Algebraic lattices for cryptography

Alice Pellet-Mary

CNRS and university of Bordeaux, France

Fundations and applications of lattice-based cryptography workshop

25-28 July 2022, Edinburgh

Algebraic lattices

What are they:

- lattices
- but also algebraic objects (e.g., ideals and modules in a number field)

Algebraic lattices

What are they:

- lattices
- but also algebraic objects (e.g., ideals and modules in a number field)

Why use them:

- mainly for efficiency (faster primitives, smaller keys)
- also sometimes for the algebraic properties
  (e.g., the first FHE schemes, or some iO candidates)

Algebraic lattices

What are they:

- lattices
- but also algebraic objects (e.g., ideals and modules in a number field)

Why use them:

- mainly for efficiency (faster primitives, smaller keys)
- also sometimes for the algebraic properties
  (e.g., the first FHE schemes, or some iO candidates)

What about security:

- most of the time no better attacks than for unstructured lattices
- but for some problems, we have specific attacks using the algebraic structure (cf second talk)

Outline of the talk

1. A bit of number theory
2. Algebraic lattices
3. Algorithmic problems for cryptography
4. Some more number theory

Outline of the talk

Number fields

Number field: $K = \mathbb{Q}[X]/P(X)$ (P irreducible, $\deg(P) = d$)

Number fields

Number field: $K = \mathbb{Q}[X]/P(X)$ (P irreducible, $\deg(P) = d$)

- $K = \mathbb{Q}$
- $K = \mathbb{Q}[X]/(X^d + 1)$ with $d = 2^\ell$ $\rightsquigarrow$ power-of-two cyclotomic field
- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRUPrime field

Number fields

Number field: $K = \mathbb{Q}[X]/P(X)$ (P irreducible, $\deg(P) = d$)

- $K = \mathbb{Q}$
- $K = \mathbb{Q}[X]/(X^d + 1)$ with $d = 2^\ell$ $\rightsquigarrow$ power-of-two cyclotomic field
- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRUPrime field

Ring of integers: $\mathcal{O}_K \subset K$, for this talk $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$
(more generally $\mathbb{Z}[X]/P(X) \subseteq \mathcal{O}_K$ but $\mathcal{O}_K$ can be larger)

Number fields

Number field: $K = \mathbb{Q}[X]/P(X)$ (P irreducible, $\deg(P) = d$)

- $K = \mathbb{Q}$
- $K = \mathbb{Q}[X]/(X^d + 1)$ with $d = 2^\ell$ $\rightsquigarrow$ power-of-two cyclotomic field
- $K = \mathbb{Q}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRUPrime field

Ring of integers: $\mathcal{O}_K \subset K$, for this talk $\mathcal{O}_K = \mathbb{Z}[X]/P(X)$

(more generally $\mathbb{Z}[X]/P(X) \subseteq \mathcal{O}_K$ but $\mathcal{O}_K$ can be larger)

- $\mathcal{O}_K = \mathbb{Z}$
- $\mathcal{O}_K = \mathbb{Z}[X]/(X^d + 1)$ with $d = 2^\ell$ $\rightsquigarrow$ power-of-two cyclotomic ring
- $\mathcal{O}_K = \mathbb{Z}[X]/(X^d - X - 1)$ with d prime $\rightsquigarrow$ NTRUPrime ring of integers

Embeddings

$(K = \mathbb{Q}[X]/P(X), \quad \alpha_1, \cdots, \alpha_d$ complex roots of $P(X))$

Coefficient embedding: $\Sigma : \begin{array}{rcl} K & \to & \mathbb{R}^d \\ \sum_{i=0}^{d-1} y_i X^i & \mapsto & (y_0, \cdots, y_{d-1}) \end{array}$

Canonical embedding: $\sigma : \begin{array}{rcl} K & \to & \mathbb{C}^d \\ y(X) & \mapsto & (y(\alpha_1), \cdots, y(\alpha_d)) \end{array}$

Embeddings

$(K = \mathbb{Q}[X]/P(X), \quad \alpha_1, \cdots, \alpha_d$ complex roots of $P(X))$

Coefficient embedding:
$$\Sigma : \begin{array}{rcl} K & \to & \mathbb{R}^d \\ \sum_{i=0}^{d-1} y_i X^i & \mapsto & (y_0, \cdots, y_{d-1}) \end{array}$$

Canonical embedding:
$$\sigma : \begin{array}{rcl} K & \to & \mathbb{C}^d \\ y(X) & \mapsto & (y(\alpha_1), \cdots, y(\alpha_d)) \end{array}$$

- both embeddings induce a (different) geometry on K

Embeddings

$(K = \mathbb{Q}[X]/P(X), \quad \alpha_1, \cdots, \alpha_d$ complex roots of $P(X))$

Coefficient embedding: $$\Sigma : \begin{array}{rcl} K & \to & \mathbb{R}^d \\ \sum_{i=0}^{d-1} y_i X^i & \mapsto & (y_0, \cdots, y_{d-1}) \end{array}$$

Canonical embedding: $$\sigma : \begin{array}{rcl} K & \to & \mathbb{C}^d \\ y(X) & \mapsto & (y(\alpha_1), \cdots, y(\alpha_d)) \end{array}$$

- both embeddings induce a (different) geometry on K

Which embedding should we choose?

- coefficient embedding is used for constructions (efficient implementation)
- canonical embedding is used in cryptanalysis / reductions (nice mathematical properties)

Embeddings

($K = \mathbb{Q}[X]/P(X)$, $\alpha_1, \cdots, \alpha_d$ complex roots of $P(X)$)

Coefficient embedding: $\Sigma : \begin{array}{rcl} K & \to & \mathbb{R}^d \\ \sum_{i=0}^{d-1} y_i X^i & \mapsto & (y_0, \cdots, y_{d-1}) \end{array}$

Canonical embedding: $\sigma : \begin{array}{rcl} K & \to & \mathbb{C}^d \\ y(X) & \mapsto & (y(\alpha_1), \cdots, y(\alpha_d)) \end{array}$

- both embeddings induce a (different) geometry on K

Which embedding should we choose?

- coefficient embedding is used for constructions (efficient implementation)
- canonical embedding is used in cryptanalysis / reductions
  (nice mathematical properties)

Embeddings

($K = \mathbb{Q}[X]/P(X)$, $\alpha_1, \cdots, \alpha_d$ complex roots of $P(X)$)

Coefficient embedding: $$\Sigma : \begin{array}{rcl} K & \to & \mathbb{R}^d \\ \sum_{i=0}^{d-1} y_i X^i & \mapsto & (y_0, \cdots, y_{d-1}) \end{array}$$

Canonical embedding: $$\sigma : \begin{array}{rcl} K & \to & \mathbb{C}^d \\ y(X) & \mapsto & (y(\alpha_1), \cdots, y(\alpha_d)) \end{array}$$

- both embeddings induce a (different) geometry on K

Which embedding should we choose?

- coefficient embedding is used for constructions (efficient implementation)
- canonical embedding is used in cryptanalysis / reductions (nice mathematical properties)
- for fields used in crypto, both geometries are $\approx$ the same

Ideals

Ideal: $I \subseteq \mathcal{O}_K$ is an ideal if

- $x + y \in I$ for all $x, y \in I$
- $a \cdot x \in I$ for all $a \in \mathcal{O}_K$ and $x \in I$

Ideals

Ideal: $I \subseteq \mathcal{O}_K$ is an ideal if

- $x + y \in I$ for all $x, y \in I$
- $a \cdot x \in I$ for all $a \in \mathcal{O}_K$ and $x \in I$

- $I_1 = \{2a \,|\, a \in \mathbb{Z}\}$ and $J_1 = \{6a \,|\, a \in \mathbb{Z}\}$ in $\mathcal{O}_K = \mathbb{Z}$
- $I_2 = \{a + b \cdot X \,|\, a + b = 0 \bmod 2,\ a, b \in \mathbb{Z}\}$ in $\mathcal{O}_K = \mathbb{Z}[X]/(X^2 + 1)$

Ideals

Ideal: $I \subseteq \mathcal{O}_K$ is an ideal if
- $x + y \in I$ for all $x, y \in I$
- $a \cdot x \in I$ for all $a \in \mathcal{O}_K$ and $x \in I$

- $I_1 = \{2a \mid a \in \mathbb{Z}\}$ and $J_1 = \{6a \mid a \in \mathbb{Z}\}$ in $\mathcal{O}_K = \mathbb{Z}$
- $I_2 = \{a + b \cdot X \mid a + b = 0 \bmod 2,\ a, b \in \mathbb{Z}\}$ in $\mathcal{O}_K = \mathbb{Z}[X]/(X^2 + 1)$

Multiplication: $I \cdot J := \{\sum_{i=1}^{r} a_i \cdot b_i \mid r > 0,\ a_i \in I,\ b_i \in J\}$
$\rightsquigarrow$ this is also an ideal

Ideals

Ideal: $I \subseteq \mathcal{O}_K$ is an ideal if

- $x + y \in I$ for all $x, y \in I$
- $a \cdot x \in I$ for all $a \in \mathcal{O}_K$ and $x \in I$

- $I_1 = \{2a \mid a \in \mathbb{Z}\}$ and $J_1 = \{6a \mid a \in \mathbb{Z}\}$ in $\mathcal{O}_K = \mathbb{Z}$
- $I_2 = \{a + b \cdot X \mid a + b = 0 \bmod 2,\ a, b \in \mathbb{Z}\}$ in $\mathcal{O}_K = \mathbb{Z}[X]/(X^2 + 1)$

Multiplication: $I \cdot J := \{\sum_{i=1}^{r} a_i \cdot b_i \mid r > 0,\ a_i \in I,\ b_i \in J\}$
$\rightsquigarrow$ this is also an ideal

- $I_1 \cdot J_1 = \{12a \mid a \in \mathbb{Z}\}$

Ideals

Ideal: $I \subseteq \mathcal{O}_K$ is an ideal if

- $x + y \in I$ for all $x, y \in I$
- $a \cdot x \in I$ for all $a \in \mathcal{O}_K$ and $x \in I$

- $I_1 = \{2a \,|\, a \in \mathbb{Z}\}$ and $J_1 = \{6a \,|\, a \in \mathbb{Z}\}$ in $\mathcal{O}_K = \mathbb{Z}$
- $I_2 = \{a + b \cdot X \,|\, a + b = 0 \bmod 2,\ a, b \in \mathbb{Z}\}$ in $\mathcal{O}_K = \mathbb{Z}[X]/(X^2 + 1)$

Multiplication: $I \cdot J := \{\sum_{i=1}^r a_i \cdot b_i \,|\, r > 0,\ a_i \in I,\ b_i \in J\}$
$\rightsquigarrow$ this is also an ideal

- $I_1 \cdot J_1 = \{12a \,|\, a \in \mathbb{Z}\}$

Algebraic norm: $\mathcal{N}(I) := |\mathcal{O}_K/I|$ ("size" of I)
$\rightsquigarrow$ norm is multiplicative: $\mathcal{N}(IJ) = \mathcal{N}(I)\mathcal{N}(J)$

Ideals

Ideal: $I \subseteq \mathcal{O}_K$ is an ideal if

- $x + y \in I$ for all $x, y \in I$
- $a \cdot x \in I$ for all $a \in \mathcal{O}_K$ and $x \in I$

- $I_1 = \{2a \,|\, a \in \mathbb{Z}\}$ and $J_1 = \{6a \,|\, a \in \mathbb{Z}\}$ in $\mathcal{O}_K = \mathbb{Z}$
- $I_2 = \{a + b \cdot X \,|\, a + b = 0 \bmod 2,\ a, b \in \mathbb{Z}\}$ in $\mathcal{O}_K = \mathbb{Z}[X]/(X^2 + 1)$

Multiplication: $I \cdot J := \{\sum_{i=1}^{r} a_i \cdot b_i \,|\, r > 0,\ a_i \in I,\ b_i \in J\}$
$\rightsquigarrow$ this is also an ideal

- $I_1 \cdot J_1 = \{12a \,|\, a \in \mathbb{Z}\}$

Algebraic norm: $\mathcal{N}(I) := |\mathcal{O}_K / I|$ ("size" of I)
$\rightsquigarrow$ norm is multiplicative: $\mathcal{N}(IJ) = \mathcal{N}(I)\mathcal{N}(J)$

- $\mathcal{N}(I_1) = 2$ and $\mathcal{N}(J_1) = 6$
- $\mathcal{N}(I_2) = 2$

Principal ideals and units

Units: $O_K^\times = \{a \in O_K \mid \exists b \in O_K, ab = 1\}$

Principal ideals and units

Units: $O_K^\times = \{a \in O_K \mid \exists b \in O_K, ab = 1\}$

- $\mathbb{Z}^\times = \{-1, 1\}$
- $(\mathbb{Z}[X]/(X^2+1))^\times = \{-1, 1, -X, X\}$
- $(\mathbb{Z}[X]/(X^4+1))^\times = \{\pm(1+X+X^2)^i \mid i \in \mathbb{Z}\}$
- in general, $\mathcal{O}_K^\times$ is infinite

Principal ideals and units

Units: $O_K^\times = \{a \in O_K \mid \exists b \in O_K, ab = 1\}$

- $\mathbb{Z}^\times = \{-1, 1\}$
- $(\mathbb{Z}[X]/(X^2+1))^\times = \{-1, 1, -X, X\}$
- $(\mathbb{Z}[X]/(X^4+1))^\times = \{\pm(1+X+X^2)^i \mid i \in \mathbb{Z}\}$
- in general, $\mathcal{O}_K^\times$ is infinite

Principal ideals: $\langle g \rangle := \{g \cdot a \mid a \in O_K\}$

Principal ideals and units

Units: $O_K^\times = \{a \in O_K \mid \exists b \in O_K, ab = 1\}$

- $\mathbb{Z}^\times = \{-1, 1\}$
- $(\mathbb{Z}[X]/(X^2+1))^\times = \{-1, 1, -X, X\}$
- $(\mathbb{Z}[X]/(X^4+1))^\times = \{\pm(1+X+X^2)^i \mid i \in \mathbb{Z}\}$
- in general, $\mathcal{O}_K^\times$ is infinite

Principal ideals: $\langle g \rangle := \{g \cdot a \mid a \in O_K\}$

- $I_1 = \{2a \mid a \in \mathbb{Z}\} = \langle 2 \rangle$
- $I_2 = \{a + b \cdot X \mid a + b = 0 \bmod 2,\ a, b \in \mathbb{Z}\} = \langle 1 + X \rangle$

Principal ideals and units

Units: $O_K^\times = \{a \in O_K \mid \exists b \in O_K, ab = 1\}$

- $\mathbb{Z}^\times = \{-1, 1\}$
- $(\mathbb{Z}[X]/(X^2+1))^\times = \{-1, 1, -X, X\}$
- $(\mathbb{Z}[X]/(X^4+1))^\times = \{\pm(1+X+X^2)^i \,|\, i \in \mathbb{Z}\}$
- in general, $\mathcal{O}_K^\times$ is infinite

Principal ideals: $\langle g\rangle := \{g \cdot a \mid a \in O_K\}$

- $I_1 = \{2a \,|\, a \in \mathbb{Z}\} = \langle 2\rangle$
- $I_2 = \{a + b \cdot X \,|\, a + b = 0 \bmod 2,\ a, b \in \mathbb{Z}\} = \langle 1 + X\rangle$

- g is a generator of $\langle g\rangle$
- $\{$ generators of $\langle g\rangle$ $\} = \{gu \,|\, u \in O_K^\times\}$
- $\mathcal{N}(\langle g\rangle) = |\mathcal{N}(g)|$, where $\mathcal{N}(g) = \prod_i g(\alpha_i)$ (α_i complex roots of $P(X)$)

Outline of the talk

Ideal lattices

$\mathcal{O}_K$ is a lattice:

- $\mathcal{O}_K = 1 \cdot \mathbb{Z} + X \cdot \mathbb{Z} + \cdots + X^{d-1} \cdot \mathbb{Z}$
- $\sigma(\mathcal{O}_K) = \sigma(1) \cdot \mathbb{Z} + \cdots + \sigma(X^{d-1}) \cdot \mathbb{Z}$

Ideal lattices

$\mathcal{O}_K$ is a lattice:

- $\mathcal{O}_K = 1 \cdot \mathbb{Z} + X \cdot \mathbb{Z} + \cdots + X^{d-1} \cdot \mathbb{Z}$
- $\sigma(\mathcal{O}_K) = \sigma(1) \cdot \mathbb{Z} + \cdots + \sigma(X^{d-1}) \cdot \mathbb{Z}$

$\sigma(\mathcal{O}_K)$ is a lattice of rank d in $\mathbb{C}^d \simeq \mathbb{R}^{2d}$ with basis $(\sigma(X^i))_{0 \leq i < d}$

Ideal lattices

$\mathcal{O}_K$ is a lattice:

- $\mathcal{O}_K = 1 \cdot \mathbb{Z} + X \cdot \mathbb{Z} + \cdots + X^{d-1} \cdot \mathbb{Z}$
- $\sigma(\mathcal{O}_K) = \sigma(1) \cdot \mathbb{Z} + \cdots + \sigma(X^{d-1}) \cdot \mathbb{Z}$

$\sigma(\mathcal{O}_K)$ is a lattice of rank d in $\mathbb{C}^d \simeq \mathbb{R}^{2d}$ with basis $(\sigma(X^i))_{0 \leq i < d}$

$\langle g \rangle$ is a lattice:

- $\langle g \rangle = g \cdot \mathcal{O}_K = g \cdot 1 \cdot \mathbb{Z} + g \cdot X \cdot \mathbb{Z} + \cdots + g \cdot X^{d-1} \cdot \mathbb{Z}$
- $\sigma(\langle g \rangle) = \sigma(g) \cdot \mathbb{Z} + \cdots + \sigma(g \cdot X^{d-1}) \cdot \mathbb{Z}$

Ideal lattices

$\mathcal{O}_K$ is a lattice:

- $\mathcal{O}_K = 1 \cdot \mathbb{Z} + X \cdot \mathbb{Z} + \cdots + X^{d-1} \cdot \mathbb{Z}$
- $\sigma(\mathcal{O}_K) = \sigma(1) \cdot \mathbb{Z} + \cdots + \sigma(X^{d-1}) \cdot \mathbb{Z}$

$\sigma(\mathcal{O}_K)$ is a lattice of rank d in $\mathbb{C}^d \simeq \mathbb{R}^{2d}$ with basis $(\sigma(X^i))_{0 \leq i < d}$

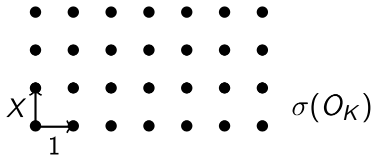
$\langle g \rangle$ is a lattice:

- $\langle g \rangle = g \cdot \mathcal{O}_K = g \cdot 1 \cdot \mathbb{Z} + g \cdot X \cdot \mathbb{Z} + \cdots + g \cdot X^{d-1} \cdot \mathbb{Z}$
- $\sigma(\langle g \rangle) = \sigma(g) \cdot \mathbb{Z} + \cdots + \sigma(g \cdot X^{d-1}) \cdot \mathbb{Z}$

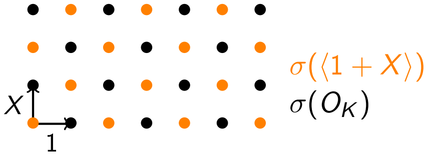
$\sigma(\langle g \rangle)$ is a lattice of rank d in $\mathbb{C}^d \simeq \mathbb{R}^{2d}$ with basis $(\sigma(g \cdot X^i))_{0 \leq i < d}$

(this is also true for non principal ideals)

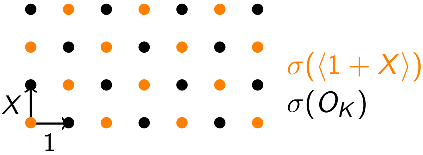
Ideal lattices (2)



Ideal lattices (2)

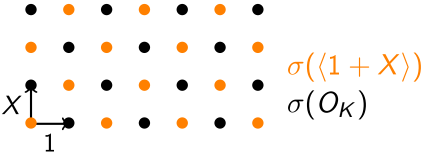


Ideal lattices (2)



Basis of $\langle g \rangle$: $g, g \cdot X, \cdots, g \cdot X^{d-1}$

Ideal lattices (2)

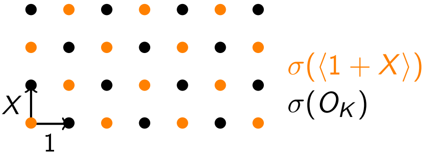


Basis of $\langle g \rangle$: $g, g \cdot X, \cdots, g \cdot X^{d-1}$

$$\begin{pmatrix} g_0 & & & \\ g_1 & & & \\ \vdots & & & \\ g_{d-1} & & & \end{pmatrix}$$

(in $K = \mathbb{Q}[X]/X^d + 1$)

Ideal lattices (2)

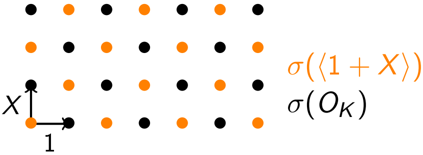


Basis of $\langle g \rangle$: $g, g \cdot X, \cdots, g \cdot X^{d-1}$

$$\begin{pmatrix} g_0 & -g_{d-1} & & \\ g_1 & g_0 & & \\ \vdots & \vdots & & \\ g_{d-1} & g_{d-2} & & \end{pmatrix}$$

(in $K = \mathbb{Q}[X]/X^d + 1$)

Ideal lattices (2)

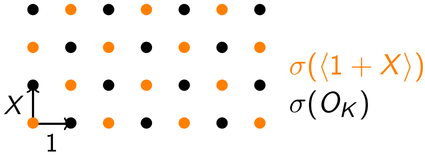


Basis of $\langle g \rangle$: $g, g \cdot X, \cdots, g \cdot X^{d-1}$

$$\begin{pmatrix} g_0 & -g_{d-1} & \cdots & -g_1 \\ g_1 & g_0 & \cdots & -g_2 \\ \vdots & \vdots & \ddots & \vdots \\ g_{d-1} & g_{d-2} & \cdots & g_0 \end{pmatrix}$$

(in $K = \mathbb{Q}[X]/X^d + 1$)

Ideal lattices (2)



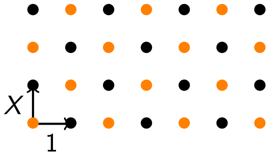
Basis of $\langle g\rangle$: $g, g\cdot X, \cdots, g\cdot X^{d-1}$

$$\begin{pmatrix} g_0 & -g_{d-1} & \cdots & -g_1 \\ g_1 & g_0 & \cdots & -g_2 \\ \vdots & \vdots & \ddots & \vdots \\ g_{d-1} & g_{d-2} & \cdots & g_0 \end{pmatrix}$$

(in $K = \mathbb{Q}[X]/X^d+1$)

Discriminant: $\Delta_K := \sqrt{\mathrm{vol}(\sigma(\mathcal{O}_K))}$

Ideal lattices (2)



Basis of $\langle g \rangle$: $g, g \cdot X, \cdots, g \cdot X^{d-1}$

$$\begin{pmatrix} g_0 & -g_{d-1} & \cdots & -g_1 \\ g_1 & g_0 & \cdots & -g_2 \\ \vdots & \vdots & \ddots & \vdots \\ g_{d-1} & g_{d-2} & \cdots & g_0 \end{pmatrix}$$

(in $K = \mathbb{Q}[X]/X^d + 1$)

Discriminant: $\Delta_K := \sqrt{\mathrm{vol}(\sigma(\mathcal{O}_K))}$

Volume of an ideal: $\mathrm{vol}(\sigma(I)) = \mathcal{N}(I) \cdot \sqrt{\Delta_K}$

Module lattices

(Free) module:

$$M = \{B \cdot x \,|\, x \in \mathcal{O}_K^k\} \text{ for some matrix } B \in \mathcal{O}_K^{k \times k} \text{ with } \det_K(B) \neq 0$$

Module lattices

(Free) module:

$$M = \{B \cdot x \,|\, x \in \mathcal{O}_K^k\} \text{ for some matrix } B \in \mathcal{O}_K^{k \times k} \text{ with } \det_K(B) \neq 0$$

- k is the module rank
- B is a module basis of M

  (if the module is not free, it has a "pseudo-basis" instead)

$\sigma(M)$ is a lattice:

- of $\mathbb{Z}$-rank $n := d \cdot k$, included in $\mathbb{C}^n$

Module lattices

(Free) module:

$$M = \{B \cdot x \,|\, x \in \mathcal{O}_K^k\} \text{ for some matrix } B \in \mathcal{O}_K^{k\times k} \text{ with } \det_K(B) \neq 0$$

- k is the module rank
- B is a module basis of M
  (if the module is not free, it has a "pseudo-basis" instead)

$\sigma(M)$ is a lattice:

- of $\mathbb{Z}$-rank $n := d \cdot k$, included in $\mathbb{C}^n$
- with basis $(\sigma(b_i X^j))_{\substack{1\leq i\leq k \\ 0\leq j<d}}$ (b_i columns of B)

Module lattices

(Free) module:

$M = \{B \cdot x \,|\, x \in \mathcal{O}_K^k\}$ for some matrix $B \in \mathcal{O}_K^{k \times k}$ with $\det_K(B) \neq 0$

- k is the module rank
- B is a module basis of M
  (if the module is not free, it has a "pseudo-basis" instead)

$\sigma(M)$ is a lattice:

- of $\mathbb{Z}$-rank $n := d \cdot k$, included in $\mathbb{C}^n$
- with basis $(\sigma(b_i X^j))_{\substack{1 \leq i \leq k \\ 0 \leq j < d}}$ (b_i columns of B)
- $\mathrm{vol}(M) = |\mathcal{N}(\det_K(B))| \cdot \Delta_K^{k/2}$

Modules vs ideals

Ideal	=	Module of rank 1
(principal ideal	=	free module of rank 1)

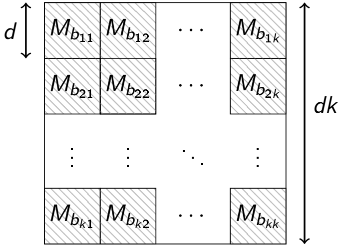
Modules vs ideals

Ideal	=	Module of rank 1
(principal ideal	=	free module of rank 1)

In $K = \mathbb{Q}[X]/(X^d + 1)$:

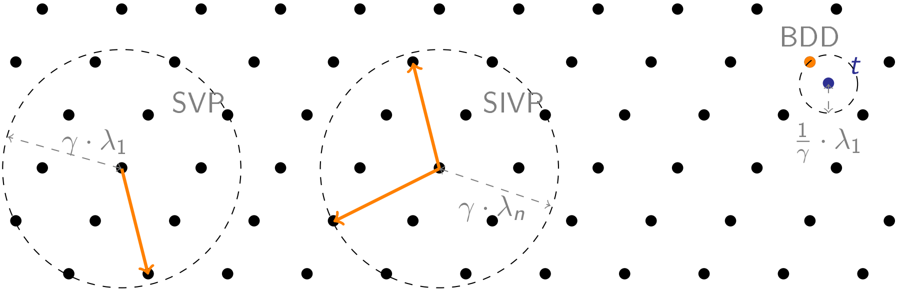
$$M_a = \begin{pmatrix} a_1 & -a_d & \cdots & -a_2 \\ a_2 & a_1 & \cdots & -a_3 \\ \vdots & \ddots & \ddots & \vdots \\ a_d & a_{d-1} & \cdots & a_1 \end{pmatrix}$$

basis of a
principal ideal lattice



basis of a free module lattice
of rank k

Algorithmic problems

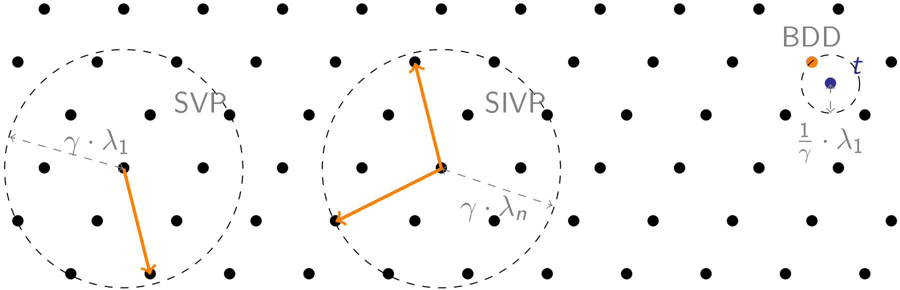


γ-SVP
shortest vector problem

γ-SIVP
shortest independent vector problem

γ-BDD
bounded distance decoding problem

Algorithmic problems



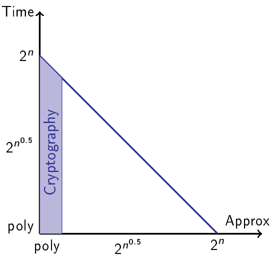
γ-SVP	γ-SIVP	γ-BDD
shortest vector problem	shortest independent vector problem	bounded distance decoding problem

Notations:

- id-X = problem X restricted to ideal lattices
- mod-X_k = problem X restricted to module lattices of rank k

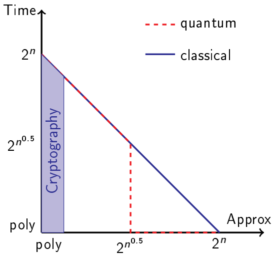
Hardness of SVP

Asymptotics:



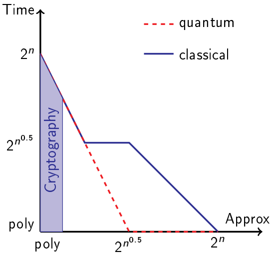
SVP and mod-SVP$_k$

($k \geq 2$)



id-SVP [CDW17]

(in cyclotomic fields)



id-SVP [PHS19,BR20]

(with $2^{O(n)}$ pre-processing)

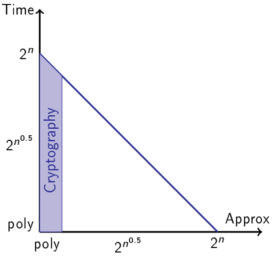
[CDW17] Cramer, Ducas, Wesolowski. Short stickelberger class relations and application to ideal-SVP. Eurocrypt.

[PHS19] Pellet-Mary, Hanrot, Stehlé. Approx-SVP in ideal lattices with pre-processing. Eurocrypt.

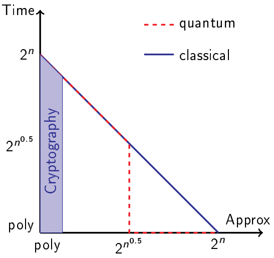
[BR20] Bernard, Roux-Langlois. Twisted-PHS: using the product formula to solve approx-SVP in ideal lattices. AC.

Hardness of SVP

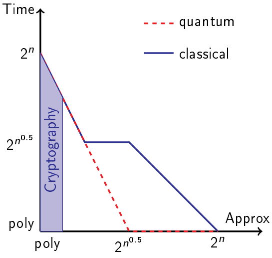
Asymptotics:



SVP and mod-SVP$_k$
($k \geq 2$)



id-SVP [CDW17]
(in cyclotomic fields)



id-SVP [PHS19,BR20]
(with $2^{O(n)}$ pre-processing)

Practice: Darmstadt challenge[1]

$\rightsquigarrow$ max dim for SVP: 180
$\rightsquigarrow$ max dim for id-SVP: 150

[1] https://www.latticechallenge.org/

Outline of the talk

Ring and Module-LWE

(search) mod-LWE$_k$

Parameters: $k, m, q \in \mathbb{Z}_{>0}$ and $\alpha \in \mathbb{R}_{>0}$

Objective: given $(A, b) \in \mathcal{O}_K^{m \times k} \times \mathcal{O}_K^m$, with

- A uniform in $\mathcal{O}_K^{m \times k}$
- s uniform in $\mathcal{O}_K^k$ and $e \in \mathcal{O}_K^m$ such that $\sigma(e) \leftarrow D_{\sigma(\mathcal{O}_K), \alpha \cdot q}$
  ($D_{L,\sigma}$ discrete Gaussian distribution over L with parameter σ)
- $b = As + e$

output s

(can also be defined using Σ instead of σ)

Ring and Module-LWE

(search) mod-LWE$_k$

Parameters: $k, m, q \in \mathbb{Z}_{>0}$ and $\alpha \in \mathbb{R}_{>0}$

Objective: given $(A, b) \in \mathcal{O}_K^{m \times k} \times \mathcal{O}_K^m$, with

- A uniform in $\mathcal{O}_K^{m \times k}$
- s uniform in $\mathcal{O}_K^k$ and $e \in \mathcal{O}_K^m$ such that $\sigma(e) \leftarrow D_{\sigma(\mathcal{O}_K), \alpha \cdot q}$
  ($D_{L,\sigma}$ discrete Gaussian distribution over L with parameter σ)
- $b = As + e$

output s

(can also be defined using Σ instead of σ)

$$\text{RLWE} = \text{mod-LWE}_1$$

Decision mod-LWE

dec-mod-LWE$_k$

Parameters: $k, m, q \in \mathbb{Z}_{>0}$ and $\alpha \in \mathbb{R}_{>0}$

Objective: distinguish between (A, b) and (A, u), where

- A and b are as on the previous slide
- u is uniform in $\mathcal{O}_K^m$

Decision mod-LWE

dec-mod-LWE$_k$

Parameters: $k, m, q \in \mathbb{Z}_{>0}$ and $\alpha \in \mathbb{R}_{>0}$

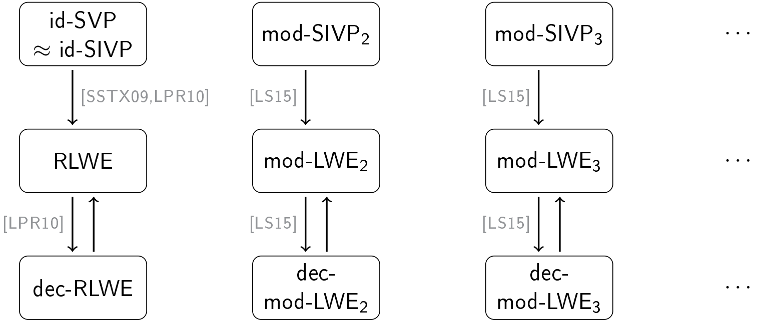
Objective: distinguish between (A, b) and (A, u), where

- A and b are as on the previous slide
- u is uniform in $\mathcal{O}_K^m$

mod-LWE$_k$ reduces to dec-mod-LWE$_k$ [LS15]

[LS15] Langlois, Stehlé. Worst-case to average-case reductions for module lattices. DCC.

Reductions



⚠ Arrows may not all compose (different parameters) ⚠

(References are for the first reductions. Better, more recent reductions may exist.)

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

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

[LS15] Langlois, Stehlé. Worst-case to average-case reductions for module lattices. DCC.

From mod-LWE$_k$ to mod-SIVP$_{k+1}$

Reminder mod-LWE$_k$: $(A, b = A \cdot s + e \bmod q)$

with $s \in \mathcal{O}_K^k$, $e \in \mathcal{O}_K^m$ and $\|\sigma(e)\| \approx \alpha \cdot q$

mod-LWE$_k$ is a BDD in the rank-m module lattice

$$\Lambda = \sigma\Big(\big\{x \in \mathcal{O}_K^m \,|\, \exists z \in \mathcal{O}_K^k,\, x = A \cdot z \bmod q\big\}\Big)$$

- BDD only if m is large enough

From mod-LWE$_k$ to mod-SIVP$_{k+1}$

Reminder mod-LWE$_k$: $(A, b = A \cdot s + e \bmod q)$

with $s \in \mathcal{O}_K^k$, $e \in \mathcal{O}_K^m$ and $\|\sigma(e)\| \approx \alpha \cdot q$

mod-LWE$_k$ is a BDD in the rank-m module lattice

$$\Lambda = \sigma\left(\left\{x \in \mathcal{O}_K^m \,|\, \exists z \in \mathcal{O}_K^k,\, x = A \cdot z \bmod q\right\}\right)$$

- BDD only if m is large enough $\rightsquigarrow$ how large?

From mod-LWE$_k$ to mod-SIVP$_{k+1}$

Reminder mod-LWE$_k$: $(A, b = A \cdot s + e \bmod q)$

with $s \in \mathcal{O}_K^k$, $e \in \mathcal{O}_K^m$ and $\|\sigma(e)\| \approx \alpha \cdot q$

mod-LWE$_k$ is a BDD in the rank-m module lattice

$$\Lambda = \sigma\Big(\big\{x \in \mathcal{O}_K^m \,|\, \exists z \in \mathcal{O}_K^k,\, x = A \cdot z \bmod q\big\}\Big)$$

- BDD only if m is large enough $\rightsquigarrow$ how large?
- $m = k$ is not sufficient

From mod-LWE$_k$ to mod-SIVP$_{k+1}$

Reminder mod-LWE$_k$: $(A, b = A \cdot s + e \bmod q)$

with $s \in \mathcal{O}_K^k$, $e \in \mathcal{O}_K^m$ and $\|\sigma(e)\| \approx \alpha \cdot q$

mod-LWE$_k$ is a BDD in the rank-m module lattice

$$\Lambda = \sigma\Big(\big\{x \in \mathcal{O}_K^m \,|\, \exists z \in \mathcal{O}_K^k,\, x = A \cdot z \bmod q\big\}\Big)$$

- BDD only if m is large enough $\rightsquigarrow$ how large?
- $m = k$ is not sufficient
- $m = k + 1$ might be sufficient depending on α and q
  - we need roughly $m = k \cdot \frac{\log(q)}{\log(1/\alpha)}$
  - for $k = 1$, $m = 2$ is possible if $\alpha \cdot q \lesssim \sqrt{q}$

From mod-LWE$_k$ to mod-SIVP$_{k+1}$

Reminder mod-LWE$_k$: $(A, b = A \cdot s + e \bmod q)$

with $s \in \mathcal{O}_K^k$, $e \in \mathcal{O}_K^m$ and $\|\sigma(e)\| \approx \alpha \cdot q$

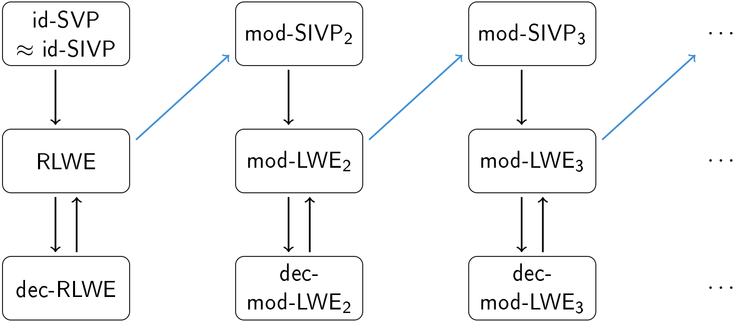
mod-LWE$_k$ is a BDD in the rank-m module lattice

$$\Lambda = \sigma\Big(\big\{x \in \mathcal{O}_K^m \,|\, \exists z \in \mathcal{O}_K^k,\, x = A \cdot z \bmod q\big\}\Big)$$

- BDD only if m is large enough $\rightsquigarrow$ how large?
- $m = k$ is not sufficient
- $m = k + 1$ might be sufficient depending on α and q
  - we need roughly $m = k \cdot \frac{\log(q)}{\log(1/\alpha)}$
  - for $k = 1$, $m = 2$ is possible if $\alpha \cdot q \lesssim \sqrt{q}$

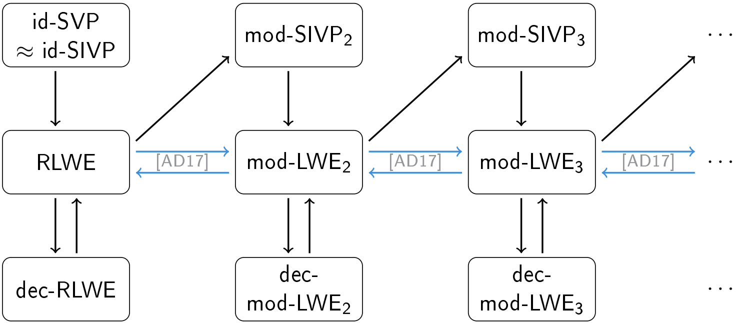
RLWE is at best a special case of mod-BDD$_2$

Reductions



⚠ Arrows may not all compose (different parameters) ⚠

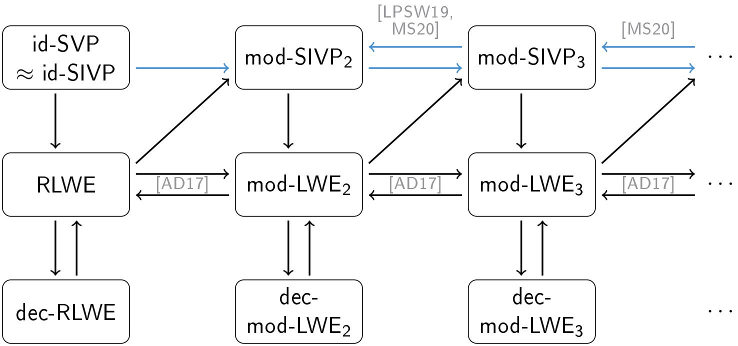
Reductions



⚠ Arrows may not all compose (different parameters) ⚠

[AD17] Albrecht, Deo. Large modulus ring-LWE $\geq$ module-LWE. Asiacrypt.

Reductions

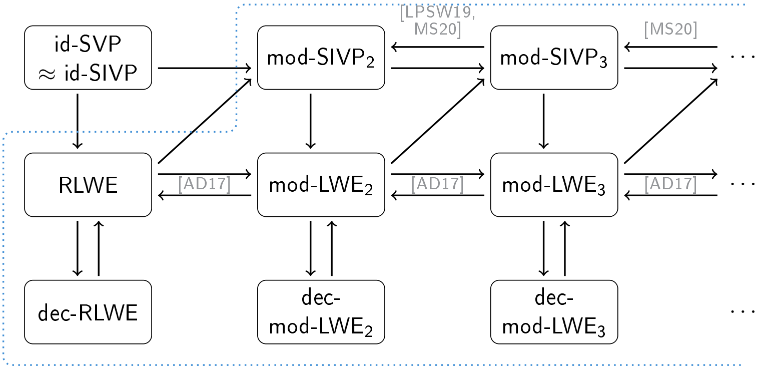


⚠ Arrows may not all compose (different parameters) ⚠

[LPSW19] Lee, Pellet-Mary, Stehlé, and Wallet. An LLL algorithm for module lattices. Asiacrypt.

[MS20] Mukherjee and Stephens-Davidowitz. Lattice reduction for modules, or how to reduce moduleSVP to moduleSVP. Crypto.

Reductions



⚠ Arrows may not all compose (different parameters) ⚠

[LPSW19] Lee, Pellet-Mary, Stehlé, and Wallet. An LLL algorithm for module lattices. Asiacrypt.

[MS20] Mukherjee and Stephens-Davidowitz. Lattice reduction for modules, or how to reduce moduleSVP to moduleSVP. Crypto.

NTRU (a.k.a, partial Fourier recovery problem [HPS98])

(search) NTRU

Parameters: $q \geq B > 1$ and ψ distribution over $\mathcal{O}_K$ outputting elements $\leq B$

Objective: given $h \in \mathcal{O}_K/(q\mathcal{O}_K)$, with

- $f, g \leftarrow \psi$ conditioned on g invertible modulo q
- $h = f \cdot g^{-1} \bmod q$

output (f, g)

(can also be defined using Σ instead of σ)

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

NTRU (a.k.a, partial Fourier recovery problem [HPS98])

(search) NTRU

Parameters: $q \geq B > 1$ and ψ distribution over $\mathcal{O}_K$ outputting elements $\leq B$

Objective: given $h \in \mathcal{O}_K/(q\mathcal{O}_K)$, with

- $f, g \leftarrow \psi$ conditioned on g invertible modulo q
- $h = f \cdot g^{-1} \bmod q$

output (f, g)

(can also be defined using Σ instead of σ)

dec-NTRU

Parameters: q, B and ψ

Objective: distinguish between h as above and u uniform in $\mathcal{O}_K/(q\mathcal{O}_K)$

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

Two regimes of NTRU

If $B \geq \sqrt{q} \cdot \mathrm{poly}(d)$

If $B \leq \sqrt{q}/\mathrm{poly}(d)$

Two regimes of NTRU

If $B \geq \sqrt{q} \cdot \mathrm{poly}(d)$

- h is statistically close to uniform mod q [SS11,WW18]
- dec-NTRU is statistically hard

If $B \leq \sqrt{q}/\mathrm{poly}(d)$

[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.

Two regimes of NTRU

If $B \geq \sqrt{q} \cdot \mathrm{poly}(d)$

- h is statistically close to uniform mod q [SS11,WW18]
- dec-NTRU is statistically hard

If $B \leq \sqrt{q}/\mathrm{poly}(d)$

- h is not statistically close to uniform mod q
- NTRU is a special case of unique-SVP

[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.

Two regimes of NTRU

If $B \geq \sqrt{q} \cdot \mathrm{poly}(d)$

- h is statistically close to uniform mod q [SS11,WW18]
- dec-NTRU is statistically hard

If $B \leq \sqrt{q}/\mathrm{poly}(d)$

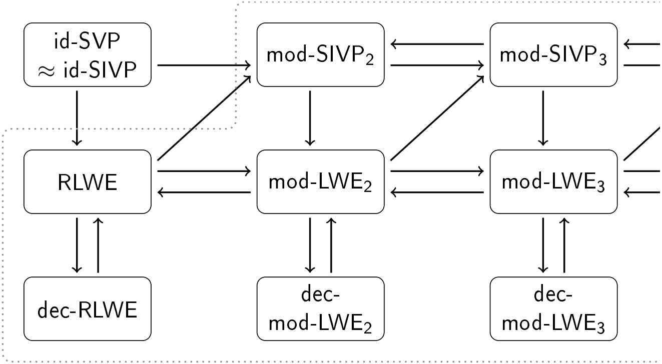
- h is not statistically close to uniform mod q
- NTRU is a special case of unique-SVP

For the rest of the talk, we consider $B \ll \sqrt{q}$

[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.

Reductions

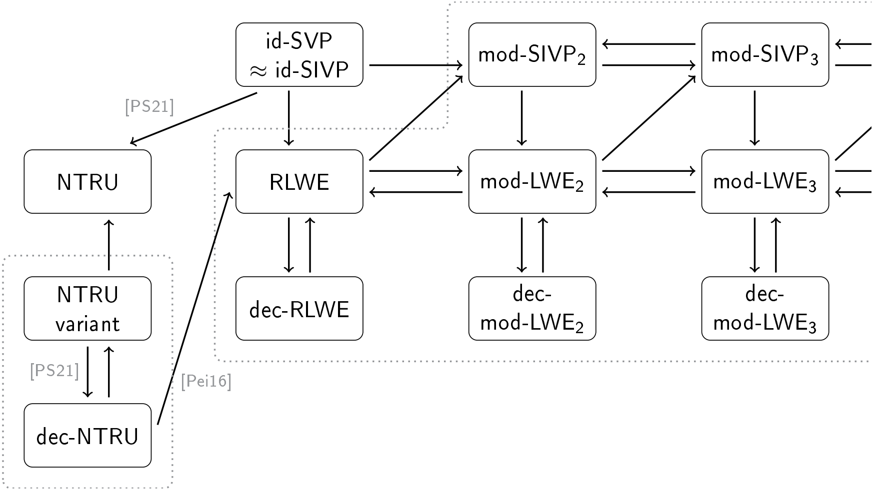


⚠ Arrows may not all compose (different parameters) ⚠

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

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

Reductions

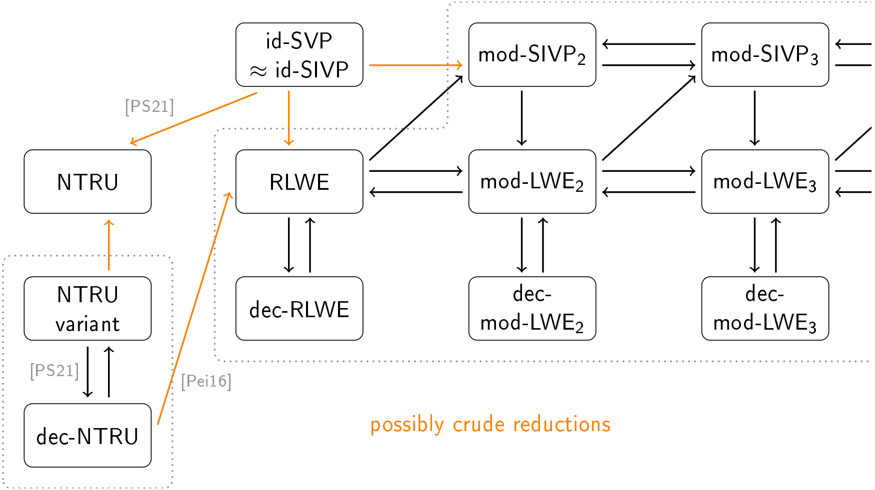


⚠ Arrows may not all compose (different parameters) ⚠

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

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

Reductions



⚠ Arrows may not all compose (different parameters) ⚠

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

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

id-SVP

id-SVP is a lower bound
on the hardness of RLWE, mod-LWE, NTRU

id-SVP

id-SVP is a lower bound
on the hardness of RLWE, mod-LWE, NTRU

Breaking id-SVP does not break:

- RLWE, mod-LWE, NTRU
- most lattice-based crypto using algebraic lattices

id-SVP

id-SVP is a lower bound
on the hardness of RLWE, mod-LWE, NTRU

Breaking id-SVP does not break:

- RLWE, mod-LWE, NTRU
- most lattice-based crypto using algebraic lattices

Breaking id-SVP do break:

- some early FHE schemes
- the PV-Knap problem (see next slides)

PV-Knap (a.k.a, partial Fourier recovery problem)

Notations:

- $K = \mathbb{Q}[X]/\Phi_N(X)$ with Φ_N cyclotomic polynomial
  - $\Phi_N(\alpha) = 0$ if and only if α is a primitive N-th root of unity

---

[HPS+14] Hoffstein, Pipher, Schanck, Silverman, and Whyte. Practical signatures from the partial Fourier recovery problem. ACNS.

PV-Knap (a.k.a, partial Fourier recovery problem)

Notations:

- $K = \mathbb{Q}[X]/\Phi_N(X)$ with Φ_N cyclotomic polynomial
  - $\Phi_N(\alpha) = 0$ if and only if α is a primitive N-th root of unity
- $q = 1 \bmod N$ prime
  - so that there exists a primitive N-th root of unity in $\mathbb{F}_q$

[HPS+14] Hoffstein, Pipher, Schanck, Silverman, and Whyte. Practical signatures from the partial Fourier recovery problem. ACNS.

PV-Knap (a.k.a, partial Fourier recovery problem)

Notations:

- $K = \mathbb{Q}[X]/\Phi_N(X)$ with Φ_N cyclotomic polynomial
  - $\Phi_N(\alpha) = 0$ if and only if α is a primitive N-th root of unity
- $q = 1 \bmod N$ prime
  - so that there exists a primitive N-th root of unity in $\mathbb{F}_q$
- $S_t \subset \{\omega, \text{ roots of } \Phi_N \text{ in } \mathbb{F}_q\}$ with size $|S_t| = t \quad (1 \leq t \leq \varphi(N))$

[HPS+14] Hoffstein, Pipher, Schanck, Silverman, and Whyte. Practical signatures from the partial Fourier recovery problem. ACNS.

PV-Knap (a.k.a, partial Fourier recovery problem)

Notations:

- $K = \mathbb{Q}[X]/\Phi_N(X)$ with Φ_N cyclotomic polynomial
  - $\Phi_N(\alpha) = 0$ if and only if α is a primitive N-th root of unity
- $q = 1 \bmod N$ prime
  - so that there exists a primitive N-th root of unity in $\mathbb{F}_q$
- $S_t \subset \{\omega, \text{ roots of } \Phi_N \text{ in } \mathbb{F}_q\}$ with size $|S_t| = t \quad (1 \leq t \leq \varphi(N))$

Partial Vandermonde Knapsack (PV-Knap) [HPS+14]

Parameters: q, S_t and $B > 1$

Objective: recover f from $(f(\omega) \bmod q)_{\omega \in S_t}$, where

- $f = f(X) \in \mathcal{O}_K$ is sampled randomly such that $\|\sigma(f)\| \leq B$

(The original article worked in $\mathbb{Q}[X]/(X^N - 1)$ and with Σ)

[HPS+14] Hoffstein, Pipher, Schanck, Silverman, and Whyte. Practical signatures from the partial Fourier recovery problem. ACNS.

PV-Knap is an (ideal) lattice problem

PV-Knap

Objective: recover f from $(f(\omega) \bmod q)_{\omega \in S_t}$, where

- $f = f(X) \in \mathcal{O}_K$ is sampled randomly such that $\|\sigma(f)\| \leq B$

A few observations:

- easy to recover a large $\tilde{f}$ such that $\tilde{f}(\omega) = f(\omega) \bmod q$, $\forall \omega \in S_t$
  $\rightsquigarrow$ polynomial interpolation in $\mathbb{F}_q$

PV-Knap is an (ideal) lattice problem

PV-Knap

Objective: recover f from $(f(\omega) \bmod q)_{\omega \in S_t}$, where

- $f = f(X) \in \mathcal{O}_K$ is sampled randomly such that $\|\sigma(f)\| \leq B$

A few observations:

- easy to recover a large $\tilde{f}$ such that $\tilde{f}(\omega) = f(\omega) \bmod q$, $\forall \omega \in S_t$
  $\rightsquigarrow$ polynomial interpolation in $\mathbb{F}_q$

- Recovering small f from large $\tilde{f}$ is a BDD in

$$\Lambda = \sigma\Big(\{g \in \mathcal{O}_K \mid g(\omega) = 0 \bmod q,\ \forall \omega \in S_t\}\Big)$$

(if parameters are well chosen)

PV-Knap is an (ideal) lattice problem

PV-Knap

Objective: recover f from $(f(\omega) \bmod q)_{\omega \in S_t}$, where

- $f = f(X) \in \mathcal{O}_K$ is sampled randomly such that $\|\sigma(f)\| \leq B$

A few observations:

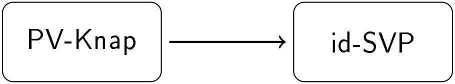
- easy to recover a large $\tilde{f}$ such that $\tilde{f}(\omega) = f(\omega) \bmod q$, $\forall \omega \in S_t$
  $\rightsquigarrow$ polynomial interpolation in $\mathbb{F}_q$
- Recovering small f from large $\tilde{f}$ is a BDD in

$$\Lambda = \sigma\Big(\{g \in \mathcal{O}_K \mid g(\omega) = 0 \bmod q,\ \forall \omega \in S_t\}\Big)$$

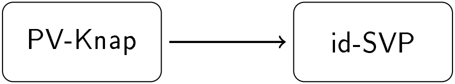
  (if parameters are well chosen)
- Λ is an ideal lattice [BSS22]

[BSS22] Boudgoust, Sakzad, and Steinfeld. Vandermonde meets Regev: Public Key Encryption Schemes Based on Partial Vandermonde Problems. DCC.

Hardness of PV-Knap



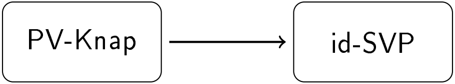
Hardness of PV-Knap



Warning:

- The reduction produces specific ideals
  (they divide $\langle q \rangle$)
  - PV-Knap might be easier than id-SVP

Hardness of PV-Knap



Warning:

- The reduction produces specific ideals
  (they divide $\langle q \rangle$)
  - PV-Knap might be easier than id-SVP
- if S_t is badly chosen, id-SVP can be solved in poly time [BGP22]
  - attacks on PV-Knap for bad choices of S_t

[BGP22] Boudgoust, Gachon, and Pellet-Mary. Some Easy Instances of Ideal-SVP and Implications on the Partial Vandermonde Knapsack Problem. Crypto.

Outline of the talk

The Log function

$$\text{Log} : K \to \mathbb{R}^d$$
$$y \mapsto (\log|y(\alpha_1)|, \cdots, \log|y(\alpha_d)|)$$

The Log function

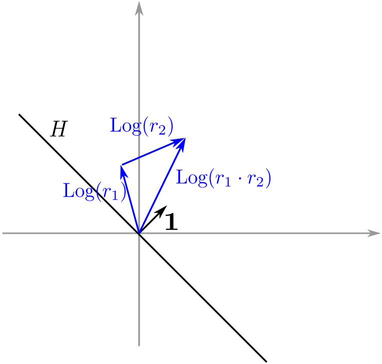
$$\text{Log} : K \to \mathbb{R}^d$$
$$y \mapsto (\log|y(\alpha_1)|, \cdots, \log|y(\alpha_d)|)$$

Let $\mathbf{1} = (1, \cdots, 1)$ and $H = \mathbf{1}^\perp$.

Properties ($r \in O_K$)

$\text{Log}\, r = h + a \cdot \mathbf{1}$, with $h \in H$

- $\text{Log}(r_1 \cdot r_2) = \text{Log}(r_1) + \text{Log}(r_2)$



The Log function

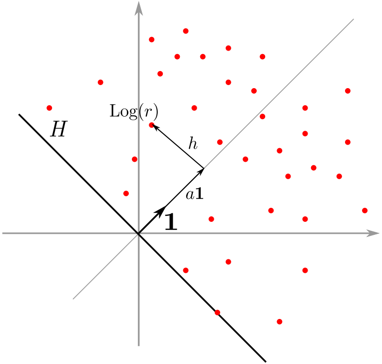
$$\text{Log} : K \to \mathbb{R}^d$$
$$y \mapsto (\log|y(\alpha_1)|, \cdots, \log|y(\alpha_d)|)$$

Let $\mathbf{1} = (1, \cdots, 1)$ and $H = \mathbf{1}^\perp$.

Properties ($r \in O_K$)

$\text{Log}\, r = h + a \cdot \mathbf{1}$, with $h \in H$

- $\text{Log}(r_1 \cdot r_2) = \text{Log}(r_1) + \text{Log}(r_2)$
- $a \geq 0$



The Log function

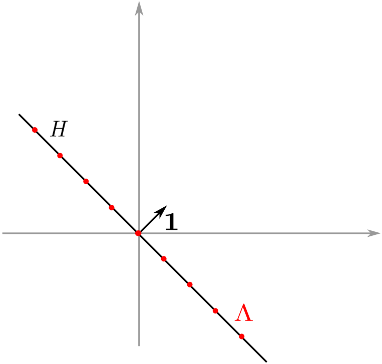
$$\mathrm{Log} : K \to \mathbb{R}^d$$
$$y \mapsto (\log|y(\alpha_1)|, \cdots, \log|y(\alpha_d)|)$$

Let $\mathbf{1} = (1, \cdots, 1)$ and $H = \mathbf{1}^\perp$.

Properties ($r \in O_K$)

$\mathrm{Log}\, r = h + a \cdot \mathbf{1}$, with $h \in H$

- $\mathrm{Log}(r_1 \cdot r_2) = \mathrm{Log}(r_1) + \mathrm{Log}(r_2)$
- $a \geq 0$
- $a = 0$ iff r is a unit



The Log function

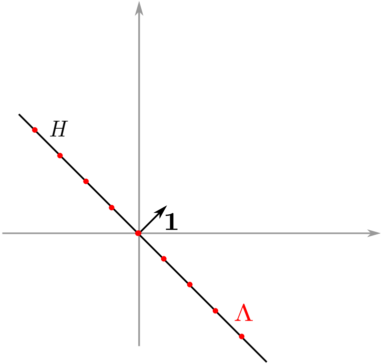
$$\text{Log} : K \to \mathbb{R}^d$$
$$y \mapsto (\log|y(\alpha_1)|, \cdots, \log|y(\alpha_d)|)$$

Let $\mathbf{1} = (1, \cdots, 1)$ and $H = \mathbf{1}^{\perp}$.

Properties ($r \in O_K$)

$\text{Log}\, r = h + a \cdot \mathbf{1}$, with $h \in H$

- $\text{Log}(r_1 \cdot r_2) = \text{Log}(r_1) + \text{Log}(r_2)$
- $a \geq 0$
- $a = 0$ iff r is a unit



The Log-unit lattice: $\Lambda := \text{Log}(O_K^{\times})$ is a lattice in H.

The Log function

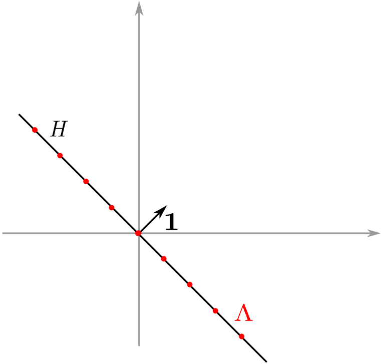
$$\mathrm{Log} : K \to \mathbb{R}^d$$
$$y \mapsto (\log|y(\alpha_1)|, \cdots, \log|y(\alpha_d)|)$$

Let $\mathbf{1} = (1, \cdots, 1)$ and $H = \mathbf{1}^\perp$.

Properties ($r \in O_K$)

$\mathrm{Log}\, r = h + a \cdot \mathbf{1}$, with $h \in H$

- $\mathrm{Log}(r_1 \cdot r_2) = \mathrm{Log}(r_1) + \mathrm{Log}(r_2)$
- $a \geq 0$
- $a = 0$ iff r is a unit
- $\|r\| \simeq \exp(\|\mathrm{Log}\, r\|_\infty)$



The Log-unit lattice: $\Lambda := \mathrm{Log}(O_K^\times)$ is a lattice in H.

Subfields

$$\begin{array}{c} K \\ \Big|\ {\scriptstyle n_1} \\ L \\ \Big|\ {\scriptstyle n_2} \\ \mathbb{Q} \end{array}$$

Meaning:

- K contains L, which contains $\mathbb{Q}$

Subfields

$$\begin{array}{c} K \\ \big|\ n_1 \\ L \\ \big|\ n_2 \\ \mathbb{Q} \end{array}$$

Meaning:

- K contains L, which contains $\mathbb{Q}$
- K is a L-vector space of degree $[K : L] = n_1$
- L is a $\mathbb{Q}$-vector space of degree $[L : \mathbb{Q}] = n_2$

Subfields

$$\begin{array}{c} K \\ \Big| \; n_1 \\ L \\ \Big| \; n_2 \\ \mathbb{Q} \end{array}$$

Meaning:

- K contains L, which contains $\mathbb{Q}$
- K is a L-vector space of degree $[K : L] = n_1$
- L is a $\mathbb{Q}$-vector space of degree $[L : \mathbb{Q}] = n_2$

$\Rightarrow K$ is a $\mathbb{Q}$-vector space of degree $n_1 \cdot n_2$

Subfields

K
$\quad | \; n_1$
L
$\quad | \; n_2$
$\mathbb{Q}$

Meaning:

- K contains L, which contains $\mathbb{Q}$
- K is a L-vector space of degree $[K : L] = n_1$
- L is a $\mathbb{Q}$-vector space of degree $[L : \mathbb{Q}] = n_2$

$\Rightarrow K$ is a $\mathbb{Q}$-vector space of degree $n_1 \cdot n_2$

Example:

$\vdots$
$\quad | \; 2$
$\mathbb{Q}[X]/(X^4+1)$
$\quad | \; 2$
$\mathbb{Q}[X]/(X^2+1)$
$\quad | \; 2$
$\mathbb{Q}$

Automorphisms and subfields

In this slide $K = \mathbb{Q}[X]/(X^d + 1)$
(or any Galois field)

Automorphisms: $\exists \sigma_1, \cdots, \sigma_d$ automorphisms of K

Automorphisms and subfields

In this slide $K = \mathbb{Q}[X]/(X^d + 1)$
(or any Galois field)

Automorphisms: $\exists\, \sigma_1, \cdots, \sigma_d$ automorphisms of K

Properties:

- if $f \in \mathcal{O}_K$ then $\sigma_i(f) \in \mathcal{O}_K$
- $\|\sigma(f)\| = \|\sigma(\sigma_i(f))\|$, for all $f \in K$

Automorphisms and subfields

In this slide $K = \mathbb{Q}[X]/(X^d + 1)$
(or any Galois field)

Automorphisms: $\exists\, \sigma_1, \cdots, \sigma_d$ automorphisms of K

Properties:

- if $f \in \mathcal{O}_K$ then $\sigma_i(f) \in \mathcal{O}_K$
- $\|\sigma(f)\| = \|\sigma(\sigma_i(f))\|$, for all $f \in K$

Subfields: If L subfield of K, there exist $S_L \subseteq \{1, \cdots, d\}$ s.t.

- $|S_L| = [K : L] - 1$
- for all $f \in K$,

$$\mathcal{N}_{K/L}(f) := f \cdot \prod_{i \in S_L} \sigma_i(f) \in L$$

Conclusion

Ideals vs modules of rank ≥ 2:

- there seem to be a gap in hardness between id-SVP and mod-SIVP$_{\geq 2}$

Conclusion

Ideals vs modules of rank ≥ 2:

- there seem to be a gap in hardness between id-SVP and mod-SIVP$_{\geq 2}$

Crypto problems:

- most problems used in crypto are module problems of rank ≥ 2
  - RLWE and mod-LWE $\approx$ mod-SIVP$_2$
  - id-SVP $\leq$ NTRU $\leq$ mod-SIVP$_2$ (where exactly?)

Conclusion

Ideals vs modules of rank ≥ 2:

- there seem to be a gap in hardness between id-SVP and mod-SIVP$_{\geq 2}$

Crypto problems:

- most problems used in crypto are module problems of rank ≥ 2
  - RLWE and mod-LWE $\approx$ mod-SIVP$_2$
  - id-SVP $\leq$ NTRU $\leq$ mod-SIVP$_2$ (where exactly?)
- but some problems are ideal problems
  - PV-Knap $\leq$ id-SVP

Conclusion

Ideals vs modules of rank ≥ 2:

- there seem to be a gap in hardness between id-SVP and mod-SIVP$_{\geq 2}$

Crypto problems:

- most problems used in crypto are module problems of rank ≥ 2
  - RLWE and mod-LWE $\approx$ mod-SIVP$_2$
  - id-SVP $\leq$ NTRU $\leq$ mod-SIVP$_2$ (where exactly?)
- but some problems are ideal problems
  - PV-Knap $\leq$ id-SVP

Next talk: attacks that exploit the algebraic structure

Conclusion

Ideals vs modules of rank ≥ 2:

- there seem to be a gap in hardness between id-SVP and mod-SIVP$_{\geq 2}$

Crypto problems:

- most problems used in crypto are module problems of rank ≥ 2
  - RLWE and mod-LWE $\approx$ mod-SIVP$_2$
  - id-SVP $\leq$ NTRU $\leq$ mod-SIVP$_2$ (where exactly?)
- but some problems are ideal problems
  - PV-Knap $\leq$ id-SVP

Next talk: attacks that exploit the algebraic structure

Thank you