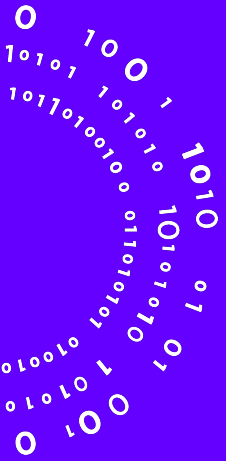


Cryptography Research Centre

Finding Dense Algebraic Submodules

Algebraic Pataki-Tural Lemma

October 2, 2025

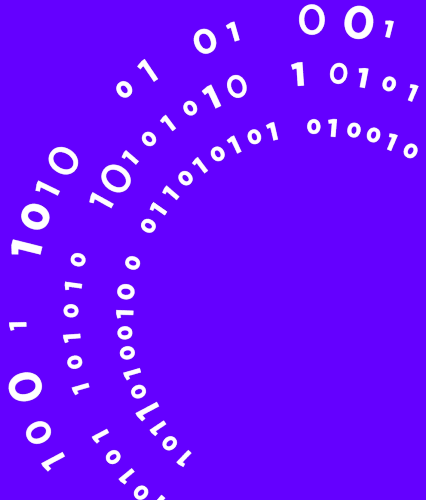
Alexander Karenin

Technology Innovation Institute

TII Technology Innovation Institute

Contents

Motivation



Lattice based crypto and attacks.

Cryptography Research Centre

- In post-quantum era PQC $>$ RSA/ECC.
- Lattice based crypto is conjectured to be postquantum.
- NTRU cryptosystem is a lattice based crypto.
- We want to study all possible attacks on NTRU.
- There is an algebraic attack on “overstretched” NTRU.

NIST PQC Standardisation

Cryptography Research Centre

FIPS 203

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Documentation Topics

Date Published: August 13, 2024

Author(s)

National Institute of Standards and Technology

Figure 1.1: Kyber

NIST PQC Standardisation

Cryptography Research Centre

FIPS 204

Module-Lattice-Based Digital Signature Standard

Documentation Topics

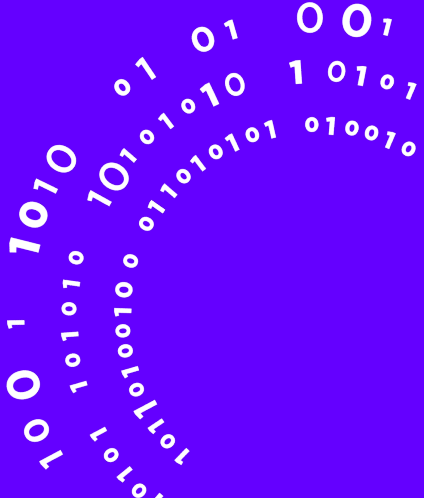
Date Published: August 13, 2024

Planning Note (10/21/2024):

We've identified two issues that will be corrected in a future update/revision of this publication. For details, see the errata (potential updates) spreadsheet listed under "Documentation."

Figure 1.1: Dilithium

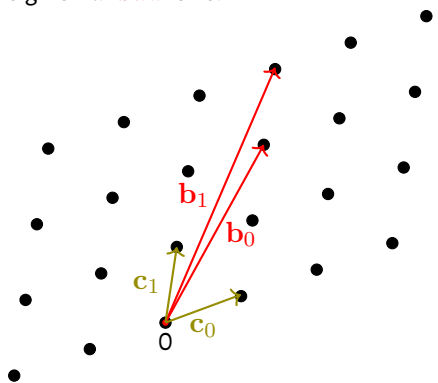
Classical lattices



Lattices: definition

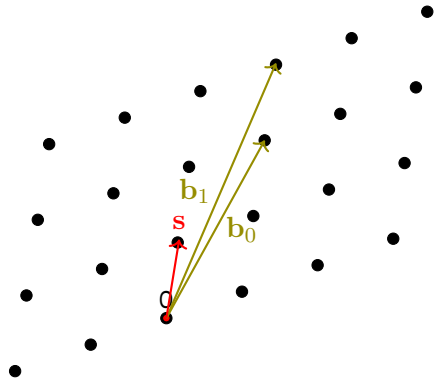
Cryptography Research Centre

- An n-dimensional lattice $\mathcal{L}$ is the a discrete additive subgroup of $\mathbb{R}^m$ given by $\bigoplus_{i=0}^{n} \mathbf{b}_i \cdot \mathbb{Z}$.
- A lattice is also a *free* $\mathbb{Z}$-module endowed with the *Euclidean* inner product.
- The matrix $\mathbf{B} = [\mathbf{b}_0 | \ldots | \mathbf{b}_{n-1}] \in \mathbb{R}^{m \times n}$ is called a lattice basis.
- Our goal: find a "good" basis given a "bad" one.



Lattices: SVP

The problem of finding a shortest nonzero vector (in Euclidean norm) $\mathbf{s} \in \mathcal{L}$ is called SVP.



Gram-Schmidt orthogonalization

Cryptography Research Centre

- The Gram matrix of $\mathbf{B}$ is defined as $\mathbf{G} = \mathbf{B}^\dagger \cdot \mathbf{B}$.
- Gram-Schmidt vectors:

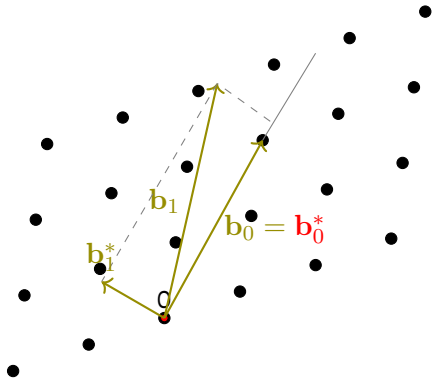
$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{k<i} \frac{\langle \mathbf{b}_i, \mathbf{b}_k^* \rangle}{\langle \mathbf{b}_k^*, \mathbf{b}_k^* \rangle} \cdot \mathbf{b}_k^* \quad \text{for } 0 \leqslant i < n. \tag{2.1}$$

- Gram-Schmidt coefficients: $r_{i,i} = \langle \mathbf{b}_i^* , \mathbf{b}_i^* \rangle \in K_{\mathbb{R}} \subset \mathbb{R}^+$, $\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\langle \mathbf{b}_j^*, \mathbf{b}_j^* \rangle}$ for $i \geqslant j$ and

$$r_{i,j} = \langle \mathbf{b}_i, \mathbf{b}_j \rangle - \sum_{k=0}^{j-1} \mu_{j,k} \cdot r_{i,k}, \; i > j. \tag{2.2}$$

Gram-Schmidt orthogonalization: example

Cryptography Research Centre



Number fields

Cryptography Research Centre

- A number field K is an extension $\mathbb{Q}(\alpha)$ for a properly chosen $\alpha \in K$.
- Such α is a solution to a polynomial equation $p(\alpha) = 0$ where $p(x)$ is monic and irreducible over $\mathbb{Q}$.
- Each $k \in K$ has such a polynomial $p_k(x)$. All $k \in K$ such that $p_k(x) \in \mathbb{Z}[x]$ form a ring of integers $\mathcal{O}_K$.
- We will focus on power-of-2 cyclotomic fields (PO2CF) defined as

$$K = \mathbb{Q}[x]/(x^d + 1),$$

  where d is a power of 2 and is called a *degree* of K.
- We pick ζ such that $\zeta^{2d} = 1$ and obtain $K = \mathbb{Q}(\zeta)$.

Number field examples

Cryptography Research Centre

- Rational field $\mathbb{Q}$.
- Cyclotomic fields $K_f = \mathbb{Q}[\zeta_f]$ where ζ_f if a primitive root of unity of degree f. Note: $K_f \cong \mathbb{Q}[x]/(\Phi_f(x))$ and $\mathcal{O}_{K_f} \cong \mathbb{Z}[x]/(\Phi_f(x))$ for $\Phi_f(x)$ – f-th cyclotomic polynomial.
- $K = \mathbb{Q}[\sqrt{5}]$. Note: corresponding $\mathcal{O}_K$ is *not* isomorphic to $\mathbb{Z}[\sqrt{5}]$ but to $\mathbb{Z}[(1+\sqrt{5})/2]$.

Number field embeddings

Cryptography Research Centre

A PO2CF K of a degree d has d complex embeddings $\sigma_0, \ldots, \sigma_{d-1}$ with $\sigma_i = \overline{\sigma}_{d/2+i}$ for $i < d/2$. We define *Minkowski embedding* of $k \in K$ as:

$$\mathcal{F}(k) = (\sigma_i)_{0 \leqslant i < d} \in \mathbb{C}^d.$$

The product of the coordinates after the Minkowski embedding $\mathcal{F}(k)$ is a rational number $\mathcal{N}(k)$ and is called *the algebraic norm* of k. Such $u \in \mathcal{O}_K$ that $\mathcal{N}(u) = \pm 1$ are called the units of K.

Number field embeddings

Cryptography Research Centre

A PO2CF K of a degree d has d complex embeddings $\sigma_0, \ldots, \sigma_{d-1}$ with $\sigma_i = \overline{\sigma}_{d/2+i}$ for $i < d/2$. We define *Minkowski embedding* of $k \in K$ as:

$$\mathcal{F}(k) = (\sigma_i)_{0 \leqslant i < d} \in \mathbb{C}^d.$$

The product of the coordinates after the Minkowski embedding $\mathcal{F}(k)$ is a rational number $\mathcal{N}(k)$ and is called *the algebraic norm* of k. Such $u \in \mathcal{O}_K$ that $\mathcal{N}(u) = \pm 1$ are called the units of K.

A *coefficient embedding* of $k = \sum_{i=0}^{d-1} \zeta^i \cdot k_i$ is:

$$\mathcal{C}(k) = (k_i)_{0 \leqslant i < d} \in \mathbb{Q}^d.$$

The NTRU problem [7]

Cryptography Research Centre

The NTRU problem is defined over an NTRU ring:

$$\mathcal{R}_q = \mathcal{O}_K/(q \cdot \mathcal{O}_K),$$

where q is prime.

- Pick $\phi, g \in \mathcal{R}_q$ where $\mathcal{C}(\phi)$ and $\mathcal{C}(g)$ are small. Set $h = \phi \cdot g^{-1}$.
- The NTRU problem is to find $\phi, g \in \mathcal{R}_q$ such that corresponding $\mathcal{C}(\phi), \mathcal{C}(g)$ are small and $h = \phi \cdot g^{-1}$.

SKR attack on NTRU [4, 5]

Cryptography Research Centre

A vector $(\phi, g)^T$ lies in the module:

$$M = \begin{pmatrix} 1 \\ h \end{pmatrix} \mathcal{O}_K \oplus \begin{pmatrix} 0 \\ q \end{pmatrix} \mathcal{O}_K$$

and is anomally short. If we embed this module in $\mathbb{R}^{2d}$, we get a lattice. Run BKZ on its basis and retrieve the secret vector!

SKR attack on NTRU: ZGSA [12]

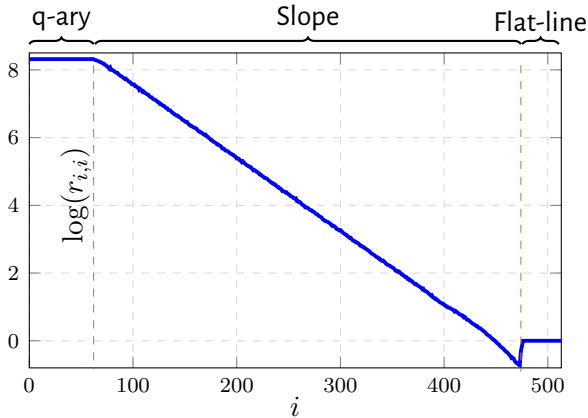


Figure 2.1: The averaged 5 profiles of the 514-dimensional NTRU lattice's bases after 8 tours of BKZ algorithm with $\beta = 76$ and approximate illustrations of both partitions.

SKR attack on NTRU: Estimation

Cryptography Research Centre

Based on ZGSA BKZ-β triggers SKR on NTRU lattice $\mathcal{L}$ of dimension $2d$ as soon as:

$$\sqrt{\beta/(2d)} \cdot \|\mathbf{v}\| < \alpha_\beta^{\beta-(d-1)/2} \cdot \det \mathcal{L},$$

where $\mathbf{v}$ is a secret vector [1]. We are interested in making β as small as possible.

SKR attack on NTRU: Estimation

Cryptography Research Centre

Based on ZGSA BKZ-β triggers SKR on NTRU lattice $\mathcal{L}$ of dimension $2d$ as soon as:

$$\sqrt{\beta/(2d)} \cdot \|\mathbf{v}\| < \alpha_\beta^{\beta-(d-1)/2} \cdot \det \mathcal{L},$$

where $\mathbf{v}$ is a secret vector [1]. We are interested in making β as small as possible.

Is this the end of story?

DSD attack on NTRU [9, 5]

Cryptography Research Centre

- Same algorithm as in the case of SKR attack.
- There are d short vectors $\zeta^i \cdot \mathbf{v}$ for $i < d$.
- If modulus q is large, BKZ outperforms estimations! All short vectors are found.
- A regime when $q \geqslant d^{2.484}$ is called *overstretched*.
- Why is this the case?

Pataki-Tural Lemma [11]. DSD estimator

Let $\mathbf{B}$ be a basis of dimension-n lattice $\mathcal{L}$. Let $\mathcal{P}$ be a rank-k sublattice of $\mathcal{L}$. Then:

$$\det \mathcal{P} \geqslant \min_{\substack{J \subset \{0,\ldots,n-1\} \\ |J|=k}} \prod_{k \in J} \|\mathbf{b}_j^*\|,$$

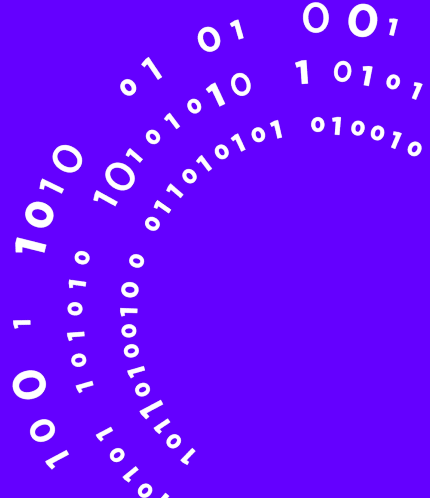
where $J \in \{0, \ldots, n-1\}$ – index set.

- The proof involves heavy usage of HNF.
- ZGSA contradicts PT when:

$$\det \mathcal{L}_{\phi,g} < q^{\frac{n'-1}{2}} \cdot \alpha_\beta^{-\frac{1}{2}(n'-1)^2},$$

where $n' = (1 + \ln q / \ln \alpha_\beta)/2$ [11]. This equation estimates DSD events.

Algebraic Pataki-Tural Lemma



Algebraic modules and lattices

Cryptography Research Centre

- A projective $\mathcal{O}_K$ module M of rank n is defined as

$$M = \mathbf{b}_0 \cdot \mathfrak{b}_0 \oplus \ldots \oplus \mathbf{b}_{n-1} \cdot \mathfrak{b}_{n-1},$$

where all $\mathbf{b}_i$'s are $K_{\mathbb{R}}$-linearly independent and $\mathfrak{b}_i$'s are fractional nonzero ideals.

Algebraic modules and lattices

Cryptography Research Centre

- A projective $\mathcal{O}_K$ module M of rank n is defined as

$$M = \mathbf{b}_0 \cdot \mathfrak{b}_0 \oplus \ldots \oplus \mathbf{b}_{n-1} \cdot \mathfrak{b}_{n-1},$$

  where all $\mathbf{b}_i$'s are $K_{\mathbb{R}}$-linearly independent and $\mathfrak{b}_i$'s are fractional nonzero ideals.
- A tuple of pairs $((\mathbf{b}_0, \mathfrak{b}_0), \ldots, (\mathbf{b}_{n-1}, \mathfrak{b}_{n-1}))$ is called a pseudobasis of M.

Algebraic modules and lattices

Cryptography Research Centre

- A projective $\mathcal{O}_K$ module M of rank n is defined as

$$M = \mathbf{b}_0 \cdot \mathfrak{b}_0 \oplus \ldots \oplus \mathbf{b}_{n-1} \cdot \mathfrak{b}_{n-1},$$

  where all $\mathbf{b}_i$'s are $K_{\mathbb{R}}$-linearly independent and $\mathfrak{b}_i$'s are fractional nonzero ideals.
- A tuple of pairs $((\mathbf{b}_0, \mathfrak{b}_0), \ldots, (\mathbf{b}_{n-1}, \mathfrak{b}_{n-1}))$ is called a pseudobasis of M.
- Define $\langle \mathbf{v} , \mathbf{u} \rangle$ for every $\mathbf{v}, \mathbf{u} \in M$ and obtain an *algebraic lattice*!

Examples

Cryptography Research Centre

- Dimension-3 lattice over $\mathbb{Q}$

$$\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \cdot \mathbb{Z} \oplus \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \cdot \mathbb{Z} \oplus \begin{pmatrix} 0 \\ -1 \\ 1/5 \end{pmatrix} \cdot \mathbb{Z}$$

- A submodule of Eisenstein integers:

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} \cdot \mathbb{Z}[\zeta_3] \oplus \begin{pmatrix} 3 \\ 4 + 5\zeta_3 \end{pmatrix} \cdot \mathbb{Z}[\zeta_3],$$

  where ζ_3 it a primitive cubic root of 1.

-

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \mathcal{O}_{K23} + \oplus \begin{pmatrix} 2 \\ 3 \end{pmatrix} \cdot \left(2 \cdot \mathcal{O}_{K23} + (z^{11} + z^9 + z^7 + z^6 + z^5 + z + 1) \cdot \mathcal{O}_{K23}\right),$$

  where K_{23} is 23-rd cyclotomic field and $z = \zeta_{23}$.

Why Algebraic?

Cryptography Research Centre

Lattice given by a (row) basis:

```
[ 5  1 -2 -2 -2  3 -1  0  1 -1  5 -4 -4  5  0  5]
[-1  5  2 -2 -3 -2  0 -1  1  1  4  5 -5 -4 -5  0]
[ 2 -2  5  1  0 -1 -2  3  4  5  1 -1 -5  0 -4  5]
[ 2  2 -1  5  1  0 -3 -2 -5  4  1  1  0 -5 -5 -4]
[ 0 -1 -2  3  5  1 -2 -2 -5  0 -4  5  1 -1  5 -4]
[ 1  0 -3 -2 -1  5  2 -2  0 -5 -5 -4  1  1  4  5]
[-3 -2  0 -1  2 -2  5  1 -5 -4 -5  0  4  5  1 -1]
[ 2 -3  1  0  2  2 -1  5  4 -5  0 -5 -5  4  1  1]
[ 4  5  2  1 -5  2  1  0  1  1  3 -3  0  1  4  1]
[-5  4 -1  2 -2 -5  0  1 -1  1  3  3 -1  0 -1  4]
[-1  2  4  5  0  1 -5  2  3  3  1  1 -1  4  0  1]
[-2 -1 -5  4 -1  0 -2 -5 -3  3 -1  1 -4 -1 -1  0]
[ 0  1 -5  2  4  5  2  1 -1  4  0  1  1  1  3 -3]
[-1  0 -2 -5 -5  4 -1  2 -4 -1 -1  0 -1  1  3  3]
[-2 -5  0  1 -1  2  4  5 -1  0 -1  4  3  3  1  1]
[ 5 -2 -1  0 -2 -1 -5  4  0 -1 -4 -1 -3  3 -1  1]
```

Can be represented with this free algebraic basis:

```
[ -2*z^6 + 3*z^5 + z^4 - z^3 - 2*z^2 - 2*z + 5 5*z^7 - 4*z^6 + 5*z^5 - z^4 + 5*z^2 - 4*z + 1]
[  z^6 + 2*z^5 + 5*z^4 + z^3 + 2*z^2 - 5*z + 4   z^7 - 3*z^6 + z^5 + z^4 + 4*z^3 + 3*z^2 + 1]
```

Working with pseudobases

Cryptography Research Centre

Definition (Lattice equivalence)

Two algebraic lattices given by $((\mathbf{a}_0, \mathfrak{a}_0), \ldots, (\mathbf{a}_{n-1}, \mathfrak{a}_{n-1}))$, $((\mathbf{b}_0, \mathfrak{b}_0), \ldots, (\mathbf{b}_{n-1}, \mathfrak{b}_{n-1}))$ are the same $\iff$ the following holds:

- $\exists \mathbf{U} \in \mathrm{GL}_K^{n \times n}$ such that $\mathbf{B} = \mathbf{A}\mathbf{U}$,
- every $\mathbf{u}_i[j] \in \mathfrak{a}_j \cdot \mathfrak{b}_i^{-1}$,
- $\mathbf{u}'_i[j] \in \mathfrak{a}_i^{-1} \cdot \mathfrak{b}_j$ for $\mathbf{u}'_i$ – columns of $\mathbf{U}' = \mathbf{U}^{-1}, 0 \leqslant i < n$.

When all ideals are $\mathcal{O}_K$ we speak of a basis $\mathbf{B}$.

Working with pseudobases

Cryptography Research Centre

Definition (Lattice equivalence)

Two algebraic lattices given by $((\mathbf{a}_0, \mathfrak{a}_0), \ldots, (\mathbf{a}_{n-1}, \mathfrak{a}_{n-1}))$, $((\mathbf{b}_0, \mathfrak{b}_0), \ldots, (\mathbf{b}_{n-1}, \mathfrak{b}_{n-1}))$ are the same $\iff$ the following holds:

- $\exists \mathbf{U} \in \mathrm{GL}_K^{n \times n}$ such that $\mathbf{B} = \mathbf{A}\mathbf{U}$,
- every $\mathbf{u}_i[j] \in \mathfrak{a}_j \cdot \mathfrak{b}_i^{-1}$,
- $\mathbf{u}'_i[j] \in \mathfrak{a}_i^{-1} \cdot \mathfrak{b}_j$ for $\mathbf{u}'_i$ – columns of $\mathbf{U}' = \mathbf{U}^{-1}, 0 \leqslant i < n$.

When all ideals are $\mathcal{O}_K$ we speak of a basis $\mathbf{B}$.

Definition (Primitive vector)

Let $\mathbf{B}$ be a basis of a free algebraic lattice. A vector $\mathbf{v}$ of that lattice with coefficients $(c_0, \ldots, c_{n-1})$ with respect to the basis $\mathbf{B}$ is said to be primitive if $\bigoplus_{0 \leqslant i < n} c_i \cdot \mathcal{O}_K = \mathcal{O}_K$.

Glossary

Cryptography Research Centre

Unstructured lattices	Algebraic lattices
$\mathbb{Z}$ and $\mathbb{Q}$	$\mathcal{O}_K$ and K
Euclidean norm $\|\mathbf{v}\|$	Algebraic norm $\mathcal{N}(\mathbf{v})$
LLL algorithm	Algebraic LLL algorithm
Log-profile	Algebraic log-profile
Basis vectors $\mathbf{b}_i$-s	Basis vectors $\mathbf{b}_i$-s and **coefficient ideals** $\mathfrak{b}_i$-s.

Table 1: The correspondence between classic and algebraic settings.

Algebraic LLL reducedness

Cryptography Research Centre

Definition (LLL reduced basis [8, 10])

A pseudobasis $(\mathbf{B}, \{\mathfrak{b}_i\}_i)$ of an algebraic lattice is said to be α-LLL reduced for some real $\alpha > 1$ if $\alpha \cdot \mathcal{N}(r_{i+1,i+1} \cdot \mathfrak{b}_{i+1}) \geqslant \mathcal{N}(r_{i,i} \cdot \mathfrak{b}_i)$.

The difference to the classical case is that we are interested in the *algebraic norm* rather than the Euclidean norm.

Algebraic ZGSA (AZGSA)

Cryptography Research Centre

Definition (AZGSA)

Let L be a number field of degree d. Let $\mathbf{B}$ be an α-LLL reduced $\mathcal{O}_L$ basis of a rank-n NTRU module for some $\alpha > 0$. Let $\mathbf{p}$ be a log-profile of $\mathbf{B}$. Then we have:

$$\mathbf{p}_i = \begin{cases} d \log q, & i \leqslant n/2 - n' \\ d \log q \cdot (1 - \frac{i - n/2 + n'}{2n'}), & n/2 - n' < i < n/2 + n' - 1 \\ 0, & i \geqslant n/2 + n' - 1, \end{cases} \tag{3.1}$$

for $n' = 1/2 + d \log d / \log \alpha$.

Algebraic ZGSA (AZGSA)

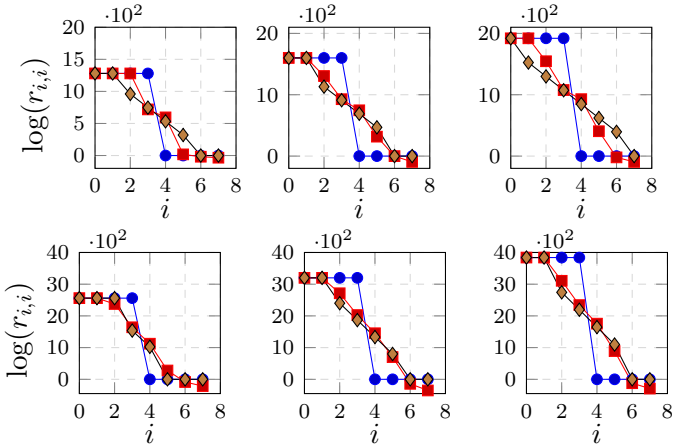


Figure 3.1: Algebraic profiles for rank-8 q-ary modules. Upper, bottom rows: conductors 64, 128. Avg. of 20 experiments. From left to right: q – primes of 20-, 25-, 30-bits. Non-reduced, reduced, AZGSA.

Algebraic Pataki-Tural lemma

Cryptography Research Centre

Theorem (Algebraic Pataki-Tural lemma, [11, Lemma 1])

Let $(\mathbf{B}, \{\mathfrak{b}_i\}_i)$ be a pseudobasis of an algebraic lattice $\mathcal{L}$ and $\mathbf{B}^*$ its Gram-Schmidt vectors. Let $\mathcal{P}$ be a rank k algebraic sublattice of $\mathcal{L}$. Then

$$\mathcal{N}(\det \mathcal{P}) \geqslant \min_{\substack{J \subset \{0,\dots,n-1\} \\ |J|=k}} \prod_{k \in J} \mathcal{N}(\mathbf{b}_j^*) \cdot \mathcal{N}(\mathfrak{b}_i).$$

Algebraic Pataki-Tural lemma

Cryptography Research Centre

Theorem (Algebraic Pataki-Tural lemma, [11, Lemma 1])

Let $(\mathbf{B}, \{\mathfrak{b}_i\}_i)$ be a pseudobasis of an algebraic lattice $\mathcal{L}$ and $\mathbf{B}^*$ its Gram-Schmidt vectors. Let $\mathcal{P}$ be a rank k algebraic sublattice of $\mathcal{L}$. Then

$$\mathcal{N}(\det \mathcal{P}) \geqslant \min_{\substack{J \subset \{0,\dots,n-1\} \\ |J|=k}} \prod_{k \in J} \mathcal{N}(\mathbf{b}_j^*) \cdot \mathcal{N}(\mathfrak{b}_i).$$

Difficulties of translating the proof:

- Ideals involved.
- We do not have HNF *for matrices* over K.

A blueprint of proof: echelon form and from sets to bases

Cryptography Research Centre

Lemma (Echelon form for matrices)

Let $\mathcal{L}$ be an algebraic lattice in K^m given by a pseudobasis $(\mathbf{B}, \{\mathfrak{b}_i\}_{i<n})$. Let $\mathcal{P}$ be rank-k algebraic sublattice. Then there exists an ordered set $\{\mathbf{y}_i\}_{i<k}$ of linearly independent vectors of $\mathcal{P}$ such that:

$$\mathbf{y}_{k-1} \in \mathbf{Span}\{\mathbf{b}_i\}_{0\leqslant i\leqslant n-1}, \ldots, \mathbf{y}_0 \in \mathbf{Span}\{\mathbf{b}_i\}_{0\leqslant i\leqslant n-k}, \text{ and}$$
$$\mathbf{y}_{k-1} \notin \mathbf{Span}\{\mathbf{b}_i\}_{0\leqslant i\leqslant n-2}, \ldots, \mathbf{y}_0 \notin \mathbf{Span}\{\mathbf{b}_i\}_{0\leqslant i\leqslant n-k-1}.$$

A blueprint of proof: echelon form and from sets to bases

Cryptography Research Centre

Lemma (Echelon form for matrices)

Let $\mathcal{L}$ be an algebraic lattice in K^m given by a pseudobasis $(\mathbf{B}, \{\mathfrak{b}_i\}_{i<n})$. Let $\mathcal{P}$ be rank-k algebraic sublattice. Then there exists an ordered set $\{\mathbf{y}_i\}_{i<k}$ of linearly independent vectors of $\mathcal{P}$ such that:

$$\mathbf{y}_{k-1} \in \mathbf{Span}\{\mathbf{b}_i\}_{0\leqslant i\leqslant n-1}, \ldots, \mathbf{y}_0 \in \mathbf{Span}\{\mathbf{b}_i\}_{0\leqslant i\leqslant n-k}, \text{ and}$$
$$\mathbf{y}_{k-1} \notin \mathbf{Span}\{\mathbf{b}_i\}_{0\leqslant i\leqslant n-2}, \ldots, \mathbf{y}_0 \notin \mathbf{Span}\{\mathbf{b}_i\}_{0\leqslant i\leqslant n-k-1}.$$

Lemma ([6, Theorem 4])

Let $\mathcal{L} \subset K^m$ be a rank-n algebraic lattice. Let $\{\mathbf{s}_i\}_i$ be a full rank set of vectors in $\mathcal{L}$. Then there exists a pseudobasis $(\mathbf{B}, \{\mathfrak{b}_i\})$ of $\mathcal{L}$ such that for all $i < n$: $\mathbf{b}_i \in \mathcal{L}, \mathbf{b}_i \in \mathbf{Span}\{\mathbf{s}_j\}_{j\leqslant i}, \mathbf{b}_i^* = \mathbf{s}_i^*$.

A blueprint of proof: sublattice basis lemma

Cryptography Research Centre

Lemma ([3, Theorem 1.2.35])

Let $\mathcal{L} \subset K^m$ be an algebraic lattice of rank n. Let $\mathcal{P}$ be its algebraic sublattice of rank $k \leqslant n$. Then there exist pseudobases $(\mathbf{X}, \{\mathfrak{x}_i\}_{i<n})$ of $\mathcal{L}$ and $((\mathbf{x}_i), \{\mathfrak{d}_i\mathfrak{x}_i\}_i)_{n-k<i<n-1}$ of $\mathcal{P}$ for some $\mathbf{X} \in K^{m\times n}$, fractional ideals $\mathfrak{x}_i$ and integral ideals $\mathfrak{d}_i$ such that:

$$\mathcal{L} = \bigoplus_{0\leqslant i<n} \mathfrak{x}_i \cdot \mathbf{x}_i \; and \; \mathcal{P} = \bigoplus_{n-k\leqslant j<n} \mathfrak{d}_j \cdot \mathfrak{x}_j \cdot \mathbf{x}_j. \tag{3.1}$$

A blueprint of proof: the proof

Cryptography Research Centre

Theorem (Algebraic Pataki-Tural lemma)

Let $(\mathbf{B}, \{\mathfrak{b}_i\}_i)$ be a pseudobasis of an algebraic lattice $\mathcal{L}$ and $\mathbf{B}^*$ its Gram-Schmidt vectors. Let $\mathcal{P}$ be a rank k algebraic sublattice of $\mathcal{L}$. Then

$$\mathcal{N}(\det \mathcal{P}) \geqslant \min_{\substack{J \subset \{0,\dots,n-1\} \\ |J|=k}} \prod_{k \in J} \mathcal{N}(\mathbf{b}_j^*) \cdot \mathcal{N}(\mathfrak{b}_i).$$

$$\mathcal{N}(\det \mathcal{P}) \geqslant \mathcal{N}(\det \mathcal{L}') \geqslant \mathcal{N}(\det(\pi_{n-k}(\mathcal{L}'))) \geqslant \min_{\substack{J \subset \{0,\dots,n-1\} \\ |J|=k}} \prod_{k \in J} \mathcal{N}(\mathbf{b}_j^*) \cdot \mathcal{N}(\mathfrak{b}_i).$$

A blueprint of proof: the proof

Cryptography Research Centre

$$\mathcal{N}(\det \mathcal{P}) \geqslant \mathcal{N}(\det \mathcal{L}') \geqslant \mathcal{N}(\det(\pi_{n-k}(\mathcal{L}'))) \geqslant \min_{\substack{J \subset \{0,\dots,n-1\} \\ |J|=k}} \prod_{k \in J} \mathcal{N}(\mathbf{b}_j^*) \cdot \mathcal{N}(\mathfrak{b}_i).$$

First, replace $\mathcal{P}$ by $\mathcal{L}'$ such that:

$$\mathcal{P} = \bigoplus_{n-k \leqslant j < n} \mathfrak{d}_j \cdot \mathfrak{x}_j \mathbf{x}_j \subset \bigoplus_{n-k \leqslant j < n} \mathfrak{x}_j \cdot \mathbf{x}_j := \mathcal{L}'$$

using the Cohen's lemma.
If the statement is true for such $\mathcal{L}'$, then it is true for all $\mathcal{P} \subseteq \mathcal{L}'$.

A blueprint of proof: the proof

Cryptography Research Centre

$$\mathcal{N}(\det \mathcal{P}) \geqslant \mathcal{N}(\det \mathcal{L}') \geqslant \mathcal{N}(\det(\pi_{n-k}(\mathcal{L}'))) \geqslant \min_{\substack{J \subset \{0,\dots,n-1\} \\ |J|=k}} \prod_{k \in J} \mathcal{N}(\mathbf{b}_j^*) \cdot \mathcal{N}(\mathfrak{b}_i).$$

Get a set $\{\mathbf{v}_\kappa\}_{\kappa<k}$ of independent vectors of $\mathcal{L}'$ using Lemma (Echelon form for matrices).

Apply (Fieker and Stehlé, 2010, Theorem 4) to $\mathcal{L}'$ and $\{\mathbf{v}_\kappa\}_{\kappa<k}$ to obtain a pseudobasis $(\mathbf{C}, (\mathfrak{c}_\kappa))$ with spans aligned:

$$\mathbf{c}_\kappa \in \mathbf{Span}\{\mathbf{v}_j\}_{j\leqslant\kappa} \subseteq \mathbf{Span}\{\mathbf{b}_j\}_{j\leqslant n-k+\kappa};\ \mathbf{c}_\kappa \notin \mathbf{Span}\{\mathbf{v}_j\}_{j<\kappa} \subseteq \mathbf{Span}\{\mathbf{b}_j\}_{j<n-k+\kappa} \quad (3.2)$$

A blueprint of proof: the proof

Cryptography Research Centre

$$\mathcal{N}(\det \mathcal{P}) \geqslant \mathcal{N}(\det \mathcal{L}') \geqslant \mathcal{N}(\det(\pi_{n-k}(\mathcal{L}'))) \geqslant \min_{\substack{J \subset \{0,\dots,n-1\} \\ |J|=k}} \prod_{k \in J} \mathcal{N}(\mathbf{b}_j^*) \cdot \mathcal{N}(\mathfrak{b}_i).$$

Now the projected lattice $\pi_{n-k}(\mathcal{L}')$ has a pseudobasis $(\pi_{n-k}(\mathbf{C}), \{\mathfrak{b}_j\}_j)$ and it holds that:

$$\pi_{n-k}(\mathcal{L}') \subseteq \pi_{n-k}(\mathcal{L}(\mathbf{B})). \tag{3.2}$$

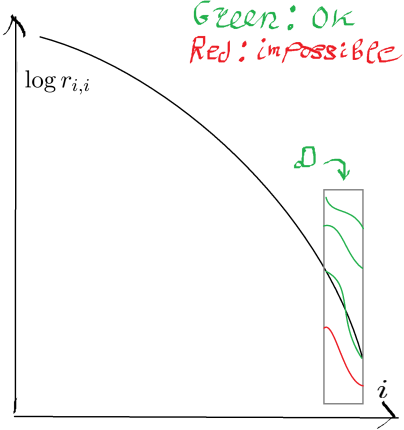
A blueprint of proof: the proof

$$\mathcal{N}(\det \mathcal{P}) \geqslant \mathcal{N}(\det \mathcal{L}') \geqslant \mathcal{N}(\det(\pi_{n-k}(\mathcal{L}'))) \geqslant \min_{\substack{J \subset \{0,\dots,n-1\} \\ |J|=k}} \prod_{k \in J} \mathcal{N}(\mathbf{b}_j^*) \cdot \mathcal{N}(\mathfrak{b}_i).$$

By (3.2) $\mathbf{D} := \pi_{n-k}(\mathbf{C})$ must be $\pi_{n-k}([\mathbf{b}_{n-\kappa}, \dots, \mathbf{b}_{n-1}]) \cdot \mathbf{U}$ for some $\mathbf{U} \in K^{n \times \kappa}$.

The transformation $\mathbf{U}$ cannot decrease the $\mathcal{N}(\det \pi_{n-k}([\mathbf{b}_{n-k}, \dots, \mathbf{b}_{n-1}]))$.

The proof is technical (studying ideals).



A blueprint of proof: the proof

Cryptography Research Centre

$$\mathcal{N}(\det \mathcal{P}) \geqslant \mathcal{N}(\det \mathcal{L}') \geqslant \mathcal{N}(\det(\pi_{n-k}(\mathcal{L}'))) \geqslant \min_{\substack{J \subset \{0,\dots,n-1\} \\ |J|=k}} \prod_{k \in J} \mathcal{N}(\mathbf{b}_j^*) \cdot \mathcal{N}(\mathfrak{b}_i)$$

The orthogonal projection cannot increase the algebraic norm of a vector:

Lemma

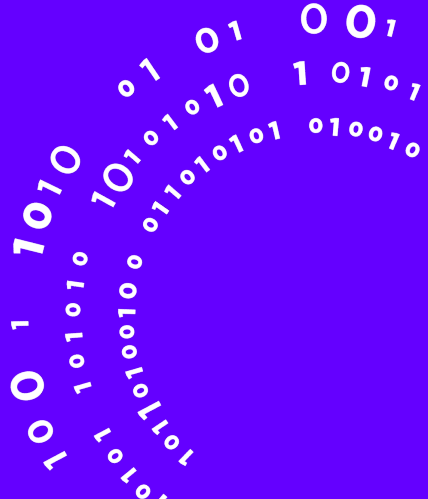
For all vectors $\mathbf{u}, \mathbf{v} \in K_{\mathbb{R}}^n$ *such that* $\mathbf{u} \perp \mathbf{v}$ *we have* $\mathcal{N}(\mathbf{u}+\mathbf{v}) \geqslant \max\{\mathcal{N}(\mathbf{u}), \mathcal{N}(\mathbf{v})\}$. *This also implies* $\mathcal{N}(\mathbf{v}) \geqslant \mathcal{N}(\pi_{\mathbf{w}}(\mathbf{v}))$ *for all* $\mathbf{w} \in K_{\mathbb{R}}^n$.

A blueprint of proof: the proof

Cryptography Research Centre

$$\mathcal{N}(\det \mathcal{P}) \geqslant \mathcal{N}(\det \mathcal{L}') \geqslant \mathcal{N}(\det(\pi_{n-k}(\mathcal{L}'))) \geqslant \min_{\substack{J \subset \{0,\ldots,n-1\} \\ |J|=k}} \prod_{k \in J} \mathcal{N}(\mathbf{b}_j^*) \cdot \mathcal{N}(\mathfrak{b}_i).$$

Algebraic DSD Attack on Overstretched NTRU



Algebraic DSD Estimator

Cryptography Research Centre

Heuristic (Condition for algebraic DSD event)

Let $\mathbf{B}$ be an α-LLL reduced basis of a rank-n algebraic NTRU module over a power-of-2 cyclotomic field L for some $\alpha > 0$. Then $\mathbf{B}$ contains a basis of a dense rank-$(n/2)$ sublattice $\mathcal{L}'$ containing $(\phi, \mathbf{g})$ as soon as:

$$\log \mathcal{N}(\det(\mathcal{L}')) < \left(\frac{n'-1}{2}\right) \log q^{\deg L} - \frac{(n'-1)^2}{2} \log \alpha \tag{4.1}$$

for $n' = 1/2 + d \log d / \log \alpha$.

Comparisons with practice

Cryptography Research Centre

Field conductor f	32	64	128
$\log q$ for classic LLL	5.95	10.4	14.85
$\log q$ for algebraic LLL	12.8	16.1	20.1

Table 2: Predicted $\log q$ sufficient to trigger a DSD event on NTRU modules: our LLL vs. classical one.

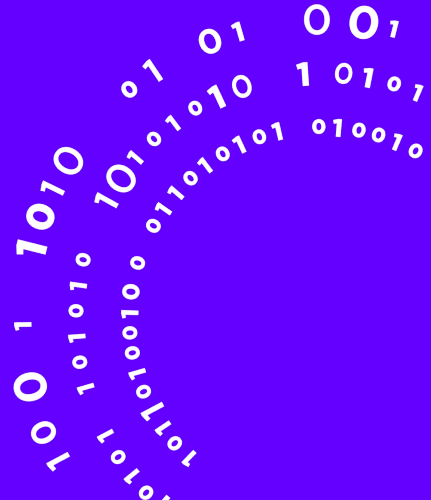
$f = 32$	
$\log_2 q$	Success rate, %
12.5	80
13.0	100
13.5	100
14.0	100
14.5	100

$f = 64$	
$\log_2 q$	Success rate, %
16.0	90
16.5	100
17.0	100
17.5	100
18.0	100

$f = 128$	
$\log_2 q$	Success rate, %
20.0	0
20.5	30
21.0	75
21.5	95
22.0	100

Table 3: Percentage of DSD events on various algebraic LLL reduced NTRU lattices.

Under the Hood: An Implementation of Algebraic LLL



Descending NTRU bases

The module $M = \mathbf{b}_0 \cdot \mathcal{O}_K + \mathbf{b}_1 \cdot \mathcal{O}_K$ decomposes over $\mathcal{O}_L$ [8] as:

$$\left(\mathbf{b}_0 \cdot \mathcal{O}_L \oplus \zeta\mathbf{b}_0 \cdot \mathcal{O}_L \oplus \ldots \oplus \zeta^{d'-1}\mathbf{b}_0 \cdot \mathcal{O}_L\right) \oplus \left(\mathbf{b}_1 \cdot \mathcal{O}_L \oplus \zeta\mathbf{b}_1 \cdot \mathcal{O}_L \oplus \ldots \oplus \zeta^{d'-1}\mathbf{b}_1 \cdot \mathcal{O}_L\right).$$

For NTRU after $\log_2 d'$ descends we have:

$$\mathbf{B}_{NTRU} = \begin{bmatrix} q & 0 & \ldots & h_0 & \zeta h_{d'-1} & \ldots & \zeta h_1 \\ 0 & q & \ldots & h_1 & h_0 & \ldots & \zeta h_2 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 1 \end{bmatrix}$$

Algebraic LLL components

1. Size reduction.
2. Unit reduction.
3. Algebraic approxSVP oracle.

Algebraic size reduction

Cryptography Research Centre

Definition (Size reduction [8])

Let K be a power-of-2 cyclotomic field of degree d. A free basis $\mathbf{B} = [\mathbf{b}_i]_{i<n} \in K^{m \times n}$ is said to be size reduced if for all $i > 0$ and $j < i$:

$$\|\mu_{i,j}\| = \|r_{i,j}/r_{j,j}\| \leqslant d/2, \tag{5.1}$$

At the i-th iteration, size reduction considers the i-th basis vector and subtracts $\lfloor \mu_{i,j} \rceil \cdot \mathbf{b}_j$ from it for all $j = i - 1, \ldots, 0$ for $\lfloor \mu_{i,j} \rceil$ – the $\mathcal{O}_K$ rounding of $\mu_{i,j}$.

Log-unit lattice

Cryptography Research Centre

- In the case of PO2CF we consider the finite group consisting of the cyclotomic units given by $\frac{\zeta^i-1}{\zeta-1}$ for all i coprime to $d = \varphi(f)$ as per [13].
- We define the log-embedding $\mathrm{Log} : K_{\mathbb{R}}^{\times} \to \mathbb{R}^d$ for some $k \in K$ as $\mathrm{Log}(k) = (\log|\sigma_0(k)|, \ldots, \log|\sigma_{d-1}(k)|)$.
- Under log-embedding units form a lattice.

Unit reduction

Cryptography Research Centre

Definition (Unit reduction [8])

A free basis $\mathbf{B} = [\mathbf{b}_i]_{i<n} \in K^{m \times n}$ is said to be unit reduced if for all $0 \leqslant i < n$:

$$||r_{i,i}||^{1/2} \leqslant 2^{O(f \log f)} \mathcal{N}(r_{i,i})^{1/d}, \tag{5.2}$$

where f is conductor of K and $d = \varphi(f)$ is the degree of K.

Unit reduction of $k \in K$ is a CVP on the log-unit lattice.
Find a unit u_i that reduces $\langle \mathbf{b}_i^* , \mathbf{b}_i^* \rangle$ and divide $\mathbf{b}_i$ by $u_i, 0 \leqslant i < n$.

Algebraic SVP

Cryptography Research Centre

- Algebraic LLL uses a dimension-2 algebraicSVP oracle.
- We descend dimension-2 algebraic lattices to $\mathbb{R}^d$ and run BKZ there. We obtain the following guarantee by returning k corresponding to the first vector of the BKZ's output:

Lemma ([8, Lemma 1])

Let K be a PO2CF. Then for all $k \in K$:

$$\mathcal{N}(k) \leqslant d^{-d/2} \cdot \|k\|^d$$

Inserting a vector into basis: issues

Cryptography Research Centre

Task: given a vector $\mathbf{v}$ with coordinates $(w_0, w_1)^T$ w.r.t. a basis $\mathbf{B} \in K^{2\times 2}$, find basis $\mathbf{C}$ of the same module where $\mathbf{C}_0 = \mathbf{v}$.

Problem: given $w_0, w_1 \in \mathcal{O}_K$ find an unimodular matrix

$$\mathbf{W} = \begin{pmatrix} w_0 & \nu \\ w_1 & \mu \end{pmatrix} \in \mathcal{O}_K^{2\times 2}.$$

Issues:

- Such ν, μ might *not exist*.
- Such ν, μ might *be large*.

Inserting a vector into the basis: Principal ideal problem

Cryptography Research Centre

Definition

Given a principal ideal $\mathfrak{a} = w_0 \cdot \mathcal{O}_K + w_1 \cdot \mathcal{O}_K$ find such $a \in K$ that $\mathfrak{a} = a \cdot \mathcal{O}_K$.

If such a exists for given w_0, w_1, then we set $w_0 := a^{-1} \cdot w_0, w_1 := a^{-1} \cdot w_1$ and, thus, $\mathbf{v} := \mathbf{v} \cdot a^{-1}$.

This makes $\mathbf{v}$ primitive and, hence, $\det \mathbf{W} = w_0 \cdot \mu + w_1 \cdot \nu = 1$ is solvable.

Inserting a vector into the basis: Bèzout equation

Cryptography Research Centre

- Given w_0 and w_1, the construction of $\mathbf{W}$ boils down to solving the Bézout equation $\mu w_o + \nu w_1 = 1$. To speed the process up we descend this equation to a subfield.

Inserting a vector into the basis: Bèzout equation

Cryptography Research Centre

- Given w_0 and w_1, the construction of $\mathbf{W}$ boils down to solving the Bézout equation $\mu w_o + \nu w_1 = 1$. To speed the process up we descend this equation to a subfield.
- Solving such equation can be performed efficiently [8].

Wrapping all up: the algebraic LLL

Cryptography Research Centre

Algorithm 1 BasicLLL

Input: $\mathbf{B} \in K^{m \times n}$ – basis matrix of a free module, $\mathbf{U} := \mathrm{Id}_n$, $\mathbf{G}$ – Gram matrix of $\mathbf{B}$, $\alpha \in \mathbb{R}$: $\alpha > \gamma_{\mathcal{N}}^{2d} 2^d \Delta_K$ – constant defining the quality of the reduction.

Output: unimodular transform $\mathbf{U}$ such that $\mathbf{B} \cdot \mathbf{U}$ is LLL-reduced.

1: **while** index i exists in Line 4 **do**
2: $\quad \mathbf{U}, \mathbf{G}, \{\mu_{i,j}\}, \{r_{i,j}\} :=$ size_reduce$(\mathbf{U}, \mathbf{G}, \{\mu_{i,j}\}, \{r_{i,j}\}, 0, n-1)$
3: $\quad \mathbf{U}, \mathbf{G}, \{\mu_{i,j}\}, \{r_{i,j}\} :=$ unit_reduce$(\mathbf{U}, \mathbf{G}, \{\mu_{i,j}\}, \{r_{i,j}\}, 0, n-1)$
4: $\quad$ Find minimal i such that $\alpha \cdot \mathcal{N}(r_{i+1,i+1}) \leqslant \mathcal{N}(r_{i,i})$
5: $\quad$ Compute Gram-Schmidt vectors $\{\mathbf{b}_\kappa^*\}_{\kappa \leqslant i}$
6: $\quad$ Find a short primitive vector $\mathbf{v}$ in $\mathbf{M}_i = [\mathbf{b}_i^*, \pi_i(\mathbf{b}_{i+1})]$
7: $\quad (w_0, w_1)^T := \mathbf{M}^{-1} \cdot \mathbf{v}$; $\mathbf{W} :=$ BezTransform(w_0, w_1)
8: $\quad$ Apply $\mathbf{W}$ to i-th and $(i+1)$-th columns of $\mathbf{U}$ and update $\mathbf{G}$ accordingly.
9: **return** $\mathbf{U}$

Measurements

Cryptography Research Centre

$\log q$	% Success	Av. Walltime, min.
	$f = 128$	
9.0	80	0.215
9.5	100	0.263
10.0	100	0.288
	$f = 256$	
13.0	85	1.6
13.2	100	1.71
13.4	100	1.68
	$f = 512$	
17.0	55	183.2
17.1	90	152.1
17.2	85	129.4
17.3	95	183.9
17.4	100	118.5
17.5	100	144.4

Table 4: Performance of our algebraic LLL on NTRU-modules over cyclotomic fields of conductor f.

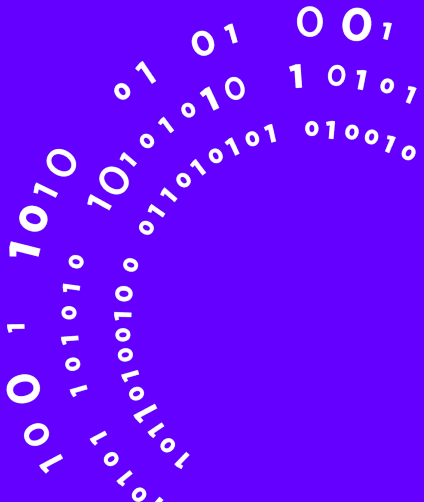
1 descend

Implementation details

Cryptography Research Centre

- We follow BKZ-2 style approach.
- We store all vectors and coefficients in FFT.
- The precomputed Log-unit lattices are stored for $4, \ldots, 1024$-th cyclotomic fields!
- We obtain projective lattices using Gram-Schmidt vectors.
- Several short vectors are outputted by BKZ and tested for insertion.
- PIP is solved with the approach by Biasse [2]. For $32, \ldots, 128$-th fields we store precomputed class group (pari gp's bnf).
- Implementation is available at `https://github.com/mooninjune/AlgebraicLLL`

Conclusion



Open problems and enhancements

Cryptography Research Centre

1. Sometimes the PIP solver fails to insert a vector.
2. Only bases supported (no pseudobases).
3. We lack a good algebraicSVP oracle.

Bases vs. pseudobases

Cryptography Research Centre

- One can always insert a vector into a pseudobasis. PIP is not needed (but shortens the vectors).
- Our algorithm can be modified to the algebraic LLL proposed in [10].

Algebraic SVP oracle

Cryptography Research Centre

- Using BKZ as an algebraic SVP oracle is likely a sub-optimal idea.
- Precision should be controlled.
- One can upgrade our algorithm to an algebraic BKZ. What about having a rank-β algebraicSVP oracle?
- Algebraic analogues to the Hermite constants and Gaussian heuristic?

References I

Cryptography Research Centre

[1] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key {Exchange—A} new hope. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 327–343, 2016.

[2] J.-F. Biasse. Subexponential time relations in the class group of large degree number fields. *Adv. Math. Commun.*, 8(4):407–425, 2014.

[3] H. Cohen. *Advanced topics in computational number theory*, volume 193. Springer Science & Business Media, 2012.

[4] D. Coppersmith and A. Shamir. Lattice attacks on NTRU. In *International conference on the theory and applications of cryptographic techniques*, pages 52–61. Springer, 1997.

[5] L. Ducas and W. P. J. van Woerden. NTRU fatigue: How stretched is overstretched? In *Advances in Cryptology - ASIACRYPT 2021*, Lecture Notes in Computer Science, pages 3–32, 2021.

References II

[6] C. Fieker and D. Stehlé. Short bases of lattices over number fields. In *Algorithmic Number Theory*, pages 157–173, 2010.

[7] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A ring-based public key cryptosystem. In J. Buhler, editor, *ANTS-III*, pages 267–288, 1998.

[8] P. Kirchner, T. Espitau, and P. Fouque. Fast reduction of algebraic lattices over cyclotomic fields. In D. Micciancio and T. Ristenpart, editors, *Advances in Cryptology - CRYPTO 2020*, pages 155–185, 2020.

[9] P. Kirchner and P. Fouque. Revisiting lattice attacks on overstretched NTRU parameters. In *Advances in Cryptology - EUROCRYPT 2017*, pages 3–26, 2017.

[10] C. Lee, A. Pellet-Mary, D. Stehlé, and A. Wallet. An LLL algorithm for module lattices. In *Advances in Cryptology – ASIACRYPT 2019*, pages 59–90, 2019.

References III

[11] G. Pataki and M. Tural. On sublattice determinants in reduced bases. *arXiv preprint arXiv:0804.4014*, 2008.

[12] C. P. Schnorr. Lattice reduction by random sampling and birthday methods. In *STACS 2003: 20th Annual Symposium on Theoretical Aspects of Computer Science Berlin, Germany, February 27–March 1, 2003 Proceedings 20*, pages 145–156. Springer, 2003.

[13] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.