On the hardness of the NTRU problem

Alice Pellet-Mary[1] and Damien Stehlé[2]

[1] Université de Bordeaux, [2] ENS de Lyon

Student seminar
CWI

NTRU

Definition (informal)

An NTRU instance is

$$h = f \cdot g^{-1} \bmod q,$$

where $f, g \in \mathbb{Z}$ and $|f|, |g| \ll \sqrt{q}$.

Decision-NTRU: Is $h = f \cdot g^{-1} \bmod q$ or not?

Search-NTRU: Recover (f, g) from h.

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

NTRU

Definition (informal)

An NTRU instance is

$$h = f \cdot g^{-1} \bmod q,$$

where $f, g \in \mathbb{Z}$ and $|f|, |g| \ll \sqrt{q}$.

Decision-NTRU: Is $h = f \cdot g^{-1} \bmod q$ or not?

Search-NTRU: Recover (f, g) from h.

- post-quantum assumption
- efficient
- used in Falcon and NTRU / NTRUPrime (NIST finalists)

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

RLWE

Definition (informal)

A RLWE instance is

$$(a_i, b_i = a_i \cdot s + e_i \bmod q)_{1 \leq i \leq m},$$

with a uniform in $\mathbb{Z}/(q\mathbb{Z})$ and $s, e \in \mathbb{Z}$ such that $|s|, |e| \ll \sqrt{q}$.

Decision-RLWE: Are $b_i = a_i \cdot s + e_i \bmod q$ or not?

Search-RLWE: Recover s from $(a_i, b_i)_i$.

[SSTX09] Stehlé, Steinfeld, Tanaka, and Xagawa. Efficient public key encryption based on ideal lattices. Asiacrypt.

[LPR10] Lyubashevsky, Peikert, and Regev. On ideal lattices and learning with errors over rings. Eurocrypt.

RLWE

Definition (informal)

A RLWE instance is

$$(a_i, b_i = a_i \cdot s + e_i \bmod q)_{1 \leq i \leq m},$$

with a uniform in $\mathbb{Z}/(q\mathbb{Z})$ and $s, e \in \mathbb{Z}$ such that $|s|, |e| \ll \sqrt{q}$.

Decision-RLWE: Are $b_i = a_i \cdot s + e_i \bmod q$ or not?

Search-RLWE: Recover s from $(a_i, b_i)_i$.

- post-quantum assumption
- efficient
- used in Kyber, Dilithium and Saber (NIST finalists)
  (more precisely, they use module-LWE)

[SSTX09] Stehlé, Steinfeld, Tanaka, and Xagawa. Efficient public key encryption based on ideal lattices. Asiacrypt.

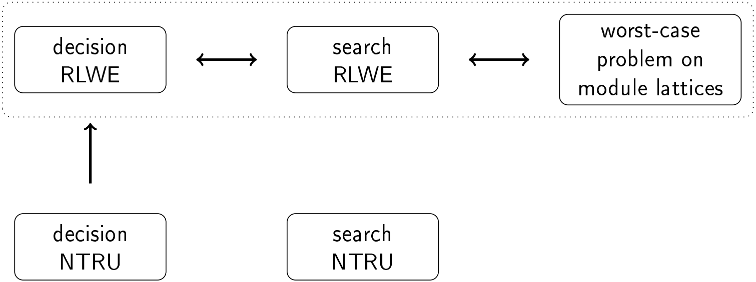
[LPR10] Lyubashevsky, Peikert, and Regev. On ideal lattices and learning with errors over rings. Eurocrypt.

NTRU vs RLWE

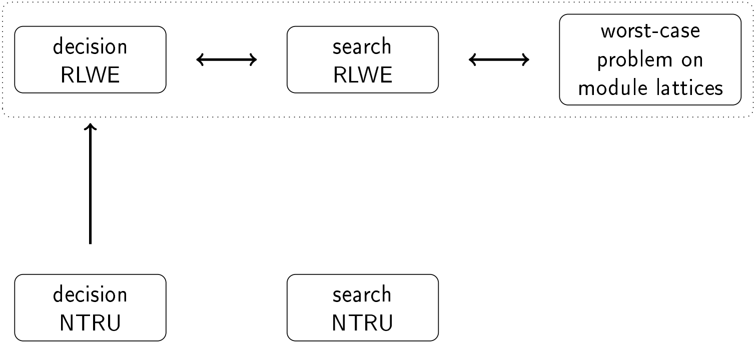
- both are efficient
- both are versatile

NTRU vs RLWE

- both are efficient
- both are versatile
- RLWE has better security guarantees

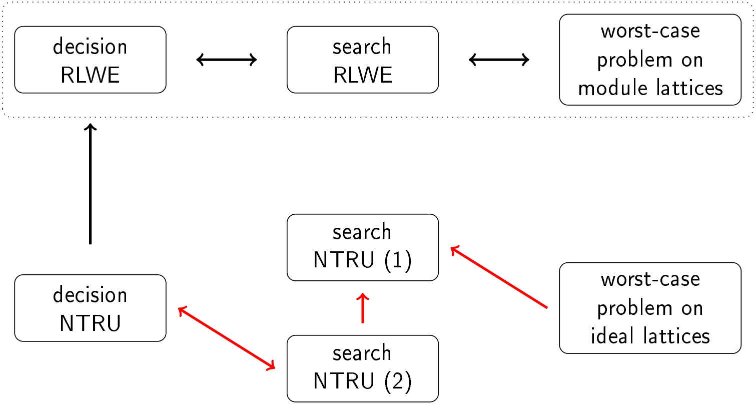


Our result



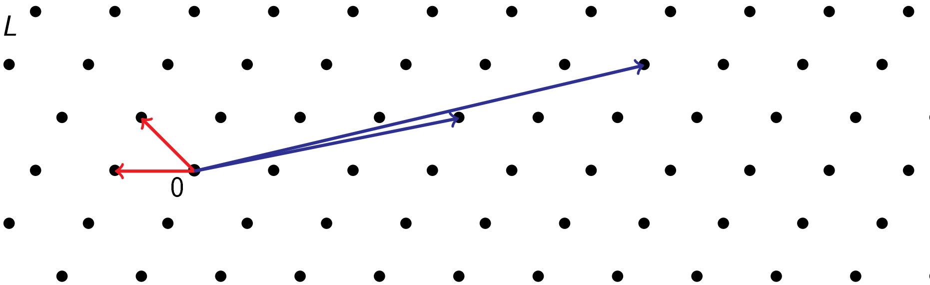
decision RLWE
search RLWE
worst-case problem on module lattices
decision NTRU
search NTRU

Our result


decision RLWE
search RLWE
worst-case problem on module lattices
search NTRU (1)
decision NTRU
worst-case problem on ideal lattices
search NTRU (2)

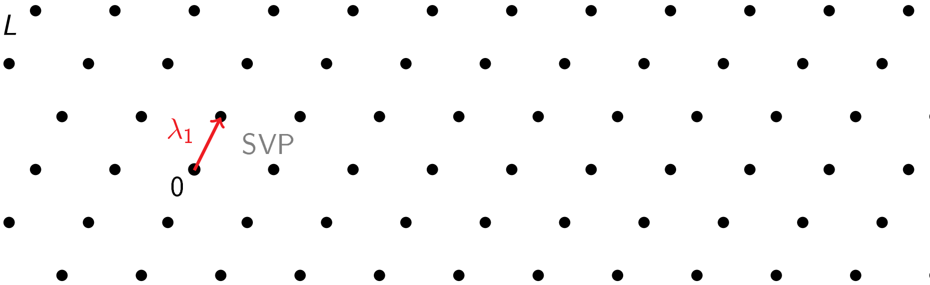
Lattices and ideals

Lattices



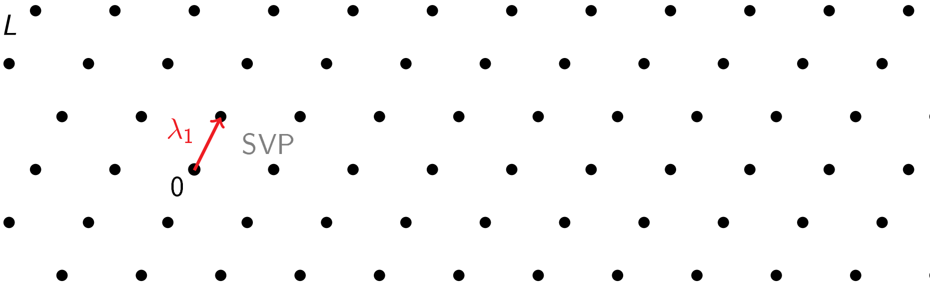
- $L = \{Bx \mid x \in \mathbb{Z}^n\}$ is a lattice
- $B \in \mathrm{GL}_n(\mathbb{R})$ is a basis
- n is the dimension of L

Shortest vector problem



SVP : Shortest Vector Problem

Shortest vector problem



SVP : Shortest Vector Problem

Supposedly hard to solve when n is large

- even with a quantum computer
- even with a small approximation factor $(\mathrm{poly}(n))$

Ideal lattices

- $R = \mathbb{Z}[X]/(X^n + 1)$ with $n = 2^k$ (or $R = \mathbb{Z}$)
- $K = \mathbb{Q}[X]/(X^n + 1)$ (or $K = \mathbb{Q}$)

Ideal lattices

- $R = \mathbb{Z}[X]/(X^n + 1)$ with $n = 2^k$ (or $R = \mathbb{Z}$)
- $K = \mathbb{Q}[X]/(X^n + 1)$ (or $K = \mathbb{Q}$)

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

(e.g., $\langle 2 \rangle = \{2x \mid x \in \mathbb{Z}\}$)

Ideal lattices

- $R = \mathbb{Z}[X]/(X^n + 1)$ with $n = 2^k$ (or $R = \mathbb{Z}$)
- $K = \mathbb{Q}[X]/(X^n + 1)$ (or $K = \mathbb{Q}$)

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

(e.g., $\langle 2 \rangle = \{2x \mid x \in \mathbb{Z}\}$)

Embedding:

$$\begin{aligned} \sigma : \quad K = \mathbb{Q}[X]/(X^n + 1) &\rightarrow \mathbb{Q}^n \\ r = \sum_{i=0}^{n-1} r_i X^i &\mapsto (r_0, \cdots, r_{n-1}) \end{aligned}$$

Ideal lattices

- $R = \mathbb{Z}[X]/(X^n+1)$ with $n = 2^k$ (or $R = \mathbb{Z}$)
- $K = \mathbb{Q}[X]/(X^n+1)$ (or $K = \mathbb{Q}$)

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

(e.g., $\langle 2 \rangle = \{2x \mid x \in \mathbb{Z}\}$)

Embedding:

$$\begin{aligned} \sigma : \quad K = \mathbb{Q}[X]/(X^n+1) &\to \mathbb{Q}^n \\ r = \sum_{i=0}^{n-1} r_i X^i &\mapsto (r_0, \cdots, r_{n-1}) \end{aligned}$$

Ideal lattice: $\sigma(\langle z \rangle) \subset \mathbb{Q}^n$ is a lattice

$\sigma(\langle 2 \rangle) \subset \mathbb{Q}$

Ideal lattices

- $R = \mathbb{Z}[X]/(X^n + 1)$ with $n = 2^k$ (or $R = \mathbb{Z}$)
- $K = \mathbb{Q}[X]/(X^n + 1)$ (or $K = \mathbb{Q}$)

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

(e.g., $\langle 2 \rangle = \{2x \mid x \in \mathbb{Z}\}$)

Embedding:

$$\sigma : \quad K = \mathbb{Q}[X]/(X^n+1) \to \mathbb{Q}^n$$

$$r = \sum_{i=0}^{n-1} r_i X^i \mapsto (r_0, \cdots, r_{n-1})$$

Ideal lattice: $\sigma(\langle z \rangle) \subset \mathbb{Q}^n$ is a lattice

ideal-SVP: Given $\langle z \rangle$, find $rz \in \langle z \rangle$ such that $\|\sigma(rz)\|$ is small

The different NTRU problems

NTRU instances

$R_q := R/(qR)$

NTRU instance

A (γ, q)-NTRU instance is $h \in R_q$ s.t.

- $h = f/g \bmod q$ (or $gh = f \bmod q$)
- $\|f\|, \|g\| \leq \frac{\sqrt{q}}{\gamma}$ (if $y = \sum_{i=0}^{n-1} y_i X^i \in R$, then $\|y\| = \sqrt{\sum_i y_i^2}$)

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

NTRU instances

$R_q := R/(qR)$

NTRU instance

A (γ, q)-NTRU instance is $h \in R_q$ s.t.

- $h = f/g \bmod q$ (or $gh = f \bmod q$)
- $\|f\|, \|g\| \leq \frac{\sqrt{q}}{\gamma}$ (if $y = \sum_{i=0}^{n-1} y_i X^i \in R$, then $\|y\| = \sqrt{\sum_i y_i^2}$)

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

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

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

Decisional NTRU problem

dNTRU

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

- $h \leftarrow \mathcal{D}$ where $\mathcal{D}$ is a distribution over (γ, q)-NTRU instances
- $h \leftarrow \mathcal{U}(R_q)$

Search NTRU problems

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

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

(The two problems exist in worst-case and average-case variants)

NTRU is a (module) lattice problem

NTRU lattice

The NTRU (module) lattice associated to an NTRU instance h is

$$\Lambda(h) = \{(g', f')^T \in R^2 \mid g'h = f' \bmod q\}.$$

Fact: $\Lambda(h)$ has basis $B_h = \begin{pmatrix} 1 & 0 \\ h & q \end{pmatrix}$ (in columns)

NTRU is a (module) lattice problem

NTRU lattice

The NTRU (module) lattice associated to an NTRU instance h is

$$\Lambda(h) = \{(g', f')^T \in R^2 \mid g'h = f' \bmod q\}.$$

Fact: $\Lambda(h)$ has basis $B_h = \begin{pmatrix} 1 & 0 \\ h & q \end{pmatrix}$ (in columns)

- Gaussian heuristic: $\lambda_1(\Lambda(h)) \approx \sqrt{q}$ (if $h \leftarrow \mathcal{U}(R_q)$)

NTRU is a (module) lattice problem

NTRU lattice

The NTRU (module) lattice associated to an NTRU instance h is

$$\Lambda(h) = \{(g', f')^T \in R^2 \mid g'h = f' \bmod q\}.$$

Fact: $\Lambda(h)$ has basis $B_h = \begin{pmatrix} 1 & 0 \\ h & q \end{pmatrix}$ (in columns)

- Gaussian heuristic: $\lambda_1(\Lambda(h)) \approx \sqrt{q}$ (if $h \leftarrow \mathcal{U}(R_q)$)
- $\Lambda(h)$ has an unexpectedly short vector $\leq \sqrt{q}/\gamma$
  - $\mathrm{NTRU}_{\mathrm{vec}}$ asks to recover (a short multiple of) the short vector

NTRU is a (module) lattice problem

NTRU lattice

The NTRU (module) lattice associated to an NTRU instance h is

$$\Lambda(h) = \{(g', f')^T \in R^2 \mid g'h = f' \bmod q\}.$$

Fact: $\Lambda(h)$ has basis $B_h = \begin{pmatrix} 1 & 0 \\ h & q \end{pmatrix}$ (in columns)

- Gaussian heuristic: $\lambda_1(\Lambda(h)) \approx \sqrt{q}$ (if $h \leftarrow \mathcal{U}(R_q)$)
- $\Lambda(h)$ has an unexpectedly short vector $\leq \sqrt{q}/\gamma$
  - $\mathrm{NTRU}_{\mathrm{vec}}$ asks to recover (a short multiple of) the short vector
- $\Lambda(h)$ has an unexpectedly dense sub-lattice $\mathrm{Span}((g, f)^T)$
  - $\mathrm{NTRU}_{\mathrm{mod}}$ asks to recover the dense sub-lattice

What we know about NTRU

Previous works

Reductions:

[SS11, WW18] If $f, g \leftarrow D_{R,\sigma}$ with $\sigma \geq \mathrm{poly}(n) \cdot \sqrt{q}$
then $f/g \approx \mathcal{U}(R_q)$ (cyclotomic fields)

- dNTRU is provably hard when $\gamma \leq \frac{1}{\mathrm{poly}(n)}$

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

[WW18] Wang and Wang. Provably secure NTRUEncrypt over any cyclotomic field. SAC.

Previous works

Reductions:

[SS11, WW18] If $f, g \leftarrow D_{R,\sigma}$ with $\sigma \geq \mathrm{poly}(n) \cdot \sqrt{q}$
then $f/g \approx \mathcal{U}(R_q)$ (cyclotomic fields)

- dNTRU is provably hard when $\gamma \leq \frac{1}{\mathrm{poly}(n)}$

[Pei16] $\mathrm{dNTRU} \leq$ RLWE

[Pei16] Peikert. A decade of lattice cryptography. Foundations and Trends in TCS.

Previous works

Reductions:

[SS11, WW18] If $f, g \leftarrow D_{R,\sigma}$ with $\sigma \geq \mathrm{poly}(n) \cdot \sqrt{q}$
then $f/g \approx \mathcal{U}(R_q)$ (cyclotomic fields)

- dNTRU is provably hard when $\gamma \leq \frac{1}{\mathrm{poly}(n)}$

[Pei16] $\mathrm{dNTRU} \leq$ RLWE

Attacks: (polynomial time)

[LLL82] dNTRU, $\mathrm{NTRU}_{\mathrm{mod}}$ broken if $\gamma \geq 2^n$

[LLL82] Lenstra, Lenstra, Lovász. Factoring polynomials with rational coefficients. Mathematische Annalen.

Previous works

Reductions:

[SS11, WW18] If $f, g \leftarrow D_{R,\sigma}$ with $\sigma \geq \mathrm{poly}(n) \cdot \sqrt{q}$
then $f/g \approx \mathcal{U}(R_q)$ (cyclotomic fields)

- dNTRU is provably hard when $\gamma \leq \frac{1}{\mathrm{poly}(n)}$

[Pei16] $\mathrm{dNTRU} \leq$ RLWE

Attacks: (polynomial time)

[LLL82] dNTRU, $\mathrm{NTRU}_{\mathrm{mod}}$ broken if $\gamma \geq 2^n$

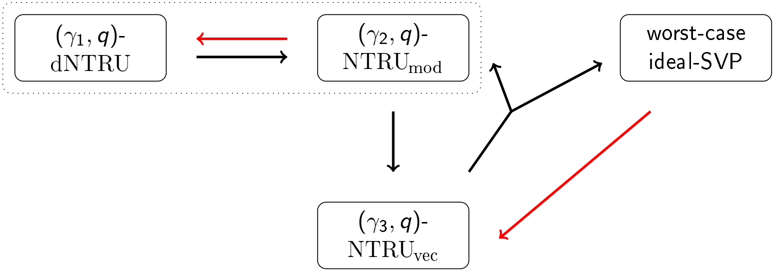
[ABD16, CLJ16] [KF17] dNTRU, $\mathrm{NTRU}_{\mathrm{mod}}$ broken if $(\log q)^2 \geq n \cdot \log \frac{\sqrt{q}}{\gamma}$
(e.g., $q \approx 2^{\sqrt{n}}$ and $\gamma = \sqrt{q}/\mathrm{poly}(n)$)

[ABD16] Albrecht, Bai, and Ducas. A subfield lattice attack on overstretched NTRU assumptions. Crypto.

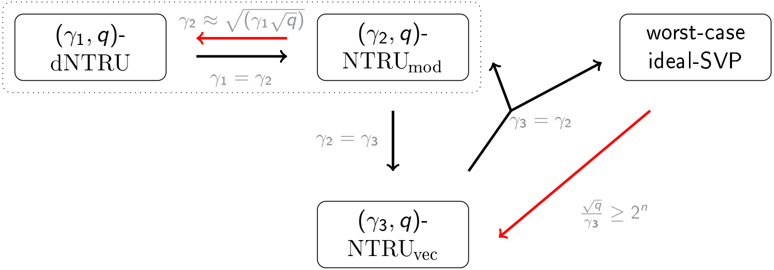
[CJL16] Cheon, Jeong, and Lee. An algorithm for NTRU problems. LMS J Comput Math.

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

Our results (with more details)



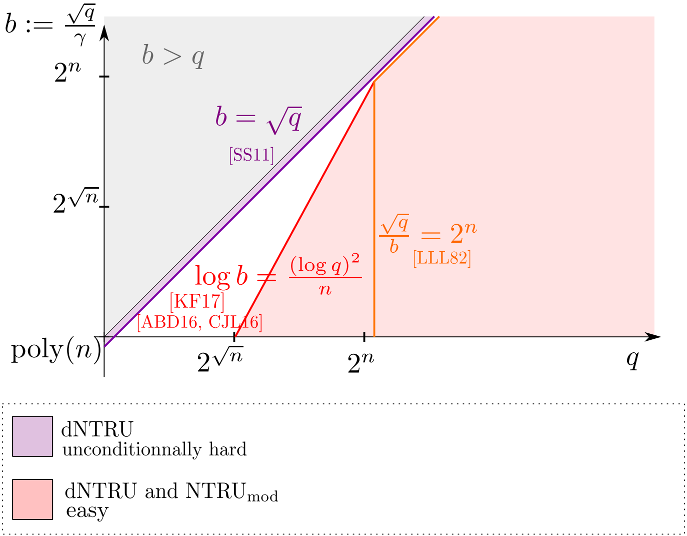
Our results (with more details)



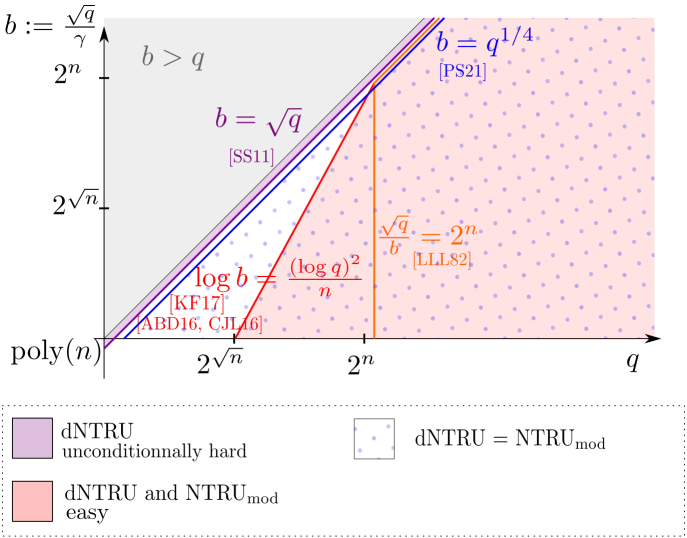
Remarks

- $a \approx b \Leftrightarrow a = \mathrm{poly}(n) \cdot b$ (cyclotomic/NTRUPrime fields)
- the reductions only work for certain distributions of NTRU instances
- the constraint $\frac{\sqrt{q}}{\gamma_4} \geq 2^n$ can be relaxed if the run time is increased

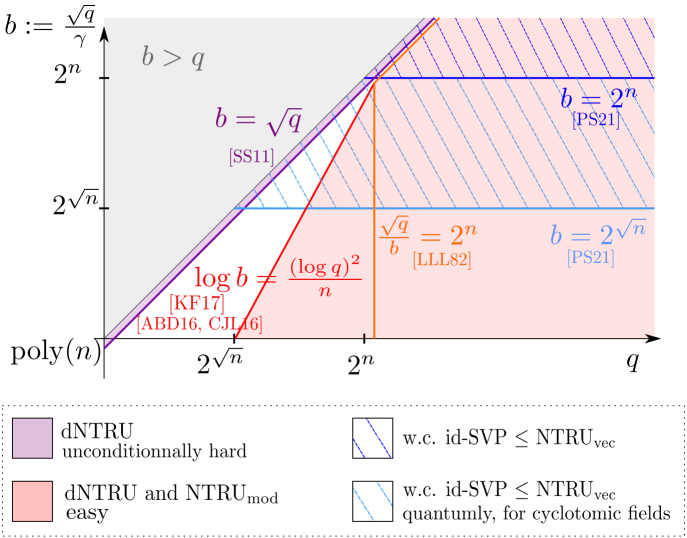
One big picture: poly time attacks and reductions (cyclotomics)



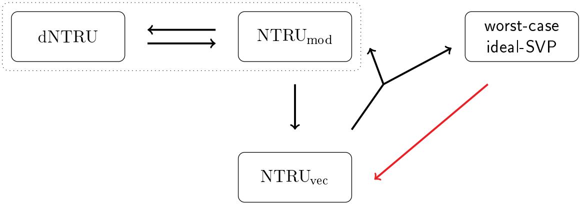
One big picture: poly time attacks and reductions (cyclotomics)



One big picture: poly time attacks and reductions (cyclotomics)



Techniques



dNTRU
$\mathrm{NTRU}_{\mathrm{mod}}$
worst-case
ideal-SVP
$\mathrm{NTRU}_{\mathrm{vec}}$

From ideal-SVP to $\mathrm{NTRU}_{\mathrm{vec}}$

Objective: Transform an ideal I into an NTRU instance h

- $I = \langle z \rangle = \{z \cdot r \mid r \in R\}$
- g short vector of I

From ideal-SVP to $\mathrm{NTRU}_{\mathrm{vec}}$

Objective: Transform an ideal I into an NTRU instance h

- $I = \langle z \rangle = \{z \cdot r \mid r \in R\}$
- g short vector of I

$$\begin{aligned} & g = z \cdot r && (r \in R) \\ \Leftrightarrow\ & g \cdot \frac{q}{z} = qr && \\ \Leftrightarrow\ & g \cdot h = f \bmod q && \end{aligned}$$

  - $h = q/z,\ f = 0$
  - $\|f\|, \|g\|$ small

From ideal-SVP to $\mathrm{NTRU}_{\mathrm{vec}}$

Objective: Transform an ideal I into an NTRU instance h

- $I = \langle z \rangle = \{z \cdot r \,|\, r \in R\}$
- g short vector of I

$$\boxed{\begin{aligned} & g = z \cdot r & (r \in R) \\ \Leftrightarrow\ & g \cdot \frac{q}{z} = qr & \\ & & \\ \Leftrightarrow\ & g \cdot h = f \bmod q & \end{aligned}}$$

- ▸ $h = q/z,\ f = 0$
- ▸ $\|f\|, \|g\|$ small

/!\ Not an NTRU instance ($h \in K$ is not in R_q)

From ideal-SVP to $\mathrm{NTRU}_{\mathrm{vec}}$

Objective: Transform an ideal I into an NTRU instance h

- $I = \langle z \rangle = \{z \cdot r \mid r \in R\}$
- g short vector of I

$$\boxed{\begin{aligned} & g = z \cdot r && (r \in R) \\ \Leftrightarrow\ & g \cdot \frac{q}{z} = qr \\ \Leftrightarrow\ & g \cdot \left\lfloor \frac{q}{z} \right\rceil = -g \cdot \left\{ \frac{q}{z} \right\} \bmod q \\ \Leftrightarrow\ & g \cdot h = f \bmod q \end{aligned}}$$

$$\{x\} = x - \lfloor x \rceil$$

  - $h = \lfloor q/z \rceil$, $f = -g\{q/z\}$
  - $\|f\| \approx \|g\|$ small

From ideal-SVP to $\mathrm{NTRU}_{\mathrm{vec}}$

Objective: Transform an ideal I into an NTRU instance h

- $I = \langle z \rangle = \{z \cdot r \,|\, r \in R\}$
- g short vector of I

$$\boxed{\begin{aligned} & g = z \cdot r && (r \in R) \\ \Leftrightarrow\ & g \cdot \frac{q}{z} = qr && \\ \Leftrightarrow\ & g \cdot \left\lfloor \frac{q}{z} \right\rceil = -g \cdot \left\{ \frac{q}{z} \right\} \bmod q && \\ \Leftrightarrow\ & g \cdot h = f \bmod q && \end{aligned}}$$

$$\{x\} = x - \lfloor x \rceil$$

- $h = \lfloor q/z \rceil$, $f = -g\{q/z\}$
- $\|f\| \approx \|g\|$ small

This is an NTRU instance ($h \in K$ is not in R_q)

From ideal-SVP to $\mathrm{NTRU}_{\mathrm{vec}}$ (2)

Summing up: If $I = \langle z \rangle = \{z \cdot r \mid r \in R\}$ and z known

- can construct an NTRU instance h from I
  - any short $g \in I$ provides a trapdoor (f, g) for h

From ideal-SVP to $\mathrm{NTRU}_{\mathrm{vec}}$ (2)

Summing up: If $I = \langle z \rangle = \{z \cdot r \,|\, r \in R\}$ and z known

- can construct an NTRU instance h from I
  - any short $g \in I$ provides a trapdoor (f, g) for h

What we need to conclude the reduction:

- any trapdoor (f', g') for h is such that $g' \in I$
  - g' solution to ideal-SVP in I

More technical details

Non principal ideals:

- $I = R \cap \langle z \rangle$ and z easily computed
  - everything still works with this z

[BDPW20] de Boer, Ducas, Pellet-Mary, and Wesolowski. Random Self-reducibility of Ideal-SVP via Arakelov Random Walks. Crypto.

More technical details

Non principal ideals:

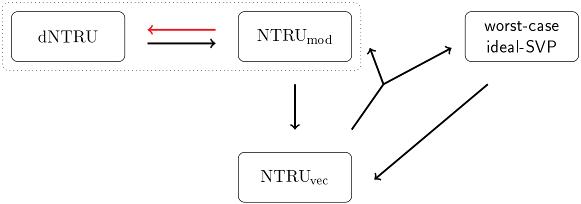
- $I = R \cap \langle z \rangle$ and z easily computed
  - everything still works with this z

Worst-case to average-case reduction:

$$\boxed{\text{worst-case ideal-SVP}} \xrightarrow{\text{[BDPW20]}} \boxed{\text{average-case ideal-SVP}} \xrightarrow{\text{previous slide}} \boxed{\text{average-case } \mathrm{NTRU}_{\mathrm{vec}}}$$

[BDPW20] de Boer, Ducas, Pellet-Mary, and Wesolowski. Random Self-reducibility of Ideal-SVP via Arakelov Random Walks. Crypto.

Techniques



dNTRU
$\mathrm{NTRU}_{\mathrm{mod}}$
worst-case
ideal-SVP
$\mathrm{NTRU}_{\mathrm{vec}}$

From $\mathrm{NTRU}_{\mathrm{mod}}$ to dNTRU

Objective: given $h = f/g \bmod q$, recover $h_K = f/g \in K$ (division in K)

Can use an oracle: given $h \in R_q$, outputs

- YES if $h = f/g \bmod q$, with f, g small $(\leq B)$
- NO otherwise

From $\mathrm{NTRU}_{\mathrm{mod}}$ to dNTRU

Objective: given $h = f/g \bmod q$, recover $h_K = f/g \in K$ (division in K)

Can use an oracle: given $h \in R_q$, outputs

- YES if $h = f/g \bmod q$, with f, g small ($\leq B$)
- NO otherwise

Idea:

- take $x, y \in R$
- create $h' = x \cdot h + y = \frac{xf+yg}{g} \bmod q$
- query the oracle on h'
- learn whether $xf + yg$ is small or not

From $\mathrm{NTRU}_{\mathrm{mod}}$ to dNTRU

Objective: given $h = f/g \bmod q$, recover $h_K = f/g \in K$ (division in K)

Can use an oracle: given $h \in R_q$, outputs

- YES if $h = f/g \bmod q$, with f, g small $(\leq B)$
- NO otherwise

Idea:

- take $x, y \in R$
- create $h' = x \cdot h + y = \frac{xf+yg}{g} \bmod q$
- query the oracle on h'
- learn whether $xf + yg$ is small or not

$\Rightarrow$ we can choose x and y

$\Rightarrow$ we can modify the coordinates one by one

From $\mathrm{NTRU}_{\mathrm{mod}}$ to dNTRU (2)

Simplified problem

$f, g \in \mathbb{R}$ secret, $B \geq 0$ unknown.
Given any $x, y \in \mathbb{R}$, we can learn whether $|xf + yg| \geq B$ or not.
Objective: recover f/g

From $\mathrm{NTRU}_{\mathrm{mod}}$ to dNTRU (2)

Simplified problem

$f, g \in \mathbb{R}$ secret, $B \geq 0$ unknown.
Given any $x, y \in \mathbb{R}$, we can learn whether $|xf + yg| \geq B$ or not.
Objective: recover f/g

Remark: if f, g, B all multiplied by $\alpha \in \mathbb{R}$, same behavior

- can only learn f/g (not f and g)
- can assume $g = 1$

From $\mathrm{NTRU}_{\mathrm{mod}}$ to dNTRU (2)

Simplified problem

$f, g \in \mathbb{R}$ secret, $B \geq 0$ unknown.
Given any $x, y \in \mathbb{R}$, we can learn whether $|xf + yg| \geq B$ or not.
Objective: recover f/g

Remark: if f, g, B all multiplied by $\alpha \in \mathbb{R}$, same behavior

- can only learn f/g (not f and g)
- can assume $g = 1$

Algorithm:

- Find x_0, y_0 such that $x_0 f + y_0 = B$
  - (Fix $x_0 \ll B/|f|$ and increase y_0 until the oracle says NO)
- Find x_1, y_1 such that $x_1 \neq x_0$ and $x_1 f + y_1 = B$

From $\mathrm{NTRU}_{\mathrm{mod}}$ to dNTRU (2)

Simplified problem

$f, g \in \mathbb{R}$ secret, $B \geq 0$ unknown.
Given any $x, y \in \mathbb{R}$, we can learn whether $|xf + yg| \geq B$ or not.
Objective: recover f/g

Remark: if f, g, B all multiplied by $\alpha \in \mathbb{R}$, same behavior

- can only learn f/g (not f and g)
- can assume $g = 1$

Algorithm:

- Find x_0, y_0 such that $x_0 f + y_0 = B$
  - (Fix $x_0 \ll B/|f|$ and increase y_0 until the oracle says NO)
- Find x_1, y_1 such that $x_1 \neq x_0$ and $x_1 f + y_1 = B$

We obtain: $x_0 f + y_0 = x_1 f + y_1$, i.e., $f = \frac{y_1 - y_0}{x_0 - x_1}$

More technical details

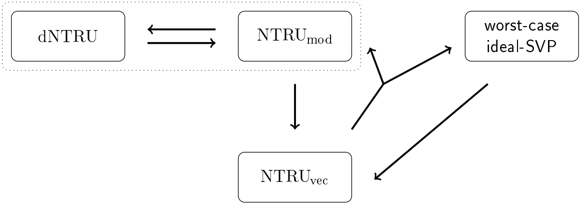
We do not have a perfect oracle

- need to handle distributions
- use the “oracle hidden center” framework [PRS17]

[PRS17] Peikert, Regev, and Stephens-Davidowitz. Pseudorandomness of ring-LWE for any ring and modulus. STOC.

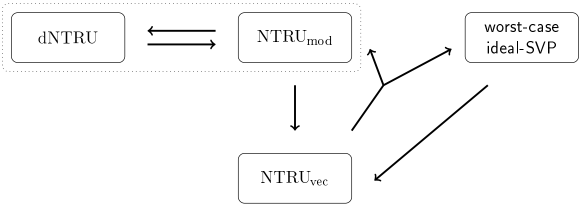
Conclusion

Conclusion and open problems



- Can we make the distributions of the reductions match?
- Can we relate $\mathrm{NTRU}_{\mathrm{mod}}$ and ideal-SVP?
  - maybe not since any "natural reduction" would provide new attacks
- Can we prove reduction from module problems with rank ≥ 2?
  - for instance, uSVP in modules of rank-2?

Conclusion and open problems



- Can we make the distributions of the reductions match?
- Can we relate $\mathrm{NTRU}_{\text{mod}}$ and ideal-SVP?
  - maybe not since any "natural reduction" would provide new attacks
- Can we prove reduction from module problems with rank ≥ 2?
  - for instance, uSVP in modules of rank-2?

Thank you