefore, a GR-LWE (Group-Ring LWE) instance $(a, b) \in \mathcal{R}_q^2$, where $b = a * s + e$, and $a \xleftarrow{\$} \mathcal{R}_q$ is sampled uniformly, the secret s and error e are sampled from $\mathcal{R}_q$ with small coefficients, can be equivalently expressed as

$$\underbrace{(\boldsymbol{b}_0, \boldsymbol{b}_1)}_{\boldsymbol{b}} = \underbrace{(\boldsymbol{s}_0, \boldsymbol{s}_1)}_{\boldsymbol{s}} \cdot \mathbf{A} + \underbrace{(\boldsymbol{e}_0, \boldsymbol{e}_1)}_{\boldsymbol{e}} \pmod{q} \implies (\boldsymbol{b}, 0) = (\boldsymbol{s}, -\boldsymbol{u}) \cdot \underbrace{\begin{pmatrix} \mathbf{A} & \mathbf{I}_n \\ q\mathbf{I}_n & \mathbf{0}_n \end{pmatrix}}_{\mathcal{L}_{\mathbf{A}}} + (\boldsymbol{e}, -\boldsymbol{s}).$$

So recovering s reduces to solving a CVP instance in a $2n$-dimensional lattice. Applying Kannan embedding gives an SVP instance in dimension $2n + 1$:

$$(-\boldsymbol{s}, \boldsymbol{u}, 1) \cdot \begin{pmatrix} \mathbf{A} & \mathbf{I}_n & 0 \\ q\mathbf{I}_n & \mathbf{0}_n & 0 \\ \boldsymbol{b} & 0 & 1 \end{pmatrix} = (\boldsymbol{e}, -\boldsymbol{s}, 1)$$

Utilizing the fact that $\begin{pmatrix} \mathbf{A}_0 & \mathbf{A}_1 \\ \mathbf{A}_1 & \mathbf{A}_0 \end{pmatrix} \mapsto \mathbf{A}_0 \pm \mathbf{A}_1$ are matrix ring homomorphisms, the problem of recovering the secret key can be reduced to solving two instances of SVP in lattices of dimension $n + 1$ as

$$(-\boldsymbol{s}_0 \mp \boldsymbol{s}_1, \boldsymbol{u}_0 \pm \boldsymbol{u}_1, 1) \cdot \underbrace{\begin{pmatrix} \mathbf{A}_0 \pm \mathbf{A}_1 & \mathbf{I}_{n/2} & 0 \\ q\mathbf{I}_{n/2} & \mathbf{0}_{n/2} & 0 \\ \boldsymbol{b}_0 \pm \boldsymbol{b}_1 & 0 & 1 \end{pmatrix}}_{\mathcal{L}_{\mathbf{A}_0 + \mathbf{A}_1}} = (\boldsymbol{e}_0 \pm \boldsymbol{e}_1, -\boldsymbol{s}_0 \mp \boldsymbol{s}_1, 1)$$

where $\|(\boldsymbol{e}_0 \pm \boldsymbol{e}_1, -\boldsymbol{s}_0 \mp \boldsymbol{s}_1, 1)\| \leq \sqrt{2}\|(\boldsymbol{e}, \boldsymbol{s}, 1)\|$ is also small.

GR-LWE over semidirect product of cyclic groups: Liu and Fu [36] extended the GR-LWE framework to group rings over semidirect products of cyclic groups, namely $\mathbb{Z}_m \ltimes \mathbb{Z}_n$ (Type I) and $\mathbb{Z}_n^\times \ltimes \mathbb{Z}_n$ (Type II). Formal definitions of these semidirect products, along with proofs of the resulting matrix representation patterns, are deferred to Appendix F. Here, we state the resulting structured matrix forms and the associated homomorphisms identified by CoNAN for these group rings.

Type I: The GR-LWE is defined over

$$\mathcal{R} = \frac{\mathbb{Z}[\mathbb{Z}_m \ltimes_k \mathbb{Z}_n]}{(t^{n/2} + 1)},$$

where $\mathbb{Z}_m \ltimes_k \mathbb{Z}_n = \langle s, t \mid s^m = t^n = 1,\ sts^{-1} = t^k \rangle$, with m even and $k^m \equiv 1 \pmod{n}$. We have shown in Appendix F, that the matrix representation of an

element $a = \sum_{i=0}^{m-1} a_i(t)s^i \in \mathcal{R}$, with $a_i(t) \in \mathbb{Z}[t]/(t^{n/2}+1)$ has the following form

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_{00} & \mathbf{A}_{01} & \cdots & \mathbf{A}_{0\,m-1} \\ \mathbf{A}_{10} & \mathbf{A}_{11} & \cdots & \mathbf{A}_{1\,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{m-1\,0} & \mathbf{A}_{m-1\,1} & \cdots & \mathbf{A}_{m-1\,m-1} \end{pmatrix},$$

where each block $\mathbf{A}_{ij}$ is a twisted circulant matrix of size $n/2$ derived from $a_i(t)$. Since m is even, $\mathbf{A}$ exhibits a symmetric 2×2 block structure $\mathbf{A} = \begin{pmatrix} \mathbf{M}_0 & \mathbf{M}_1 \\ \mathbf{M}_1 & \mathbf{M}_0 \end{pmatrix}$, which induces homomorphisms $\mathbf{A} \mapsto \mathbf{M}_0 \pm \mathbf{M}_1$. Consequently, as in the dihedral case, a GR-LWE instance over $\mathcal{R}$ decomposes into two independent subproblems, reducing the lattice dimension by a factor of 2.

Type II: The group ring considered to define GR-LWE is

$$\mathcal{R} = \frac{\mathbb{Z}[\mathbb{Z}_n^{\times} \ltimes_{\Psi} \mathbb{Z}_n]}{((1, \frac{n}{2}) + (1, 0))} \quad \text{where} \quad \mathbb{Z}_n^{\times} \ltimes_{\Psi} \mathbb{Z}_n = \{\, (a, x) \mid a \in \mathbb{Z}_n^{\times},\, x \in \mathbb{Z}_n \,\},$$

with multiplication: $(a, x)(b, y) = (ab, \Psi(b^{-1})(x) + y) = (ab, b^{-1}x + y)$
where b^{-1} denotes the inverse of b modulo n. We consider the case when n is a positive integer such that $4|n$. Refer to F, to find that the matrix representation of an element

$$z = \sum_{r=0}^{n/2-1} \sum_{s=0}^{m-1} \alpha_{r,s}\, (a_s, r),$$

has the form $\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{B} & \mathbf{A} \end{pmatrix}$. Thus, a similar dimension reduction for GR-LWE follows as for the dihedral group ring-based GR-LWE.

SQTRU over split quaternions: Thakur [50] proposed an NTRU-like cryptosystem, namely, SQTRU over split quaternion algebra

$$\mathcal{A} = \left(\frac{-1, 1}{\mathbb{Z}[x]/(x^N - 1)} \right) \tag{20}$$

whose each element $h = h_0 + h_1 i + h_2 j + h_3 k$ where $h_i \in \mathbb{Z}[x]/(x^N - 1)$ has the matrix representation

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_0 & \mathbf{H}_1 & \mathbf{H}_2 & \mathbf{H}_3 \\ -\mathbf{H}_1 & \mathbf{H}_0 & -\mathbf{H}_3 & \mathbf{H}_2 \\ \mathbf{H}_2 & -\mathbf{H}_3 & \mathbf{H}_0 & -\mathbf{H}_1 \\ \mathbf{H}_3 & \mathbf{H}_2 & \mathbf{H}_1 & \mathbf{H}_0 \end{pmatrix}. \tag{21}$$

More details about the split quaternion algebra can be found in [50] and Appendix D. CoNAN found the following dimension-reduction homomorphism for SQTRU that reduces the dimension of the lattice by half.

$$\phi(\mathbf{H}) \longrightarrow \begin{pmatrix} \mathbf{H}_0 + \mathbf{H}_3 & \mathbf{H}_1 + \mathbf{H}_2 \\ -\mathbf{H}_1 + \mathbf{H}_2 & \mathbf{H}_0 - \mathbf{H}_3 \end{pmatrix} \tag{22}$$

Additional results for other considered NTRU-variants reproduced by CoNAN are provided in Table 1.

References

1. Albrecht, M.R., Ducas, L., Herold, G., Kirshanova, E., Postlethwaite, E.W., Stevens, M.: The general sieve kernel and new records in lattice reduction. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2019. pp. 717–746. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-17656-3_25
2. Albrecht, M.R., Player, R., Scott, S.: On the concrete hardness of learning with errors. Journal of Mathematical Cryptology **9**(3), 169–203 (2015). https://doi.org/doi:10.1515/jmc-2015-0016, https://doi.org/10.1515/jmc-2015-0016
3. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key {Exchange—A} new hope. In: 25th USENIX Security Symposium (USENIX Security 16). pp. 327–343 (2016), https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_alkim.pdf
4. Bagheri, K., Sadeghi, M.R., Panario, D.: A non-commutative cryptosystem based on quaternion algebras. Designs, Codes and Cryptography **86**, 2345–2377 (10 2018). https://doi.org/10.1007/s10623-017-0451-4
5. Becker, A., Ducas, L., Gama, N., Laarhoven, T.: New directions in nearest neighbor searching with applications to lattice sieving. In: Proceedings of the twenty-seventh annual ACM-SIAM symposium on Discrete algorithms. pp. 10–24. SIAM (2016). https://doi.org/10.1137/1.9781611974331.ch2
6. Bernstein, D.J., Chuengsatiansup, C., Lange, T., van Vredendaal, C.: NTRU Prime: Reducing Attack Surface at Low Cost. In: Selected Areas in Cryptography – SAC 2017. pp. 235–260. Springer International Publishing (2018). https://doi.org/10.1007/978-3-319-72565-9_12
7. Bindel, N., Buchmann, J., Göpfert, F., Schmidt, M.: Estimation of the hardness of the learning with errors problem with a restricted number of samples. Journal of Mathematical Cryptology **13**(1), 47–67 (2019). https://doi.org/doi:10.1515/jmc-2017-0040, https://doi.org/10.1515/jmc-2017-0040
8. Bootland, C., Castryck, W., Vercauteren, F.: On the security of the multivariate ring learning with errors problem. Open Book Series **4**(1), 57–71 (2020), published in the proceedings of the 14th 14th Algorithmic Number Theory Symposium
9. Chen, C., Danba, O., Hoffstein, J., H¨ulsing, A., Rijneveld, J., Schanck, J.M., Saito, T., Schwade, P.S., Whyte, W.W., Xagawa, K.X., Yamakawa, T., Zhang, Z.: PQC round-3 candidate: NTRU. technical report. Tech. rep., NTRU Cryptosystems Technical Report No.11, Version 2, March 2001. Report (2019), https://ntru.org/f/ntru-20190330.pdf
10. Cheng, Q., Zhang, J., Zhuang, J.: Lwe from non-commutative group rings. Des. Codes Cryptography **90**(1), 239–263 (Jan 2022), https://doi.org/10.1007/s10623-021-00973-6
11. Coppersmith, D., Shamir, A.: Lattice Attacks on NTRU. In: Advances in Cryptology — EUROCRYPT '97. pp. 52–61. Springer Berlin Heidelberg, Berlin, Heidelberg (1997). https://doi.org/10.1007/3-540-69053-0_5
12. Dachman-Soled, D., Ducas, L., Gong, H., Rossi, M.: Lwe with side information: Attacks and concrete security estimation. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology – CRYPTO 2020. pp. 329–358. Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-56880-1_12
13. Ducas, L., Engelberts, L., de Perthuis, P.: Predicting module-lattice reduction. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 133–166. Springer (2025). https://doi.org/10.1007/978-981-95-5099-9_5

14. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS–Dilithium: Algorithm Specifications and Supporting Documentation (Round 3 Submission). Tech. rep., NIST Post-Quantum Cryptography Standardization Project (2020), https://pq-crystals.org/dilithium/data/dilithium-specification-round3.pdf
15. Ducas, L., van Woerden, W.: NTRU Fatigue: How Stretched is Overstretched? In: Advances in Cryptology – ASIACRYPT 2021. pp. 3–32. Springer International Publishing (2021). https://doi.org/10.1007/978-3-030-92068-5_1
16. Esser, A., Girme, R., Mukherjee, A., Sarkar, S.: Memory-efficient attacks on small lwe keys. In: Guo, J., Steinfeld, R. (eds.) Advances in Cryptology – ASIACRYPT 2023. pp. 72–105. Springer Nature Singapore, Singapore (2023). https://doi.org/10.1007/978-981-99-8730-6_3
17. Fouque, P.A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., Zhan, Z.: FALCON: Fast-Fourier lattice-based compact signatures over NTRU. Tech. rep., National Institute of Standards and Technology (NIST) (2018), https://www.di.ens.fr/~prest/Publications/falcon.pdf
18. Fox, N.: Spectra of Semidirect Products of Cyclic Groups. Rose-Hulman Undergraduate Mathematics Journal **11** (2010), https://scholar.rose-hulman.edu/rhumj/vol11/iss2/7
19. Furst, M.L., Kannan, R.: Succinct certificates for almost all subset sum problems. SIAM J. Comput. **18**(3), 550–558 (1989), https://doi.org/10.1137/0218037
20. Gentry, C.: Key recovery and message attacks on NTRU-composite. In: Pfitzmann, B. (ed.) Advances in Cryptology — EUROCRYPT 2001. pp. 182–194. Springer Berlin Heidelberg, Berlin, Heidelberg (2001). https://doi.org/https://doi.org/10.1007/3-540-44987-6_12
21. Grover, C., Mendelsohn, A., Ling, C., Vehkalahti, R.: Non-commutative Ring Learning with Errors from Cyclic Algebras. Journal of Cryptology **35**(22) (2022), https://doi.org/10.1007/s00145-022-09430-6
22. Hoffstein, J., Pipher, J., Schanck, J.M., Silverman, J.H., Whyte, W., Zhang, Z.: Choosing parameters for ntruencrypt. In: Handschuh, H. (ed.) Topics in Cryptology – CT-RSA 2017 (2017). https://doi.org/10.1007/978-3-319-52153-4_1
23. Hoffstein, J., Pipher, J., Silverman, J.H.: NTRU: A ring-based public key cryptosystem. In: International algorithmic number theory symposium. pp. 267–288. Springer, Berlin, Heidelberg (1998). https://doi.org/10.1007/BFb0054868
24. Hoffstein, J., Silverman, J.H., Whyte, W.: Meet-in-the-middle attack on an NTRU private key. Tech. rep., Technical report, NTRU Cryptosystems, July 2006. Report (2006), https://ntru.org/f/tr/tr004v2.pdf
25. Howgrave-Graham, N.: A hybrid lattice-reduction and meet-in-the-middle attack against ntru. In: Advances in Cryptology - CRYPTO 2007. pp. 150–169. Springer Berlin Heidelberg (2007). https://doi.org/10.1007/978-3-540-74143-5_9
26. Howgrave-Graham, N., Nguyen, P.Q., Pointcheval, D., Proos, J., Silverman, J.H., Singer, A., Whyte, W.: The impact of decryption failures on the security of ntru encryption. In: Boneh, D. (ed.) Advances in Cryptology - CRYPTO 2003. pp. 226–246. Springer Berlin Heidelberg, Berlin, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45146-4_14
27. Hurley, T.: Group rings and rings of matrices. International Journal of Pure and Applied Mathematics **31**, 319–335 (01 2006), https://www.researchgate.net/publication/228928727_Group_rings_and_rings_of_matrices
28. Jarvis, K., Nevins, M.: ETRU: NTRU over the eisenstein integers. Des. Codes Cryptogr. **74**, 219–242 (2015), https://doi.org/10.1007/s10623-013-9850-3

29. Kannan, R.: Improved algorithms for integer programming and related lattice problems. In: Proceedings of the fifteenth annual ACM symposium on Theory of computing. pp. 193–206 (1983), https://doi.org/10.1145/800061.808749
30. Kim, J., Park, J.H.: NTRU+: Compact Construction of NTRU Using Simple Encoding Method. IEEE Transactions on Information Forensics and Security **18**, 4760–4774 (2023), https://sites.google.com/view/ntruplus
31. Kirchner, P., Fouque, P.A.: Revisiting lattice attacks on overstretched NTRU parameters. In: Advances in Cryptology – EUROCRYPT 2017. pp. 3–26. Springer International Publishing (2017). https://doi.org/10.1007/978-3-319-56620-7_1
32. Kirshanova, E., May, A., Nowakowski, J.: New NTRU Records with Improved Lattice Bases. In: Post-Quantum Cryptography. pp. 167–195 (2023). https://doi.org/10.1007/978-3-031-40003-2_7
33. Kumar, V., Raya, A., Gangopadhyay, A.K., Gangopadhyay, S., Hussain, M.T.: An Efficient Noncommutative NTRU from Semidirect Product. In: Mukhopadhyay, S., Stănică, P. (eds.) Progress in Cryptology – INDOCRYPT 2024. pp. 3–27. Springer Nature Switzerland, Cham (2025). https://doi.org/10.1007/978-3-031-80308-6_1
34. Laarhoven, T.: Search problems in cryptography: from fingerprinting to lattice sieving. Phd thesis, Eindhoven University of Technology (2015), https://research.tue.nl/en/publications/search-problems-in-cryptography-from-fingerprinting-to-lattice-si
35. Ling, C., Mendelsohn, A.: NTRU in Quaternion Algebras of Bounded Discriminant. In: Post-Quantum Cryptography. pp. 256–290. Springer Nature Switzerland (2023). https://doi.org/10.1007/978-3-031-40003-2_10
36. Liu, J., Fu, F.W.: Learning with Errors over Group Rings Constructed by Semidirect Product. Des. Codes Cryptography **94** (2026). https://doi.org/https://doi.org/10.1007/s10623-026-01809-x
37. Lyubashevsky, V., Seiler, G.: NTTRU: Truly Fast NTRU Using NTT. IACR Transactions on Cryptographic Hardware and Embedded Systems **2019**(3), 180–201 (May 2019). https://doi.org/10.13154/tches.v2019.i3.180-201, https://tches.iacr.org/index.php/TCHES/article/view/8293
38. Malekian, E., Zakerolhosseini, A., Mashatan, A.: QTRU : a lattice attack resistant version of NTRU PKCS based on quaternion algebra. IACR Cryptology ePrint Archive **386** (2009), https://eprint.iacr.org/2009/386
39. May, A.: How to meet ternary LWE keys. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology – CRYPTO 2021. pp. 701–731. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-84245-1_24
40. Mendelsohn, A., Grover, C., Ling, C.: On the security of group ring learning with errors. IACR Communications in Cryptology **2**(2) (2025). https://doi.org/10.62056/ahey76bm
41. Pedrouzo-Ulloa, A., Troncoso-Pastoriza, J.R., Pérez-González, F.: Multivariate lattices for encrypted image processing. In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). pp. 1707–1711. IEEE (2015)
42. Pedrouzo-Ulloa, A., Troncoso-Pastoriza, J.R., Pérez-González, F.: On ring learning with errors over the tensor product of number fields (2016), https://arxiv.org/abs/1607.05244
43. Pedrouzo-Ulloa, A., Troncoso-Pastoriza, J.R., Pérez-González, F.: Multivariate cryptosystems for secure processing of multidimensional signals (2017), https://arxiv.org/abs/1712.00848

44. de Perthuis, P., Trenkić, F.: Refined modelling of the primal attack, and variants against module-lwe. In: International Conference on Post-Quantum Cryptography. pp. 342–376. Springer (2026). https://doi.org/10.1007/978-3-032-22698-3_11
45. Raya, A., Kumar, V., Gangopadhyay, A.K., Gangopadhyay, S.: Giant does not mean strong: Cryptanalysis of bqtru. In: Niederhagen, R., Saarinen, M.J.O. (eds.) Post-Quantum Cryptography. pp. 312–348. Springer Nature Switzerland, Cham (2025). https://doi.org/10.1007/978-3-031-86599-2_11
46. 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), 10.1007/978-3-031-64381-1_16
47. Raya, A., Kumar, V., Gangopadhyay, S., Gangopadhyay, A.K.: Efficient Key Encapsulation Mechanisms from Noncommutative NTRU. Computer Networks **272**, 111704 (2025). https://doi.org/https://doi.org/10.1016/j.comnet.2025.111704
48. Schwabe, P., Avanzi, R., Bos, J.B., Ducas, L.D., Kiltz, E., crede Lepoint, T., Lyubashevsky, V., M. Schanck, J., Seiler, G., Stehle, D.: Crystals-kyber. Tech. rep., National Institute of Standards and Technology (NIST) (2017), https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions
49. Silverman, J.: Wraps, gaps, and lattice constants. Tech. rep., NTRU Cryptosystems Technical Report No.11, Version 2, March 2001. Report (2001), https://ntru.org/f/tr/tr011v2.pdf
50. Thakur, K.: A variant of NTRU with split quaternions algebra. Palestine J. of Mathematics **6**(2), 598–610 (2017), https://pjm.ppu.edu/sites/default/files/papers/PJM_April_2017_28.pdf
51. Yasuda, T., Dahan, X., Sakurai, K.: Characterizing NTRU-variants using group ring and evaluating their lattice security. IACR Cryptol. ePrint Arch. p. 1170 (2015), http://eprint.iacr.org/2015/1170

A Algorithm Execution Example

– **Initialization:** Given the symbolic block matrix $\mathbf{M}$:

$$\mathbf{M} = \begin{pmatrix} H_0 & H_1 \\ H_1 & H_0 \end{pmatrix}$$

We decompose this into a sum of matrices $\mathbf{A}_i$ representing the positions of the blocks H_i:

$$\mathbf{M} = H_0 \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{\mathbf{A}_0} + H_1 \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{\mathbf{A}_1}$$

– **Commutant Basis:** We compute the commutant $\mathcal{C} = \{\mathbf{X} \mid \mathbf{X}\mathbf{A}_i = \mathbf{A}_i\mathbf{X}\ \forall i\}$. The basis matrices of $\mathcal{C}$ are:

$$\mathbf{C}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{C}_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

– **Characteristic Polynomial & Factorization:** We skip the matrix $\mathbf{C}_1$. Selecting $\mathbf{C}_2$, we compute its characteristic polynomial:

$$p(x) = \det(x\mathbf{I} - \mathbf{C}_2) = x^2 - 1$$

This factors completely over the field into two coprime polynomials:

$$p_1(x) = x - 1, \quad p_2(x) = x + 1$$

– **Idempotent Projector Construction:** Using the extended Euclidean algorithm to solve $s(x)p_1(x) + t(x)p_2(x) = 1$, we find the coefficients $s(x) = -1/2$ and $t(x) = 1/2$. The idempotent projector $\mathbf{P}$ is constructed as:

$$\mathbf{P} = t(\mathbf{C}_2) \cdot p_2(\mathbf{C}_2) = \frac{1}{2}(\mathbf{C}_2 + \mathbf{I}) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

– **Image and Kernel Basis (T-Matrix):** We compute the bases for $\mathrm{Im}(\mathbf{P})$ and $\mathrm{Ker}(\mathbf{P})$ to construct our change-of-basis matrix $\mathbf{T}$:

$$\mathrm{Im}(\mathbf{P}) = \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle, \quad \mathrm{Ker}(\mathbf{P}) = \left\langle \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\rangle \implies \mathbf{T} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

– **Block Decomposition:** Applying the transformation $\mathbf{T}^{-1}\mathbf{M}\mathbf{T}$, we isolate the decoupled blocks:

$$\begin{aligned} \mathbf{T}^{-1}\mathbf{M}\mathbf{T} &= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} H_0 & H_1 \\ H_1 & H_0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} H_0 + H_1 & H_0 - H_1 \\ H_1 + H_0 & H_1 - H_0 \end{pmatrix} \\ &= \begin{pmatrix} H_0 + H_1 & \mathbf{0} \\ \mathbf{0} & H_0 - H_1 \end{pmatrix} \end{aligned}$$

A.1 Demonstration of the Security Estimator

We first define the multiplication rule corresponding to the NTRU ring $R_q = \mathbb{Z}_q[x]/(x^N - 1)$.

The multiplication routine is stored in the file `examples.py`.

```
python: def mul_NTRU(f, g, h, n):
....: for i in range(n):
....: for j in range(n):
....: h[(i+j)%n] += f[i]*g[j]
```

We then instantiate an NTRU problem with Gaussian secret and error distributions of variance $4/3$.

```
python: n = 512
....: q = 7681
....: base_var = 4/3.
```

Next, we initialize the estimator. The parameter `level=1` enables the fast decomposition procedure.

```
python: from security_estimator import SecurityEstimator

....: estimator = SecurityEstimator(
....: n=n,
....: q=q,
....: base_var=base_var,
....: mul_function="mul_NTRU",
....: level=1,
....: lattice="NTRU",
....: mul_type="LL",
....: filename="examples.py"
....: )
```

Finally, we estimate the security of the instance. The estimator detects a decomposition of the original 512-dimensional problem into two independent 256-dimensional subproblems corresponding to $H_0 + H_1 \quad \text{and} \quad H_0 - H_1$.

The resulting estimated BKZ blocksize is $\beta = 157$, leading to an estimated concrete security of approximately 45.84 bits.

```
python: result = estimator.estimate_security(
....: verbose=True
....: )
```

```
best_global_integer:
{
  'path': [
      [512, 1.3333333333333333, 'integer', 'combine',
       {'transform':
           (Matrix([
           [1/2,  1/2],
           [1/2, -1/2]]),
            Matrix([
           [1,  1],
           [1, -1]]))
       }],
      (256, 2.6666666666666665, 'integer', 'solve',
       {'matrix': Matrix([[H0 + H1]])}),
      (256, 2.6666666666666665, 'integer', 'solve',
       {'matrix': Matrix([[H0 - H1]])})
  ],
  'beta': 157,
  'complex': False,
  'critical_node': 1,
  'tree_index': 0
}

concrete_beta: 157

security according to CoNAN: 45.844 bits
```

B Decomposed Algebras as found by CoNAN

Table 2. Overview of some representative NTRU-like/LWE constructions over commutative and noncommutative rings.

Scheme	Ring $\mathcal{R}$	Key remarks
Commutative polynomial rings		
NTRU-HPS [23]	$\mathbb{Z}[x]/(x^N-1)$, N prime	Original NTRU instantiation.
NTRU Composite [49]	$\mathbb{Z}[x]/(x^N-1)$, $N=2^n$	Vulnerable to Gentry's attack [20].
NTRUPrime [6]	$\mathbb{Z}[x]/(x^N-x-1)$	Reduces attack's surface.
Falcon [17]	$\mathbb{Z}[x]/(x^N+1)$, $N=2^n$	NTT-friendly parameters.
NTRU+[30], NTTRU[37]	$\mathbb{Z}[x]/(x^N-x^{N/2}+1)$	Fast NTT multiplication.
ETRU [28]	$\mathbb{Z}[\omega][x]/(x^N-1)$	Eisenstein integers; faster multiplication.
Noncommutative rings		
DiTRU [46]	$\mathbb{Z}[x,y]/(x^N-1,\, y^2-1,\, xy=yx^{N-1})$	Dihedral group ring
DiTRU$^+$ [47]	$\mathbb{Z}[x,y]/(x^N-1,\, y^2+1,\, xy=yx^{N-1})$	Twisted multiplication; attack mitigation.
NTRU (semidirect) [33]	$\mathbb{Z}[x,y]/(x^N=y^3=1,\, xy=yx^t)$	Improved efficiency over DiTRU variants.
QTRU [38]	$\{f_0+f_1i+f_2j+f_3k \mid f_i\in\mathbb{Z}[x]/(x^N-1)\}$	Quaternion algebra, $i^2=-1$, $j^2=-1$, $ij=-ji=k$.
BQTRU [4]	$\{f_0+f_1i+f_2j+f_3k \mid f_i\in\mathbb{Z}[x,y]/(x^N-1,y^N-1)\}$.	Bivariate quaternion algebra, $i^2=1$, $j^2=1$, $ij=-ji=k$.
SQTRU [50]	$\{f_0+f_1i+f_2j+f_3k \mid f_i\in\mathbb{Z}[x]/(x^N-1)\}$	Split quaternion algebra, $i^2=-1$, $j^2=k^2=1$, $ij=-ji=k$.
Noncommutative LWE [10]	$\mathbb{Z}[x,y]/(x^N-1,\, y^2+1,\, xy=yx^{N-1})$	Twisted dihedral group ring with even N.
SDP-LWE (Type 1) [36]	$\mathbb{Z}[x,y]/(x^m-1,y^n-1,xy-y^kx^{m-1})$	Group ring of semidirect product group of cyclic groups
SDP-LWE (Type 2) [36]	$\mathbb{Z}[\mathbb{Z}_n^\times \ltimes \mathbb{Z}_n]$	Group ring of semidirect product group of cyclic groups and its group if units

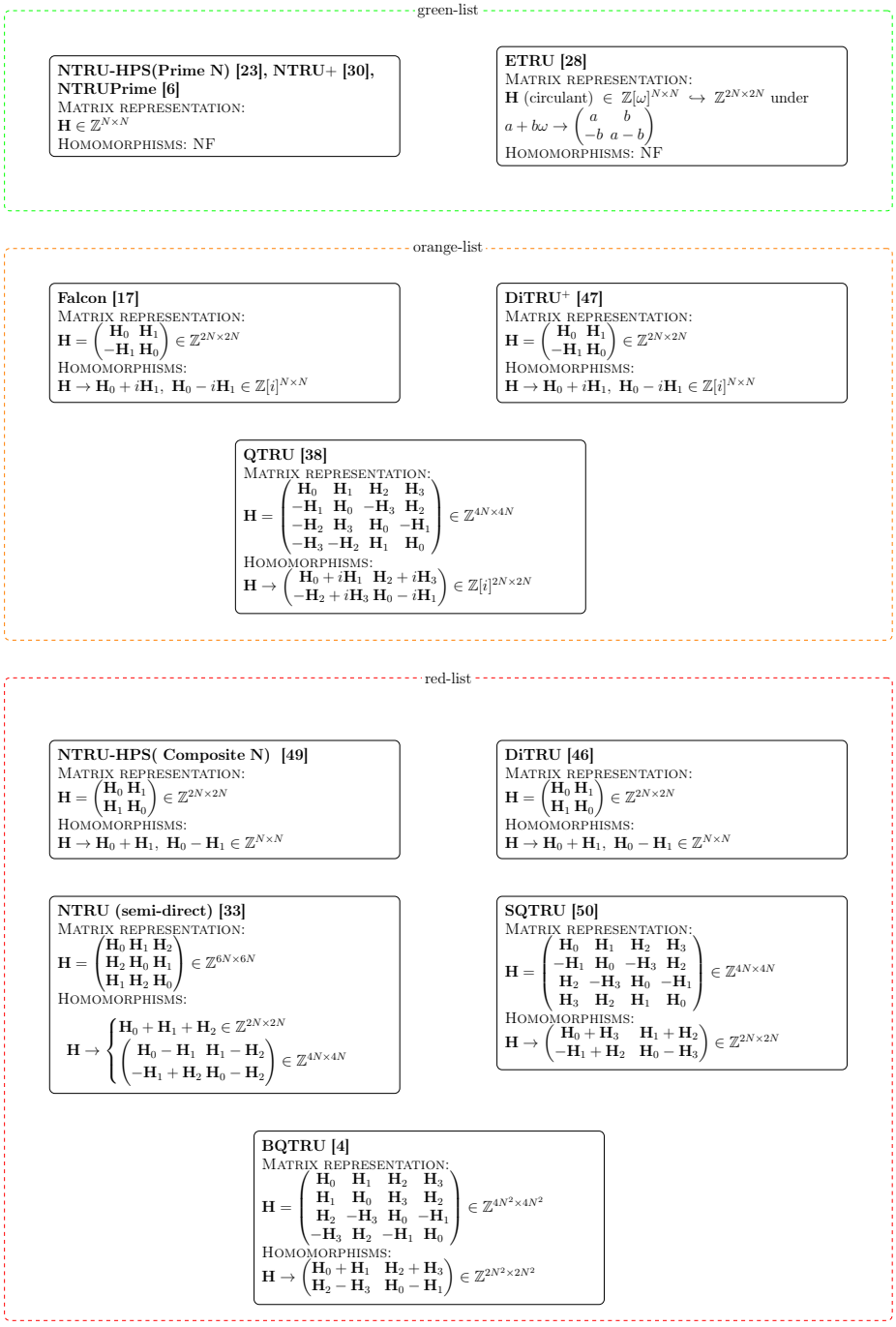


Fig. 7. *Green*: no asymptotic exploitable homomorphism detected. *Orange*: smallness-preserving dimension-reduction homomorphisms over Gaussian integers. *Red*: stronger homomorphic reductions enabling more efficient attacks than the original lattice. *NF*: no beneficial homomorphism found.

C Examples of Gen-NTRU Instances

NTRU Prime: This variant of NTRU is defined over the ring $\mathcal{R} = \frac{\mathbb{Z}[x]}{(x^N - x - 1)}$. This ring cannot be represented in the twisted group ring form. However, it can be expressed within the Gen-NTRU framework by considering a $\mathbb{Z}$-algebra $\mathcal{A}$ with basis elements $\{b_0, b_1, \ldots, b_{N-1}\}$ in bijection with $\{1, x, x^2, \ldots, x^{N-1}\}$ in $\mathcal{R}$. For convenience, we index basis elements starting from 0.

The multiplication in $\mathcal{A}$ is defined via structure constants $c_{ijk} \in \mathbb{Z}$ such that

$$c_{ijk} = \begin{cases} 1 & \text{if } i + j \equiv k \pmod{N}, \\ 1 & \text{if } i + j \geq N \text{ and } i + j \equiv k - 1 \pmod{N}, \\ 0 & \text{otherwise.} \end{cases}$$

These structure constants follow directly from the defining relation $x^N = x + 1$ in $\mathcal{R}$. Therefore, the algebra $\mathcal{A}$ is isomorphic to $\mathcal{R}$.

NTTRU/NTRU+: Similarly, the NTTRU/NTRU+ variant is defined over the ring $\mathcal{R} = \frac{\mathbb{Z}[x]}{(x^N - x^{N/2} + 1)}$. This ring can also be expressed within the Gen-NTRU framework by considering a $\mathbb{Z}$-algebra $\mathcal{A}$ with basis elements $\{b_0, b_1, \ldots, b_{N-1}\}$ in bijection with $\{1, x, x^2, \ldots, x^{N-1}\}$ in $\mathcal{R}$.

The multiplication is defined using structure constants

$$c_{ijk} = \begin{cases} 1 & \text{if } i + j < N \text{ and } i + j \equiv k \pmod{N}, \\ -1 & \text{if } i + j \geq N \text{ and } i + j \equiv k \pmod{N}, \\ 1 & \text{if } i + j \geq N \text{ and } i + j \equiv k - \frac{N}{2} \pmod{N}, \\ 0 & \text{otherwise.} \end{cases}$$

These structure constants follow from the defining relation $x^N = x^{N/2} - 1$ in $\mathcal{R}$. Hence, the algebra $\mathcal{A}$ is isomorphic to $\mathcal{R}$.

D SQTRU attack (new)

Definition 12 (Quaternion algebra). *Let $\mathbb{F}$ be a field and $a, b \in \mathbb{F}/\{0\}$ be two non-zero elements. The quaternion algebra $\mathcal{A}$ over $\mathbb{F}$ by a and b is a 4-dimensional vector space defined as*

$$\mathcal{A} = \left(\frac{a, b}{\mathbb{F}}\right) = \{q_0 + q_1 i + q_2 j + q_3 k \mid q_i \in \mathbb{F}\} \tag{23}$$

and the multiplication is defined by the conditions

$$i^2 = a, j^2 = b, ij = -ji = k.$$

As a result,

$$k^2 = -ab, jk = -kj = -ib, ki = -ik = -ja. \tag{24}$$

Definition 13 (Split quaternion algebra). *Split quaternions is a quaternion algebra with* $a = -1, b = 1$*, i.e.,* $\left(\frac{-1,1}{\mathbb{F}}\right)$.

In general, quaternion algebra, and consequently, split quaternion algebra can be defined over any commutative ring R with unity as

$$\left(\frac{a,b}{R}\right) = \{q_0 + q_1 i + q_2 j + q_3 k \mid q_i \in R\} \tag{25}$$

SQTRU by Thakur [50] is an NTRU-like cryptosystem that operates over the split quaternion algebra defined as:

$$\mathcal{A} = \left(\frac{-1,1}{\mathbb{Z}[x]/(x^N - 1)}\right) \tag{26}$$

for some security parameter N. The lattice $\mathcal{L}_{CS}$ associated with SQTRU, is generated by the basis matrix

$$\mathbf{B}_{CS} = \begin{pmatrix} \mathbf{I}_{4N} & \mathbf{H} \\ \mathbf{0}_{4N} & q\mathbf{I}_{4N} \end{pmatrix} \tag{27}$$

where $\mathbf{H}$ is the matrix corresponding to public key $h = h_0 + h_1 i + h_2 j + h_3 k$ that has a special structure:

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_0 & \mathbf{H}_1 & \mathbf{H}_2 & \mathbf{H}_3 \\ -\mathbf{H}_1 & \mathbf{H}_0 & -\mathbf{H}_3 & \mathbf{H}_2 \\ \mathbf{H}_2 & -\mathbf{H}_3 & \mathbf{H}_0 & -\mathbf{H}_1 \\ \mathbf{H}_3 & \mathbf{H}_2 & \mathbf{H}_1 & \mathbf{H}_0 \end{pmatrix}. \tag{28}$$

where each $\mathbf{H}_i$ is a $N \times N$ circulant matrix associated to $h_i \in \mathbb{Z}[x]/(x^N - 1)$. We *fold* the matrix representation of split quaternions, which reduces the problem of finding short vectors in the lattice $\mathcal{L}_{CS}$ of dimension $8N$, to solving SVP in a lattice of half the dimension as follows.

Define a map from $\mathbf{H}$ to a matrix of half the dimension given by

$$\phi(\mathbf{H}) \longrightarrow \begin{pmatrix} \mathbf{H}_0 + \mathbf{H}_3 & \mathbf{H}_1 + \mathbf{H}_2 \\ -\mathbf{H}_1 + \mathbf{H}_2 & \mathbf{H}_0 - \mathbf{H}_3 \end{pmatrix} \tag{29}$$

One can verify that the map ϕ is a homomorphism on the ring of matrix representations of the split quaternions, i.e., ϕ preserves the matrix addition and multiplication. The private key, therefore, can be recovered by searching for its image, which can be proven to be a short vector in the lattice $\mathcal{L}_{CS,\phi}$ generated by the basis

$$\mathbf{B}_{CS,\phi} = \begin{pmatrix} \mathbf{I}_{2N} & \phi(\mathbf{H}) \\ \mathbf{0}_{2N} & q\mathbf{I}_{2N} \end{pmatrix}. \tag{30}$$

Precisely, if $(\boldsymbol{f}, \boldsymbol{g}) \in \mathcal{L}_{CS}$, where $\boldsymbol{f} = (\boldsymbol{f}_0, \boldsymbol{f}_1, \boldsymbol{f}_2, \boldsymbol{f}_3)$ and $\boldsymbol{g} = (\boldsymbol{g}_0, \boldsymbol{g}_1, \boldsymbol{g}_2, \boldsymbol{g}_3)$, is one of the shortest vectors then $(\boldsymbol{f}_0 + \boldsymbol{f}_3, \boldsymbol{f}_1 + \boldsymbol{f}_2, \boldsymbol{g}_0 + \boldsymbol{g}_3, \boldsymbol{g}_1 + \boldsymbol{g}_2)$ and $(-\boldsymbol{f}_1 + \boldsymbol{f}_2, \boldsymbol{f}_0 - \boldsymbol{f}_3, -\boldsymbol{g}_1 + \boldsymbol{g}_2, \boldsymbol{g}_0 - \boldsymbol{g}_3)$ are among the shortest vectors in the lattice $\mathcal{L}_{CS,\phi}$ with a very high probability.

It is possible that applying the lattice reduction algorithms on the lattice $\mathcal{L}_{CS,\phi}$ do not yield the exact images of the private keys. Such a situation can also be handled by the following *lift-back* approach.

Theorem 1 (Lift-back). *Let the vectors* $(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{x}_0, \boldsymbol{x}_1, \boldsymbol{y}_0, \boldsymbol{y}_1)$ *and* $(\boldsymbol{w}, \boldsymbol{z}) = (\boldsymbol{w}_0, \boldsymbol{w}_1, \boldsymbol{z}_0, \boldsymbol{z}_1)$ *belonging to the lattice* $\mathcal{L}_{CS,\phi}$*. Then the vector*

$$lift(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{w}, \boldsymbol{z}) = (\boldsymbol{x}_0 + \boldsymbol{w}_1, \boldsymbol{x}_1 - \boldsymbol{w}_0, \boldsymbol{x}_1 + \boldsymbol{w}_0, \boldsymbol{x}_0 - \boldsymbol{w}_1, \boldsymbol{y}_0 + \boldsymbol{z}_1, \boldsymbol{y}_1 - \boldsymbol{z}_0, \boldsymbol{y}_1 + \boldsymbol{z}_0, \boldsymbol{y}_0 - \boldsymbol{z}_1)$$

belongs to the lattice $\mathcal{L}_{CS}$*.*

Proof. Let $\boldsymbol{a} = (\boldsymbol{a}_0, \boldsymbol{a}_1), \boldsymbol{b} = (\boldsymbol{b}_0, \boldsymbol{b}_1) \in \mathbb{Z}^{2n^2}$ be such that

$$(\boldsymbol{x}, \boldsymbol{a}) \cdot \mathbf{B}_{CS,\phi} = (\boldsymbol{x}, \boldsymbol{y}) \quad \text{and} \quad (\boldsymbol{w}, \boldsymbol{b}) \cdot \mathbf{B}_{CS,\phi} = (\boldsymbol{w}, \boldsymbol{z}). \tag{31}$$

From (31), we get

$$\left.\begin{aligned} \boldsymbol{x}_0 \cdot (\mathbf{H}_0 + \mathbf{H}_3) + \boldsymbol{x}_1 \cdot (-\mathbf{H}_1 + \mathbf{H}_2) + q\boldsymbol{a}_0 &= \boldsymbol{y}_0 \\ \boldsymbol{x}_0 \cdot (\mathbf{H}_1 + \mathbf{H}_2) + \boldsymbol{x}_1 \cdot (\mathbf{H}_0 - \mathbf{H}_3) + q\boldsymbol{a}_1 &= \boldsymbol{y}_1 \\ \boldsymbol{w}_0 \cdot (\mathbf{H}_0 + \mathbf{H}_3) + \boldsymbol{w}_1 \cdot (-\mathbf{H}_1 + \mathbf{H}_2) + q\boldsymbol{b}_0 &= \boldsymbol{z}_0 \\ \boldsymbol{w}_0 \cdot (\mathbf{H}_1 + \mathbf{H}_2) + \boldsymbol{w}_1 \cdot (\mathbf{H}_0 - \mathbf{H}_3) + q\boldsymbol{b}_1 &= \boldsymbol{z}_1 \end{aligned}\right\} \tag{32}$$

Using (32), one can show that

$$lift(\boldsymbol{x}, \boldsymbol{a}, \boldsymbol{w}, \boldsymbol{b}) \cdot \mathbf{B}_{CS} = lift(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{w}, \boldsymbol{z}).$$

This proves the claimed result. □

Moreover,

$$\|lift(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{w}, \boldsymbol{z})\| \leq 2\sqrt{\|(\boldsymbol{x}, \boldsymbol{y})\|^2 + \|(\boldsymbol{w}, \boldsymbol{z})\|^2}. \tag{33}$$

Therefore, recovering two short enough vectors in the lattice $\mathcal{L}_{CS,\phi}$ and lifting them back to $\mathcal{L}_{CS}$ enables obtaining a possible decryption key with high probability.

E LWE from dihedral group ring attack (new)

Cheng *et al.* [10] introduced a variant of the Learning With Errors (LWE) problem over noncommutative group rings, with a particular focus on dihedral group rings. Their motivation is to broaden the algebraic foundations underlying LWE-based constructions and to potentially mitigate certain algebraic attacks by exploiting noncommutativity. They further propose a public-key encryption scheme whose security is based on the hardness of the corresponding group ring LWE (GR-LWE) problem. We briefly review GR-LWE over dihedral group rings and the key generation procedure of their scheme, and refer the reader to [10] for full details.

The authors argue the semantic security of the scheme by establishing the pseudorandomness of the public key via a reduction from worst-case lattice problems to the average-case decision GR-LWE problem. However, we observe that the specific algebraic structure of dihedral group rings enables additional algebraic attacks. The existence of dimension-reduction homomorphisms allows one to map GR-LWE instances to lower-dimensional lattices, leading to more efficient attacks. Consequently, while the scheme enjoys a worst-case to average-case reduction, its concrete security, which is ultimately tied to the hardness of problems such as the Shortest Vector Problem (SVP) in the associated lattices, may be significantly weakened due to these structural vulnerabilities.

Definition 14 (GR-LWE over dihedral group). *Let $\mathcal{R}_q$ be the quotient of the dihedral group ring*

$$\mathcal{R}_q = \frac{\mathbb{Z}D_n}{(q, x^{n/2}+1)\mathbb{Z}D_n}$$

where D_n is a dihedral group of order $2n$, n is a power of 2, and q is an odd prime modulus.

1. *The search GR-LWE over $\mathcal{R}_q$ problem asks to find the secret $s \in \mathcal{R}_q$, given a sequence of samples $(a_i, b_i) \in \mathcal{R}_q^2$ where a_i is selected uniformly and independently from $\mathcal{R}_q$, and $b_i = a_i * s + e_i$ where e_i is sampled according to some error distribution.*
2. *The decision GR-LWE problem over $\mathcal{R}_q$ is to distinguish with nonnegligible advantage between many independent samples $(a_i, a_i * s + e_i)$ of GR-LWE instances over $\mathcal{R}_q^2$, and the same number of uniformly random samples from $\mathcal{R}_q^2$.*

The PKC proposed is similar to the traditional ring LWE-based encryption scheme, with the only difference that the underlying ring is the group ring of the dihedral group $\mathcal{R}_q$. The secret key $s \in \mathcal{R}_q$ is an element with small coefficients, and $(a, b = a * s + e \pmod q)$ is the corresponding public key, where $a \leftarrow \mathcal{R}_q$ is uniformly sampled, and the error $e \in \mathcal{R}_q$ has small coefficients.

Every element in $\mathcal{R}_q$ can be expressed as $a = a_0(x) + y a_1(x)$ where $a_0(x), a_1(x) \in \mathbb{Z}[x]/(x^{n/2}+1)$. Interestingly, the matrix representation of the elements of $\mathcal{R}_q$ exhibit a pattern

$$\begin{pmatrix} \mathbf{A}_0 & \mathbf{A}_1 \\ \mathbf{A}_1 & \mathbf{A}_0 \end{pmatrix}$$

similar to the elements of dihedral group ring $\mathbb{Z}D_n$. However, the difference is that, here, $\mathbf{A}_0$ and $\mathbf{A}_1$ are skew-circulant matrices of order $n/2$ instead of circulant matrices of order n for dihedral group ring $\mathbb{Z}D_n$. As a result, the public key equation $b = a * s + e \pmod q$ or $b = a * s + e - qu$ for some $u \in \mathcal{R}_q$, can be expressed as

$$\underbrace{(\boldsymbol{b}_0, \boldsymbol{b}_1)}_{\boldsymbol{b}} = \underbrace{(\boldsymbol{s}_0, \boldsymbol{s}_1)}_{\boldsymbol{s}} \cdot \underbrace{\begin{pmatrix} \mathbf{A}_0 & \mathbf{A}_1 \\ \mathbf{A}_1 & \mathbf{A}_0 \end{pmatrix}}_{\mathbf{A}} + \underbrace{(\boldsymbol{e}_0, \boldsymbol{e}_1)}_{\boldsymbol{e}} \pmod q,$$

i.e.,

$$(\boldsymbol{b}, 0) = (\boldsymbol{s}, -\boldsymbol{u}) \cdot \underbrace{\begin{pmatrix} \mathbf{A} & \mathbf{I}_n \\ q\mathbf{I}_n & \mathbf{0}_n \end{pmatrix}}_{\mathcal{L}_{\mathbf{A}}} + (\boldsymbol{e}, -\boldsymbol{s}).$$

Since $\|(\boldsymbol{e}, -\boldsymbol{s})\|$ is small, consequently, the secret key can be recovered by solving CVP (closest vector problem) in a $2n$-dimensional lattice generated by the matrix $\mathcal{L}_{\mathbf{A}}$ with target vector $(\boldsymbol{b}, 0)$. Further, applying Kannan embedding, we have

$$(-\boldsymbol{s}, \boldsymbol{u}, 1) \cdot \begin{pmatrix} \mathbf{A} & \mathbf{I}_n & 0 \\ q\mathbf{I}_n & \mathbf{0}_n & 0 \\ \boldsymbol{b} & 0 & 1 \end{pmatrix} = (\boldsymbol{e}, -\boldsymbol{s}, 1)$$

Hence, the secret key can be recovered by solving SVP in a $(2n+1)$-dimensional lattice generated with high probability.

Now utilizing the fact that $\begin{pmatrix} \mathbf{A}_0 & \mathbf{A}_1 \\ \mathbf{A}_1 & \mathbf{A}_0 \end{pmatrix} \mapsto \mathbf{A}_0 + \mathbf{A}_1, \mathbf{A}_0 - \mathbf{A}_1$ are matrix ring homomorphisms, the problem of recovering the secret key can be reduced to solving two instances of SVP in lattices of dimension $n+1$ as

$$(-\boldsymbol{s}_0 - \boldsymbol{s}_1, \boldsymbol{u}_0 + \boldsymbol{u}_1, 1) \cdot \underbrace{\begin{pmatrix} \mathbf{A}_0 + \mathbf{A}_1 & \mathbf{I}_{n/2} & 0 \\ q\mathbf{I}_{n/2} & \mathbf{0}_{n/2} & 0 \\ \boldsymbol{b}_0 + \boldsymbol{b}_1 & 0 & 1 \end{pmatrix}}_{\mathcal{L}_{\mathbf{A}_0+\mathbf{A}_1}} = (\boldsymbol{e}_0 + \boldsymbol{e}_1, -\boldsymbol{s}_0 - \boldsymbol{s}_1, 1)$$

and

$$(-\boldsymbol{s}_0 + \boldsymbol{s}_1, \boldsymbol{u}_0 - \boldsymbol{u}_1, 1) \cdot \underbrace{\begin{pmatrix} \mathbf{A}_0 - \mathbf{A}_1 & \mathbf{I}_{n/2} & 0 \\ q\mathbf{I}_{n/2} & \mathbf{0}_{n/2} & 0 \\ \boldsymbol{b}_0 - \boldsymbol{b}_1 & 0 & 1 \end{pmatrix}}_{\mathcal{L}_{\mathbf{A}_0-\mathbf{A}_1}} = (\boldsymbol{e}_0 - \boldsymbol{e}_1, -\boldsymbol{s}_0 + \boldsymbol{s}_1, 1),$$

where $\|(\boldsymbol{e}_0 \pm \boldsymbol{e}_1, -\boldsymbol{s}_0 \mp \boldsymbol{s}_1, 1)\| \leq \sqrt{2}\|(\boldsymbol{e}, \boldsymbol{s}, 1)\|$ is also small.

F LWE from group ring of semidirect product of cyclic groups (new)

Following the approach of [10], Liu and Fu [36] extended the GR-LWE framework to group rings of ① semidirect products of cyclic groups, namely $\mathbb{Z}_m \ltimes \mathbb{Z}_n$ (Type I) and ② $\mathbb{Z}_n^\times \ltimes \mathbb{Z}_n$ (Type II). We provide formal explanations of the resulting matrix representations and the corresponding dimension-reducing homomorphisms for both types, as obtained via CoNAN.

Type I: Let us first consider the Type I group rings. The general expression for the semidirect product of cyclic groups is given by the following theorem.

Theorem 2. *[18, Proposition 2.1] Let $\mathbb{Z}_m$ and $\mathbb{Z}_n$ be two cyclic groups of order m and n, respectively. A semidirect product $\mathbb{Z}_m \ltimes_k \mathbb{Z}_n$ corresponds to a choice of integer k such that $k^m \equiv 1 \bmod n$. The semidirect product group is given by*

$$\mathbb{Z}_m \ltimes_k \mathbb{Z}_n = \left\langle s, t \mid s^m = t^n = 1, sts^{-1} = t^k \right\rangle. \tag{34}$$

When there is no confusion of k, we denote the semidirect product by $C_m \ltimes C_n$.

Since $sts^{-1} = t^k$, therefore, $(sts^{-1})^{k^{m-1}} = t^{k^m} = t$ as $k^m = 1 \pmod n$. Hence, we have $ts = st^{k^{m-1}}$. In particular, for $ts = st^{-1}$ for $k = 1$.

The Type I group rings take m and n to be positive even integers and define the GR-LWE over the quotient group ring

$$\mathcal{R} = \frac{\mathbb{Z}[\mathbb{Z}_m \ltimes_k \mathbb{Z}_n]}{(t^{n/2}+1)}$$

with $k = -1$. However, our results hold for any $k \in \mathbb{Z}$ that satisfies $k^m \equiv 1 \pmod{n}$. For a fixed k such that $k^m \equiv 1 \pmod{n}$, order the elements of the group $C_m \ltimes_k C_n$ as follows:

$$Z_m \ltimes_k Z_n = \{1, t, \ldots, t^{n-1}, s, ts, \ldots, t^{n-1}s, \ldots, s^{m-1}, ts^{m-1}, \ldots, t^{n-1}s^{m-1}\}.$$

Therefore, the elements in the group ring R can be expressed as

$$a = \sum_{i=0}^{m-1} a_i(t)s^i \quad \text{where} \quad a_i(t) \in \frac{\mathbb{Z}[t]}{(t^{n/2}+1)}.$$

Write the matrix $\mathbf{M}_{RG}(a)$ into blocks as

$$\mathbf{M}_{RG}(a) = \begin{pmatrix} \mathbf{A}_{00} & \mathbf{A}_{01} & \ldots & \mathbf{A}_{0\,m-1} \\ \mathbf{A}_{10} & \mathbf{A}_{11} & \ldots & \mathbf{A}_{1\,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{m-1\,0} & \mathbf{A}_{m-1\,1} & \ldots & \mathbf{A}_{m-1\,m-1} \end{pmatrix},$$

where, $\mathbf{A}_{xy}$ is an $n/2 \times n/2$ matrix over $\mathbb{Z}$, for $x, y \in \{0, 1, \ldots m-1\}$. From the definition of group ring matrix, for every $0 \leq i, j \leq n/2 - 1$, we have

$$(\mathbf{A}_{xy})_{i,j} = \text{ coefficient of } (t^x s^i)^{-1}(t^y s^j) \text{ in } a.$$

Consider

$$\begin{aligned}(t^x s^i)^{-1}(t^y s^j) &= s^{m-i} t^{(y-x) \bmod n} s^j \\ &= t^{k^{m-i}(y-x) \bmod n} s^{(j-i) \bmod n}\end{aligned}$$

Consequently, the matrix $\mathbf{M}_{RG}(f)$ is a block circulant matrix of the form

$$\mathbf{M}_{RG}(a) = \begin{pmatrix} \mathbf{A}_0 & \mathbf{A}_1 & \ldots & \mathbf{A}_{m-1} \\ \mathbf{A}_{m-1} & \mathbf{A}_0 & \ldots & \mathbf{A}_{m-2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_1 & \mathbf{A}_2 & \ldots & \mathbf{A}_0 \end{pmatrix},$$

where each $\mathbf{A}_i$ is a twisted circulant matrix of order $n/2$ corresponding to $a_i(t)$. Further, since m is even, the matrix has a pattern similar to the group ring of the cyclic group with even order and the dihedral group ring, i.e., $\begin{pmatrix} \mathbf{M}_0 & \mathbf{M}_1 \\ \mathbf{M}_1 & \mathbf{M}_0 \end{pmatrix}$ and thus the dimension of the lattice to be attacked can be reduced in a similar way shown for LWE over the dihedral group ring above.

Type II: Let n be a positive integer and $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ be the cyclic group of order n under addition modulo n, and let $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\} = \{a_0, a_1, \ldots, a_{m-1}\}$ where $m = \varphi(n)$ (totient function) and $a_i \in \mathbb{Z}_n$ such that $\gcd(a_i, n) = 1$, be the multiplicative group of units modulo n. Define a map $\Psi : \mathbb{Z}_n^\times \to \mathrm{Aut}(\mathbb{Z}_n)$ by

$$\Psi(a) = \psi_a,$$

where $\psi_a : \mathbb{Z}_n \to \mathbb{Z}_n$ is given by $\psi_a(x) = ax \pmod{n}$. Since $a \in \mathbb{Z}_n^\times$, multiplication by a is invertible modulo n, and hence ψ_a is an automorphism of $\mathbb{Z}_n$, i.e., $\psi_a \in \mathrm{Aut}(\mathbb{Z}_n)$. Moreover, for $a, b \in \mathbb{Z}_n^\times$ and $x \in \mathbb{Z}_n$, we have

$$\psi_{ab}(x) = (ab)x = a(bx) = \psi_a(\psi_b(x)),$$

which implies

$$\Psi(ab) = \psi_{ab} = \psi_a \circ \psi_b = \Psi(a)\Psi(b).$$

Therefore, Ψ is a group homomorphism. We consider the semidirect product

$$\mathbb{Z}_n^\times \ltimes_\Psi \mathbb{Z}_n = \{\, (a, x) \mid a \in \mathbb{Z}_n^\times,\, x \in \mathbb{Z}_n \,\},$$

with multiplication given by

$$(a, x)(b, y) = (ab, \Psi(b^{-1})(x) + y) = (ab, b^{-1}x + y)$$

where b^{-1} denotes the inverse of b modulo n. We fix the following ordering of the elements of group $G = \mathbb{Z}_n^\times \ltimes_\Psi \mathbb{Z}_n$:

$$\{(a_0, 0), \ldots, (a_{m-1}, 0),\ (a_0, 1), \ldots, (a_{m-1}, 1),\ \ldots,\ (a_0, n-1), \ldots, (a_{m-1}, n-1)\}.$$

Thus, for every index i with $0 \le i < nm$, we can uniquely write $i = rm + s$, where $0 \le r < n$ and $0 \le s < m$. Under this indexing, the i-th element of G is

$$g_i = (a_s, r).$$

Therefore, a general element of the group ring $\mathbb{Z}[G]$ has the form

$$z = \sum_{r=0}^{n-1} \sum_{s=0}^{m-1} \alpha_{r,s}\, (a_s, r),$$

where $\alpha_{r,s} \in \mathbb{Z}$. The Type II group rings are

$$\mathcal{R} = \frac{\mathbb{Z}[G]}{((1, \frac{n}{2}) + (1, 0))}$$

I.e., in the quotient ring, for $x \in \mathbb{Z}_n$, we have $(a, x + \frac{n}{2}) = (-a, x)$. Therefore, every element of the quotient ring $\mathcal{R}$ has the form

$$z = \sum_{r=0}^{n/2-1} \sum_{s=0}^{m-1} \alpha_{r,s}\, (a_s, r),$$

for $\alpha_{r,s} \in \mathbb{Z}$. The matrix representation of z is defined by

$$\mathbf{M}_{RG}(z)_{ij} = \text{coefficient of } g_i^{-1} g_j \text{ in } z,$$

where $\mathbf{M}_{RG}(z)_{ij}$ denotes the (i, j)-th entry of the matrix $\mathbf{M}_{RG}(z)$. Now let

$$i = pm + q, \quad j = rm + s,$$

where $0 \le p, r < n/2$ and $0 \le q, s < m$. Then $g_i = (a_q, p)$, $g_j = (a_s, r)$. The inverse of g_i is given by $g_i^{-1} = (a_q^{-1}, -a_q p)$ since

$$(a_q, p)(a_q^{-1}, -a_q p) = (a_q a_q^{-1}, a_q p - a_q p) = (1, 0).$$

Therefore,

$$g_i^{-1}g_j = (a_q^{-1}, -a_q p)(a_s, r) = (a_q^{-1}a_s, r - a_s^{-1}a_q p).$$

Now write the matrix $\mathbf{M}_{RG}(z)$ in block form:

$$\mathbf{M}_{RG}(z) = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{pmatrix},$$

where each block is a matrix of order $\frac{nm}{4}$. For $0 \leq i, j < \frac{nm}{4}$, we have

$$\mathbf{A}_{ij} = \mathbf{M}_{RG}(z)_{ij} \quad \text{and} \quad \mathbf{D}_{ij} = \mathbf{M}_{RG}(z)_{i+\frac{nm}{4},\ j+\frac{nm}{4}}.$$

Since $i + \frac{mn}{4} = (p + \frac{n}{4})m + q$ and $j + \frac{nm}{4} = (r + \frac{n}{4})m + s$, therefore,

$$g_{i+\frac{nm}{4}} = \left(a_q, p + \frac{n}{4}\right) \quad \text{and} \quad g_{j+\frac{nm}{4}} = \left(a_s, r + \frac{n}{4}\right)$$

and

$$g_{i+\frac{nm}{4}}^{-1} g_{j+\frac{nm}{4}} = \left(a_q^{-1}a_s, r - a_s^{-1}a_q p + \frac{n}{4}\left(1 - a_s^{-1}a_q\right)\right)$$

We consider the case when n is even such that $4|n$. Therefore, $a_q, a_s \in \mathbb{Z}_n^{\times}$, and consequently, $a_s^{-1}a_q$ is odd and $(1 - a_s^{-1}a_q)$ is even. As a result, $n/2$ divides $\frac{n}{4}\left(1 - a_s^{-1}a_q\right)$. Thus,

$$g_{i+\frac{nm}{4}}^{-1} g_{j+\frac{nm}{4}} = \left(a_q^{-1}a_s, r - a_s^{-1}a_q p\right) = g_i^{-1}g_j.$$

Therefore, $\mathbf{A} = \mathbf{D}$. Similarly, one can show that $\mathbf{B} = \mathbf{C}$. Therefore, the dimension of the lattice to be attacked can be reduced by half, in a similar way shown for GR-LWE over the dihedral group ring.

G Attacks against NTRU-like Construction

Definition 15 (Gram-Schmidt orthogonalization). *Let $\mathcal{L}$ be the lattice generated by a basis $\mathbf{B} = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \dots \boldsymbol{b}_n | \boldsymbol{b}_i \in \mathbb{Z}^n\}$, then the corresponding Gram-Schmidt vectors $\mathbf{B}^* = \{\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \dots \boldsymbol{b}_n^* | \boldsymbol{b}_i^* \in \mathbb{R}^n\}$ are calculated as $\boldsymbol{b}_i^* = \boldsymbol{b}_i - \sum_{j=1}^{i-1} \mu_{i,j}\boldsymbol{b}_j^*$ with $\mu_{i,j} = \langle \boldsymbol{b}_i, \boldsymbol{b}_j^* \rangle / \langle \boldsymbol{b}_j^*, \boldsymbol{b}_j^* \rangle$.*

Definition 16 (basis projection). *Let $\mathcal{L}(\mathbf{B})$ be the lattice defined from basis $\mathbf{B} = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \dots \boldsymbol{b}_n\}$; then π_i is defined to be the projection on the space orthogonal to the span of $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \dots \boldsymbol{b}_{i-1}\}$.*

Definition 17 (Block-Korkine–Zolotarev). *Let $\mathcal{L}(\mathbf{B})$ be the lattice generated from the basis $\mathbf{B} = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \dots \boldsymbol{b}_n\}$ and $\mathcal{L}_i^{(k)}$ be a $k-$rank projected lattice generated from $\{\pi_i(\boldsymbol{b}_i), \pi_i(\boldsymbol{b}_{i+1}), \dots \pi_i(\boldsymbol{b}_{i+k-1})\}$. For a blocksize β, the basis $\mathbf{B}$ is called Block-Korkine–Zolotarev ($BKZ-\beta$) reduced basis if $|\mu_{i,j}| \leq 1/2$, for $1 \leq j < i \leq n$ and $\|\boldsymbol{b}_i^*\| = \lambda_1(\mathcal{L}_i^{min(n-i+1,\beta)})$ for $1 \leq i \leq n$. For $\beta = 2$, the reduced basis can be called LLL-reduced.*

Primal attack: A key-recovery attack proceeds by embedding the public key into the Coppersmith–Shamir lattice $\mathcal{L}_{CS}$ of dimension $n = 2N$. A basis of $\mathcal{L}_{CS}$ is given by

$$\mathbf{B}_{CS} = \begin{pmatrix} \mathbf{I}_N & \mathbf{H} \\ \mathbf{0}_N & q\mathbf{I}_N \end{pmatrix}, \tag{35}$$

where $\mathbf{H}$ denotes the right-circulant matrix associated with the ring $\mathcal{R} = \mathbb{Z}[x]/(x^N - 1)$, whose first row is the coefficient vector of the public key h. Explicitly,

$$\mathbf{H} = \begin{pmatrix} h_0 & h_1 & \dots & h_{N-1} \\ h_{N-1} & h_0 & \dots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \dots & h_0 \end{pmatrix}. \tag{36}$$

The goal of the attack is to reduce $\mathbf{B}_{CS}$ until a sufficiently short vector $(\boldsymbol{f}', \boldsymbol{g}')$ is found, which can be interpreted as a valid secret key. The attack cost is therefore governed by the blocksize β required for BKZ to reveal such a vector. By Definition 17, a BKZ-β reduced basis satisfies

$$\|\boldsymbol{b}_i^*\| = \lambda_1\Big(\mathcal{L}_i^{\min(n-i+1,\beta)}\Big), \qquad 1 \le i \le n,$$

so increasing β yields shorter vectors in the reduced basis. Since the runtime of BKZ is dominated by calls to an SVP oracle in β-dimensional projected sublattices, estimating the minimal β sufficient to recover the secret key provides a concrete estimate of the attack complexity. Following the 2016-estimation [3], a target vector $\boldsymbol{v}$ (here $\boldsymbol{v} = (\boldsymbol{f}', \boldsymbol{g}')$) is expected to be recovered by BKZ-β as soon as

$$\|\pi_{n-\beta+1}(\boldsymbol{v})\| \le \|\boldsymbol{b}_{n-\beta+1}^*\|, \tag{37}$$

where $\pi_{n-\beta+1}$ denotes projection onto the span of the last β Gram–Schmidt vectors. The left-hand side is expected to be $\sqrt{\frac{n}{\beta}}\|\boldsymbol{v}\|$, while the right-hand side depends on the Gram–Schmidt profile of a BKZ-β reduced basis. This profile is commonly modeled using the Geometry Series Assumption (GSA), which predicts

$$\|\boldsymbol{b}_i^*\| \approx \delta_\beta^{-2}\|\boldsymbol{b}_{i-1}^*\|, \tag{38}$$

where δ_β denotes the root-Hermite factor, defined via $\|\boldsymbol{b}_1\| = \delta_\beta^n \det(\mathcal{L}_{CS})^{1/n}$. For $\beta > 50$ and $\beta \ll n$, δ_β can be accurately approximated by

$$\delta_\beta = \left(\frac{\beta}{2\pi e}(\pi\beta)^{\frac{1}{\beta}}\right)^{\frac{1}{2(\beta-1)}}. \tag{39}$$

Substituting these estimates into (37) yields the 2016-estimation condition

$$\sqrt{\beta/n}\,\|\boldsymbol{v}\| \;\le\; \delta_\beta^{2\beta-n-1} \cdot \det(\mathcal{L}_{CS})^{1/n}. \tag{40}$$

For NTRU-like lattices, a more refined model is provided by the Z-GSA, which accounts for the q-ary structure of $\mathcal{L}_{CS}$. In dimension $2N$, it predicts the Gram–Schmidt norms

$$\|\boldsymbol{b}_i^*\| = \begin{cases} q, & i \in [1,\, N-m], \\ \sqrt{q}\,\delta_\beta^{2N-1-2i}, & i \in (N-m,\, N+m), \\ 1, & i \in [N+m,\, 2N), \end{cases} \tag{41}$$

where $m = \frac{1}{2} + \frac{\ln(q)}{\ln(\delta_\beta)}$. For the relevant blocksizes, $\|\boldsymbol{b}^*_{n-\beta+1}\|$ lies in the middle regime, so the resulting success condition coincides with (40).

Consequently, security estimates typically rely on the *Core-SVP* heuristic, which assumes that a single call to an SVP oracle suffices to recover the target short vector $\boldsymbol{v}$. Under this assumption, concrete security is estimated by the cost of solving SVP in dimension β. Classical enumeration-based SVP algorithms run in super-exponential time while requiring only polynomial space, whereas sieving-based algorithms achieve exponential time complexity at the cost of exponential memory. Recent advances [1,32] indicate that sieving outperforms enumeration for blocksizes $\beta \geq 65$, and it is therefore standard to base concrete security estimates on sieving models. In particular, the cost of SVP in dimension β is commonly approximated by $2^{0.292\beta+o(\beta)}$ in the classical setting [5] and $2^{0.265\beta+o(\beta)}$ against quantum adversaries [34]

Hybrid attack: The combination of lattice reduction with search techniques yields more efficient attacks, particularly against instances with sparse secret keys. Such attacks are commonly referred to as *hybrid attacks* [25]. Consider the Coppersmith–Shamir lattice $\mathcal{L}_{CS}$ with a reordered basis

$$\mathbf{B}_{CS} = \left(\begin{array}{c|c} q\mathbf{I}_N & \mathbf{0}_N \\ \hline \mathbf{H} & \mathbf{I}_N \end{array}\right) = \left(\begin{array}{c|c|c} q\mathbf{I}_{r_1} & 0 & 0 \\ \hline * & \mathbf{L}' & 0 \\ \hline * & * & \mathbf{I}_{2N-r_2} \end{array}\right), \tag{42}$$

where $\mathbf{L}'$ denotes a sublattice of dimension $r_2 - r_1$. A hybrid attack proceeds by applying lattice reduction to the block $\mathbf{L}'$ while exhaustively enumerating the remaining $K = 2N - r_2$ coefficients of the secret key.

Let $\mathbf{U}'$ be a unimodular transformation that reduces the block $\mathbf{L}'$. Since the secret vector $\boldsymbol{v} = (\boldsymbol{g}, \boldsymbol{f}) \in \mathcal{L}_{CS}$, it also lies in the lattice generated by $\mathbf{UB}_{CS}$, where

$$\mathbf{U} = \left(\begin{array}{c|c|c} \mathbf{I}_{r_1} & 0 & 0 \\ \hline 0 & \mathbf{U}' & 0 \\ \hline 0 & 0 & \mathbf{I}_{2N-r_2} \end{array}\right). \tag{43}$$

Let $\mathbf{Y}'$ be an orthogonal transformation such that $\mathbf{U}' \cdot \mathbf{L}' \cdot \mathbf{Y}'$ is lower triangular. Then $(\boldsymbol{g}, \boldsymbol{f}) \cdot \mathbf{Y}$ is a short vector in the lattice generated by $\mathbf{T} = \mathbf{UB}_{CS} \cdot \mathbf{Y}$, where

$$\mathbf{Y} = \left(\begin{array}{c|c|c} \mathbf{I}_{r_1} & 0 & 0 \\ \hline 0 & \mathbf{Y}' & 0 \\ \hline 0 & 0 & \mathbf{I}_{2N-r_2} \end{array}\right). \tag{44}$$

The diagonal entries of $\mathbf{T}$ belong to $\{q^{\alpha_1}, \ldots, q^{\alpha_{2N}}\}$ with $\sum_{i=1}^{2N} \alpha_i = N$. More precisely, $\alpha_i = 1$ for $i < r_1$, $\alpha_i = 0$ for $i > r_2$, while for $i \in [r_1, r_2]$ the exponents decrease according to the Geometric Series Assumption (GSA) (cf. (38)). Following [22], these values can be approximated as

$$\alpha_{r_1} = \frac{N - r_1}{r_2 - r_1} + (r_2 - r_1)\log_q(\delta_\beta), \tag{45}$$

$$\alpha_{r_2} = \frac{N - r_1}{r_2 - r_1} - (r_2 - r_1)\log_q(\delta_\beta), \tag{46}$$

where δ_β denotes the root-Hermite factor (see (39)).

Lemma 4 ([19]). *Let $\boldsymbol{y} = \boldsymbol{a} \cdot \mathbf{T} + \boldsymbol{x}$ with $\boldsymbol{a} \in \mathbb{Z}^n$, $\boldsymbol{x} \in \mathbb{R}^n$, and $\mathbf{T} \in M_n(\mathbb{R})$ lower triangular. If $-\mathbf{T}_{i,i}/2 \leq x_i \leq \mathbf{T}_{i,i}/2$ for all i, then $\boldsymbol{x}$ can be recovered exactly by reducing $\boldsymbol{y}$ against $\mathbf{T}$ using Babai's nearest-plane algorithm.*

Assume $\boldsymbol{u} \cdot \mathbf{T} = (\boldsymbol{g}, \boldsymbol{f}) \cdot \mathbf{Y}$ for some $\boldsymbol{u} \in \mathbb{Z}^{2N}$. Writing $\boldsymbol{u} = (\boldsymbol{u}_1 \mid \boldsymbol{u}_2)$ with $\boldsymbol{u}_1 \in \mathbb{Z}^{r_2}$ and $\boldsymbol{u}_2 \in \mathbb{Z}^{2N-r_2}$ yields

$$(\boldsymbol{u}_1 \mid \boldsymbol{u}_2) \cdot \mathbf{T} = (\boldsymbol{g}, \boldsymbol{f}) \cdot \mathbf{Y} = (\boldsymbol{s} \mid \boldsymbol{u}_2), \tag{47}$$

where $\|\boldsymbol{s}\|_\infty = \|(\boldsymbol{g}, \boldsymbol{f})\|_\infty$, since $\mathbf{Y}'$ is orthogonal. Moreover, $\boldsymbol{u}_2$ corresponds exactly to the last $2N - r_2$ coefficients of $\boldsymbol{f}$. Rearranging (47), we obtain

$$\begin{aligned} (\boldsymbol{u}_1 \mid \mathbf{0}) \cdot \mathbf{T} + (\mathbf{0} \mid \boldsymbol{u}_2) \cdot \mathbf{T} &= (\boldsymbol{s} \mid \mathbf{0}) + (\mathbf{0} \mid \boldsymbol{u}_2), \\ (\boldsymbol{u}_1 \mid \mathbf{0}) \cdot \mathbf{T} - (\boldsymbol{s} \mid \mathbf{0}) &= -(\mathbf{0} \mid \boldsymbol{u}_2) \cdot \mathbf{T} + (\mathbf{0} \mid \boldsymbol{u}_2). \end{aligned} \tag{48}$$

Hence, guessing the coefficients of $\boldsymbol{u}_2$ enables recovery of $\boldsymbol{s}$ provided that $-\mathbf{T}_{i,i}/2 \leq s_i \leq \mathbf{T}_{i,i}/2$, as guaranteed by Lemma 4. Consequently, if $\mathbf{L}'$ is reduced with blocksize β such that

$$q^{\alpha_{r_2}} \geq 2\|(\boldsymbol{g}, \boldsymbol{f})\|_\infty, \tag{49}$$

then $\boldsymbol{s}$ can be efficiently recovered. The attacker, therefore, chooses optimal parameters (r_1, r_2) to balance the cost of lattice reduction on a block of dimension $r_2 - r_1$ and the exhaustive search over the remaining $2N - r_2$ coefficients. Hence, the overall complexity of the hybrid attack is given by the maximum of these two costs.