Theoretical hardness of NTRU

Alice Pellet-Mary

RISC seminar

CWI, Amsterdam

Context: NTRU

NTRU

(N-th degree truncated polynomial ring units)

- algorithmic problem based on lattices
- supposedly hard even with a quantum computer
- efficient
- used in post-quantum crypto: e.g., Falcon, NTRU and NTRUPrime
- old (for lattice-based crypto): introduced in 1996

[HPS98] Hoffstein, Pipher, and Silverman. NTRU: a ring based public key cryptosystem. ANTS.

Outline of the talk

1. Defining NTRU
2. NTRU is a module lattice problems
3. Reductions
4. Attacks
5. One open problem I like

Defining NTRU

Some definitions

If you like number fields

- $R = \mathbb{Z}[X]/(X^n + 1)$ $(n = 2^k)$
- $K = \mathbb{Q}[X]/(X^n + 1)$
- $q \in \mathbb{Z}$, $q \geq 2$
  ($q \in R$, polynomial of degree 0)
- $R_q = (\mathbb{Z}/q\mathbb{Z})[X]/(X^n + 1)$
- $\|a\| = \sqrt{\sum_i a_i^2}$ $(a = \sum_{i=0}^{n-1} a_i X^i \in R)$

(K can be any other number field)

If you don't

- $R = \mathbb{Z}$
- $K = \mathbb{Q}$
- $q \in \mathbb{Z}$, $q \geq 2$
- $R_q = \mathbb{Z}/q\mathbb{Z}$
- $\|a\| = |a|$ $(a \in R)$

Many NTRU variants

- search vs decision

Many NTRU variants

- search vs decision
- worst-case vs average case

Many NTRU variants

- search vs decision
- worst-case vs average case
- short vector vs dense sub-lattice

Many NTRU variants

- search vs decision
- worst-case vs average case
- short vector vs dense sub-lattice

In this talk: only worst-case variants (3 variants in total)

NTRU instances

NTRU instance

A γ-NTRU instance is $h \in R_q$ s.t.

- $h = f/g \bmod q$ (or $gh = f \bmod q$)
- $\|f\|, \|g\| \leq \frac{\sqrt{q}}{\gamma}$

The pair (f, g) is a trapdoor for h.

NTRU instances

NTRU instance

A γ-NTRU instance is $h \in R_q$ s.t.

- $h = f/g \bmod q$ (or $gh = f \bmod q$)
- $\|f\|, \|g\| \leq \frac{\sqrt{q}}{\gamma}$

The pair (f, g) is a trapdoor for h.

Claim: if (f, g) and (f', g') are two trapdoors for the same h,

$$\frac{f'}{g'} = \frac{f}{g} =: h_K \in K \quad \text{(division performed in K)}$$

NTRU instances

NTRU instance

A γ-NTRU instance is $h \in R_q$ s.t.

- $h = f/g \bmod q$ (or $gh = f \bmod q$)
- $\|f\|, \|g\| \le \frac{\sqrt{q}}{\gamma}$

The pair (f, g) is a trapdoor for h.

Claim: if (f, g) and (f', g') are two trapdoors for the same h,

$$\frac{f'}{g'} = \frac{f}{g} =: h_K \in K \quad \text{(division performed in K)}$$

Proof: $\frac{f}{g} = \frac{f'}{g'} \bmod q \Rightarrow fg' = f'g \bmod q \Rightarrow fg' = f'g \Rightarrow \frac{f}{g} = \frac{f'}{g'}$

Decisional NTRU problem

(worst-case) decision NTRU

The γ-decisional NTRU problem asks, given $h \in R_q$, to decide whether

- h is a γ-NTRU instance (i.e., $h = f/g \bmod q$ with $\|f\|, \|g\| \leq \sqrt{q}/\gamma$)
- or not

Search NTRU problems

$\mathrm{NTRU}_{\mathrm{vec}}$

The γ-search NTRU vector problem (γ-$\mathrm{NTRU}_{\mathrm{vec}}$) asks, given a γ-NTRU instance h, to recover $(f, g) \in R^2$ s.t.

- $h = f/g \bmod q$
- $\|f\|, \|g\| \leq \sqrt{q}/\gamma$

Search NTRU problems

$\mathrm{NTRU}_{\mathrm{vec}}$

The γ-search NTRU vector problem ($\gamma\text{-}\mathrm{NTRU}_{\mathrm{vec}}$) asks, given a γ-NTRU instance h, to recover $(f, g) \in R^2$ s.t.

- $h = f/g \bmod q$
- $\|f\|, \|g\| \leq \sqrt{q}/\gamma$

$\mathrm{NTRU}_{\mathrm{mod}}$

The γ-search NTRU module problem ($\gamma\text{-}\mathrm{NTRU}_{\mathrm{mod}}$) asks, given a γ-NTRU instance h, to recover h_K.
(Recall $h_K = f/g \in K$ for any trapdoor (f, g))
$\Leftrightarrow$ recover $(\alpha f, \alpha g)$ for any $\alpha \in K$

Remark: NTRU with large f and g

If $\|f\|, \|g\| \geq \sqrt{q} \cdot \mathrm{poly}(n)$:

- still an interesting regime (useful for crypto)
- decision-NTRU is provably hard [SS11]
- $\mathrm{NTRU}_{\mathrm{mod}}$ does not make sens anymore
- different problem from a geometric point of view

[SS11] Stehlé and Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. Eurocrypt.

Remark: NTRU with large f and g

If $\|f\|, \|g\| \geq \sqrt{q} \cdot \mathrm{poly}(n)$:

- still an interesting regime (useful for crypto)
- decision-NTRU is provably hard [SS11]
- $\mathrm{NTRU}_{\mathrm{mod}}$ does not make sens anymore
- different problem from a geometric point of view

$\rightsquigarrow$ we do not consider this regime here

[SS11] Stehlé and Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. Eurocrypt.

NTRU is a module lattice problems

Module lattices

For this talk: pretend all modules are free

(free) Module: $M = \{\sum_{i=1}^{k} x_i \cdot \boldsymbol{b}_i \mid x_i \in R\}$,
where $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_k \in K^k$ are linearly independent

Module lattices

For this talk: pretend all modules are free

(free) Module: $M = \{\sum_{i=1}^{k} x_i \cdot \boldsymbol{b}_i \mid x_i \in R\}$,
where $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_k \in K^k$ are linearly independent

Properties:

- k is the rank of M

Module lattices

For this talk: pretend all modules are free

(free) Module: $M = \{\sum_{i=1}^{k} x_i \cdot \boldsymbol{b}_i \mid x_i \in R\}$,
where $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_k \in K^k$ are linearly independent

Properties:

- k is the rank of M
- rank-1 module = ideal

Module lattices

For this talk: pretend all modules are free

(free) Module: $M = \{\sum_{i=1}^{k} x_i \cdot \boldsymbol{b}_i \mid x_i \in R\}$,
where $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_k \in K^k$ are linearly independent

Properties:

- k is the rank of M
- rank-1 module = ideal
- $\sigma(M)$ is a lattice of rank kn, where

$$\sigma : K = \mathbb{Q}[X]/(X^n + 1) \to \mathbb{Q}^n$$
$$\sum_{i=0}^{n-1} a_i X^i \mapsto (a_0, \cdots, a_{n-1})$$

$\sigma(M)$ is a module lattice

Modules with exceptionally short vectors

unique-SVP (uSVP): input is a rank-N lattice L with

$$\lambda_1(L) \ll \det(L)^{1/N}$$

Modules with exceptionally short vectors

unique-SVP (uSVP): input is a rank-N lattice L with

$$\lambda_1(L) \ll \det(L)^{1/N}$$

Special case of module: if $L = \sigma(M)$ is a module-lattice $(N = nk)$

- 1 short vector in $L \Rightarrow n$ short vectors in L

Modules with exceptionally short vectors

unique-SVP (uSVP): input is a rank-N lattice L with

$$\lambda_1(L) \ll \det(L)^{1/N}$$

Special case of module: if $L = \sigma(M)$ is a module-lattice ($N = nk$)

- 1 short vector in $L \Rightarrow n$ short vectors in L
  If $\boldsymbol{s} \in M$ is small, then $\boldsymbol{b}_i = X^i \cdot \boldsymbol{s} \in M$ satisfies
  - $\|\boldsymbol{b}_i\| = \|\boldsymbol{s}\|$
  - $\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{n-1}$ are $\mathbb{Z}$-linearly independent

Modules with exceptionally short vectors

unique-SVP (uSVP): input is a rank-N lattice L with

$$\lambda_1(L) \ll \det(L)^{1/N}$$

Special case of module: if $L = \sigma(M)$ is a module-lattice ($N = nk$)

- 1 short vector in $L \Rightarrow n$ short vectors in L
  If $\boldsymbol{s} \in M$ is small, then $\boldsymbol{b}_i = X^i \cdot \boldsymbol{s} \in M$ satisfies
  - $\|\boldsymbol{b}_i\| = \|\boldsymbol{s}\|$
  - $\boldsymbol{b}_0, \ldots, \boldsymbol{b}_{n-1}$ are $\mathbb{Z}$-linearly independent
- 1 exceptionally short vector in L
  $\Rightarrow$ an exceptionally dense rank-n sublattice (rank-1 submodule)

mod-uSVP instances (in rank 2)

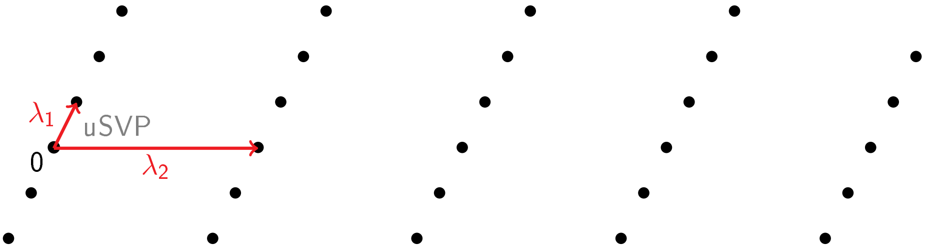
From now on: all modules have rank 2

mod-uSVP instance

A module unique SVP instance (γ-mod-uSVP) is $\boldsymbol{B} \in K^{2\times 2}$, basis of a rank-2 module M, s.t.

$$\lambda_1(M) \le 1/\gamma \cdot \det(M)^{1/(2n)}.$$

(when $K = \mathbb{Q}$)



NTRU is a mod-uSVP

NTRU lattice: For $h \in R$, define

$$\boldsymbol{B}_h = \begin{pmatrix} 1 & 0 \\ h & q \end{pmatrix} \quad \text{(in columns)}$$

h is an NTRU instance $\Leftrightarrow$ $\boldsymbol{B}_h$ is a mod-uSVP instance

NTRU is a mod-uSVP

NTRU lattice: For $h \in R$, define

$$\boldsymbol{B}_h = \begin{pmatrix} 1 & 0 \\ h & q \end{pmatrix} \quad \text{(in columns)}$$

h is an NTRU instance $\Leftrightarrow$ $\boldsymbol{B}_h$ is a mod-uSVP instance

Proof of $\Rightarrow$: assume $h = f/g \bmod q$ with $\|f\|, \|g\| \leq \sqrt{q}/\gamma$
Define M_h rank-2 module spanned by $\boldsymbol{B}_h$

- $(g, f)^T \in M_h \Rightarrow \lambda_1(M_h) \leq \sqrt{2q}/\gamma$
- $\det(M_h) = q^n \Rightarrow \det(M_h)^{1/(2n)} = \sqrt{q}$

$\Rightarrow$ $\boldsymbol{B}_h$ is a $(\gamma/\sqrt{2})$-mod-uSVP instance

NTRU is a mod-uSVP

NTRU lattice: For $h \in R$, define

$$\boldsymbol{B}_h = \begin{pmatrix} 1 & 0 \\ h & q \end{pmatrix} \quad \text{(in columns)}$$

h is an NTRU instance $\Leftrightarrow$ $\boldsymbol{B}_h$ is a mod-uSVP instance

Proof of $\Rightarrow$: assume $h = f/g \bmod q$ with $\|f\|, \|g\| \leq \sqrt{q}/\gamma$
Define M_h rank-2 module spanned by $\boldsymbol{B}_h$

- $(g, f)^T \in M_h \Rightarrow \lambda_1(M_h) \leq \sqrt{2q}/\gamma$
- $\det(M_h) = q^n \Rightarrow \det(M_h)^{1/(2n)} = \sqrt{q}$

$\Rightarrow$ $\boldsymbol{B}_h$ is a $(\gamma/\sqrt{2})$-mod-uSVP instance

Proof of $\Leftarrow$: similar, but requires a slightly more general definition of NTRU
($gh = f \bmod q$ instead of $h = f/g \bmod q$)

mod-uSVP problems

mod-uSVP$_{\mathrm{vec}}$

The γ-mod-uSVP vector problem (γ-mod-uSVP$_{\mathrm{vec}}$) asks, given a γ-mod-uSVP instance $\boldsymbol{B}$ spanning a module M, to recover $\boldsymbol{s} \in M$ s.t.

$$\|\boldsymbol{s}\| \leq 1/\gamma \cdot \det(M)^{1/(2n)}.$$

mod-uSVP problems

mod-uSVP$_{\mathrm{vec}}$

The γ-mod-uSVP vector problem (γ-mod-uSVP$_{\mathrm{vec}}$) asks, given a γ-mod-uSVP instance $\boldsymbol{B}$ spanning a module M, to recover $\boldsymbol{s} \in M$ s.t.

$$\|\boldsymbol{s}\| \leq 1/\gamma \cdot \det(M)^{1/(2n)}.$$

mod-uSVP$_{\mathrm{mod}}$

The γ-mod-uSVP module problem (γ-mod-uSVP$_{\mathrm{mod}}$) asks, given a γ-mod-uSVP instance $\boldsymbol{B}$ spanning a module M, to recover $\boldsymbol{v} \in M$ s.t.

$$\det(R \cdot \boldsymbol{v})^{1/n} \leq 1/\gamma \cdot \det(M)^{1/(2n)}.$$

($R \cdot \boldsymbol{v}$ is a dense rank-1 submodule of M)

NTRU is a mod-uSVP (2)

$\mathrm{NTRU}_{\mathrm{vec}} = \text{mod-uSVP}_{\mathrm{vec}}$ restricted to NTRU modules

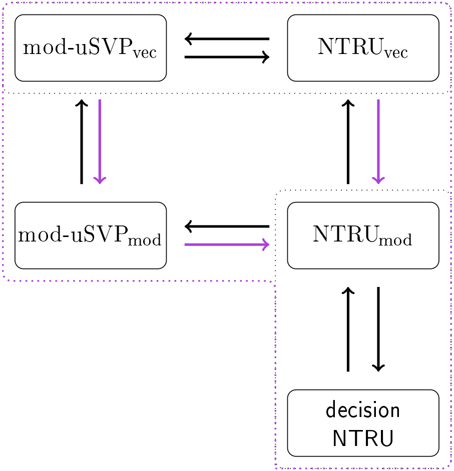
NTRU is a mod-uSVP (2)

$\boxed{\mathrm{NTRU}_{\mathrm{vec}} = \text{mod-uSVP}_{\mathrm{vec}} \text{ restricted to NTRU modules}}$

$\boxed{\mathrm{NTRU}_{\mathrm{mod}} = \text{mod-uSVP}_{\mathrm{mod}} \text{ restricted to NTRU modules}}$

Reductions

Known reductions



$\longrightarrow$ requires ideal-SVP oracle

SVP in ideal lattices

Recall: $R = \mathbb{Z}[X]/(X^n + 1)$ (or $R = \mathbb{Z}$)

(Principal) Ideals: $I = \langle z \rangle = \{zr \mid r \in R\}$

SVP in ideal lattices

Recall: $R = \mathbb{Z}[X]/(X^n + 1)$ (or $R = \mathbb{Z}$)

(Principal) Ideals: $I = \langle z \rangle = \{zr \mid r \in R\}$

ideal-SVP: Given $\langle z \rangle$, find $zr \in \langle z \rangle$ such that $\|zr\|$ is small
(recall: $\|a\| = \sqrt{\sum_i |a_i|^2}$ if $a = \sum_i a_i X^i$)

SVP in ideal lattices

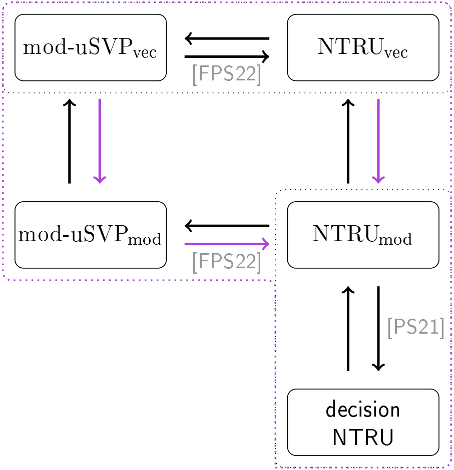
Recall: $R = \mathbb{Z}[X]/(X^n + 1)$ (or $R = \mathbb{Z}$)

(Principal) Ideals: $I = \langle z \rangle = \{zr \mid r \in R\}$

ideal-SVP: Given $\langle z \rangle$, find $zr \in \langle z \rangle$ such that $\|zr\|$ is small
(recall: $\|a\| = \sqrt{\sum_i |a_i|^2}$ if $a = \sum_i a_i X^i$)

Remark: $a|b \not\Rightarrow \|a\| \leq \|b\|$
smallness for divisibility is different from smallness for Euclidean norm

Known reductions

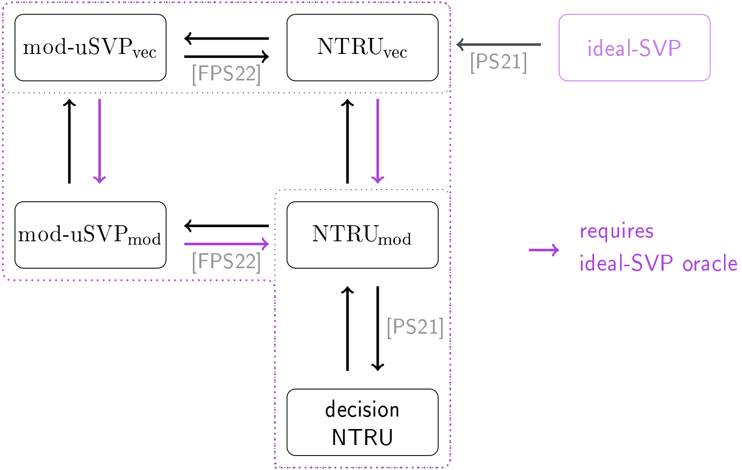


$\longrightarrow$ requires ideal-SVP oracle

[PS21] Pellet-Mary and Stehlé. On the hardness of the NTRU problem. Asiacrypt.

[FPS22] Felderhoff, Pellet-Mary, and Stehlé. On Module Unique-SVP and NTRU. Asiacrypt.

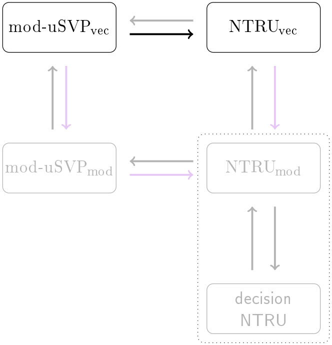
Known reductions



[PS21] Pellet-Mary and Stehlé. On the hardness of the NTRU problem. Asiacrypt.

[FPS22] Felderhoff, Pellet-Mary, and Stehlé. On Module Unique-SVP and NTRU. Asiacrypt.

Proof: from mod-uSVP$_{\text{vec}}$ to NTRU$_{\text{vec}}$



Reminder and objective

mod-uSVP$_{\text{vec}}$

find a short vector in rank 2 module generated by

$$\boldsymbol{B} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

with $b_{ij} \in R$.

NTRU$_{\text{vec}}$

find a short vector in rank 2 module generated by

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

with $h \in R$ (and $q \in \mathbb{Z}$).

In both cases, promise that there exists an exceptionally short vector

Reminder and objective

mod-uSVP$_{\text{vec}}$

find a short vector in rank 2 module generated by

$$\boldsymbol{B} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

with $b_{ij} \in R$.

NTRU$_{\text{vec}}$

find a short vector in rank 2 module generated by

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

with $h \in R$ (and $q \in \mathbb{Z}$).

In both cases, promise that there exists an exceptionally short vector

Strategy: transform input $\boldsymbol{B}$ into some $\boldsymbol{B}_h$ with $\approx$ the same geometry

Reminder and objective

$\text{mod-uSVP}_{\text{vec}}$

find a short vector in rank 2 module generated by

$$\boldsymbol{B} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

with $b_{ij} \in R$.

NTRU_{vec}

find a short vector in rank 2 module generated by

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

with $h \in R$ (and $q \in \mathbb{Z}$).

In both cases, promise that there exists an exceptionally short vector

Strategy: transform input $\boldsymbol{B}$ into some $\boldsymbol{B}_h$ with $\approx$ the same geometry

Limitation: we will use an ideal-SVP oracle

(ok because we have a reduction ideal-SVP $\to \text{NTRU}_{\text{vec}}$)

Step 1: HNF

Input: M_0	$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$	Compute the (module) HNF
	$\downarrow$	$\downarrow$
$M_1 = M_0$	$\begin{pmatrix} 1 & 0 \\ b'_{21} & b'_{22} \end{pmatrix}$	(with good probability $\gcd(b_{11}, b_{12}) = 1$)

Module unchanged $\Rightarrow$ geometry unchanged

Step 2: ideal-SVP

M_1 $\left| \begin{pmatrix} 1 & 0 \\ b'_{21} & b'_{22} \end{pmatrix} \right|$

Step 2: ideal-SVP

$$M_1 \quad \left| \begin{pmatrix} 1 & 0 \\ b'_{21} & b'_{22} \end{pmatrix} \right| \quad \begin{array}{c} \text{compute } s = r \cdot b'_{22} \text{ with } r \in R \\ \text{s.t. } s = q + \varepsilon \ (\varepsilon \in R \text{ and } \|\varepsilon\| < q/n) \end{array}$$

- requires $q \geq \det(M_1)^{1/n} \cdot \mathrm{poly}(n)$
- uses an ideal-SVP solver

Step 2: ideal-SVP

M_1	$\begin{pmatrix} 1 & 0 \\ b'_{21} & b'_{22} \end{pmatrix}$	compute $s = r \cdot b'_{22}$ with $r \in R$ s.t. $s = q + \varepsilon$ ($\varepsilon \in R$ and $\|\varepsilon\| < q/n$)
	$\downarrow$	$\downarrow$
$M_2 \subseteq M_1$	$\begin{pmatrix} 1 & 0 \\ b'_{21} & s \end{pmatrix}$	$(s \in \langle b'_{22} \rangle \Rightarrow M_2 \subseteq M_1)$

- requires $q \geq \det(M_1)^{1/n} \cdot \mathrm{poly}(n)$
- uses an ideal-SVP solver

Step 2: ideal-SVP

M_1	$\begin{pmatrix} 1 & 0 \\ b'_{21} & b'_{22} \end{pmatrix}$	compute $s = r \cdot b'_{22}$ with $r \in R$ s.t. $s = q + \varepsilon$ ($\varepsilon \in R$ and $\\|\varepsilon\\| < q/n$)
	$\downarrow$	$\downarrow$
$M_2 \subseteq M_1$	$\begin{pmatrix} 1 & 0 \\ b'_{21} & s \end{pmatrix}$	$(s \in \langle b'_{22} \rangle \Rightarrow M_2 \subseteq M_1)$

- requires $q \geq \det(M_1)^{1/n} \cdot \mathrm{poly}(n)$
- uses an ideal-SVP solver

$$\boxed{\lambda_1(M_2) \leq \lambda_1(M_1) \cdot \mathrm{poly}(n) \quad \text{and} \quad \det(M_2)^{1/(2n)} \geq \det(M_1)^{1/(2n)}}$$

(provided $q \approx \det(M_1)^{1/n}$)

Step 3: distortion

M_2	$\begin{pmatrix} 1 & 0 \\ b'_{21} & s \end{pmatrix}$	$s = q + \varepsilon \quad (\|\varepsilon\| \leq q/n)$

Step 3: distortion

M_2	$\begin{pmatrix} 1 & 0 \\ b'_{21} & s \end{pmatrix}$	$s = q + \varepsilon \quad (\|\varepsilon\| \leq q/n)$
	$\downarrow$	distort (second coordinate $\times q/s \approx 1 + \frac{1}{n}$) $\downarrow$
$M_3 \approx M_2$	$\begin{pmatrix} 1 & 0 \\ b'_{21} \cdot q/s & q \end{pmatrix}$	

Step 3: distortion

$$
\begin{array}{l|c|c}
M_2 & \begin{pmatrix} 1 & 0 \\ b'_{21} & s \end{pmatrix} & s = q + \varepsilon \quad (\|\varepsilon\| \leq q/n) \\
 & & \text{distort (second coordinate } \times q/s \approx 1 + \frac{1}{n}) \\
 & \downarrow & \downarrow \\
M_3 \approx M_2 & \begin{pmatrix} 1 & 0 \\ b'_{21} \cdot q/s & q \end{pmatrix} & \text{round} \\
 & \downarrow & \downarrow \\
M_4 \approx M_3 & \begin{pmatrix} 1 & 0 \\ \lfloor b'_{21} \cdot q/s \rceil & q \end{pmatrix} & h = \lfloor b'_{21} \cdot q/s \rceil \in R
\end{array}
$$

Step 3: distortion

M_2	$\begin{pmatrix} 1 & 0 \\ b'_{21} & s \end{pmatrix}$	$s = q + \varepsilon \quad (\|\varepsilon\| \leq q/n)$ distort (second coordinate $\times q/s \approx 1 + \frac{1}{n}$)
	$\downarrow$	$\downarrow$
$M_3 \approx M_2$	$\begin{pmatrix} 1 & 0 \\ b'_{21} \cdot q/s & q \end{pmatrix}$	round
	$\downarrow$	$\downarrow$
$M_4 \approx M_3$	$\begin{pmatrix} 1 & 0 \\ \lfloor b'_{21} \cdot q/s \rceil & q \end{pmatrix}$	$h = \lfloor b'_{21} \cdot q/s \rceil \in R$

$M_4 \approx M_2$ is still a mod-uSVP instance

$+$

$\boldsymbol{B}_4$ has NTRU shape

Attacks

Two kind of lattice attacks

We describe only attacks on decision NTRU here.

NTRU instance: $\|f\|, \|g\| \leq \sqrt{q}/\gamma =: b$

[KF17] Kirchner and Fouque. Revisiting lattice attacks on overstretched NTRU parameters. Eurocrypt

Two kind of lattice attacks

We describe only attacks on decision NTRU here.

NTRU instance: $\|f\|, \|g\| \leq \sqrt{q}/\gamma =: b$

Standard lattice attack (BKZ):

$$\text{time} \approx \exp\left(\frac{n}{\log \gamma}\right)$$

[KF17] Kirchner and Fouque. Revisiting lattice attacks on overstretched NTRU parameters. Eurocrypt

Two kind of lattice attacks

We describe only attacks on decision NTRU here.

NTRU instance: $\|f\|, \|g\| \leq \sqrt{q}/\gamma =: b$

Standard lattice attack (BKZ):

$$\text{time} \approx \exp\left(\frac{n}{\log \gamma}\right)$$

Kirchner-Fouque attack [KF17]:

$$\text{time} \approx \exp\left(\frac{n \cdot \log b}{(\log q)^2}\right)$$

[KF17] Kirchner and Fouque. Revisiting lattice attacks on overstretched NTRU parameters. Eurocrypt

Two kind of lattice attacks

We describe only attacks on decision NTRU here.

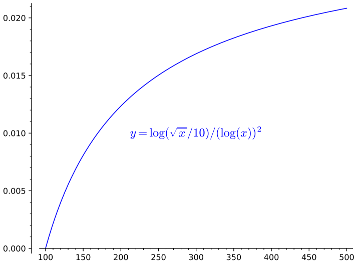
NTRU instance: $\|f\|, \|g\| \leq \sqrt{q}/\gamma =: b$

Standard lattice attack (BKZ):

$$\text{time} \approx \exp\left(\frac{n}{\log \gamma}\right)$$

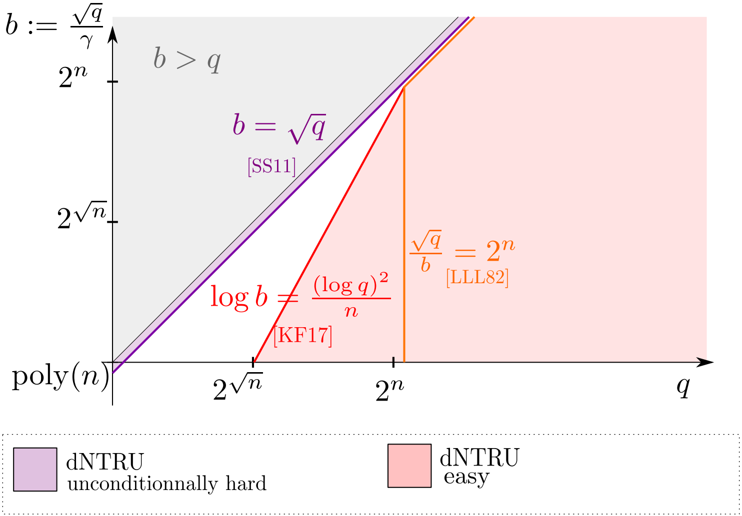
Kirchner-Fouque attack [KF17]:

$$\text{time} \approx \exp\left(\frac{n \cdot \log b}{(\log q)^2}\right)$$



[KF17] Kirchner and Fouque. Revisiting lattice attacks on overstretched NTRU parameters. Eurocrypt

Picture



$b := \frac{\sqrt{q}}{\gamma}$
$b > q$
2^n
$b = \sqrt{q}$
[SS11]
$2^{\sqrt{n}}$
$\frac{\sqrt{q}}{b} = 2^n$
[LLL82]
$\log b = \frac{(\log q)^2}{n}$
[KF17]
$\mathrm{poly}(n)$
$2^{\sqrt{n}}$
2^n
q
dNTRU
unconditionnally hard
dNTRU
easy

One open problem I like

The case of SVP

Finding short vectors in modules of rank k.

$k = 1$: can exploit S-units and do better than BKZ

$k \geq 2$: do not know how to do (significantly) better than BKZ

The case of SVP

Finding short vectors in modules of rank k.

$k = 1$: can exploit S-units and do better than BKZ

$k \geq 2$: do not know how to do (significantly) better than BKZ

$\boxed{\text{Ideals may be weaker than modules of rank } k \geq 2}$

The case of uSVP

Solving uSVP in modules of rank k

$k = 1$: does not make sens

The case of uSVP

Solving uSVP in modules of rank k

$k = 1$: does not make sens

$k = 2$: Kirchner-Fouque-like attacks $\rightsquigarrow$ better than BKZ (?)

The case of uSVP

Solving uSVP in modules of rank k

$k = 1$: does not make sens

$k = 2$: Kirchner-Fouque-like attacks $\rightsquigarrow$ better than BKZ (?)

$k = 3$: nothing (significantly) better than BKZ (?)

- RLWE reduces to uSVP in modules of rank 3

The case of uSVP

Solving uSVP in modules of rank k

$k = 1$: does not make sens

$k = 2$: Kirchner-Fouque-like attacks $\rightsquigarrow$ better than BKZ (?)

$k = 3$: nothing (significantly) better than BKZ (?)

- RLWE reduces to uSVP in modules of rank 3

Can we relate uSVP in rank k to SVP in rank $k - 1$?

The case of uSVP

Solving uSVP in modules of rank k

$k = 1$: does not make sens

$k = 2$: Kirchner-Fouque-like attacks $\rightsquigarrow$ better than BKZ (?)

$k = 3$: nothing (significantly) better than BKZ (?)

- RLWE reduces to uSVP in modules of rank 3

Can we relate uSVP in rank k to SVP in rank $k - 1$?

Thank you