On mod-uSVP$_2$ and NTRU

Joël Felderhoff, Alice Pellet-Mary and Damien Stehlé

INRIA Lyon
Contributions

- Reduction from mod-uSVP\(_2\) to NTRU.
- Random self-reduction for mod-uSVP\(_1\).

NTRU and mod-uSVP\(_2\)
Definitions
We work with elements of $R = \mathbb{Z}[X]/(X^n + 1)$ for $n = 2^r$.

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

**Definition ($NTRU_q$)**

Let $f, g \in R$ with coefficients $\ll \sqrt{q}$ and $f$ invertible mod $q$.

Given $h \in R$ such that $f \cdot h = g \mod q$, find a small multiple of $(f, g)$.

**Advantages:**

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

Proposed first in [HPS96].

Used in NIST’s post-quantum standardization process: **NTRU** and **NTRUPrime**.

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

$$M = \{(f_0, g_0)^T \in R^2, \ f_0 \cdot h = g_0 \mod q\}$$

This is a “polynomial” lattice (a module) generated by the matrix

$$B = \begin{pmatrix} 1 & 0 \\ h & q \end{pmatrix}$$

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

**Big gap**

$$\lambda_1 \leq \|(f, g)^T\| \ll \sqrt{q} \text{ versus } \lambda_2 \geq \det(B)/\lambda_1 \gg \sqrt{q}.$$
Rank-2 Unique-SVP

**mod-SVP**

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

**\(\gamma\)-mod-uSVP: “generalized NTRU”**

Given a basis $B$ 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 Works

For \(\mathbb{Z}\)-lattices

- BDD
- uSVP
- SIVP

Quantum

For \(R\)-modules

For worst-case:
- mod-SIVP

For average-case:
- RingLWE

\[\text{[LS15, AD17]}\]

NTRU (search)

\[\text{mod-uSVP}_2\]

\[\text{mod-SVP}_1\]

\[\text{[PS21]}\]


Joël Felderhoff

NTRU and mod-uSVP\(_2\)
mod-uSVP_2 = NTRU
We will need that the first row spans the entire \( R \), i.e., \( \gcd(b_{11}, b_{12}) = 1 \).

<table>
<thead>
<tr>
<th>Basis</th>
<th>Short vector</th>
</tr>
</thead>
</table>
| \[
\begin{pmatrix}
  b_{11} & b_{12} \\
  b_{21} & b_{22}
\end{pmatrix}
\] | \[
\begin{pmatrix}
  u \\
  v
\end{pmatrix}
\] |
| \((I + \varepsilon) \times \downarrow\)   | \((I + \varepsilon) \times \downarrow\) |
| \[
\begin{pmatrix}
  b'_{11} & b'_{12} \\
  b'_{21} & b'_{22}
\end{pmatrix}
\] | \[
\begin{pmatrix}
  s'
\end{pmatrix}
\] = \((I + \varepsilon)s\) |

We do that until \( \gcd(b'_{11}, b'_{12}) = 1 \)

It takes \( O(\zeta_K(2)) \) trials.
Hermite Normal Form

\[
\begin{pmatrix}
  b_{11} & b_{12} \\
  b_{21} & b_{22}
\end{pmatrix}
\]

Using that \( \gcd(b_{11}, b_{12}) = 1 \).

\[
\begin{pmatrix}
  1 & b_{12} \\
  b'_{21} & b_{22}
\end{pmatrix}
\]

Columns operations on the basis.

\[
\begin{pmatrix}
  1 & 0 \\
  a & b
\end{pmatrix}
\]

Similar to the NTRU matrix

\[
\begin{pmatrix}
  1 & 0 \\
  h & q
\end{pmatrix}
\]

This changes neither the module nor the minimal vector.

**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).

<table>
<thead>
<tr>
<th>Basis</th>
<th>Short vector</th>
</tr>
</thead>
</table>
| \[
\begin{pmatrix}
1 & 0 \\
 a & b \\
\end{pmatrix}
\] | \[
\begin{pmatrix}
u \\
v \\
\end{pmatrix}
\] |
| ↓ | ↓ |
| \[
\begin{pmatrix}
1 & 0 \\
\lfloor a \cdot q/b \rfloor & q \\
\end{pmatrix}
\] | \[
\begin{pmatrix}
u \\
v \cdot q/b - u \cdot \{a \cdot q/b\} \\
\end{pmatrix}
\] |

We can use an NTRU solver to solve a mod-uSVP$_2$ instance!
Random Self-reducibility of \( \text{mod-}u\text{SVP}_2 \)
Anatomy of a mod-uSVP\textsubscript{2} instance: QR factorization

Any (free) mod-uSVP\textsubscript{2} instance has a basis

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

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

Goal for the randomization:
- Randomize \( Q \).
- Randomize \( r_{11} \) and \( r_{22} \).
- Randomize \( r_{12} \).

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

**Solution**: sparsification by a prime \( p \).

\[
\text{Sparsification by } (p, \mathbf{b}^\vee) \\
\text{For } p \text{ prime and } \mathbf{b}^\vee \in \mathcal{M}^\vee, \quad M_p = \{ \mathbf{m} \in \mathcal{M}, \quad \langle \mathbf{m}, \mathbf{b}^\vee \rangle = 0 \mod p \}. 
\]

This multiplies the non-zero shortest vector by \( p \) with high probability: this multiplies \( r_{11} \) by \( p \) and leaves \( r_{22} \) unchanged.
Randomization of $r_{12}$

Idea: blur the space by a gaussian $D$. 

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

Then 

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

where 

$$r'_{12} = (b + ar_{12}) \mod r'_{11} \approx \text{Unif}(R \mod r'_{11}).$$
Rounding

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

<table>
<thead>
<tr>
<th>Basis</th>
<th>Short vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\begin{pmatrix} \tilde{b}<em>{11} &amp; \tilde{b}</em>{12} \ \tilde{b}<em>{21} &amp; \tilde{b}</em>{22} \end{pmatrix} \in K_{\mathbb{R}}^{2 \times 2}$</td>
<td>$\tilde{s} = \begin{pmatrix} \tilde{u} \ \tilde{v} \end{pmatrix}$</td>
</tr>
</tbody>
</table>

$(M^\top)^2 \ni (\lambda I + \varepsilon) \times \downarrow$

$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in R^{2 \times 2}$

$s = (\lambda I + \varepsilon) \tilde{s} \in R^2$

Then take HNF.
What did I hide?

- We work over number fields all along.
- Modules are not necessarily free.
- We use an \( \text{mod-SVP}_1 \)-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

Worst-case

- mod-uSVP$_2$
  - NTRU (search)
  - mod-SVP$_1$

Average-case

- mod-uSVP$_2$
  - NTRU (search)
  - mod-SVP$_1$

[PS21]  [BDPW20]

[This Talk]  NTRU and mod-uSVP$_2$
Open problems

- We need a mod-SVP\(_1\) solver to sample from our average-case distribution, can we get rid of it?

- Can we construct a random NTRU instance with a trapdoor?

- Composability of our reduction with the NTRU search-to-decision reduction from [PS21].

- For which \( K \) is \( \zeta_K(2) \) polynomial?
Newton’s fractal of the NTRUPrime polynomial for $p = 7$. 

Any question?