Algorithmic problems over ideal lattices

Alice Pellet-Mary

CNRS, université de Bordeaux

Discrete Mathematics, Codes and Cryptography eSeminar, Paris 8

(Partly based on a joint work with Guillaume Hanrot and Damien Stehlé)

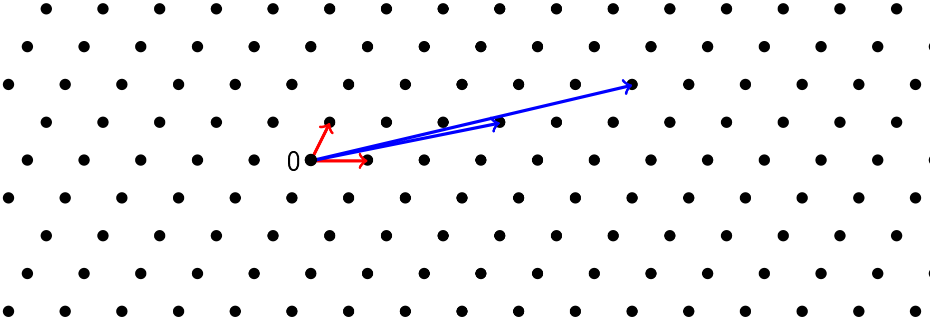
Outline of the talk

1. Lattice problems and LWE
2. Adding algebraic structure
3. Algorithms for ideal-SVP

Outline of the talk

1. Lattice problems and LWE
2. Adding algebraic structure
3. Algorithms for ideal-SVP

Lattices

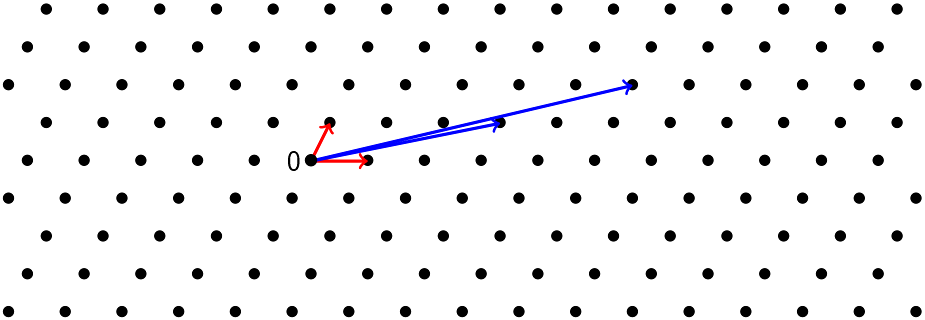


Lattice

A lattice L is a subset of $\mathbb{R}^n$ of the form $L = \{Bx \mid x \in \mathbb{Z}^n\}$, with $B \in \mathbb{R}^{n \times n}$ invertible. B is a basis of L, and n is its rank.

$\begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix}$ and $\begin{pmatrix} 17 & 11 \\ 4 & 2 \end{pmatrix}$ are two bases of the above lattice.

Lattices

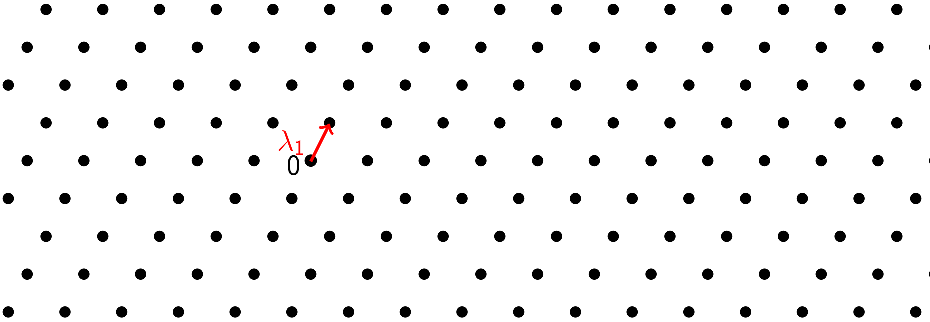


Lattice

A lattice L is a subset of $\mathbb{R}^n$ of the form $L = \{Bx \mid x \in \mathbb{Z}^n\}$, with $B \in \mathbb{R}^{n \times n}$ invertible. B is a basis of L, and n is its rank.

We represent a lattice by any of its basis

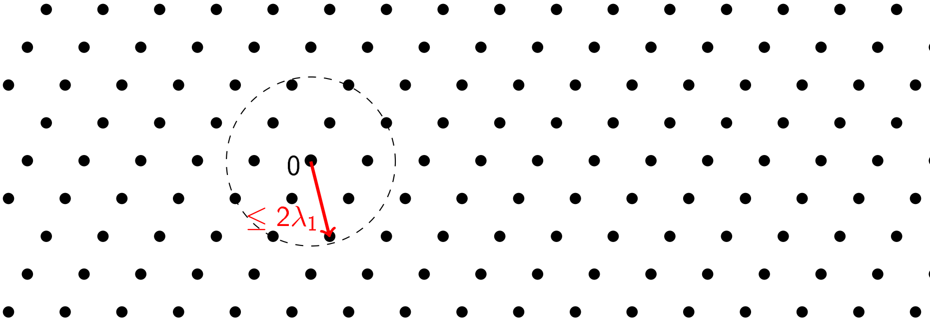
Shortest and Closest vector problems



Shortest Vector Problem (SVP)

Find a shortest (in Euclidean norm) non-zero vector.
Its Euclidean norm is denoted λ_1.

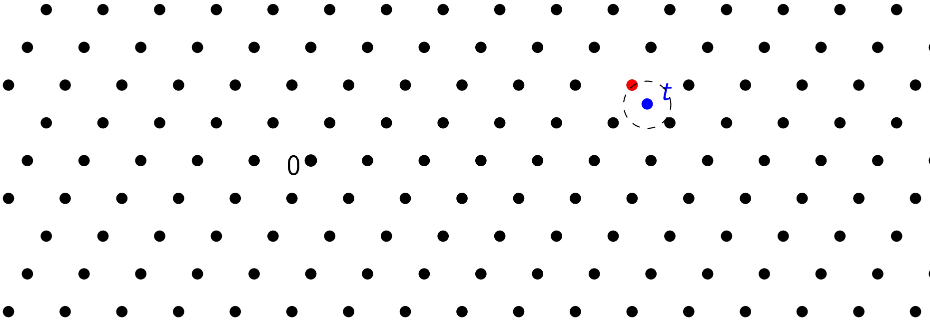
Shortest and Closest vector problems



Approximate Shortest Vector Problem (approx-SVP)

Find a short (in Euclidean norm) non-zero vector.
(e.g. of norm $\leq 2\lambda_1$).

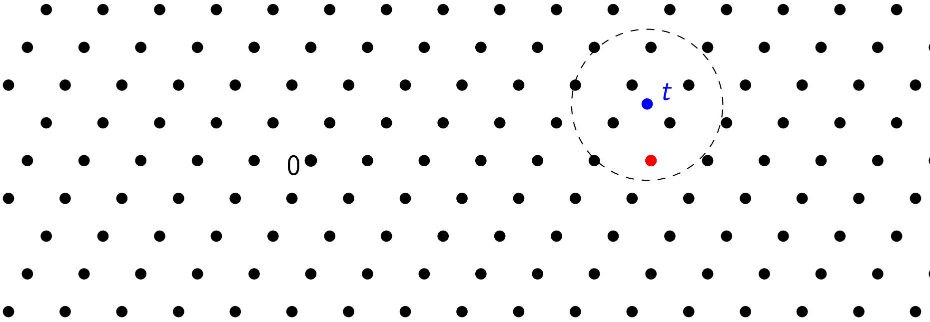
Shortest and Closest vector problems



Closest Vector Problem (CVP)

Given a target point t, find a point of the lattice closest to t.

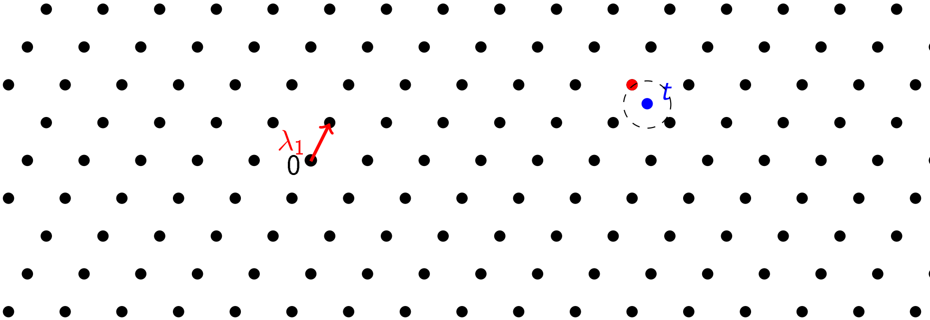
Shortest and Closest vector problems



Approximate Closest Vector Problem (approx-CVP)

Given a target point t, find a point of the lattice close to t.

Shortest and Closest vector problems

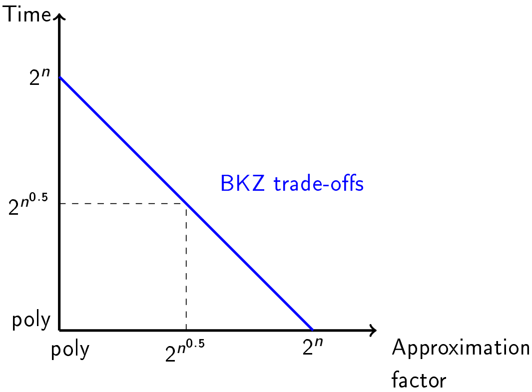


SVP and CVP are hard to solve when n increases

- even with a quantum computer
- even if we allow small approximation factor $(\gamma = \mathrm{poly}(n))$

Hardness of SVP and CVP

Best Time/Approximation trade-off for SVP, CVP (even quantumly):
BKZ algorithm [Sch87,SE94]

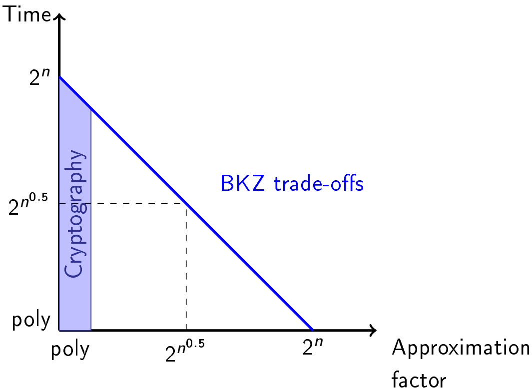


[Sch87] C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. TCS.

[SE94] C.-P. Schnorr and M. Euchner. Lattice basis reduction: improved practical algorithms and solving subset sum problems. Mathematical programming.

Hardness of SVP and CVP

Best Time/Approximation trade-off for SVP, CVP (even quantumly):
BKZ algorithm [Sch87,SE94]



[Sch87] C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. TCS.
[SE94] C.-P. Schnorr and M. Euchner. Lattice basis reduction: improved practical algorithms and solving subset sum problems. Mathematical programming.

The LWE problem

LWE (Learning With Errors)

Sample $\boxed{A} \leftarrow \text{Uniform}(\mathbb{Z}_q^{n\times n})$ and $\boxed{s}$, $\boxed{e} \leftarrow \text{Uniform}(\{-B,\cdots,B\}^n)$

Given $\boxed{A}$ and $\boxed{b}$, where $\boxed{b} := \boxed{A}\boxed{s} + \boxed{e} \bmod q$

Recover s or e

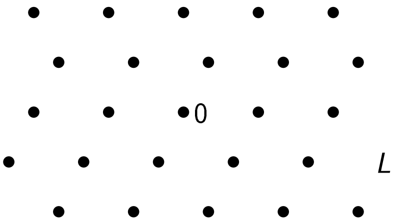
The LWE problem

LWE (Learning With Errors)

Sample $\boxed{A} \leftarrow \mathrm{Uniform}(\mathbb{Z}_q^{n\times n})$ and $\boxed{s}$, $\boxed{e} \leftarrow \mathrm{Uniform}(\{-B, \cdots, B\}^n)$

Given $\boxed{A}$ and $\boxed{b}$, where $\boxed{b} := \boxed{A}\boxed{s} + \boxed{e} \bmod q$

Recover s or e



$$L = \{x \in \mathbb{Z}^n \mid \exists s \in \mathbb{Z}^n, As = x \bmod q\}$$

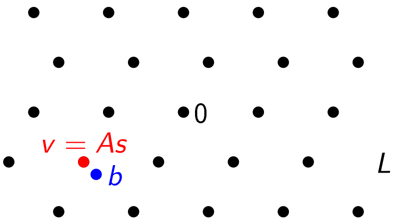
The LWE problem

LWE (Learning With Errors)

Sample $\boxed{A} \leftarrow \text{Uniform}(\mathbb{Z}_q^{n\times n})$ and $\boxed{s}$, $\boxed{e} \leftarrow \text{Uniform}(\{-B, \cdots, B\}^n)$

Given $\boxed{A}$ and $\boxed{b}$, where $\boxed{b} := \boxed{A}\boxed{s} + \boxed{e} \bmod q$

Recover s or e



$$L = \{x \in \mathbb{Z}^n \,|\, \exists s \in \mathbb{Z}^n, As = x \bmod q\}$$

$$b = v + e,$$

where $v \in L$ and e small

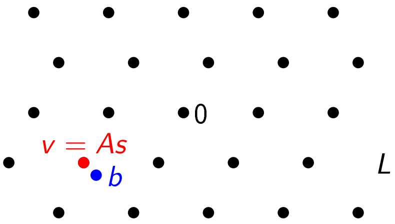
The LWE problem

LWE (Learning With Errors)

Sample $\boxed{A} \leftarrow \text{Uniform}(\mathbb{Z}_q^{n \times n})$ and $\boxed{s}$, $\boxed{e} \leftarrow \text{Uniform}(\{-B, \cdots, B\}^n)$

Given $\boxed{A}$ and $\boxed{b}$, where $\boxed{b} := \boxed{A}\boxed{s} + \boxed{e} \bmod q$

Recover s or e



$$L = \{x \in \mathbb{Z}^n \mid \exists s \in \mathbb{Z}^n, As = x \bmod q\}$$

$$b = v + e,$$
where $v \in L$ and e small

$\boxed{\text{LWE} \approx \text{CVP in } L}$

The LWE problem: advantages

$$\boxed{\text{LWE}} \qquad \boxed{\text{SVP}} \longleftrightarrow \boxed{\text{CVP}}$$

The LWE problem: advantages

$$\boxed{\text{LWE}} \xleftrightarrow{\quad * \quad} \boxed{\text{SVP}} \longleftrightarrow \boxed{\text{CVP}}$$

* Not completely exact: it should be LWE $\leftrightarrow$ SIVP (= short independent vectors problem)

The LWE problem: advantages

$$\boxed{\text{LWE}} \overset{*}{\longleftrightarrow} \boxed{\text{SVP}} \longleftrightarrow \boxed{\text{CVP}}$$

Advantages of LWE over SVP/CVP:

- problem hard on average

* Not completely exact: it should be LWE $\leftrightarrow$ SIVP (= short independent vectors problem)

The LWE problem: advantages

decision-LWE $\longleftrightarrow$ LWE $\xleftrightarrow{\quad * \quad}$ SVP $\longleftrightarrow$ CVP

Advantages of LWE over SVP/CVP:

- problem hard on average
- decision variant as hard as the search variant

* Not completely exact: it should be LWE $\leftrightarrow$ SIVP (= short independent vectors problem)

Outline of the talk

1 Lattice problems and LWE

2 Adding algebraic structure

3 Algorithms for ideal-SVP

Adding structure

Why: to improve efficiency of cryptographic schemes

Adding structure

Why: to improve efficiency of cryptographic schemes
How: use structured matrices

Adding structure

Why: to improve efficiency of cryptographic schemes
How: use structured matrices

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \ddots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{pmatrix}$$

non structured matrix

- storage: n^2
- matrix $\times$ vector : $O(n^2)$

Adding structure

Why: to improve efficiency of cryptographic schemes
How: use structured matrices

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \ddots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{pmatrix}$$

non structured matrix

- storage: n^2
- matrix $\times$ vector : $O(n^2)$

$$\begin{pmatrix} a_1 & -a_n & \cdots & -a_2 \\ a_2 & a_1 & \cdots & -a_3 \\ \vdots & \ddots & \ddots & \vdots \\ a_n & a_{n-1} & \dots & a_1 \end{pmatrix}$$

structured matrix

- storage: n
- matrix $\times$ vector : $\widetilde{O}(n)$

SVP + structure = ideal-SVP

Definition

An ideal lattice is a lattice which has a basis (in columns) of the form

$$B = \begin{pmatrix} a_1 & -a_n & \cdots & -a_2 \\ a_2 & a_1 & \cdots & -a_3 \\ \vdots & \ddots & \ddots & \vdots \\ a_n & a_{n-1} & \dots & a_1 \end{pmatrix}$$

Remark. Not all bases of an ideal lattice have this shape.

SVP + structure = ideal-SVP

Definition

An ideal lattice is a lattice which has a basis (in columns) of the form

$$B = \begin{pmatrix} a_1 & -a_n & \cdots & -a_2 \\ a_2 & a_1 & \cdots & -a_3 \\ \vdots & \ddots & \ddots & \vdots \\ a_n & a_{n-1} & \dots & a_1 \end{pmatrix}$$

Remark. Not all bases of an ideal lattice have this shape.

$\boxed{\text{Ideal-SVP = SVP restricted to ideal lattices}}$

SVP + structure = ideal-SVP

Definition

An ideal lattice is a lattice which has a basis (in columns) of the form

$$B = \begin{pmatrix} a_1 & -a_n & \cdots & -a_2 \\ a_2 & a_1 & \cdots & -a_3 \\ \vdots & \ddots & \ddots & \vdots \\ a_n & a_{n-1} & \dots & a_1 \end{pmatrix}$$

Remark. Not all bases of an ideal lattice have this shape.

Ideal-SVP = SVP restricted to ideal lattices

Why is it called an ideal lattice?

Some definitions

Notation

$R = \mathbb{Z}[X]/(X^n + 1)$ for $n = 2^k$

Some definitions

Notation

$R = \mathbb{Z}[X]/(X^n + 1)$ for $n = 2^k$

- Units: $R^\times = \{a \in R \mid \exists b \in R, ab = 1\}$
  - e.g. $\mathbb{Z}^\times = \{-1, 1\}$

Some definitions

Notation

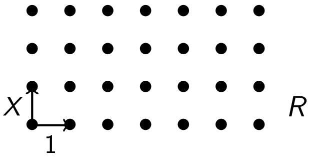
$R = \mathbb{Z}[X]/(X^n + 1)$ for $n = 2^k$

- Units: $R^\times = \{a \in R \mid \exists b \in R, ab = 1\}$
  - e.g. $\mathbb{Z}^\times = \{-1, 1\}$
- Principal ideals: $\langle g \rangle = \{gr \mid r \in R\}$ (i.e. all multiples of g)
  - e.g. $\langle 2 \rangle = \{\text{even numbers}\}$ in $\mathbb{Z}$
  - g is called a generator of $\langle g \rangle$
  - The generators of $\langle g \rangle$ are exactly the ug for $u \in R^\times$

$\langle g \rangle$ is an ideal lattice

$R \simeq \mathbb{Z}^n$

$$R = \mathbb{Z}[X]/(X^n + 1) \to \mathbb{Z}^n$$
$$r = r_0 + r_1 X + \cdots + r_{n-1} X^{n-1} \mapsto (r_0, r_1, \ldots, r_{n-1})$$

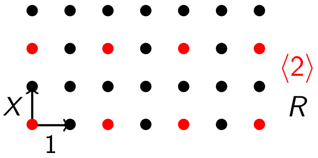


$\langle g \rangle$ is an ideal lattice

$R \simeq \mathbb{Z}^n$

$$R = \mathbb{Z}[X]/(X^n + 1) \to \mathbb{Z}^n$$
$$r = r_0 + r_1 X + \cdots + r_{n-1}X^{n-1} \mapsto (r_0, r_1, \ldots, r_{n-1})$$

$$\begin{cases} \langle g \rangle \subseteq R \simeq \mathbb{Z}^n \\ \text{stable by `$+$' and `-'} \end{cases} \Rightarrow \text{ lattice}$$



$\langle g \rangle$ is an ideal lattice

$R \simeq \mathbb{Z}^n$

$$R = \mathbb{Z}[X]/(X^n + 1) \to \mathbb{Z}^n$$
$$r = r_0 + r_1 X + \cdots + r_{n-1} X^{n-1} \mapsto (r_0, r_1, \ldots, r_{n-1})$$

$$\begin{cases} \langle g \rangle \subseteq R \simeq \mathbb{Z}^n \\ \text{stable by `}+\text{' and `-'} \end{cases} \Rightarrow \text{ lattice}$$

Basis: $g, gX, gX^2, \ldots, gX^{n-1}$

$\langle g \rangle$ is an ideal lattice

$R \simeq \mathbb{Z}^n$

$$R = \mathbb{Z}[X]/(X^n+1) \to \mathbb{Z}^n$$
$$r = r_0 + r_1 X + \cdots + r_{n-1}X^{n-1} \mapsto (r_0, r_1, \dots, r_{n-1})$$

$$\begin{cases} \langle g \rangle \subseteq R \simeq \mathbb{Z}^n \\ \text{stable by `+' and `-'} \end{cases} \Rightarrow \text{ lattice}$$

Basis: $g, gX, gX^2, \dots, gX^{n-1}$

$$\text{i.e.,} \quad \begin{pmatrix} g_0 & & & \\ g_1 & & & \\ \vdots & & & \\ g_{n-1} & & & \end{pmatrix}$$

$\langle g \rangle$ is an ideal lattice

$R \simeq \mathbb{Z}^n$

$$R = \mathbb{Z}[X]/(X^n + 1) \to \mathbb{Z}^n$$
$$r = r_0 + r_1 X + \cdots + r_{n-1} X^{n-1} \mapsto (r_0, r_1, \ldots, r_{n-1})$$

$$\begin{cases} \langle g \rangle \subseteq R \simeq \mathbb{Z}^n \\ \text{stable by `$+$' and `-'} \end{cases} \Rightarrow \text{ lattice}$$

Basis: $g, gX, gX^2, \ldots, gX^{n-1}$

$$\text{i.e.,} \quad \begin{pmatrix} g_0 & -g_{n-1} & & \\ g_1 & g_0 & & \\ \vdots & \vdots & & \\ g_{n-1} & g_{n-2} & & \end{pmatrix}$$

$\langle g \rangle$ is an ideal lattice

$R \simeq \mathbb{Z}^n$

$$R = \mathbb{Z}[X]/(X^n + 1) \to \mathbb{Z}^n$$
$$r = r_0 + r_1 X + \cdots + r_{n-1} X^{n-1} \mapsto (r_0, r_1, \ldots, r_{n-1})$$

$$\begin{cases} \langle g \rangle \subseteq R \simeq \mathbb{Z}^n \\ \text{stable by '+' and '-'} \end{cases} \Rightarrow \text{lattice}$$

Basis: $g, gX, gX^2, \ldots, gX^{n-1}$

$$\text{i.e., } \begin{pmatrix} g_0 & -g_{n-1} & \cdots & -g_1 \\ g_1 & g_0 & \cdots & -g_2 \\ \vdots & \vdots & \ddots & \vdots \\ g_{n-1} & g_{n-2} & \cdots & g_0 \end{pmatrix} \Rightarrow \text{Ideal lattice}$$

LWE + structure = Ring-LWE

LWE

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} + \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

LWE + structure = Ring-LWE

LWE

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix} \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} + \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

Ring-LWE

(more exactly Poly-LWE)

$$\begin{pmatrix} a_1 & \cdots & -a_2 \\ \vdots & \ddots & \vdots \\ a_n & \dots & a_1 \end{pmatrix} \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} + \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

LWE + structure = Ring-LWE

LWE

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix} \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} + \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

Ring-LWE

(more exactly Poly-LWE)

$$\begin{pmatrix} a_1 & \cdots & -a_2 \\ \vdots & \ddots & \vdots \\ a_n & \dots & a_1 \end{pmatrix} \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} + \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

$$= \ a(X) \cdot s(X) + e(X) \in R$$

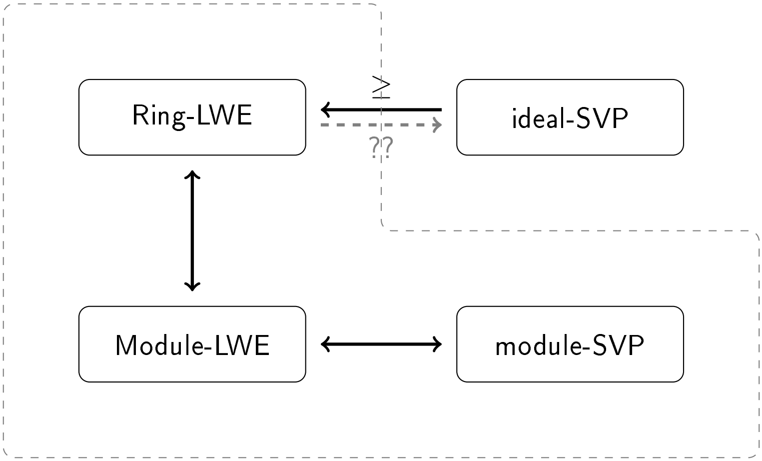
$R = \mathbb{Z}[X]/(X^n + 1)$

$a(X) := \sum_i a_i X^i, \quad s(X) := \sum_i s_i X^i, \quad e(X) := \sum_i e_i X^i \ \in R$

Ring-LWE vs ideal-SVP

$$\begin{tikzcd} \boxed{\text{Ring-LWE}} \arrow[r, dashed, "??"', shift right] & \boxed{\text{ideal-SVP}} \arrow[l, "\geq"', shift right] \end{tikzcd}$$

Ring-LWE vs ideal-SVP



Outline of the talk

1. Lattice problems and LWE
2. Adding algebraic structure
3. Algorithms for ideal-SVP

The problem to solve

ideal-SVP

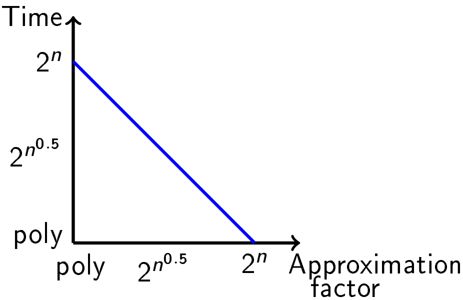
Given a basis of a principal ideal $\langle g \rangle$ and $\alpha \in (0, 1]$,
Find $r \in \langle g \rangle$ such that $\|r\| \leq 2^{n^\alpha} \cdot \lambda_1$.

The problem to solve

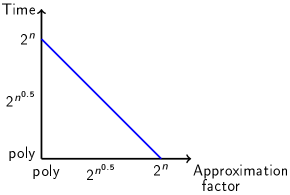
ideal-SVP

Given a basis of a principal ideal $\langle g \rangle$ and $\alpha \in (0, 1]$,
Find $r \in \langle g \rangle$ such that $\|r\| \le 2^{n^{\alpha}} \cdot \lambda_1$.

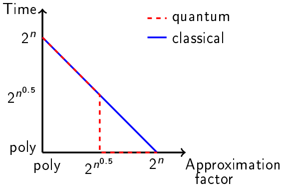
BKZ algorithm can do it in time $2^{O(n^{1-\alpha})}$, can we do better (using the structure)?



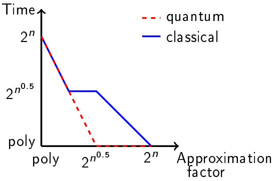
Known algorithms for ideal-SVP



BKZ algorithm



[CDPR16,CDW17]



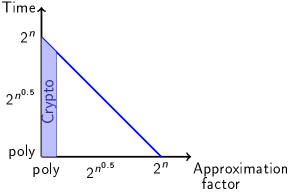
[PHS19]
(with $2^{O(n)}$ pre-processing)

[CDPR16] Cramer, Ducas, Peikert and Regev. Recovering Short Generators of Principal Ideals in Cyclotomic Rings, Eurocrypt.

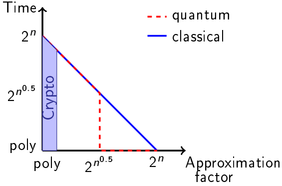
[CDW17] Cramer, Ducas and Wesolowski. Short Stickelberger Class Relations and Application to Ideal-SVP, Eurocrypt.

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

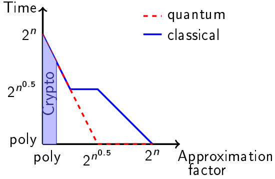
Known algorithms for ideal-SVP



BKZ algorithm



[CDPR16,CDW17]



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

Ring-LWE is not broken:

- Standard parameters of Ring-LWE are too small for the algorithms

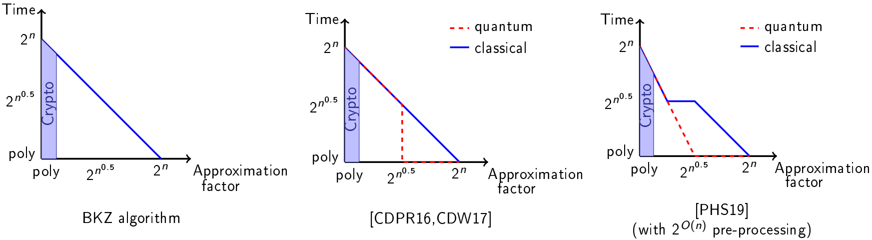
---

[CDPR16] Cramer, Ducas, Peikert and Regev. Recovering Short Generators of Principal Ideals in Cyclotomic Rings, Eurocrypt.

[CDW17] Cramer, Ducas and Wesolowski. Short Stickelberger Class Relations and Application to Ideal-SVP, Eurocrypt.

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

Known algorithms for ideal-SVP



Ring-LWE is not broken:

- Standard parameters of Ring-LWE are too small for the algorithms
- We don't know how to use an ideal-SVP solver to break Ring-LWE

[CDPR16] Cramer, Ducas, Peikert and Regev. Recovering Short Generators of Principal Ideals in Cyclotomic Rings, Eurocrypt.

[CDW17] Cramer, Ducas and Wesolowski. Short Stickelberger Class Relations and Application to Ideal-SVP, Eurocrypt.

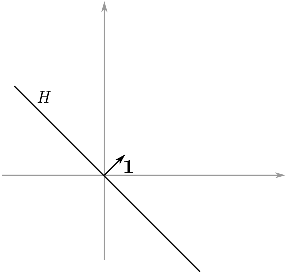
[PHS19] Pellet-Mary, Hanrot and Stehlé. Approx-SVP in ideal lattices with pre-processing, Eurocrypt.

Main ideas of the ideal-SVP algorithms

A tool: the Log space

Log : $R \to \mathbb{R}^n$ (somehow generalising log to R)

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



A tool: the Log space

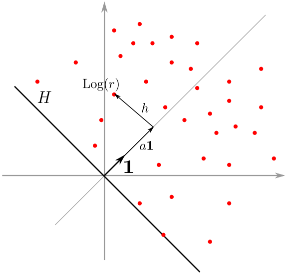
Log : $R \to \mathbb{R}^n$ (somehow generalising log to R)

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

Properties

$\mathrm{Log}\, r = h + a1$, with $h \in H$

- $a \geq 0$



A tool: the Log space

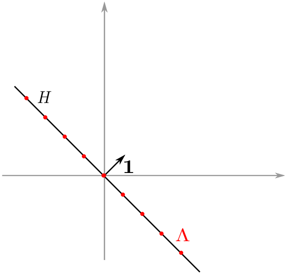
Log : $R \to \mathbb{R}^n$ (somehow generalising log to R)

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

Properties

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

- $a \geq 0$
- $a = 0$ iff r is a unit
- $\Lambda := \mathrm{Log}(R^{\times})$ is a lattice



A tool: the Log space

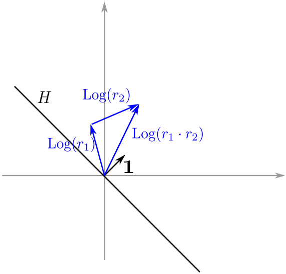
$\text{Log} : R \to \mathbb{R}^n$ (somehow generalising log to R)

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

Properties

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

- $a \geq 0$
- $a = 0$ iff r is a unit
- $\Lambda := \text{Log}(R^\times)$ is a lattice
- $\text{Log}(r_1 \cdot r_2) = \text{Log}(r_1) + \text{Log}(r_2)$



A tool: the Log space

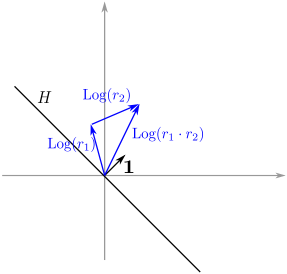
Log : $R \to \mathbb{R}^n$ (somehow generalising log to R)

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

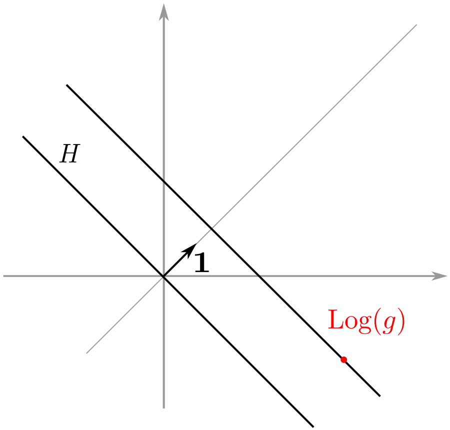
Properties

$\mathrm{Log}\, r = h + a1$, with $h \in H$

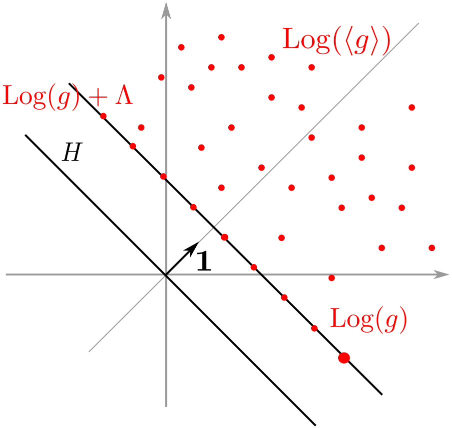
- $a \geq 0$
- $a = 0$ iff r is a unit
- $\Lambda := \mathrm{Log}(R^\times)$ is a lattice
- $\mathrm{Log}(r_1 \cdot r_2) = \mathrm{Log}(r_1) + \mathrm{Log}(r_2)$
- $\|r\| \simeq 2^{\|\mathrm{Log}\, r\|_\infty}$



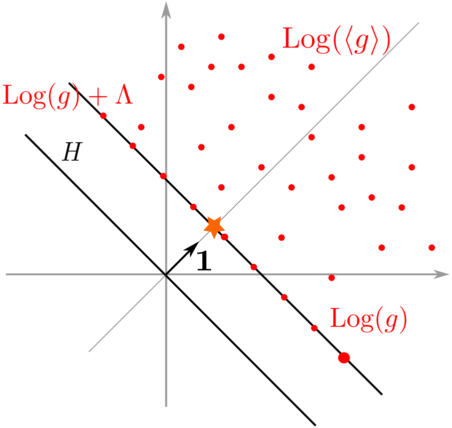
What does $\mathrm{Log}\langle g\rangle$ look like?



What does $\mathrm{Log}\langle g\rangle$ look like?

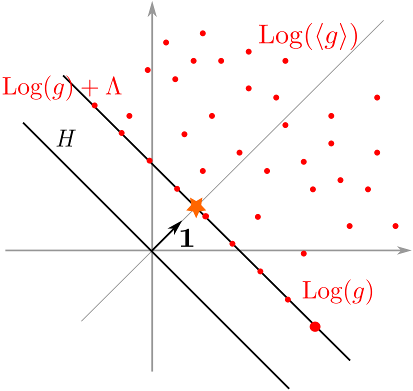


What does $\mathrm{Log}\langle g\rangle$ look like?



Objective: Find a point • as close as possible from ★

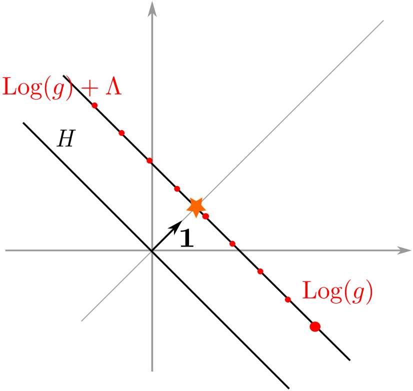
First method: [CGS14, CDPR16, CDW17]



[CGS14]: P. Campbell, M. Groves, and D. Shepherd. Soliloquy: A cautionary tale.

First method: [CGS14, CDPR16, CDW17]

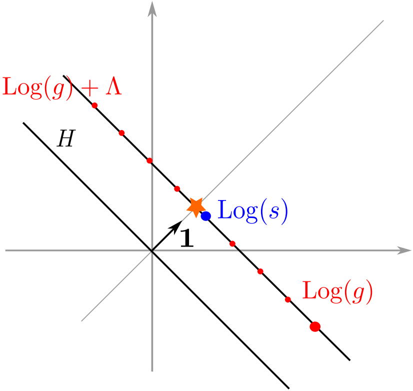
Idea: Only keep the points of $\mathrm{Log}(g) + \Lambda$



[CGS14]: P. Campbell, M. Groves, and D. Shepherd. Soliloquy: A cautionary tale.

First method: [CGS14, CDPR16, CDW17]

Idea: Only keep the points of $\mathrm{Log}(g) + \Lambda$



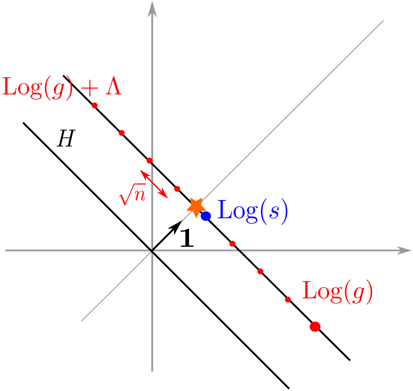
Properties:

- Λ is a nice lattice
  - Poly time to recover the closest point $\mathrm{Log}(s)$

[CGS14]: P. Campbell, M. Groves, and D. Shepherd. Soliloquy: A cautionary tale.

First method: [CGS14, CDPR16, CDW17]

Idea: Only keep the points of $\mathrm{Log}(g) + \Lambda$



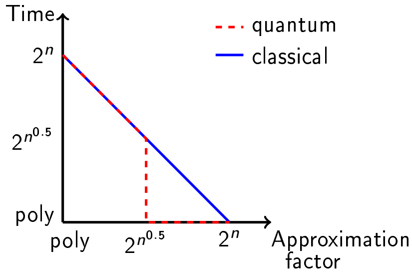
Properties:

- Λ is a nice lattice
  - Poly time to recover the closest point $\mathrm{Log}(s)$
- Distance $\sqrt{n}$ between points of Λ
  - approx factor $\sqrt{n}$ in Log space
  - approx factor $2^{\sqrt{n}}$ in real space

[CGS14]: P. Campbell, M. Groves, and D. Shepherd. Soliloquy: A cautionary tale.

First method: [CGS14, CDPR16, CDW17]

Idea: Only keep the points of $\mathrm{Log}(g) + \Lambda$

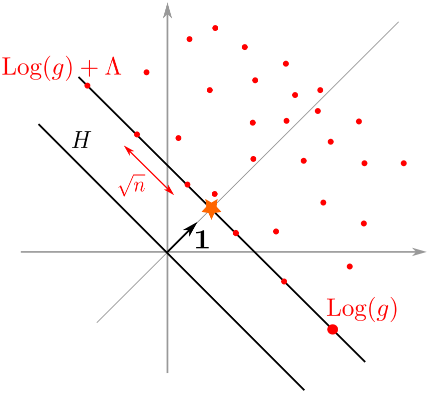


Properties:

- Λ is a nice lattice
  - Poly time to recover the closest point $\mathrm{Log}(s)$
- Distance $\sqrt{n}$ between points of Λ
  - approx factor $\sqrt{n}$ in Log space
  - approx factor $2^{\sqrt{n}}$ in real space

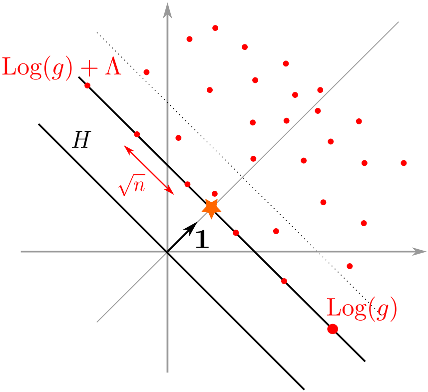
[CGS14]: P. Campbell, M. Groves, and D. Shepherd. Soliloquy: A cautionary tale.

Second method: [PHS19]



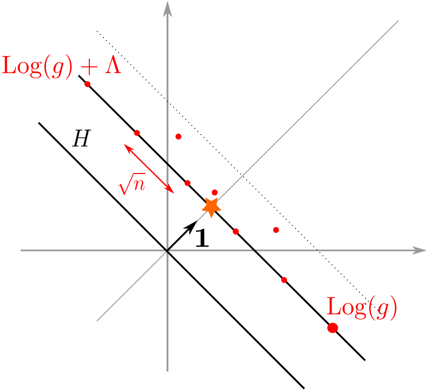
Second method: [PHS19]

Idea: Keep more points



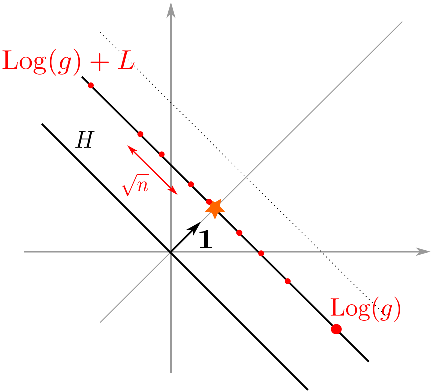
Second method: [PHS19]

Idea: Keep more points



Second method: [PHS19]

Idea: Keep more points

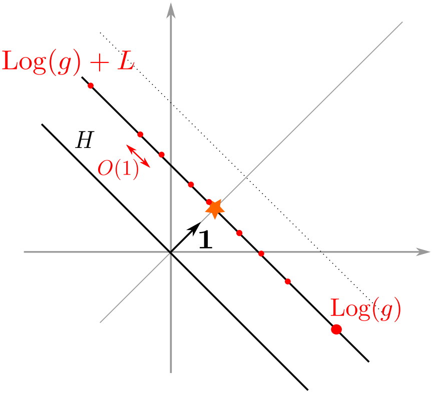


Properties:

- Project the points on $\mathrm{Log}(g) + H$
  - shifted lattice $\mathrm{Log}(g) + L$

Second method: [PHS19]

Idea: Keep more points



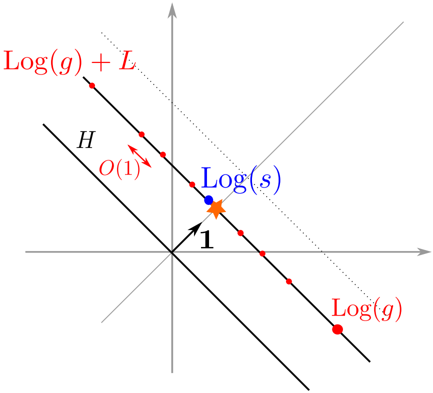
Properties:

- Project the points on $\mathrm{Log}(g) + H$
  - shifted lattice $\mathrm{Log}(g) + L$

+ Distance $O(1)$ between points of L
  - approx factor $O(1)$

Second method: [PHS19]

Idea: Keep more points



Properties:

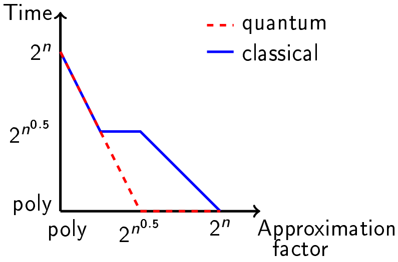
- Project the points on $\mathrm{Log}(g) + H$
  - shifted lattice $\mathrm{Log}(g) + L$

+ Distance $O(1)$ between points of L
  - approx factor $O(1)$

− L is not a nice lattice
  - cannot find close point $\mathrm{Log}(s)$ efficiently
  - can pre-process L to improve efficiency

Second method: [PHS19]

Idea: Keep more points



Properties:

- Project the points on $\text{Log}(g) + H$
  - shifted lattice $\text{Log}(g) + L$

\+ Distance $O(1)$ between points of L
  - approx factor $O(1)$

− L is not a nice lattice
  - cannot find close point $\text{Log}(s)$ efficiently
  - can pre-process L to improve efficiency

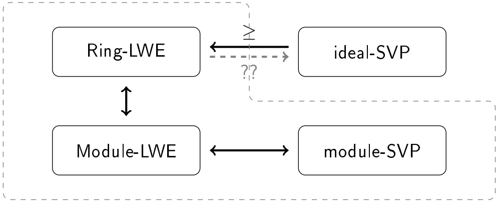
Conclusion

Some open problems

- Are there number fields in which ideal-SVP is significantly easier?

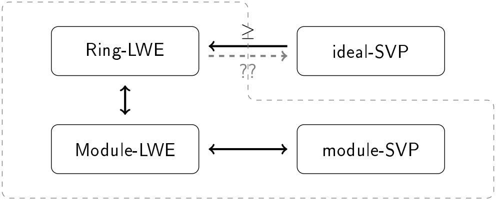
Some open problems

- Are there number fields in which ideal-SVP is significantly easier?
- Is there a gap between ideal-SVP and Ring-LWE?



Some open problems

- Are there number fields in which ideal-SVP is significantly easier?
- Is there a gap between ideal-SVP and Ring-LWE?



Questions?