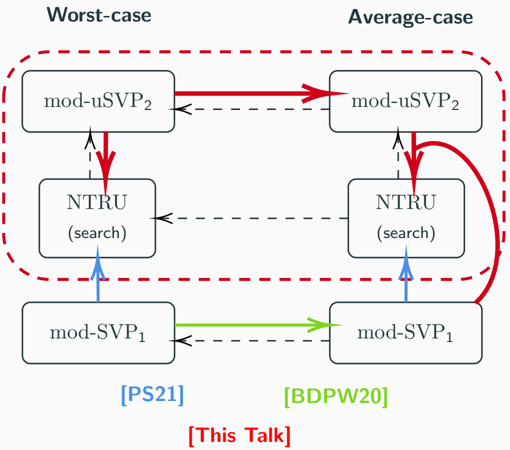
NTRU **and** $\mathrm{mod}\text{-}\mathrm{uSVP}_2$

Joël Felderhoff, Alice Pellet-Mary and Damien Stehlé

INRIA Lyon

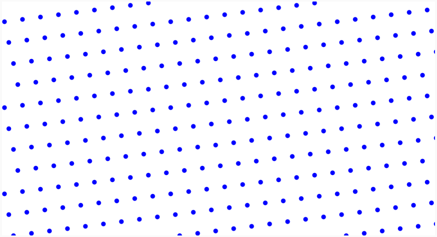
Contributions



- Reduction from $\mathrm{mod\text{-}uSVP}_2$ to NTRU.
- Random self-reduction for $\mathrm{mod\text{-}uSVP}_2$.

Definitions

Lattices



A 2-dimensional lattice

Definition

For $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Z}^n$ linearly independent, the lattice spanned by the basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is $\mathcal{L} = \sum_i \mathbb{Z} \cdot \mathbf{b}_i \subset \mathbb{R}^n$.
It is discrete and has a shortest non-zero vector.

Finding any short non-zero vector in $\mathcal{L}$ given the $(\mathbf{b}_i)_i$ is hard in general.

NTRU

We work with elements of $R = \mathbb{Z}[X]/(X^n + 1)$ for $n = 2^r$. $(R = \mathcal{O}_K)$.

The size of an element $a \in R$ is $\|a\| = \left(\sum_i |a_i|^2\right)^{1/2}$.

The size of an element is the ℓ_2-norm of its Minkowski embedding.

Definition ($NTRU_q$)

Let $f, g \in R$ with coefficients $\ll \sqrt{q}$ and f invertible mod q.
Given $h \in R$ such that $f \cdot h = g \bmod q$, find a small multiple of (f, g).

Proposed first in [HPS96].
Used in NIST's post-quantum standardization process:
NTRU and **NTRUPrime**.

Advantages:

- Small keys.
- Fast encryption/decryption (much faster than RSA).
- Old.

[HPS96]: J. Hoffstein, J. Pipher, J. Silverman. ANTS 1998.

Module of rank 2

They are lattices where $\mathbb{Z}$ becomes $R = \mathbb{Z}[X]/(X^n + 1)$.

Definition (Rank-2 module over R)

We take $\mathbf{b}_1, \mathbf{b}_2 \in R^2$. We define the module of basis $(\mathbf{b}_1, \mathbf{b}_2)$ to be

$$M = R \cdot \mathbf{b}_1 + R \cdot \mathbf{b}_2$$

Let $\mathcal{O}_K$ for a number field K. Let $\mathfrak{b}_1, \mathfrak{b}_2$ ideals of $\mathcal{O}_K$ and $\mathbf{b}_1, \mathbf{b}_2 \in R^2$. The module of pseudo-basis $(\mathfrak{b}_1, \mathbf{b}_1), (\mathfrak{b}_2, \mathbf{b}_2)$ is $M = \mathfrak{b}_1 \cdot \mathbf{b}_1 + \mathfrak{b}_2 \cdot \mathbf{b}_2$.

Difficulty

Here the security parameter is n, we work at fixed rank. Even finding short elements in Rank-1 modules is hard (Ideal-SVP).

The NTRU module

Given $h \in R$, the set of solutions for (f, g) is

$$M = \left\{(f_0, g_0)^T \in R^2, \quad f_0 \cdot h = g_0 \bmod q\right\}$$

This is a **module** spanned by:

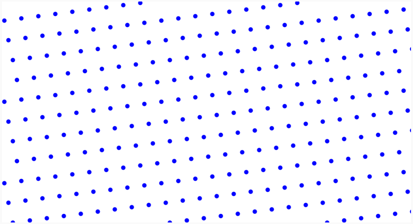
$$\mathbf{B} = \begin{pmatrix} 1 & 0 \\ h & q \end{pmatrix} \qquad \left(\mathcal{O}_K, \begin{bmatrix} 1 \\ h \end{bmatrix}\right), \left(\mathcal{O}_K, \begin{bmatrix} 0 \\ q \end{bmatrix}\right)$$

Solving NTRU is finding a short non-zero vector in M.

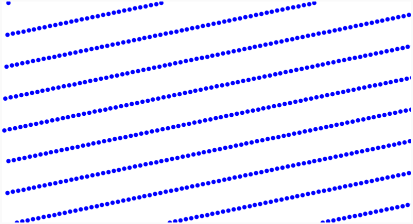
Big gap

$$\lambda_1 \leq \|(f, g)^T\| \ll \sqrt{q} \text{ versus } \lambda_2 \geq \det(\mathbf{B})/\lambda_1 \gg \sqrt{q}.$$

Rank-2 Unique-SVP



Typical lattice



$\mathrm{mod\text{-}uSVP}_2$ instance

$\mathrm{mod\text{-}SVP}_2$

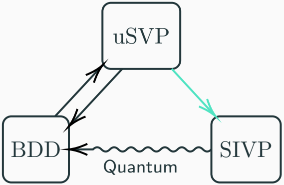
Given a basis $\mathbf{B}$ of a module $M \subset R^2$, find a short non-zero vector in it.

$\gamma\text{-}\mathrm{mod\text{-}uSVP}_2$: "generalized NTRU"

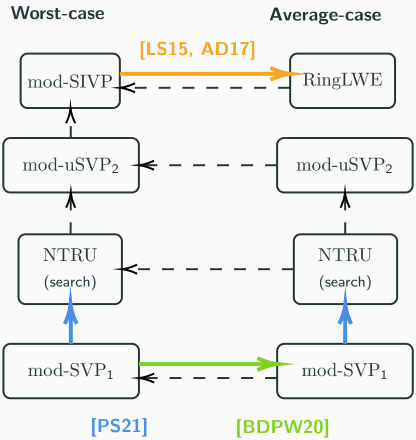
Given a basis $\mathbf{B}$ of a module $M \subset R^2$ s.t. $\lambda_1(M) \leq \sqrt{\det(M)}/\gamma$, find a short non-zero vector in it.

Prior Work

For $\mathbb{Z}$-lattices



For R-modules



[LS15]: A. Langlois, D. Stehlé. Des. Codes Cryptogr. 2015.
[AD17]: M. Albrecht, A. Deo. ASIACRYPT 2017.
[BDPW20]: K. Boer, L. Ducas, A. Pellet-Mary, B. Wesolowski. CRYPTO 2020.
[PS21]: A. Pellet-Mary, D. Stehlé. ASIACRYPT 2021.

mod-uSVP$_2$ = NTRU

Pre-HNF step

We will need that the first row spans the entire R, *i.e.*, $\gcd(b_{11}, b_{12}) = 1$.

Basis	Short vector
$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$	$\mathbf{s} = \begin{bmatrix} u \\ v \end{bmatrix}$
$(\mathbf{I} + \varepsilon) \times \downarrow$	$(\mathbf{I} + \varepsilon) \times \downarrow$
$\begin{pmatrix} b'_{11} & b'_{12} \\ b'_{21} & b'_{22} \end{pmatrix}$	$\mathbf{s}' = (\mathbf{I} + \varepsilon)\, \mathbf{s}$

We do that until $\gcd(b'_{11}, b'_{12}) = 1$. Until $\gcd(\mathfrak{b}_1 b'_{11}, \mathfrak{b}_2 b'_{12}) = \mathcal{O}_K$

It takes $O(\zeta_K(2))$ trials.

Hermite Normal Form

$$\begin{array}{cc} \mathfrak{b}_1 & \mathfrak{b}_2 \end{array}$$
$$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

Using that $\gcd(b_{11}, b_{12}) = 1$.
Using that $\gcd(\mathfrak{b}_1 b'_{11}, \mathfrak{b}_2 b'_{12}) = \mathcal{O}_K$.

$\downarrow$ $\downarrow$

$$\begin{array}{cc} \mathfrak{b}_1 & \mathfrak{b}_2 \end{array}$$
$$\begin{pmatrix} 1 & b_{12} \\ b'_{21} & b_{22} \end{pmatrix}$$

Columns operations on the basis.
$+$ Principalisation by finding shorts vectors in $\mathfrak{b}_i$.

$\downarrow$ $\downarrow$

$$\begin{array}{cc} \mathcal{O}_K & \mathcal{O}_K \end{array}$$
$$\begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix}$$

Similar to the NTRU module $\begin{array}{cc} \mathcal{O}_K & \mathcal{O}_K \end{array}$ $\begin{pmatrix} 1 & 0 \\ a & q \end{pmatrix}$

This changes neither the module nor the minimal vector. (Yes it does).

Difference with NTRU: $q \in \mathbb{Z}$ versus $b \in R$.

From the HNF to NTRU

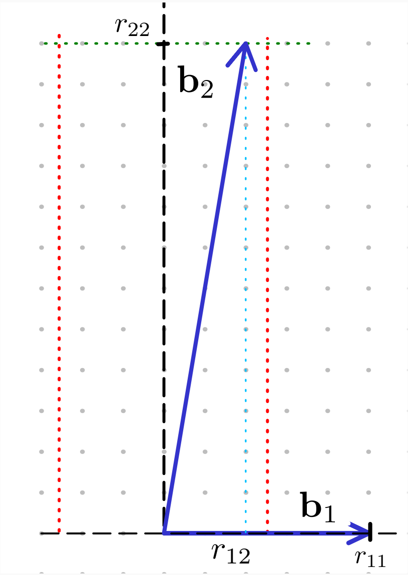
We multiply the bottom row by q/b and round.
If $q \approx b$, this does not change the geometry (much).

Basis	Short vector
$\begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix}$	$\mathbf{s} = \begin{bmatrix} u \\ v \end{bmatrix}$
$\downarrow$	$\downarrow$
$\begin{pmatrix} 1 & 0 \\ \lfloor a \cdot q/b \rceil & q \end{pmatrix}$	$\mathbf{s}' = \begin{bmatrix} u \\ v \cdot q/b - u \cdot \{a \cdot q/b\} \end{bmatrix}$

We can use an NTRU solver to solve a $\mathrm{mod\text{-}uSVP}_2$ instance!

Random Self-reducibility of mod-uSVP_2

Anatomy of a $\mathrm{mod}\text{-}\mathrm{uSVP}_2$ instance: QR factorization



Any (free) $\mathrm{mod}\text{-}\mathrm{uSVP}_2$ instance has a basis

$$\mathbf{B} = \mathbf{Q} \cdot \begin{pmatrix} r_{11} & r_{12} \\ 0 & r_{22} \end{pmatrix}$$

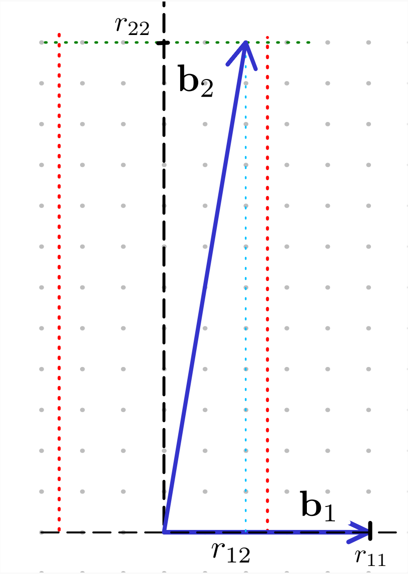
with $r_{11} \ll r_{22}$, $r_{12} \in \left(\frac{-r_{11}}{2}, \frac{r_{11}}{2}\right)$ and $\mathbf{Q}$ orthogonal.

Goal for the randomization:

- Randomize $\mathbf{Q}$.
- Randomize r_{11} and r_{22}.
- Randomize r_{12}.

Difficulty: we don't have access to the good basis.

Anatomy of a $\mathrm{mod\text{-}uSVP}_2$ instance (true version)



Any $\mathrm{mod\text{-}uSVP}_2$ instance of norm 1 and gap γ has a basis

$$\mathbf{B} = \mathbf{Q} \cdot \begin{array}{cc} \mathfrak{b}_1/\gamma & \mathfrak{b}_2 \cdot \gamma \\ \multicolumn{2}{c}{\begin{pmatrix} 1 & r_{12} \\ 0 & 1 \end{pmatrix}} \end{array}$$

with

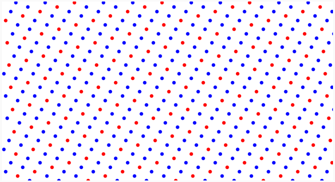
- $\mathfrak{b}_1, \mathfrak{b}_2$ (replete) ideals of norm 1.
- $r_{12} \in K \otimes \mathbb{R}$ defined modulo the ideal $\mathfrak{b}_1\mathfrak{b}_2 \cdot \gamma^{-2}$.
- $\mathbf{Q}$ orthogonal.

Randomization of r_{11} and r_{22}

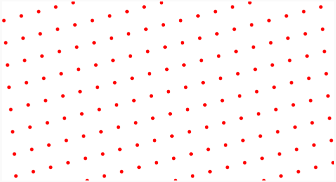
We multiply by a scalar: this changes r_{11} and r_{22} but r_{11}/r_{22} is fixed.

We multiply by a random ideal: this changes $\mathfrak{b}_1$ and $\mathfrak{b}_2$ but $\mathfrak{b}_1/\mathfrak{b}_2$ is fixed.

Solution: sparsification by a prime p (a prime ideal $\mathfrak{p}$).



$\Longrightarrow$



Sparsification by $(p, \mathbf{b}^\vee)$

For p prime and $\mathbf{b}^\vee \in M^\vee$, $M_p = \{\mathbf{m} \in M, \quad \langle \mathbf{m}, \mathbf{b}^\vee \rangle = 0 \bmod p\}$.

This multiplies the non-zero shortest vector by p with high probability: this multiplies r_{11} by p and leaves r_{22} unchanged.

Interlude: how to sample random ideals?

Let K be a number field of degree d. We denote $K_{\mathbb{R}} = K \otimes \mathbb{R}$.

Theorem ([BDPW20, Theorem 3.3])

If $\mathfrak{p}$ is uniform in the set of prime ideals of norm less than $d^{O}(d)$, $x \leftarrow \mathcal{N}_H(0, d^{-3/2})$ and $r \in K_{\mathbb{R}}$ uniform such that $|r_i| = 1$ for all i, then

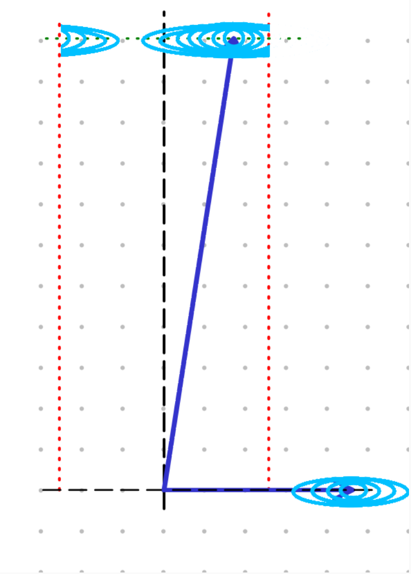
$$r \cdot \exp(x) \cdot \mathfrak{p} / \mathcal{N}^{\frac{1}{d}}(\mathfrak{p}) \simeq \mathcal{U}(\textit{ideals of norm } 1)$$

We consider the set of replete ideals of norm 1, i.e. the set of ideals times an element of $K_{\mathbb{R}}$.
H is the space of element of trace 0.

Take away: multiplying by a uniform prime (times a small element) is the same as multiplying by a uniform ideal, up to scaling.

[BDPW20]: K. de Boer, L. Ducas, A. Pellet--Mary, B. Wesolowski. CRYPTO 2020.

Randomization of r_{12}



Idea: blur the space by a gaussian $\mathbf{D}$.

$$\mathbf{D} \cdot \mathbf{Q} \sim \mathbf{D} = \mathbf{Q}' \cdot \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}.$$

Then

$$M' = \mathbf{D} \cdot M \sim \mathbf{Q}' \cdot \begin{pmatrix} r'_{11} & r'_{12} \\ 0 & r'_{22} \end{pmatrix}$$

where

$$\begin{aligned} r'_{12} =& (b + a r_{12}) \bmod r'_{11} \\ \approx& \mathrm{Unif}(R \bmod r'_{11}). \end{aligned}$$

Rounding

The "good basis" is randomized, but not the "bad" one.

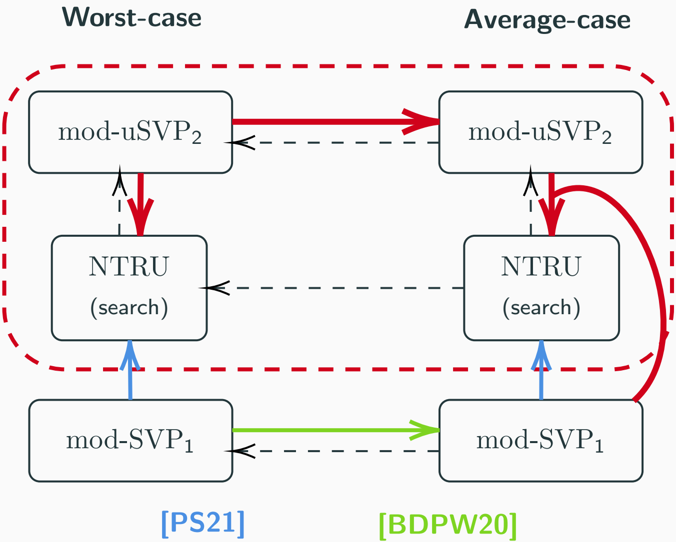
Basis	Short vector
$\begin{pmatrix} \tilde{b}_{11} & \tilde{b}_{12} \\ \tilde{b}_{21} & \tilde{b}_{22} \end{pmatrix} \in {K_{\mathbb{R}}}^{2\times 2}$	$\tilde{\mathbf{s}} = \begin{bmatrix} \tilde{u} \\ \tilde{v} \end{bmatrix}$
$(M^{\vee})^2 \ni (\lambda \mathbf{I} + \varepsilon) \times \downarrow$	$(\lambda \mathbf{I} + \varepsilon) \times \downarrow$
$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in R^{2\times 2}$	$\mathbf{s} = (\lambda \mathbf{I} + \varepsilon)\,\tilde{\mathbf{s}} \in R^2$

Then take HNF.

What did I hide?

- We work over number fields all along.
- Modules are not necessarily free (everything in grey).
- We use a $\mathrm{mod}\text{-}\mathrm{SVP}_1$-solver to take care of non-free modules.
- The HNF can take a $O(\zeta_K(2))$ running time due to the Pre-HNF step.
- Polynomial losses in approximation factors.
- The distribution analysis uses Rényi divergence and statistical distance.

Contributions



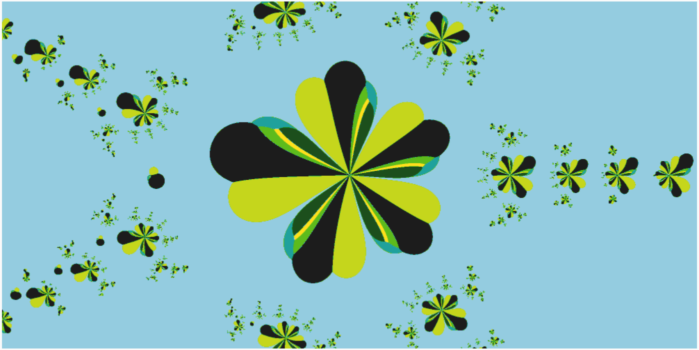
[This Talk]

Open problems

- We need a $\mathrm{mod}\text{-}\mathrm{SVP}_1$ solver to sample from our average-case distribution, can we get rid of it?
- Can we sample a NTRU instance with a trapdoor from our distribution, without a $\mathrm{mod}\text{-}\mathrm{SVP}_1$ solver?
- Composability of our reduction with the NTRU search-to-decision reduction from [PS21].
- For which K is $\zeta_K(2)$ polynomial?

Thank you for your attention

Any question?



Newton's fractal of the NTRUPrime polynomial for $p = 7$.