Introduction to lattice-based cryptography

Elena Kirshanova

Quantum algorithms for analysis of public-key crypto
American Institute of Mathematics, San Jose, California
February 5, 2019

UNIVERSITÉ DE LYON
ENS DE LYON

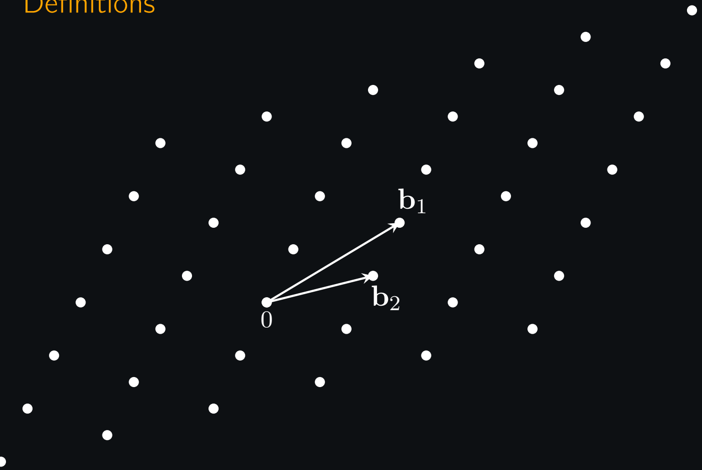
Outline

- Euclidean lattices
- The Learning with Errors problem
- Efficient lattice-based schemes
- Known quantum speed-ups

Part I

Euclidean lattices

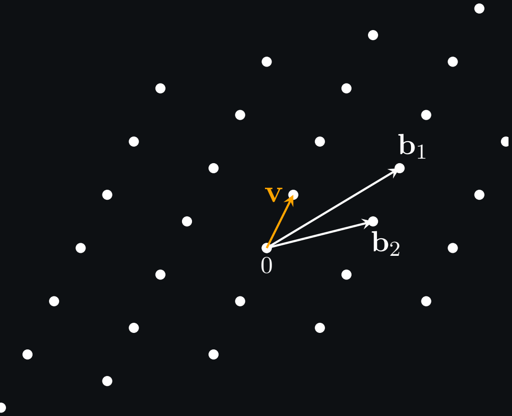
Definitions



A lattice is a set $\mathcal{L} = \{\sum_{i \le n} x_i \mathbf{b}_i \;:\; x_i \in \mathbb{Z}\}$ for some linearly independent $\mathbf{b}_i \in \mathbb{R}^n$

$\{\mathbf{b}_i\}_i$ – a basis of $\mathcal{L}$

Definitions



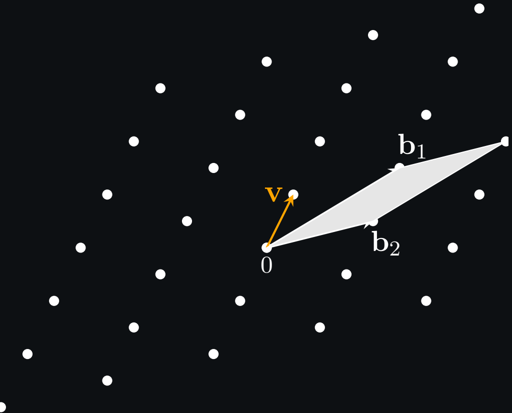
Minimum

$$\lambda_1(\mathcal{L}) = \min_{\mathbf{v}\in\mathcal{L}\setminus\mathbf{0}} \|\mathbf{v}\|$$

A lattice is a set $\mathcal{L} = \{\sum_{i\le n} x_i \mathbf{b}_i \ : \ x_i \in \mathbb{Z}\}$ for some linearly independent $\mathbf{b}_i \in \mathbb{R}^n$

$\{\mathbf{b}_i\}_i$– a basis of $\mathcal{L}$

Definitions



Minimum

$$\lambda_1(\mathcal{L}) = \min_{\mathbf{v}\in\mathcal{L}\setminus\mathbf{0}} \|\mathbf{v}\|$$

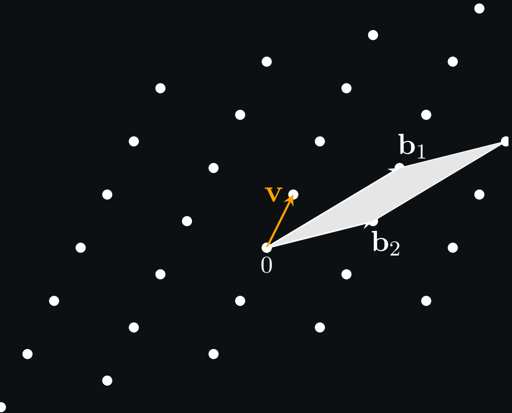
Determinant

$$\det(\mathcal{L}) = |\det(\mathbf{b}_i)_i|$$

A lattice is a set $\mathcal{L} = \{\sum_{i\leq n} x_i\mathbf{b}_i \ : \ x_i \in \mathbb{Z}\}$ for some linearly independent $\mathbf{b}_i \in \mathbb{R}^n$

$\{\mathbf{b}_i\}_i$– a basis of $\mathcal{L}$

Definitions



Minimum

$$\lambda_1(\mathcal{L}) = \min_{\mathbf{v}\in\mathcal{L}\setminus\mathbf{0}} \|\mathbf{v}\|$$

Determinant

$$\det(\mathcal{L}) = |\det(\mathbf{b}_i)_i|$$

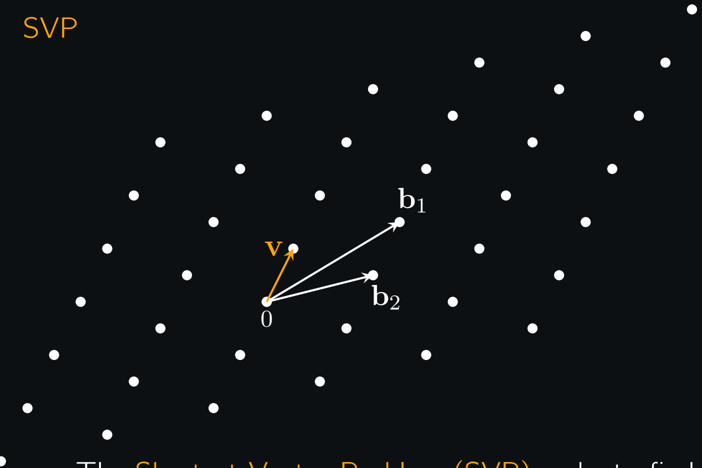
Minkowski bound

$$\lambda_1(\mathcal{L}) \leq \sqrt{n}\cdot\det(\mathcal{L})^{\frac{1}{n}}$$

A lattice is a set $\mathcal{L} = \{\sum_{i\leq n} x_i\mathbf{b}_i \ : \ x_i \in \mathbb{Z}\}$ for some linearly independent $\mathbf{b}_i \in \mathbb{R}^n$

$\{\mathbf{b}_i\}_i$ – a basis of $\mathcal{L}$

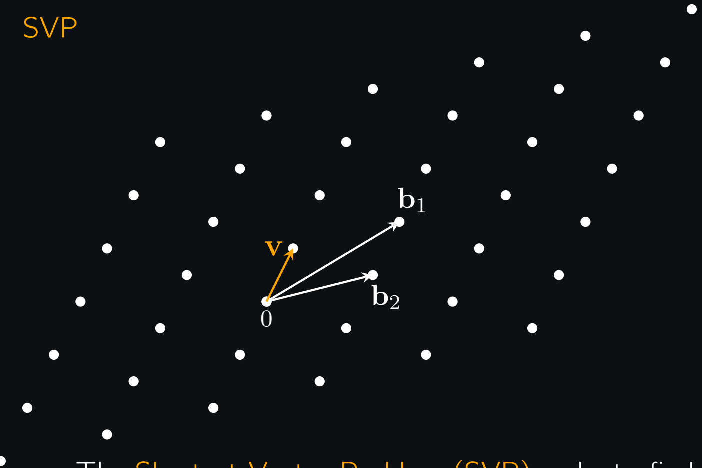
SVP



The Shortest Vector Problem (SVP) asks to find $\mathbf{v}_{\text{shortest}} \in \mathcal{L}$:

$$\|\mathbf{v}_{\text{shortest}}\| = \lambda_1(\mathcal{L})$$

SVP



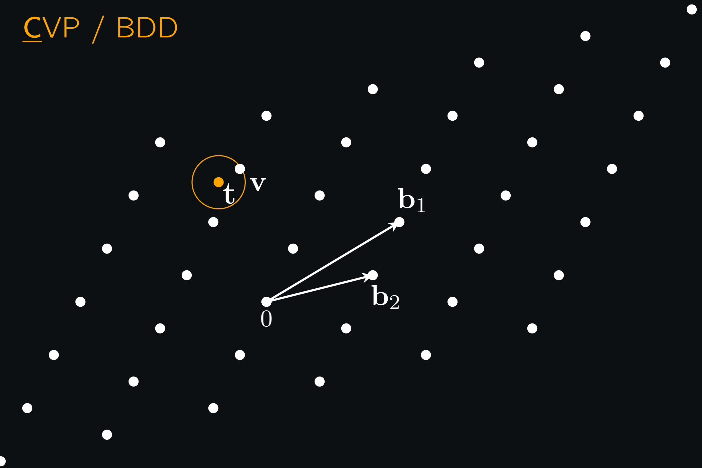
The Shortest Vector Problem (SVP) asks to find $\mathbf{v}_{\text{shortest}} \in \mathcal{L}$:

$$||\mathbf{v}_{\text{shortest}}|| = \lambda_1(\mathcal{L})$$

Often we are satisfied with an approximation (γ-SVP) to $\mathbf{v}_{\text{shortest}}$:

$$||\mathbf{v}_{\text{short}}|| \leq \gamma \cdot \lambda_1(\mathcal{L})$$

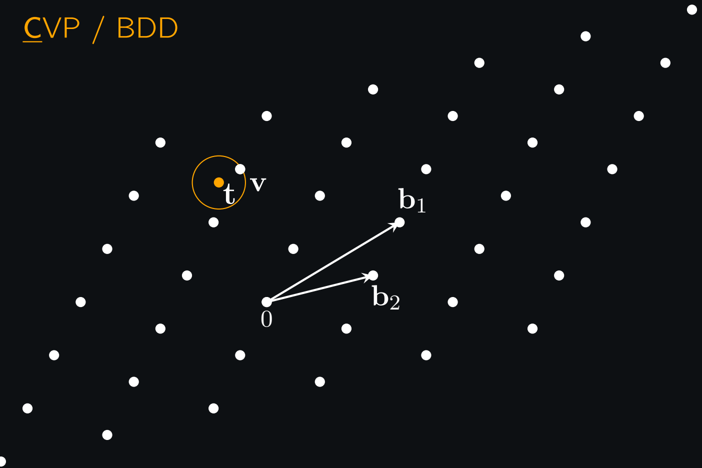
CVP / BDD



The Closest Vector Problem (CVP), given $\mathbf{t} \notin \mathcal{L}$ asks to find $\mathbf{v} \in \mathcal{L}$ s.t.

$$\|\mathbf{v} - \mathbf{t}\| \text{ is minimized over all } \mathbf{v} \in \mathcal{L}$$

CVP / BDD



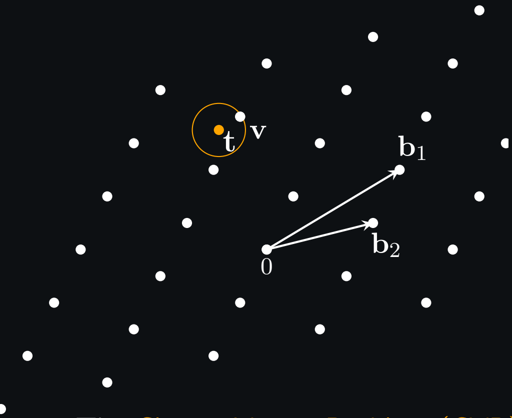
The Closest Vector Problem (CVP), given $\mathbf{t} \notin \mathcal{L}$ asks to find $\mathbf{v} \in \mathcal{L}$ s.t.

$$\|\mathbf{v} - \mathbf{t}\| \text{ is minimized over all } \mathbf{v} \in \mathcal{L}$$

Often we have $\mathrm{dist}(t, \mathcal{L}) \leq \frac{1}{\gamma}\lambda_1(\mathcal{L})$.

This is the Bounded Distance Decoding Problem γ-BDD

CVP / BDD



To solve BDD on $\mathcal{L}$,
we call approx-SVP on
a related lattice of dim+1.
We concentrate on SVP

The Closest Vector Problem (CVP), given $\mathbf{t} \notin \mathcal{L}$ asks to find $\mathbf{v} \in \mathcal{L}$ s.t.

$$\|\mathbf{v} - \mathbf{t}\| \text{ is minimized over all } \mathbf{v} \in \mathcal{L}$$

Often we have $\mathrm{dist}(t, \mathcal{L}) \leq \frac{1}{\gamma}\lambda_1(\mathcal{L})$.

This is the Bounded Distance Decoding Problem γ-BDD

From BDD to approxSVP: Kannan's embedding

Given a BDD instance $(\mathcal{L}, \mathbf{t})$, where $\mathcal{L}$ has a basis B, consider for a certain constant c

$$B' = \begin{bmatrix} B & \mathbf{t} \\ \mathbf{0} & \mathsf{c} \end{bmatrix}.$$

- the columns of B' are lin. independent
- If c is appropriately chosen and $\mathbf{t}$ is close enough to $\mathcal{L}$,

$$\begin{bmatrix} B & \mathbf{t} \\ \mathbf{0} & \mathsf{c} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{x} \\ -1 \end{bmatrix} = \begin{bmatrix} B\mathbf{x} - \mathbf{t} \\ \mathsf{c} \end{bmatrix}$$

is short (much shorter than any $\mathbf{v} \in \mathcal{L}(B')$ not parallel to it) in $\mathcal{L}(B')$.

Asymptotical Hardness of SVP (non-leading order terms omitted)

$$||\mathbf{v}_{\text{shortest}}|| \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$$

$$||\mathbf{v}_{\text{short}}|| \leq \gamma \cdot \|\mathbf{v}_{\text{shortest}}\|$$

$2^{\mathsf{c}\cdot n}$ / $2^{\mathsf{c}\cdot n \log n}$

$2^{\mathsf{c}\cdot\beta}$, `BKZ`

$\mathrm{poly}(n)$, `LLL`

Time

γ

$\mathrm{poly}(n)$

$2^{\frac{n}{\beta}\log\beta}$

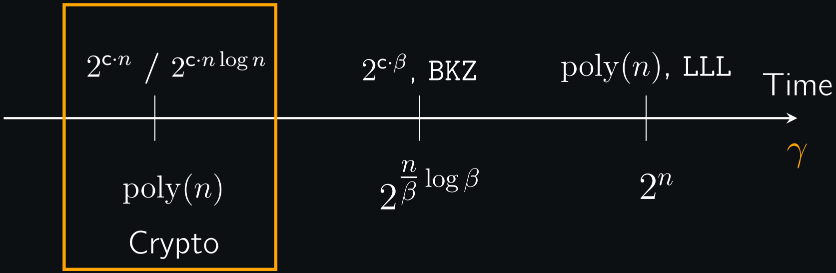
2^{n}

Crypto

Asymptotical Hardness of SVP (non-leading order terms omitted)

$$||\mathbf{v}_{\text{shortest}}|| \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$$

$$||\mathbf{v}_{\text{short}}|| \leq \gamma \cdot ||\mathbf{v}_{\text{shortest}}||$$

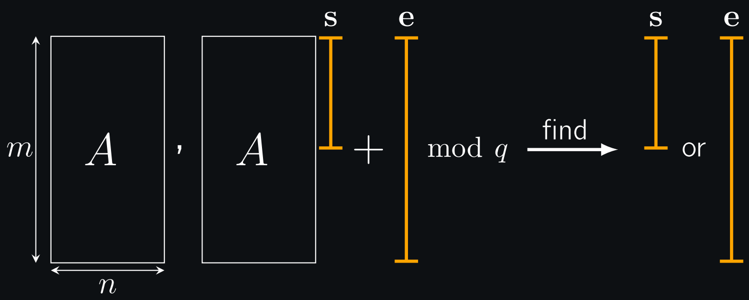


- Sieving (heuristical), assumed in this talk:
  Time(exactSVP) $= 2^{0.292n}$ Memory $= 2^{0.2075n}$
- Enumeration:
  Time(exactSVP) $= 2^{(1/2e) n \log n}$ Memory $= \text{poly}(n)$

Part II

The Learning with Errors problem

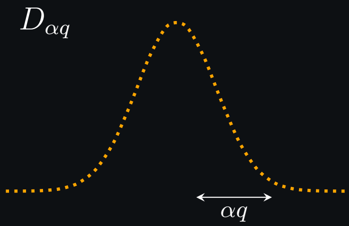
LWE (Regev'05)



$$A \xleftarrow{\$} \mathbb{Z}_q^{m\times n}$$

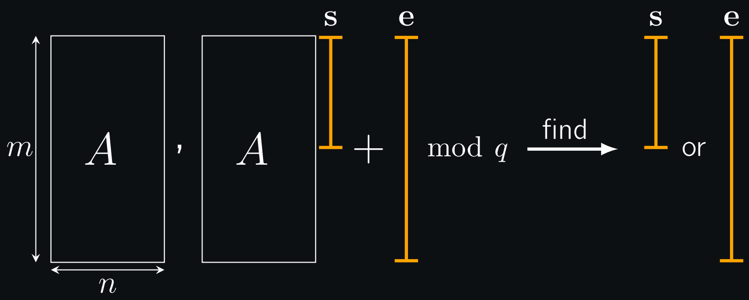
$$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^{n}$$

$$\mathbf{e} \leftarrow D_{\alpha q}^{m}$$



Typical parameters: $n = \Theta(\text{bit security})$, $q = n^{\Theta(1)}$, $m = \Theta(n \log q)$, $\alpha = \sqrt{n}/q$.

LWE is BDD

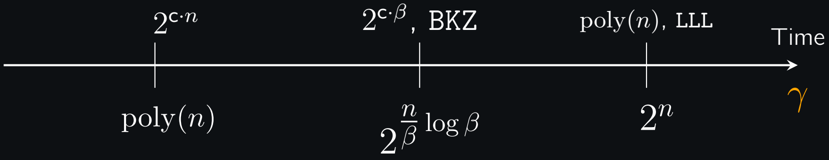


- A defines the Construction-A lattice

$$\mathcal{L}_q(A) = A\mathbb{Z}_q^n + q\mathbb{Z}^m$$

- W.h.p., $\mathcal{L}_q(A)$ is of dim. m and $\det(\mathcal{L}_q(A)) = q^{m-n}$.
- $As + e \bmod q$ is a point near $\mathcal{L}_q(A)$ at distance $\Theta(\sqrt{m}\alpha q)$
- $(A, As + e)$ is a BDD instance on $\mathcal{L}_q(A)$ with $\gamma = \frac{q^{1-n/m}}{\alpha q}$

Hardness of LWE under lattice-based attacks (non-leading terms omitted)



For LWE parameters (n, m, q, α), $\gamma = \frac{q^{1-n/m}}{\alpha q}$

$$T(\mathsf{LWE}) = \exp\left(\mathsf{c}\cdot\frac{\lg q}{\lg^2\alpha}\lg\left(\frac{n\lg q}{\lg^2\alpha}\right)\cdot n\right)$$

This complexity is obtained by solving for β

$$2^{\frac{m}{\beta}\log\beta} = \frac{q^{1-n/m}}{\alpha q}$$

and choosing $m = \Omega(n)$ that minimizes the solution.

LWE vs. Dihedral Coset Problem

Dimension: n, modulus: $q = \mathrm{poly}(n)$, $\alpha > 0$

LWE: Given

$$(\mathbf{a}_1, \langle \mathbf{a}_1 , \mathbf{s} \rangle + e_1 \bmod q)$$
$$\vdots$$
$$(\mathbf{a}_m, \langle \mathbf{a}_m , \mathbf{s} \rangle + e_m \bmod q),$$

find $\mathbf{s}$.

LWE vs. Dihedral Coset Problem

Dimension: n, modulus: $q = \mathrm{poly}(n)$, $\alpha > 0$

LWE: Given

$(\mathbf{a}_1, \langle \mathbf{a}_1 , \mathbf{s}\rangle + e_1 \bmod q)$

$\vdots$

$(\mathbf{a}_m, \langle \mathbf{a}_m , \mathbf{s}\rangle + e_m \bmod q)$,

find $\mathbf{s}$.

DCP: Given

$|0, x_1\rangle + |1, x_1 + s \bmod N\rangle$

$\vdots$

$|0, x_\ell\rangle + |1, x_\ell + s \bmod N\rangle$

find s.

LWE vs. Dihedral Coset Problem

Dimension: n, modulus: $q = \mathrm{poly}(n)$, $\alpha > 0$

LWE: Given	$\leq$ [Regev'02]	DCP: Given
$(\mathbf{a}_1, \langle \mathbf{a}_1, \mathbf{s} \rangle + e_1 \bmod q)$		$\lvert 0, x_1 \rangle + \lvert 1, x_1 + s \bmod N \rangle$
$\vdots$		$\vdots$
$(\mathbf{a}_m, \langle \mathbf{a}_m, \mathbf{s} \rangle + e_m \bmod q)$,		$\lvert 0, x_\ell \rangle + \lvert 1, x_\ell + s \bmod N \rangle$
find $\mathbf{s}$.		find s.

LWE vs. Dihedral Coset Problem

Dimension: n, modulus: $q = \mathrm{poly}(n)$, $\alpha > 0$

<u>LWE</u>: Given

$(\mathbf{a}_1, \langle \mathbf{a}_1 , \mathbf{s} \rangle + e_1 \bmod q)$

$\vdots$

$(\mathbf{a}_m, \langle \mathbf{a}_m , \mathbf{s} \rangle + e_m \bmod q)$,

find $\mathbf{s}$.

$\leq$

[Regev'02]

<u>DCP</u>: Given

$|0, x_1\rangle + |1, x_1 + s \bmod N\rangle$

$\vdots$

$|0, x_\ell\rangle + |1, x_\ell + s \bmod N\rangle$

find s.

Does not asymptotically improve upon classical algorithms

LWE vs. Dihedral Coset Problem

Dimension: n, modulus: $q = \mathrm{poly}(n)$, $\alpha > 0$

<u>LWE</u>: Given

$(\mathbf{a}_1, \langle \mathbf{a}_1 , \mathbf{s} \rangle + e_1 \bmod q)$

$\vdots$

$(\mathbf{a}_m, \langle \mathbf{a}_m , \mathbf{s} \rangle + e_m \bmod q)$,

find $\mathbf{s}$.

$\leq$
[Regev'02]

<u>DCP</u>: Given

$|0, x_1\rangle + |1, x_1 + s \bmod N\rangle$

$\vdots$

$|0, x_\ell\rangle + |1, x_\ell + s \bmod N\rangle$

find s.

Does not asymptotically improve upon classical algorithms

Lattices:

$$\exp\left(\mathsf{c} \cdot \frac{\lg q \lg n}{(\lg \alpha)^2} \cdot n\right)$$

Kuperberg's alg:

$$\exp\left(\mathsf{c}'(\log \ell + \log N / \log \ell)\right)$$

The reduction produces $\ell = \mathrm{poly}(n)$, $N = 2^{n \log q}$

Q: What is c'?

LWE vs. Dihedral Coset Problem

Dimension: n, modulus: $q = \mathrm{poly}(n)$, $\alpha > 0$

LWE: Given	$\leq$ [Regev'02]	DCP: Given
$(\mathbf{a}_1, \langle \mathbf{a}_1, \mathbf{s}\rangle + e_1 \bmod q)$		$\|0, x_1\rangle + \|1, x_1 + s \bmod N\rangle$
$\vdots$	$\overset{?}{\geq}$	$\vdots$
$(\mathbf{a}_m, \langle \mathbf{a}_m, \mathbf{s}\rangle + e_m \bmod q)$,		$\|0, x_\ell\rangle + \|1, x_\ell + s \bmod N\rangle$
find $\mathbf{s}$.		find s.

Does not asymptotically improve upon classical algorithms

Lattices:
$$\exp\left(\mathsf{c} \cdot \frac{\lg q \lg n}{(\lg \alpha)^2} \cdot n\right)$$

Kuperberg's alg:
$$\exp\left(\mathsf{c}'(\log \ell + \log N / \log \ell)\right)$$

The reduction produces $\ell = \mathrm{poly}(n)$, $N = 2^{n \log q}$

Q: What is c'?

Extended DCP, BKSW'18

EDCP

for a distr. $\mathcal{D}$

$$\sum_{j \in \mathsf{sup}(\mathcal{D})} \mathcal{D}(j) \left|j\right\rangle \left|\mathbf{x} + j \cdot \mathbf{s}\right\rangle$$

DCP

$$\left|0\right\rangle \left|x\right\rangle + \left|1\right\rangle \left|x + s\right\rangle$$

Extended DCP, BKSW'18

EDCP

for a distr. $\mathcal{D}$

$$\sum_{j \in \mathsf{sup}(\mathcal{D})} \mathcal{D}(j) \left|j\right\rangle \left|\mathbf{x} + j \cdot \mathbf{s}\right\rangle$$

DCP

$$\left|0\right\rangle \left|x\right\rangle + \left|1\right\rangle \left|x + s\right\rangle$$

G-EDCP

$$\sum_{j \in \mathbb{Z}} \rho_r(j) \left|j\right\rangle \left|\mathbf{x} + j \cdot \mathbf{s}\right\rangle$$

U-EDCP

$$\sum_{j=0}^{M-1} \left|j\right\rangle \left|\mathbf{x} + j \cdot \mathbf{s}\right\rangle$$

Extended DCP, BKSW'18

EDCP

for a distr. $\mathcal{D}$

$$\sum_{j \in \mathsf{sup}(\mathcal{D})} \mathcal{D}(j) \left|j\right\rangle \left|\mathbf{x} + j \cdot \mathbf{s}\right\rangle$$

DCP

$$\left|0\right\rangle \left|x\right\rangle + \left|1\right\rangle \left|x + s\right\rangle$$

G-EDCP

$$\sum_{j \in \mathbb{Z}} \rho_r(j) \left|j\right\rangle \left|\mathbf{x} + j \cdot \mathbf{s}\right\rangle$$

U-EDCP

$$\sum_{j=0}^{M-1} \left|j\right\rangle \left|\mathbf{x} + j \cdot \mathbf{s}\right\rangle$$

We can show that

$$\boxed{\text{LWE} \iff \text{G-EDCP} \iff \text{U-EDCP} < \text{DCP}}$$

$\iff$ hides polynomial loses

Extended DCP, BKSW'18

EDCP

for a distr. $\mathcal{D}$

$$\sum_{j \in \mathsf{sup}(\mathcal{D})} \mathcal{D}(j) \left|j\right\rangle \left|\mathbf{x} + j \cdot \mathbf{s}\right\rangle$$

DCP

$$\left|0\right\rangle \left|x\right\rangle + \left|1\right\rangle \left|x + s\right\rangle$$

G-EDCP

$$\sum_{j \in \mathbb{Z}} \rho_r(j) \left|j\right\rangle \left|\mathbf{x} + j \cdot \mathbf{s}\right\rangle$$

U-EDCP

$$\sum_{j=0}^{M-1} \left|j\right\rangle \left|\mathbf{x} + j \cdot \mathbf{s}\right\rangle$$

We can show that

$$\boxed{\text{LWE} \iff \text{G-EDCP} \iff \text{U-EDCP} < \text{DCP}}$$

$\iff$ hides polynomial loses

Q: Complexity of Kuperberg's algorithm for EDCP?

Part III

Efficient lattice-based crypto

Algebraic assumptions

- To store an instance of LWE we need $\Omega(n^2 \log q)$ bits
- Matrix-vector multiplication costs $O(n^2)$ operations in $\mathbb{Z}_q$

$\Longrightarrow$ 'standard' LWE-based primitives are slow

Solutions:

1. Algebraic versions of LWE
2. NTRU

Polynomial-LWE, SSTX'09

Let $f \in \mathbb{Z}[x]$ - monic irreduc. of degree n, $q \geq 2, \alpha > 0$

$$a = \sum_i a_i x^i \in \mathbb{Z}[x]/f \;\longrightarrow\; (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

Search Poly-LWE$_f$:

- Choose $s \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Choose a_i's $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample coeffs of e_i from $D_{\alpha q}$

Given $(a_1, \ldots, a_m)$ and
$(a_1 \cdot s + e_1, \ldots a_m \cdot s + e_m)$, find s.

Polynomial-LWE, SSTX'09

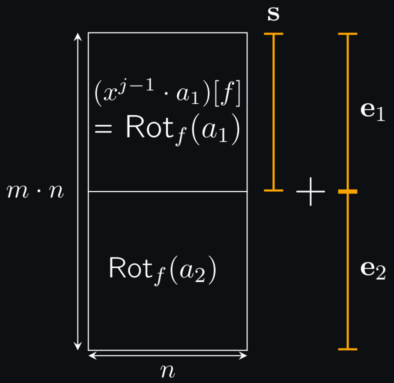
Let $f \in \mathbb{Z}[x]$ - monic irreduc. of degree n, $q \geq 2, \alpha > 0$

$$a = \sum_i a_i x^i \in \mathbb{Z}[x]/f \;\longrightarrow\; (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

Search Poly-LWE$_f$:

- Choose $s \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Choose a_i's $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample coeffs of e_i from $D_{\alpha q}$

Given $(a_1, \ldots, a_m)$ and $(a_1 \cdot s + e_1, \ldots a_m \cdot s + e_m)$, find s.



Polynomial-LWE, SSTX'09

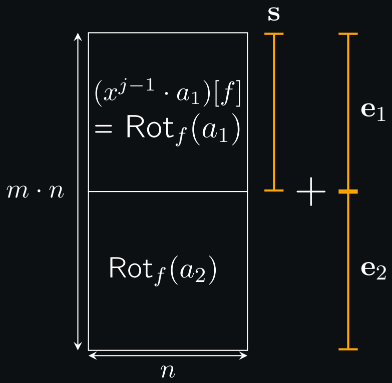
Let $f \in \mathbb{Z}[x]$ - monic irreduc. of degree n, $q \geq 2, \alpha > 0$

$$a = \sum_i a_i x^i \in \mathbb{Z}[x]/f \;\longrightarrow\; (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$$

Search Poly-LWE$_f$:

- Choose $s \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Choose a_i's $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample coeffs of e_i from $D_{\alpha q}$

Given $(a_1, \ldots, a_m)$ and $(a_1 \cdot s + e_1, \ldots a_m \cdot s + e_m)$, find s.



One sample $(a_i, a_i s + e_i)$ gives n correlated LWE samples

We can multiply polynomials in time $\widetilde{\mathcal{O}}(n)$

Ring-LWE for $f = x^{2^k} + 1$, LPR'10

Let $f = x^n + 1$ - cyclotomic of degree $n = 2^k$, $q \geq 2, \alpha > 0$

Let $\omega_1, \ldots, \omega_n \in \mathbb{C}$ - roots of f, V_f - Vandermonde for ω_i's

$$\sigma : \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a(\omega_0), \ldots, a(\omega_{n-1})) \in \mathbb{C}^n$$

Search Ring-LWE$_f$:

- Choose $s \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Choose a_i's $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample $\sigma(e_i)$'s from $D_{\alpha q}$

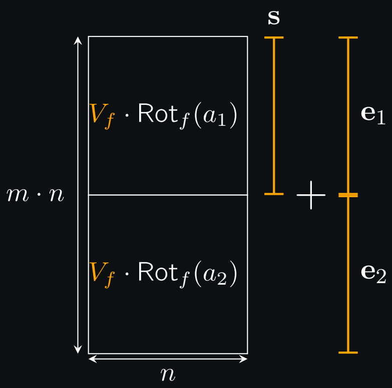
Ring-LWE for $f = x^{2^k} + 1$, LPR'10

Let $f = x^n + 1$ - cyclotomic of degree $n = 2^k$, $q \geq 2, \alpha > 0$
Let $\omega_1, \ldots, \omega_n \in \mathbb{C}$ - roots of f, V_f - Vandermonde for ω_i's

$$\sigma : \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a(\omega_0), \ldots, a(\omega_{n-1})) \in \mathbb{C}^n$$

Search Ring-LWE$_f$:

- Choose $s \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Choose a_i's $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample $\sigma(e_i)$'s from $D_{\alpha q}$



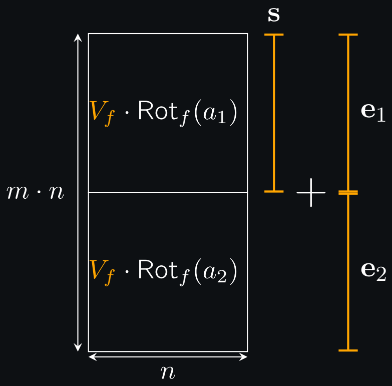
Ring-LWE for $f = x^{2^k} + 1$, LPR'10

Let $f = x^n + 1$ - cyclotomic of degree $n = 2^k$, $q \geq 2, \alpha > 0$
Let $\omega_1, \ldots, \omega_n \in \mathbb{C}$ - roots of f, V_f - Vandermonde for ω_i's

$$\sigma : \sum_i a_i x^i \in \mathbb{Z}[x]/f \longrightarrow (a(\omega_0), \ldots, a(\omega_{n-1})) \in \mathbb{C}^n$$

Search Ring-LWE$_f$:

- Choose $s \xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Choose a_i's $\xleftarrow{\$} \mathbb{Z}_q[x]/f$
- Sample $\sigma(e_i)$'s from $D_{\alpha q}$



- Multiply in time $O(n \log q)$
- Poly-LWE and Ring-LWE are closely related for f's with well-conditioned V_f, [RSW'18]

NTRU, HPS'98

Let $q \geq 2$, Φ - polynomial of degree n,

$$R_\Phi = \mathbb{Z}_q[x]/(\Phi)$$

E.g., $\Phi = x^n - 1$ or $\Phi = x^n + 1$ or $\Phi = x^p - x - 1$

Search NTRU assumption:

- Choose f invertible in R_Φ and with coeffs in $\{-1, 0, 1\}$
- Choose g and with coeffs in $\{-1, 0, 1\}$
- Publish $h = g/f \in R_\Phi$

Given h, it is hard to find 'small' (f, g) s.t. $h = g/f \in R_\Phi$.

NTRU, HPS'98

Let $q \geq 2$, Φ - polynomial of degree n,

$$R_\Phi = \mathbb{Z}_q[x]/(\Phi)$$

E.g., $\Phi = x^n - 1$ or $\Phi = x^n + 1$ or $\Phi = x^p - x - 1$

Search NTRU assumption:

- Choose f invertible in R_Φ and with coeffs in $\{-1, 0, 1\}$
- Choose g and with coeffs in $\{-1, 0, 1\}$
- Publish $h = g/f \in R_\Phi$

Given h, it is hard to find 'small' (f, g) s.t. $h = g/f \in R_\Phi$.

NTRU lattice:

$$\begin{bmatrix} \mathrm{Rot}(h) & q\mathbf{I} \\ \mathbf{I} & \mathbf{0} \end{bmatrix} \cdot \begin{bmatrix} \vec{f} \\ \vec{k} \end{bmatrix} = \begin{bmatrix} \vec{g} \\ \vec{f} \end{bmatrix}$$

- h defines a $2n$-dim lattice

$$\mathcal{L} = \left\{ \begin{bmatrix} \mathrm{Rot}(h) & q\mathbf{I} \\ \mathbf{I} & \mathbf{0} \end{bmatrix} \cdot R_\Phi^2 \right\}$$

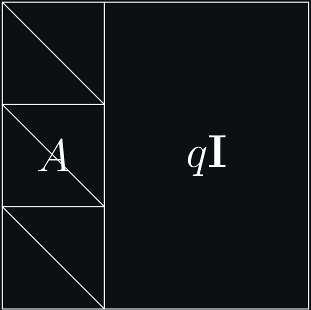
- $(\vec{g}, \vec{f})$ - short vector in $\mathcal{L}$

Classical hardness of Poly/Ring LWE and NTRU under lattice attacks

Let $q \geq 2$, Φ - polynomial of degree n,

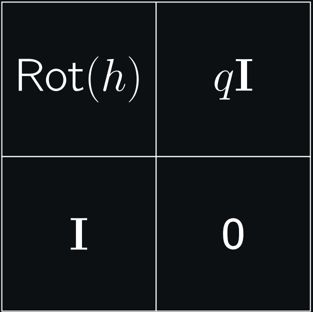
$$R_\Phi = \mathbb{Z}_q[x]/(\Phi)$$

Ring-/Poly-LWE



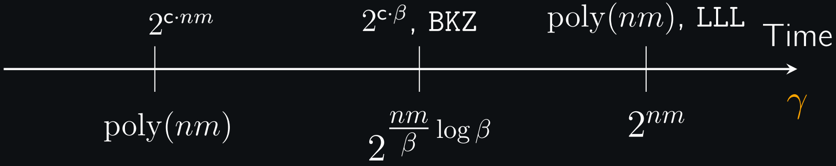
A defines rank-m module over R_Φ

NTRU



h defines rank-2 module over R_Φ

For $m > 1$, SVP in arbitrary rank-m module over R_Φ is not known to be easier than 'standard' SVP on an arbitrary nm-dimensional lattice ($\mathrm{poly}(n)$ accelerations exist):



Classical hardness of Poly/Ring LWE and NTRU under lattice attacks

Caveats:

- For SVP in arbitrary rank-1 module from cyclotomic R_Φ, can achieve $\gamma = 2^{\widetilde{\mathcal{O}}(\sqrt{n})}$ in time $2^{\widetilde{\mathcal{O}}(\sqrt{n})}$ using Biasse-Espitau-Fouque-Gélin-Kirchner'17 / Cramer-Ducas-Peikert-Regev'16/ Cramer-Ducas-Wesolowski'17

Classical hardness of Poly/Ring LWE and NTRU under lattice attacks

Caveats:

- For SVP in arbitrary rank-1 module from cyclotomic R_Φ, can achieve $\gamma = 2^{\widetilde{\mathcal{O}}(\sqrt{n})}$ in time $2^{\widetilde{\mathcal{O}}(\sqrt{n})}$ using Biasse-Espitau-Fouque-Gélin-Kirchner'17 / Cramer-Ducas-Peikert-Regev'16/ Cramer-Ducas-Wesolowski'17
- Can do better for ideals from R_Φ if allow precomputations on R_Φ (see Hanrot-Pellet–Mary-Stehlé'19)

Classical hardness of Poly/Ring LWE and NTRU under lattice attacks

Caveats:

- For SVP in arbitrary rank-1 module from cyclotomic R_Φ, can achieve $\gamma = 2^{\widetilde{\mathcal{O}}(\sqrt{n})}$ in time $2^{\widetilde{\mathcal{O}}(\sqrt{n})}$ using Biasse-Espitau-Fouque-Gélin-Kirchner'17 / Cramer-Ducas-Peikert-Regev'16/ Cramer-Ducas-Wesolowski'17
- Can do better for ideals from R_Φ if allow precomputations on R_Φ (see Hanrot-Pellet–Mary-Stehlé'19)
- Using Pataki-Tural result on small volume sublattices, Fouque-Kirchner show that $(f, g) \leftarrow D_{\alpha q}^{2n}$ of NTRU can be recovered using β-BKZ with

$$\beta = \widetilde{\mathcal{O}}\left(\frac{n \lg(\alpha q)}{\lg^2 q}\right)$$

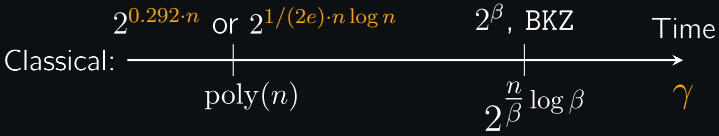
for large enough q and αq. This is $\mathrm{poly}(n)$ for $q = 2^{\widetilde{\mathcal{O}}(\sqrt{n})}$.

Part IV

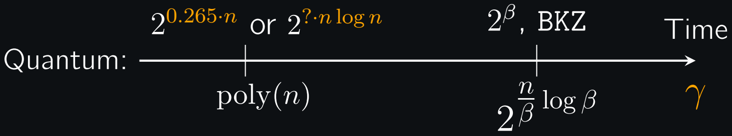
Known quantum speed-ups for SVP

Quantum speed-ups for SVP/γ-SVP

I. (A bit) faster SVP for 'standard' lattices



- for $0.292n$ see [BDGL16]
- for $1/(2e)$ see [HS07]



- for $0.265n$ see [Laarhoven16]
- for $?n \log n$ see [ANS18]

Quantum speed-ups for SVP/γ-SVP

II. (A lot) faster SVP for ideal lattices

Quantum: $2^{0.265 \cdot n}$ or $2^{? \cdot n \log n}$ — 2^{β} — $\mathrm{poly}(n)$ — Time

$\mathrm{poly}(n)$ — $2^{\frac{n}{\beta}\log\beta}$ — $2^{\sqrt{n}}$ — γ

- see [BF16] and [CDPR16] for $2^{\widetilde{\mathcal{O}}(\sqrt{n})}$-SVP in time $\mathrm{poly}(n)$ for a principal ideal in prime-power cyclotomics
- see [CDW17] for $2^{\widetilde{\mathcal{O}}(\sqrt{n})}$-SVP algorithm in time $\mathrm{poly}(n)$ for an arbitrary ideal in prime-power cyclotomics

Open questions

- Quantum speed-ups for memory-efficient single-exponential SVP algorithms
- Quantum hardness of LWE under Kuperberg's algorithm for the Dihedral Coset Problem
- Quantum acceleration for LLL/BKZ

References I

- [ANS18] Y. Aono, P. Q. Nguyen, Y. Shen. Quantum Lattice Enumeration and Tweaking Discrete Pruning
- [BDGL16] A. Becker, L. Ducas, N. Gama, T. Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving.
- [BEF+17] J.-F. Biasse, T. Espitau, P.-A. Fouque, A. Gélin, P. Kirchner. Computing generator in cyclotomic integer rings.
- [BF16] J.-F. Biasse F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields.
- [BKSW18] Z. Brakerski, E. Kirshanova, D. Stehlé, W. Wen. Learning With Errors and Extrapolated Dihedral Cosets
- [CDPR16] R. Cramer, L. Ducas, C. Peikert, O. Regev. Recovering short generators of principal ideals in cyclotomic rings.
- [CDW17] R. Cramer, L. Ducas, B. Wesolowski. Short Stickelberger class relations and application to ideal-SVP.
- [HPS98] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: a ring based public key cryptosystem

References II

- [HS07] G.Hanrot, D.Stehlé. Improved Analysis of Kannan's Shortest Lattice Vector Algorithm
- [HMPS19] G.Hanrot, A.Mary–Pellet, D.Stehlé. Approx-SVP in Ideal Lattices with Pre-processing
- [RSW18]M. Rosca, D.Stehlé, A. Wallet. On the ring-LWE and polynomial-LWE problems.
- [LPR10] V. Lyubashevsky, C. Peikert, O. Regev. On ideal lattices and learning with errors over rings.
- [Regev02] O.Regev. Quantum computation and lattice problems
- [SSTX09] R. Steinfeld, D.Stehlé. K. Tanaka, K. Xagawa. Efficient Public-Key Encryption Based on Ideal Lattices (Extended Abstract)