NTRU and mod-uSVP$_2$

Joël Felderhoff, Alice Pellet–Mary and Damien Stehlé

INRIA Lyon
Contributions

Worst-case

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

\[ \text{NTRU (search)} \]

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

Average-case

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

\[ \text{NTRU (search)} \]

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

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

[PS21] [BDPW20] [This Talk]
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.

---

The NTRU module

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

Typical lattice  mod-uSVP₂ instance

**mod-SVP₂**
Given a basis $\mathbf{B}$ of a module $M \subset \mathbb{R}^2$, find a short non-zero vector in it.

**$\gamma$-mod-uSVP₂: “generalized NTRU”**
Given a basis $\mathbf{B}$ of a module $M \subset \mathbb{R}^2$ s.t. $\lambda_1(M) \leq \sqrt{\det(M)}/\gamma$, find a short non-zero vector in it.
**Prior Work**

For $\mathbb{Z}$-lattices:

- BDD
- SIVP
- uSVP
- Quantum

For $R$-modules:

**Worst-case**

- mod-SIVP
- mod-uSVP$^2$
- NTRU (search)
- mod-SVP$^1$

**Average-case**

- RingLWE
- mod-uSVP$^2$
- NTRU (search)
- mod-SVP$^1$


Joël Felderhoff

NTRU and mod-uSVP$^2$ Journées C2
mod-uSVP_2 = NTRU
Pre-HNF step

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

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

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 \( b \in \mathbb{R} \).
### 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>
| \[
\begin{pmatrix}
1 & 0 \\
\frac{a}{b} & \frac{b}{b}
\end{pmatrix}
\]
| \[
\begin{pmatrix}
s' = \\
\downarrow
\end{pmatrix}
\]
| \[
\begin{pmatrix}
1 & 0 \\
\lfloor \frac{a}{q/b} \rfloor & q
\end{pmatrix}
\]
| \[
\begin{pmatrix}
s = \\
\downarrow
\end{pmatrix}
\]

We use an NTRU solver to solve a mod-uSVP\(_2\) instance!
Random Self-reducibility of \( \text{mod-uSVP}_2 \)
Any (free) mod-uSVP$_2$ 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 $p$.

**Sparsification by** $(p, b^\vee)$

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

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

\[ r'_{12} = (b + ar_{12}) \mod r'_{11} \]

\[ \approx \text{Unif}(R \mod r'_{11}). \]
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>$(\tilde{b}<em>{11} \ \tilde{b}</em>{12}) \in K^{2 \times 2}_\mathbb{R}$</td>
<td>$\tilde{s} = \begin{bmatrix} \tilde{u} \ \tilde{v} \end{bmatrix}$</td>
</tr>
<tr>
<td>$(M^\vee)^2 \ni (\lambda I + \varepsilon) \times \downarrow$</td>
<td>$(\lambda I + \varepsilon) \times \downarrow$</td>
</tr>
<tr>
<td>$(b_{11} \ b_{12}) \in R^{2 \times 2}$</td>
<td>$s = (\lambda I + \varepsilon) \tilde{s} \in R^2$</td>
</tr>
<tr>
<td>$(b_{21} \ b_{22})$</td>
<td></td>
</tr>
</tbody>
</table>

Then take HNF.
What did I hide?

- We work over number fields all along.
- Modules are not necessarily free.
- We use an mod-$\text{SVP}_1$-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 $\text{mod-}\text{SVP}_1$ 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 $p = 7$. 