On algorithms for solving Euclidean lattice problems in cryptography

Weiqiang Wen

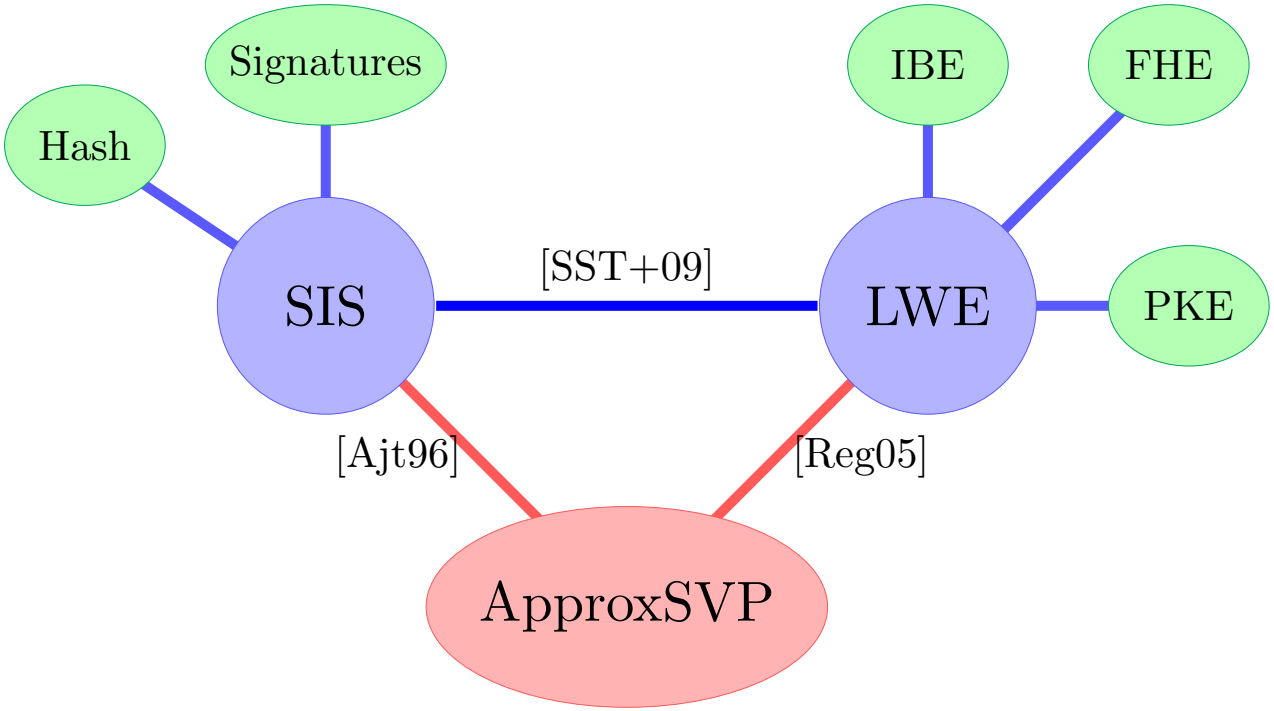
Based on joint works with M.R. Albrecht, S. Bai, Z. Brakerski,

P.A. Fouque, P. Kirchner, E. Kirshanova and D. Stehlé

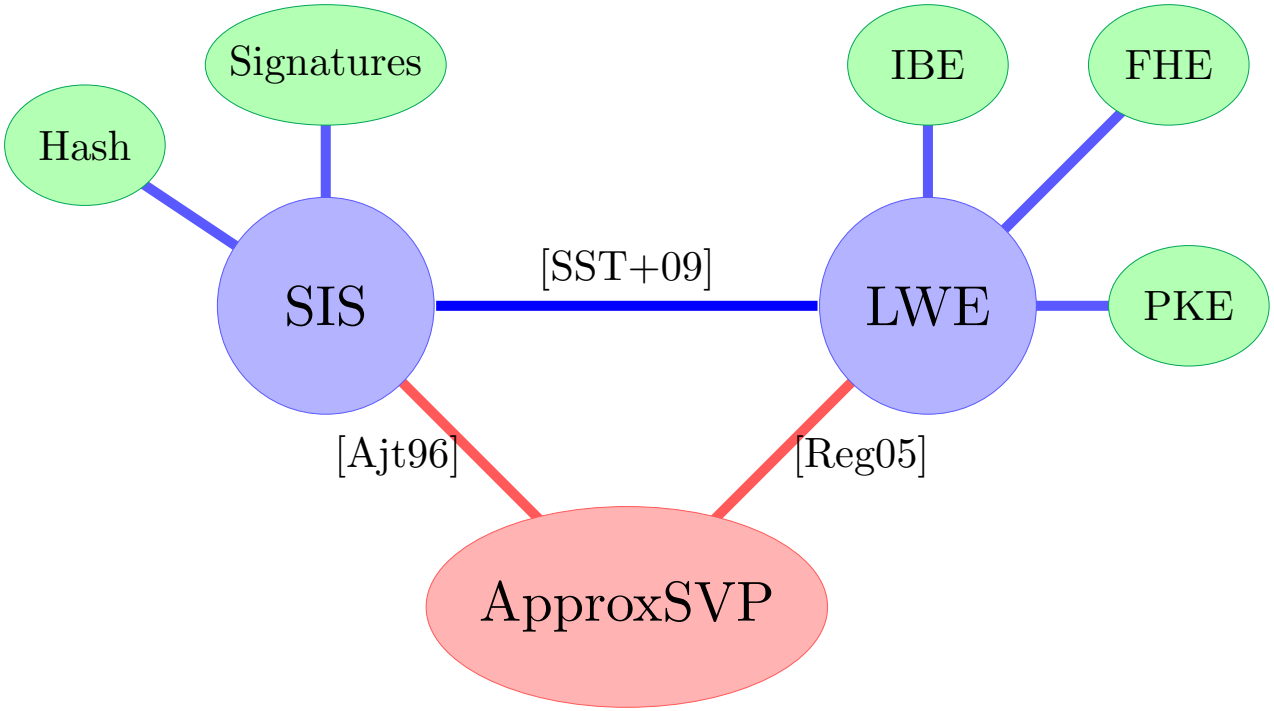
Séminaire Caramba, Nancy

June 14th, 2021

What is this talk about

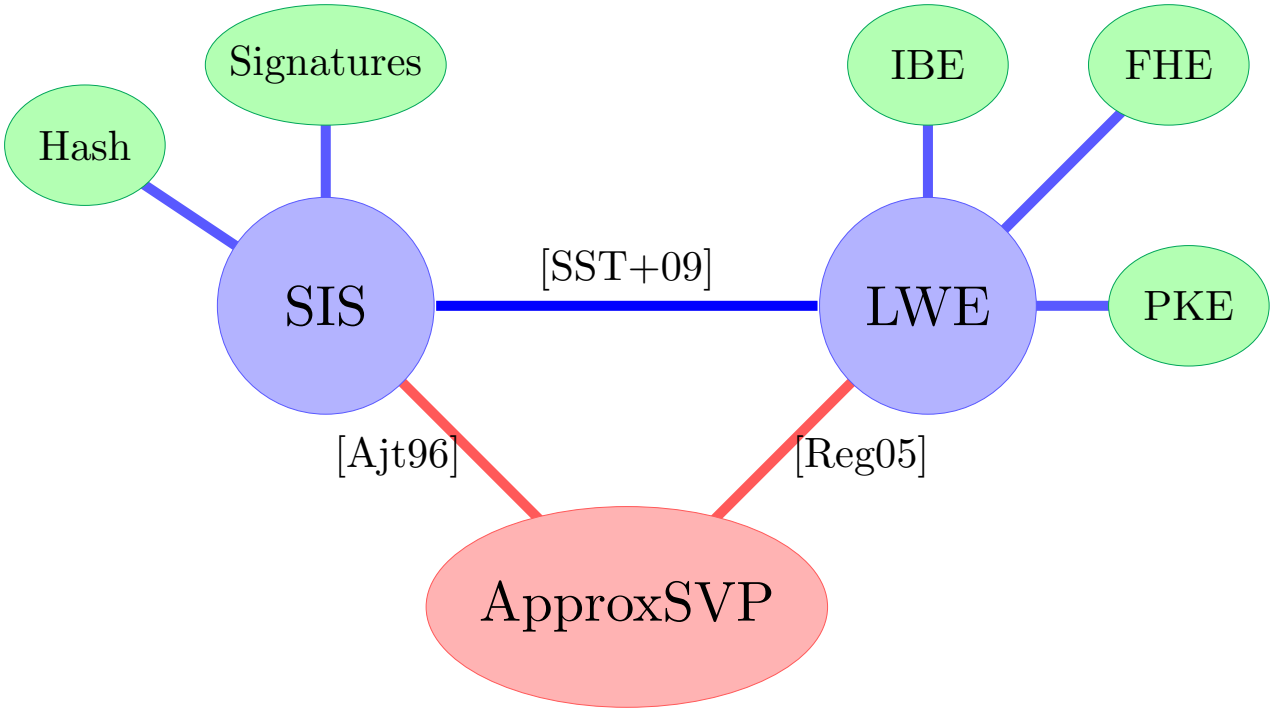


What is this talk about



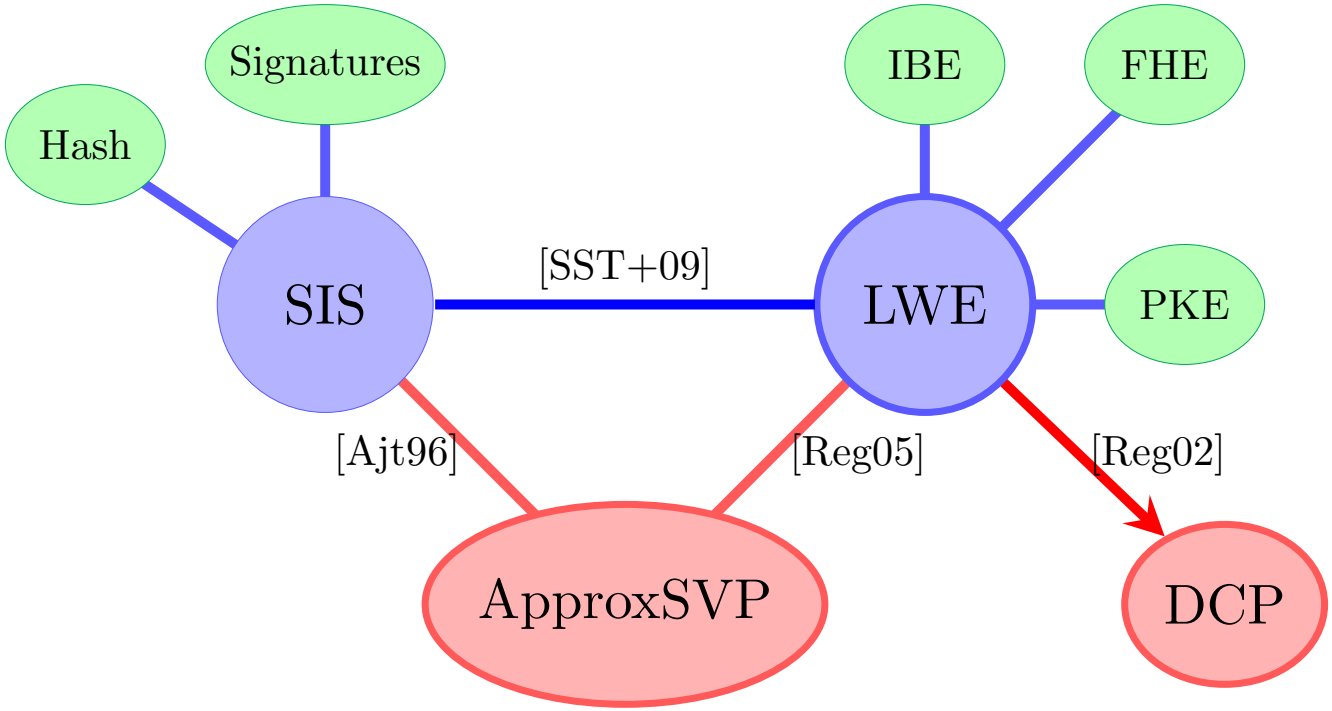
- The NIST post-quantum cryptography candidates (Round 3):
  1. PKE: **3** (lattice-based: KYBER, NTRU, SABER) / 4;
  2. Signature: **2** (lattice-based: DILITHIUM, FALCON) / 3.

What is this talk about



- **Algorithms** for solving ApproxSVP over Euclidean lattices via
  1. Lattice reduction algorithms;

What is this talk about

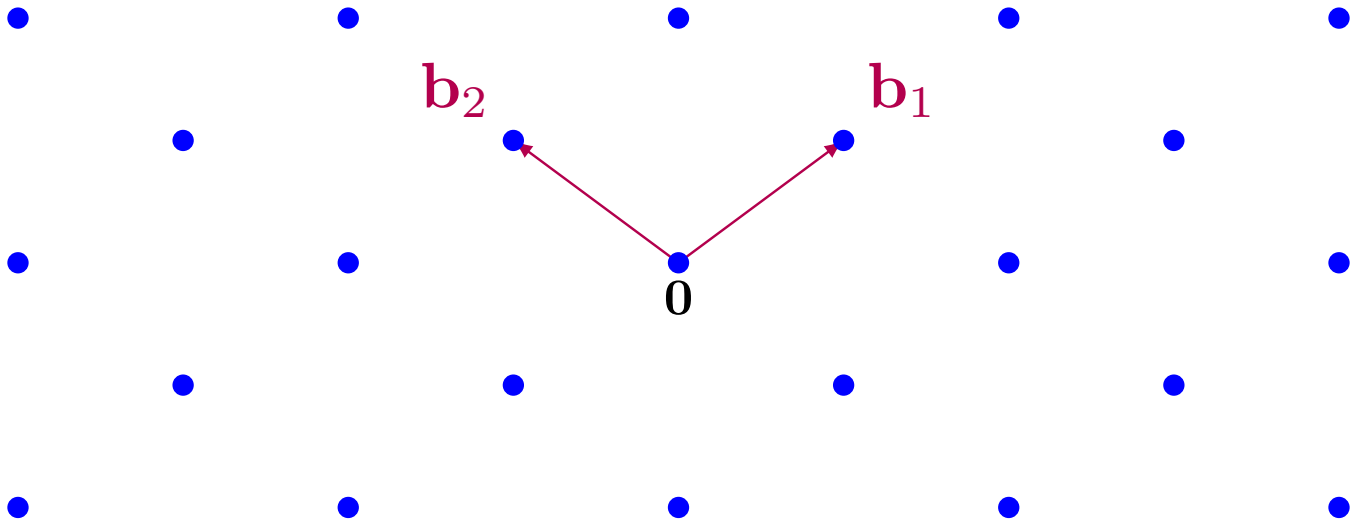


- **Algorithms** for solving ApproxSVP over Euclidean lattices via
  1. Lattice reduction algorithms;
  2. Solving quantum problems (ApproxSVP $\leq$ LWE $\leq$ DCP).

Part I: ApproxSVP and lattice reduction

Part I: **The Approximate Shortest Vector Problem and lattice reduction algorithms.**

Lattices

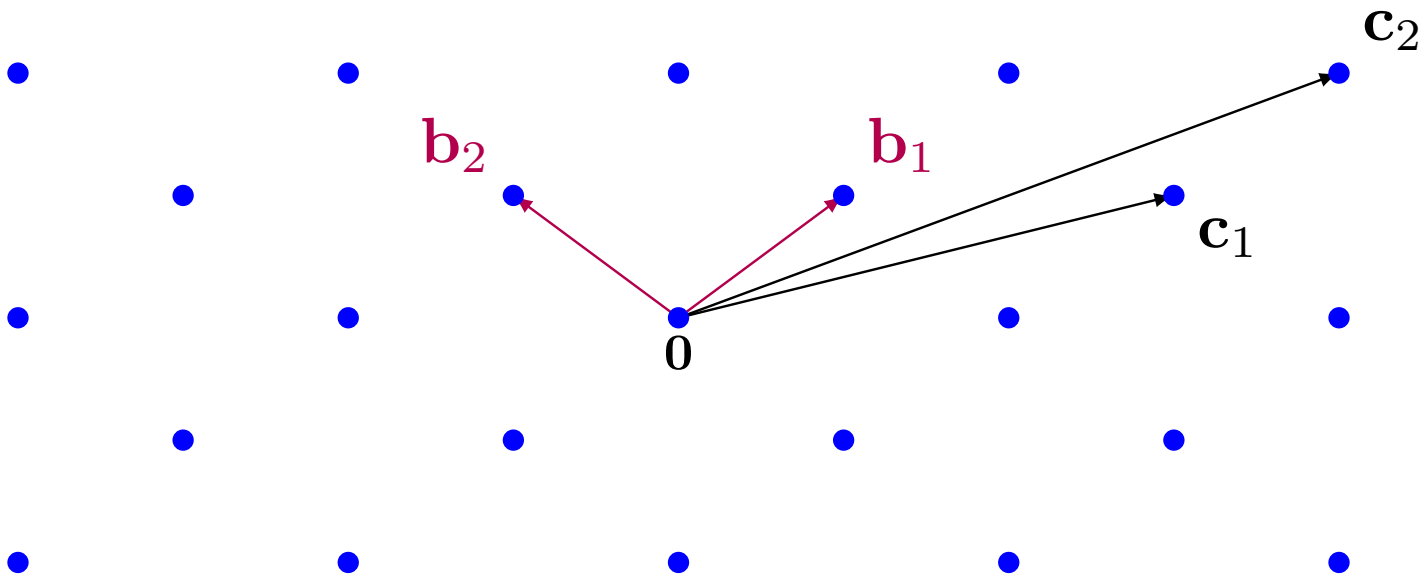


A definition of lattice

Given $\mathbf{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\} \subseteq \mathbb{Q}^m$ a set of linearly independent vectors, the lattice $\mathcal{L}$ spanned by the $\mathbf{b}_i$'s is

$$\mathcal{L}(\mathbf{B}) = \left\{ \sum_{i \in [n]} u_i \mathbf{b}_i \, : \, \mathbf{u} \in \mathbb{Z}^n \right\}.$$

Lattices

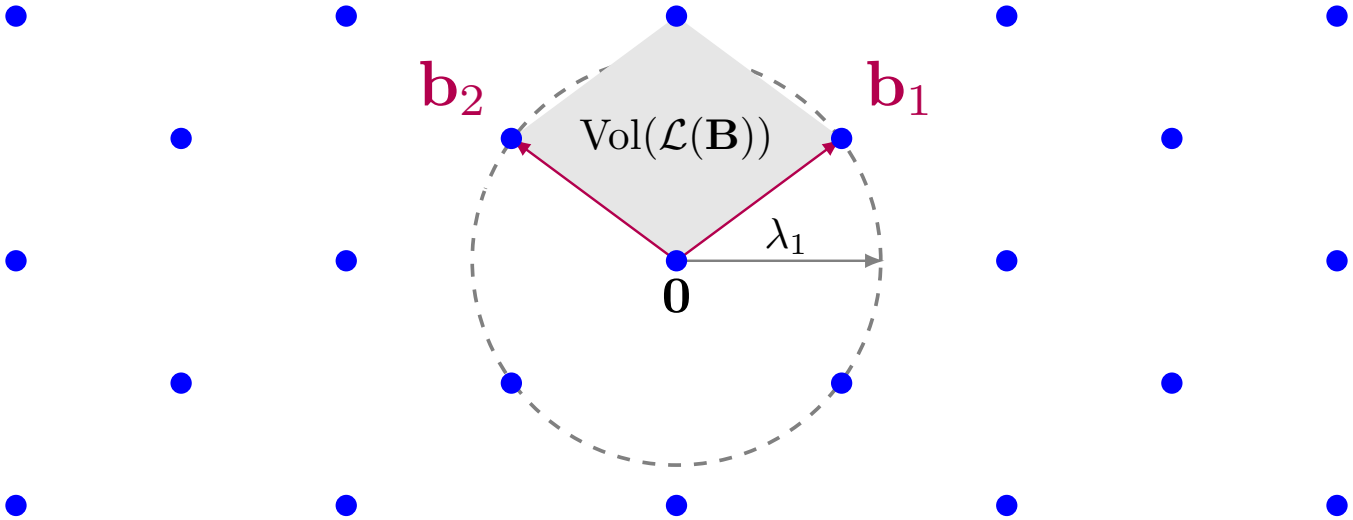


A definition of lattice

Given $\mathbf{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\} \subseteq \mathbb{Q}^m$ a set of linearly independent vectors, the lattice $\mathcal{L}$ spanned by the $\mathbf{b}_i$'s is

$$\mathcal{L}(\mathbf{B}) = \left\{ \sum_{i \in [n]} u_i \mathbf{b}_i \, : \, \mathbf{u} \in \mathbb{Z}^n \right\}.$$

Invariants in lattices



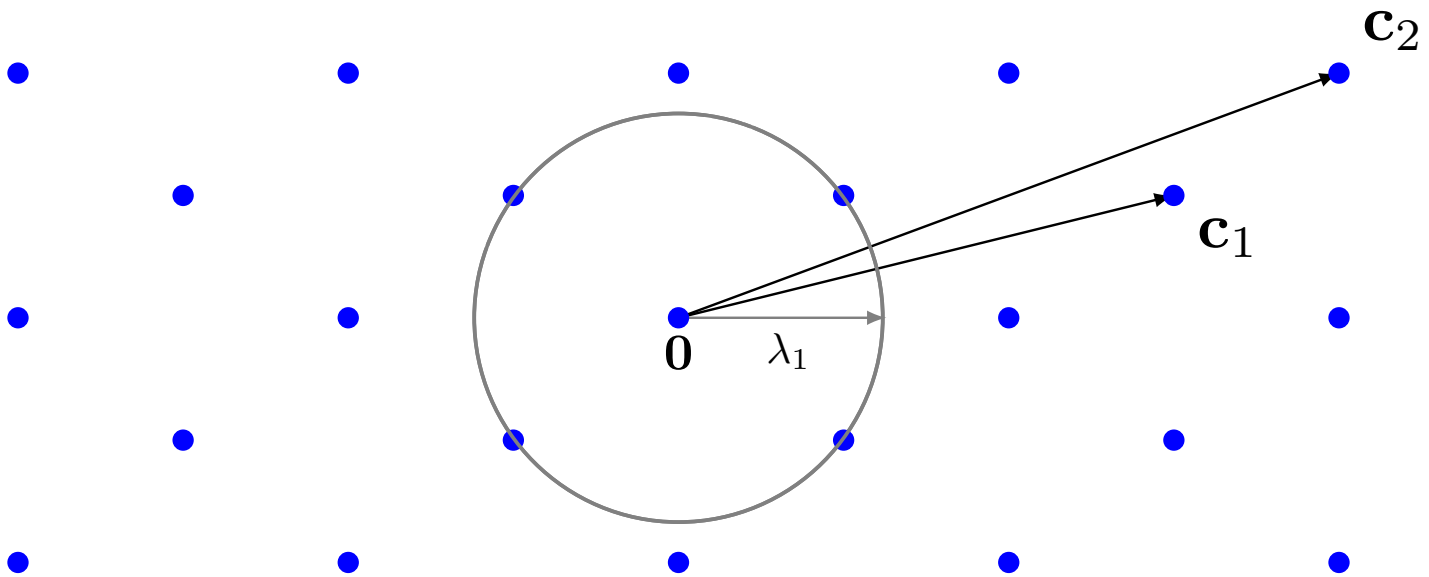
First minimum

$\lambda_1(\mathcal{L}) = \min\{\|\mathbf{b}\| : \mathbf{b} \in \mathcal{L}\backslash\{\mathbf{0}\}\}$.

Volume of lattice

$\mathrm{Vol}(\mathcal{L}(\mathbf{B})) = \sqrt{\det(\mathbf{B}^{\mathrm{T}}\mathbf{B})}$ for any basis $\mathbf{B}$.

Lattice problems

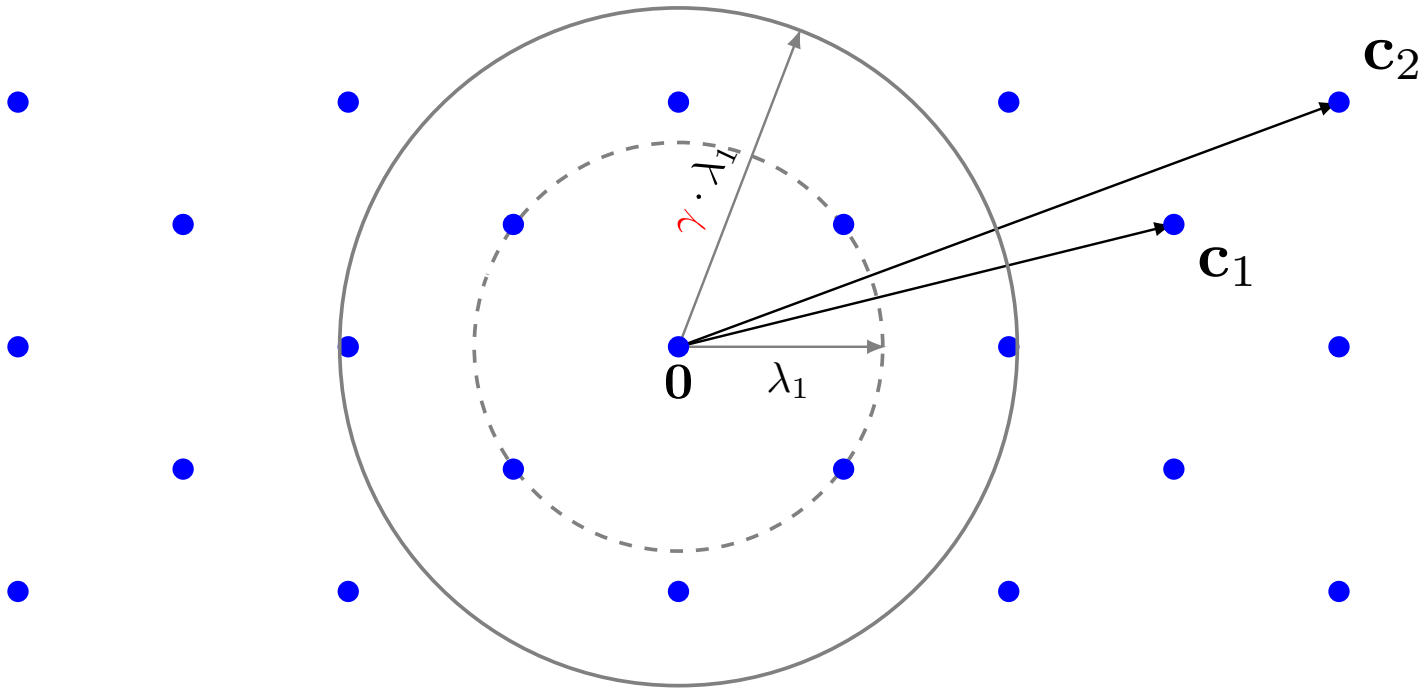


Shortest vector problem (SVP)

Given $\mathbf{B} \subseteq \mathbb{Q}^m$ a basis of the lattice $\mathcal{L}$, it asks to find a vector $\mathbf{s}$ in the lattice such that

$$\|\mathbf{s}\| = \lambda_1(\mathcal{L}).$$

Lattice problems



SVP

Given $\mathbf{B} \subseteq \mathbb{Q}^m$ a basis of the lattice $\mathcal{L}$, finds a vector $\mathbf{s}$ in the lattice such that

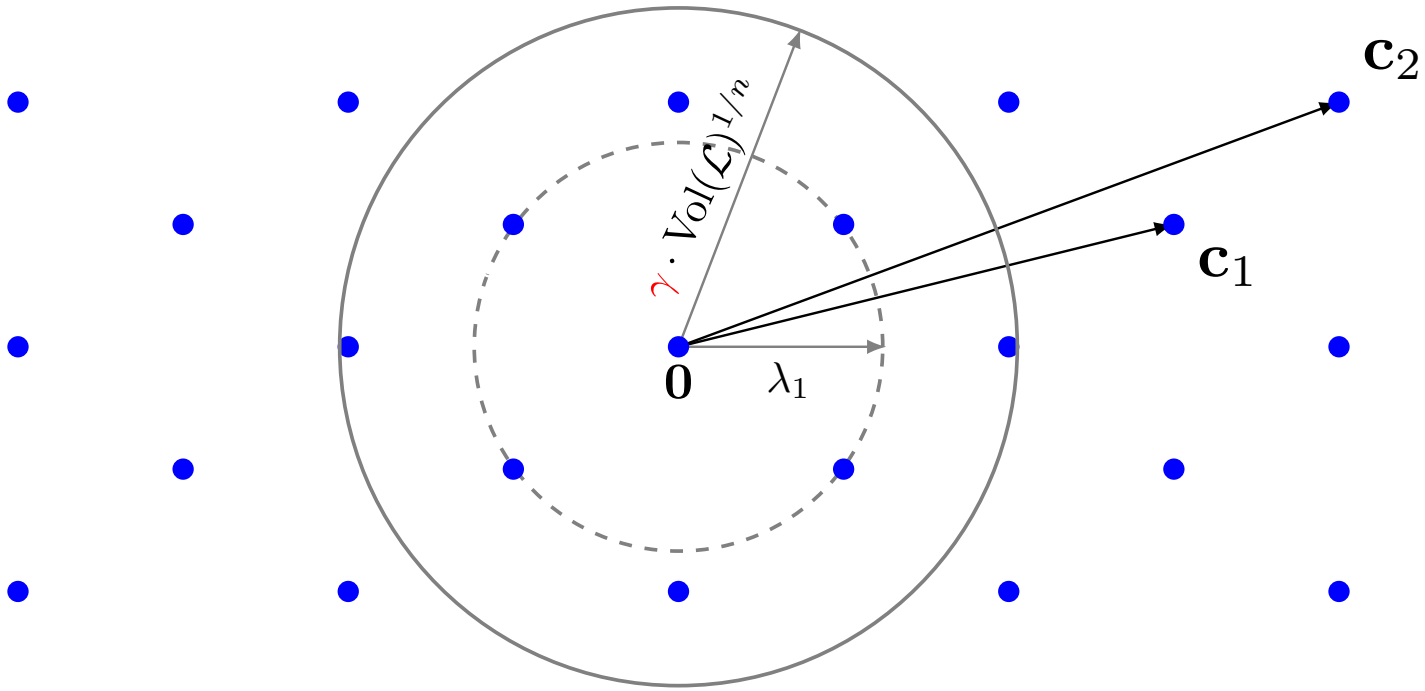
$$\|\mathbf{s}\| = \lambda_1(\mathcal{L}).$$

γ-SVP

Given $\mathbf{B} \subseteq \mathbb{Q}^m$ a basis of the lattice $\mathcal{L}$, finds a non-zero vector $\mathbf{s}$ in the lattice such that

$$\|\mathbf{s}\| \leq \gamma \cdot \lambda_1(\mathcal{L}).$$

Lattice problems



γ-SVP

Given $\mathbf{B} \subseteq \mathbb{Q}^m$ a basis of the lattice $\mathcal{L}$, finds a non-zero vector $\mathbf{s}$ in the lattice such that

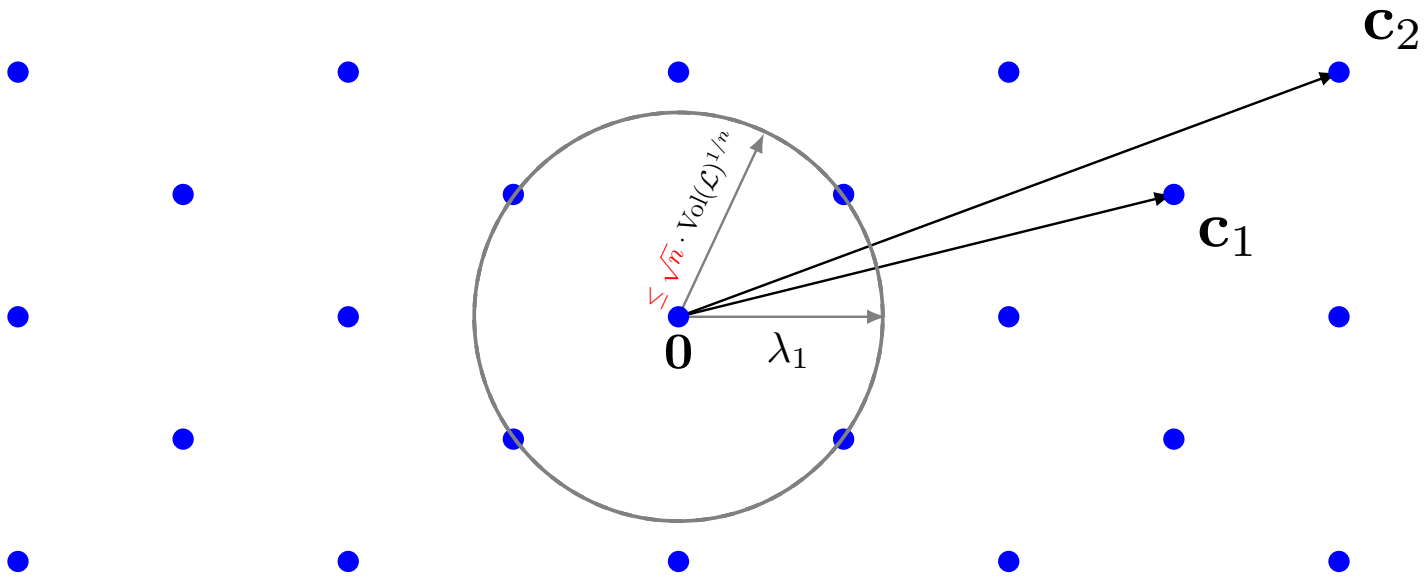
$$\|\mathbf{s}\| \leq \gamma \cdot \lambda_1(\mathcal{L}).$$

γ-Hermite SVP (γ-HSVP)

Given $\mathbf{B}$ a basis of $\mathcal{L}$, finds a non-zero vector $\mathbf{s}$ in $\mathcal{L}$ such that

$$\|\mathbf{s}\| \leq \gamma \cdot \mathrm{Vol}(\mathcal{L})^{\frac{1}{n}}.$$

Lattice problems



Minkowski's theorem: $\mathrm{SVP} \Rightarrow \sqrt{n}$-$\mathrm{HSVP}$.
$(\lambda_1 \leq \sqrt{n} \cdot \mathrm{Vol}(\mathcal{L})^{1/n})$

γ-SVP

Given $\mathbf{B} \subseteq \mathbb{Q}^m$ a basis of the lattice $\mathcal{L}$, finds a non-zero vector $\mathbf{s}$ in the lattice such that

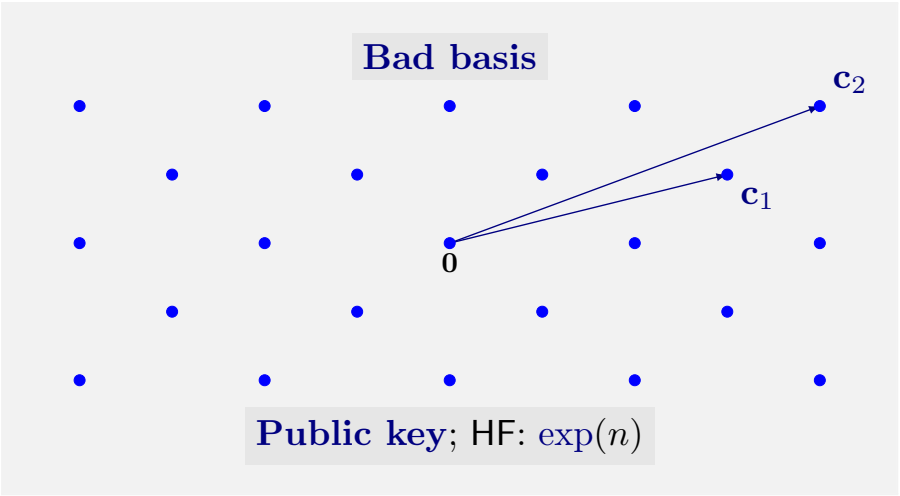
$$\|\mathbf{s}\| \leq \gamma \cdot \lambda_1(\mathcal{L}).$$

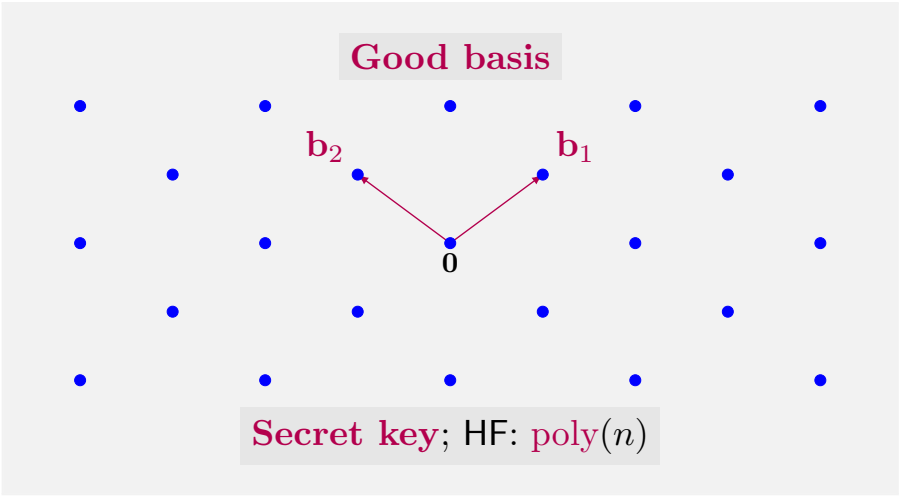
γ-Hermite SVP (γ-HSVP)

Given $\mathbf{B}$ a basis of $\mathcal{L}$, finds a non-zero vector $\mathbf{s}$ in $\mathcal{L}$ such that

$$\|\mathbf{s}\| \leq \gamma \cdot \mathrm{Vol}(\mathcal{L})^{\frac{1}{n}}.$$

Best known solution: reduce the basis



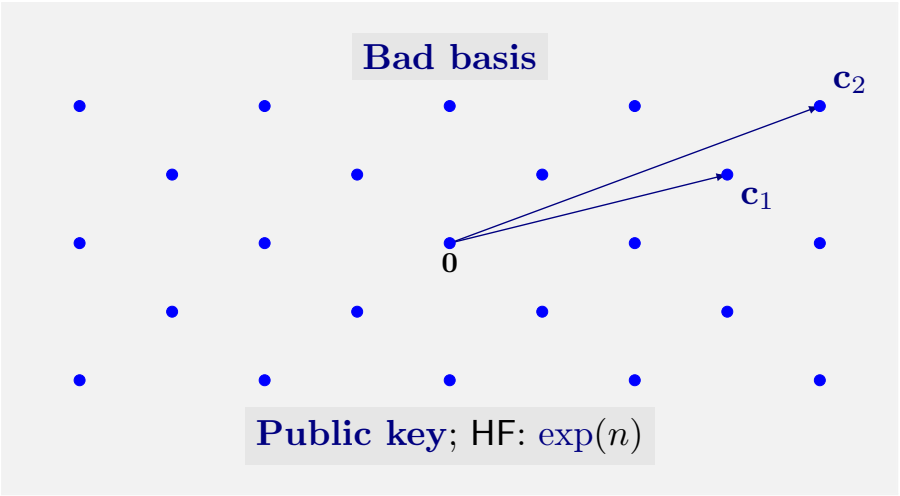


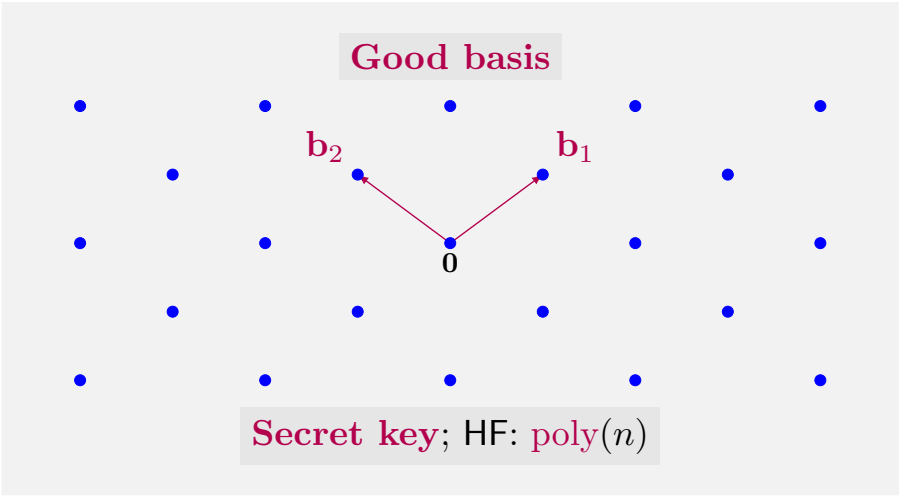
Hermite factor

Given $\mathbf{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\} \subseteq \mathbb{Q}^m$ a basis of the lattice $\mathcal{L}$, its Hermite factor is

$$\mathrm{HF}(\mathbf{B}) = \frac{\|\mathbf{b}_1\|}{\mathrm{Vol}(\mathcal{L})^{\frac{1}{n}}}.$$

Best known solution: reduce the basis





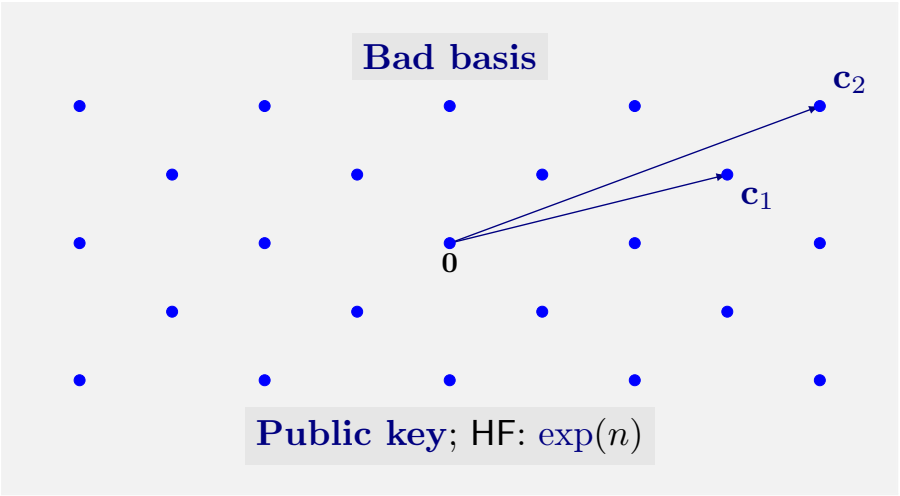
This process of reducing basis is known as lattice reduction:
$\Rightarrow$ BKZ reduction [SE94] & Slide reduction [GN08; Wal20]

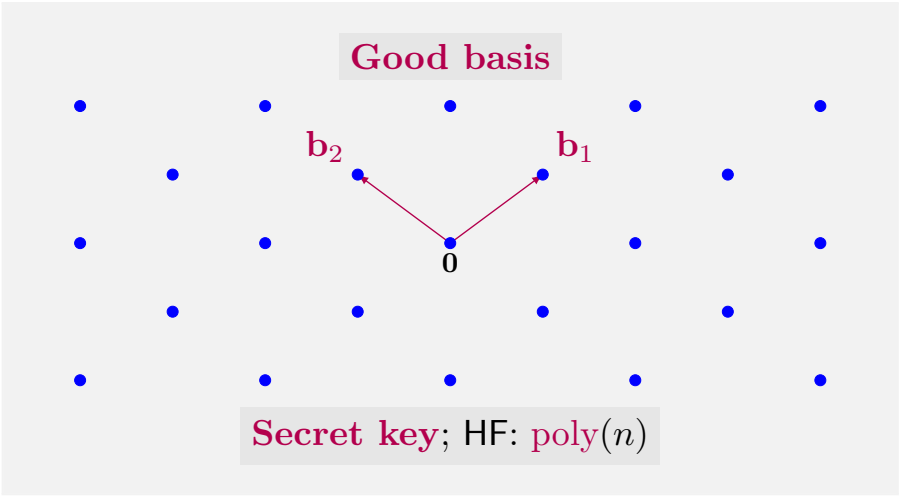
Hermite factor

Given $\mathbf{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\} \subseteq \mathbb{Q}^m$ a basis of the lattice $\mathcal{L}$, its Hermite factor is

$$\mathrm{HF}(\mathbf{B}) = \frac{\|\mathbf{b}_1\|}{\mathrm{Vol}(\mathcal{L})^{\frac{1}{n}}}.$$

Introduce root Hermite factor to quantify lattice reduction





This process of reducing basis is known as lattice reduction:
$\Rightarrow$ **BKZ reduction** [SE94] & Slide reduction [GN08; Wal20]

Hermite factor

Given $\mathbf{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_n\} \subseteq \mathbb{Q}^m$ a basis of the lattice $\mathcal{L}$, its Hermite factor is

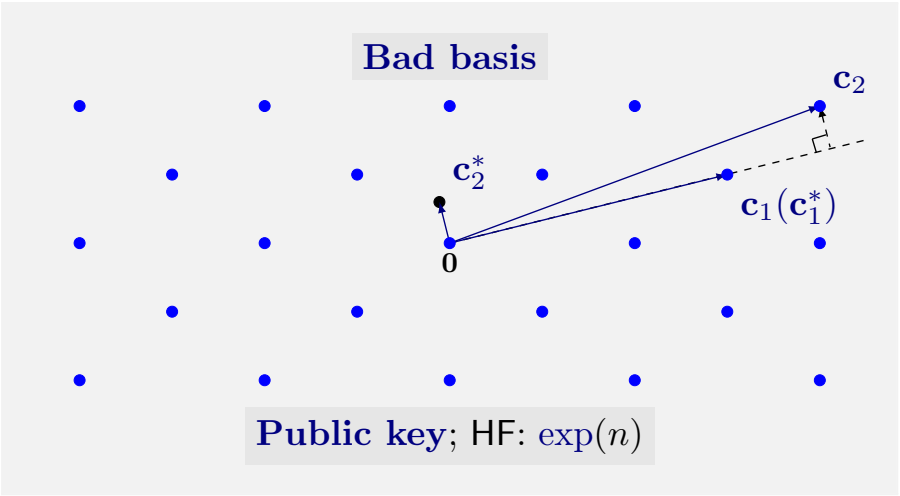
$$\mathrm{HF}(\mathbf{B}) = \frac{\|\mathbf{b}_1\|}{\mathrm{Vol}(\mathcal{L})^{\frac{1}{n}}}.$$

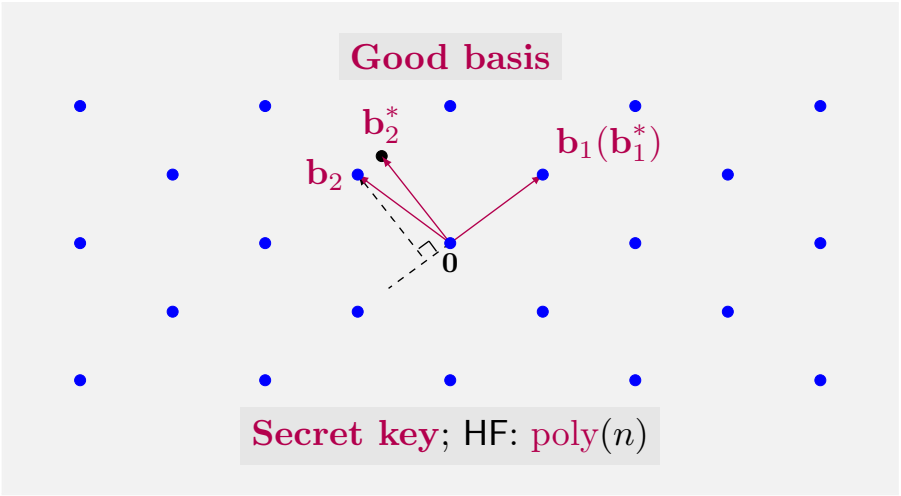
Root Hermite factor

Given $\mathbf{B} \subseteq \mathbb{Q}^m$ a basis of the lattice $\mathcal{L}$, its root Hermite factor is

$$\mathrm{RHF}(\mathbf{B}) = \mathrm{HF}(\mathbf{B})^{\frac{1}{n-1}}.$$

Gram-Schmidt orthogonalization



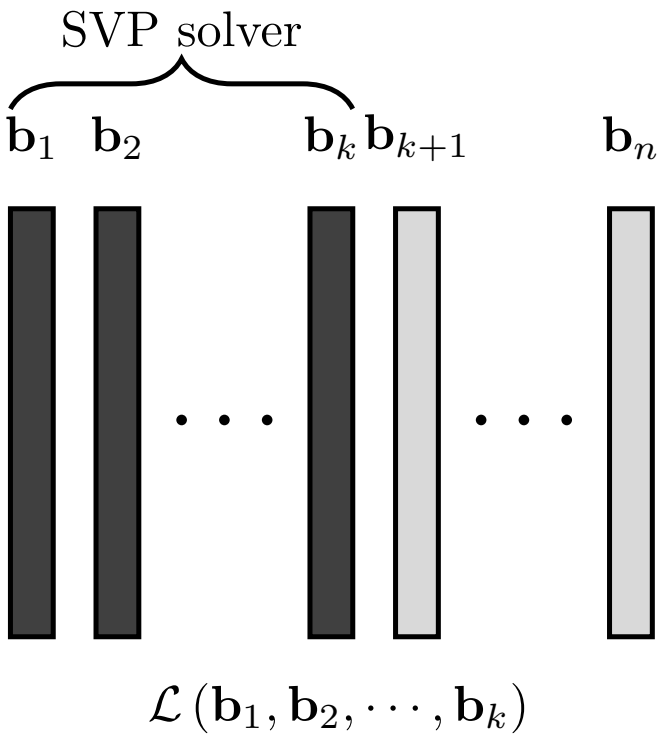


This process of reducing basis is known as lattice reduction:
$\Rightarrow$ **BKZ reduction** [SE94] & Slide reduction [GN08; Wal20]

Gram-Schmidt orthogonalization

A matrix $\mathbf{B}^* = (\mathbf{b}_1^*, ..., \mathbf{b}_n^*)$ is the Gram-Schmidt orthogonalization of $\mathbf{B}$,
if $\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j}\mathbf{b}_j^*$, where $\mu_{i,j} = \frac{\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle}{\|\mathbf{b}_j^*\|^2}$.

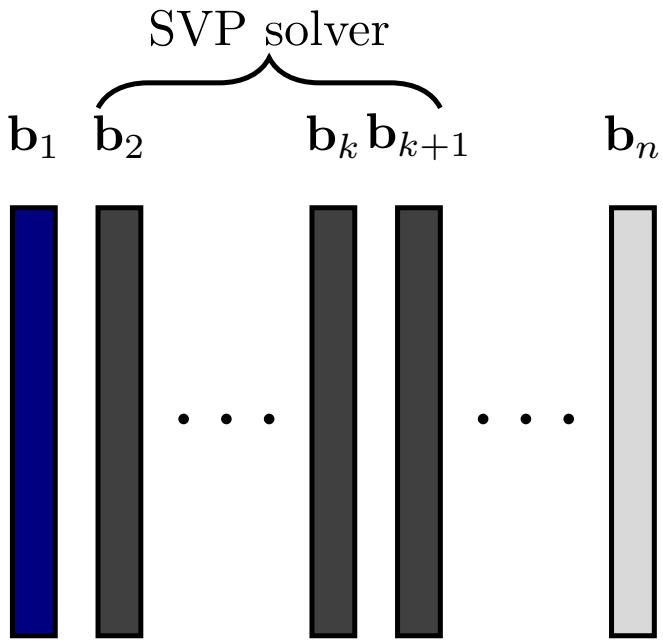
The BKZ algorithm [SE94]



Notation of projection

Given a basis $\mathbf{B} = (\mathbf{b}_1, \cdots, \mathbf{b}_n) \in \mathbb{Q}^m$, we let $\mathbf{b}_i^{(j)}$ denote the orthogonal projection over $(\mathbf{b}_1, \cdots, \mathbf{b}_j)^{\perp}$ of $\mathbf{b}_i$.

The BKZ algorithm [SE94]



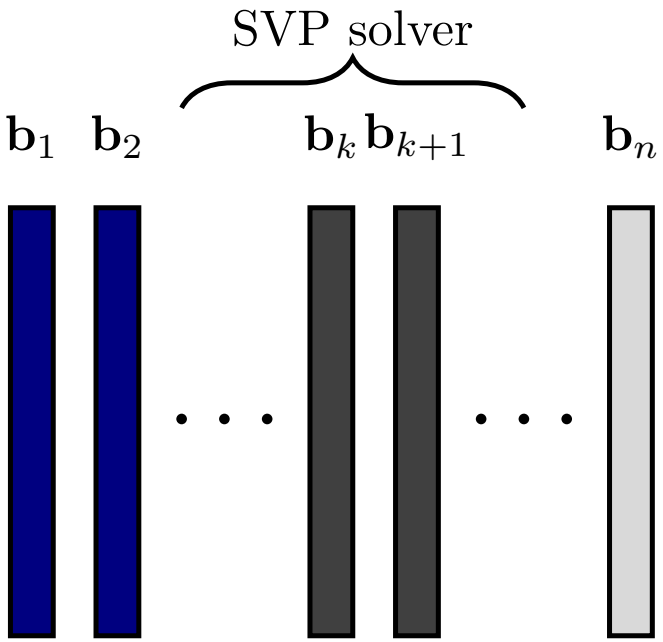
$$\|\mathbf{b}_1^*\| = \|\mathbf{b}_1\| = \lambda_1\left(\mathcal{L}\left(\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_k\right)\right)$$

$$\mathcal{L}\left(\mathbf{b}_2^{(1)}, \mathbf{b}_3^{(1)}, \cdots, \mathbf{b}_{k+1}^{(1)}\right)$$

Notation of projection

Given a basis $\mathbf{B} = (\mathbf{b}_1, \cdots, \mathbf{b}_n) \in \mathbb{Q}^m$, we let $\mathbf{b}_i^{(j)}$ denote the orthogonal projection over $(\mathbf{b}_1, \cdots, \mathbf{b}_j)^{\perp}$ of $\mathbf{b}_i$.

The BKZ algorithm [SE94]

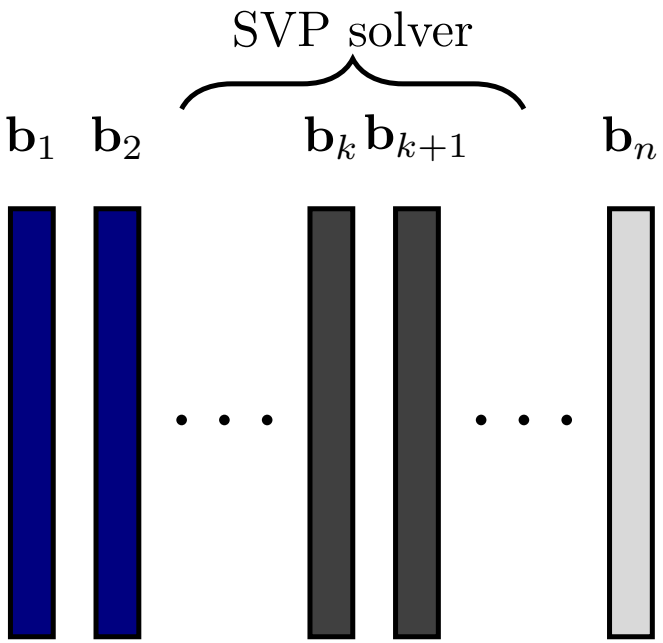


$$\|\mathbf{b}_2^*\| = \|\mathbf{b}_2^{(1)}\| = \lambda_1\left(\mathcal{L}\left(\mathbf{b}_2^{(1)}, \mathbf{b}_3^{(1)}, \cdots, \mathbf{b}_{k+1}^{(1)}\right)\right)$$

Notation of projection

Given a basis $\mathbf{B} = (\mathbf{b}_1, \cdots, \mathbf{b}_n) \in \mathbb{Q}^m$, we let $\mathbf{b}_i^{(j)}$ denote the orthogonal projection over $(\mathbf{b}_1, \cdots, \mathbf{b}_j)^{\perp}$ of $\mathbf{b}_i$.

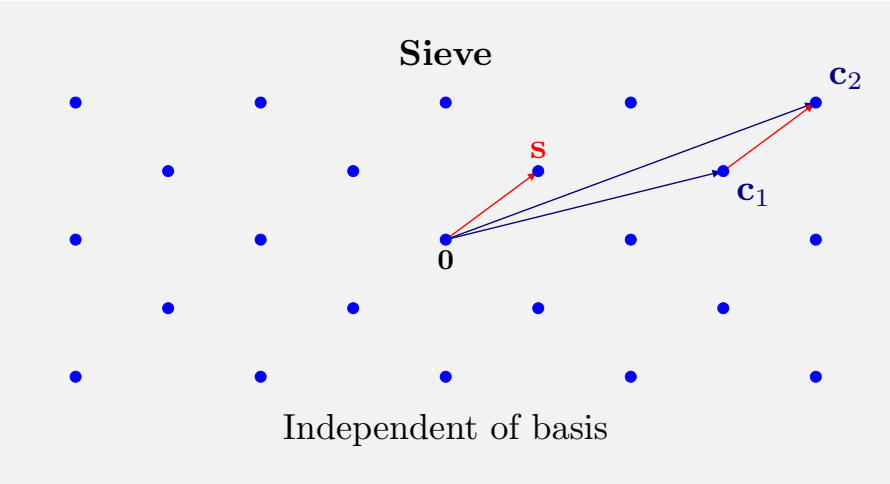
The BKZ algorithm [SE94]

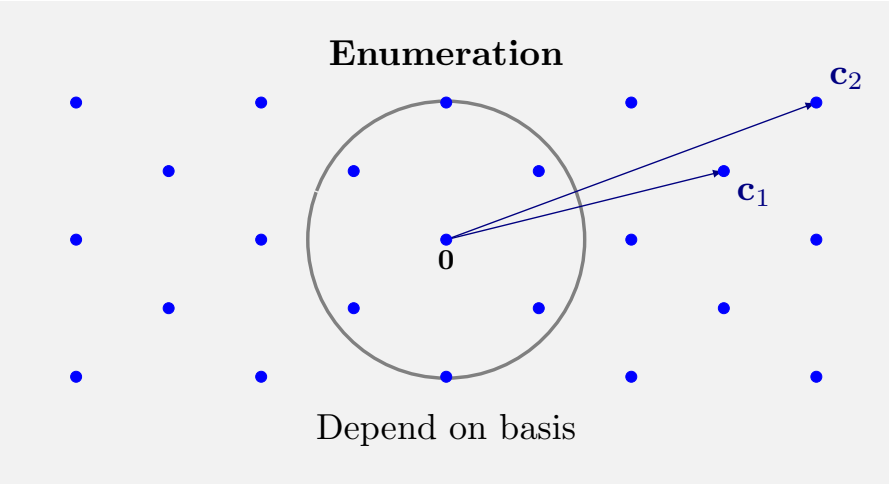


$$\|\mathbf{b}_2^*\| = \|\mathbf{b}_2^{(1)}\| = \lambda_1\left(\mathcal{L}\left(\mathbf{b}_2^{(1)}, \mathbf{b}_3^{(1)}, \cdots, \mathbf{b}_{k+1}^{(1)}\right)\right)$$

- [HPS11]: poly(n) tours are sufficient to approximate the reduced basis produced by the (full) BKZ.

The two most practical SVP solvers

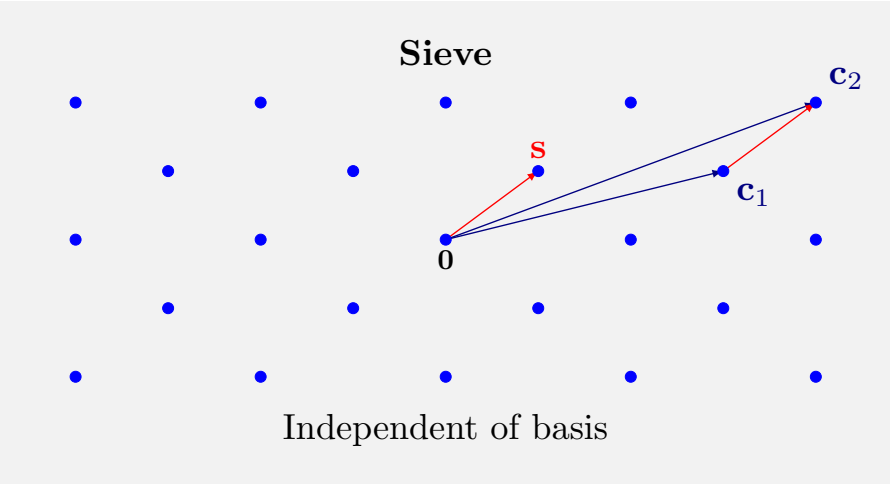


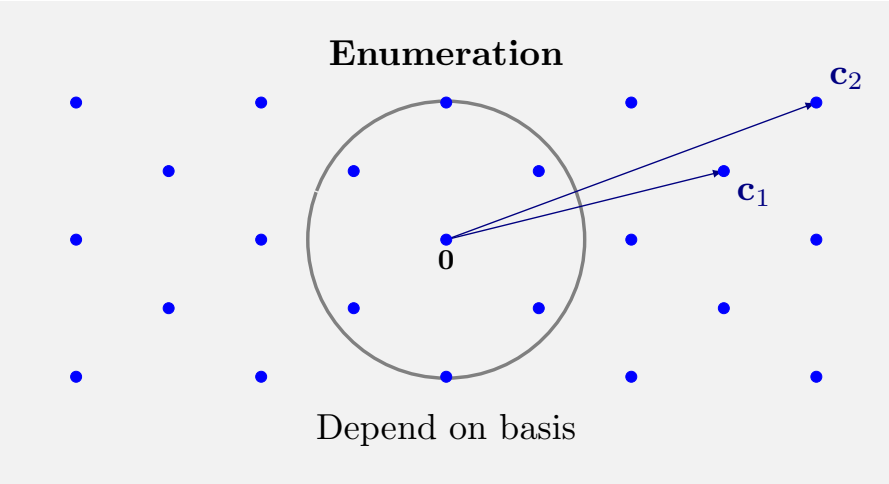


The two practical SVP solver families		
	Sieve (heuristic) [AKS01; BDGL16]	Enumeration [Kan83; FP83; HS07; GNR10]
Space	$2^{0.208k+o(k)}$	$\mathrm{poly}(k)$
Time	$2^{0.292k+o(k)}$	$k^{k/(2e)+o(k)}$ $(\approx k^{0.184k})$

- Sieve (provable) [PS09]: $2^{1.325k+o(k)}$ space and $2^{2.465k+o(k)}$ time.
- Discrete Gaussian samplers [ADRS15]: $2^{k+o(k)}$ space and $2^{k+o(k)}$ time.

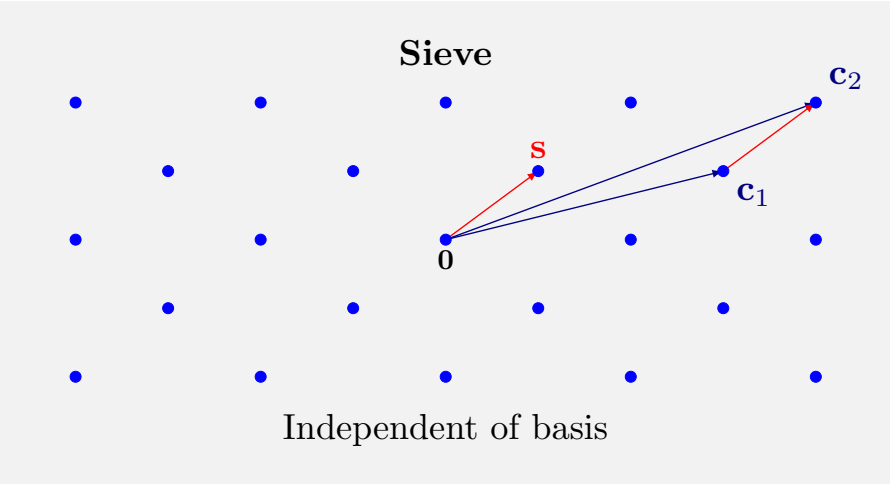
The two most practical SVP solvers

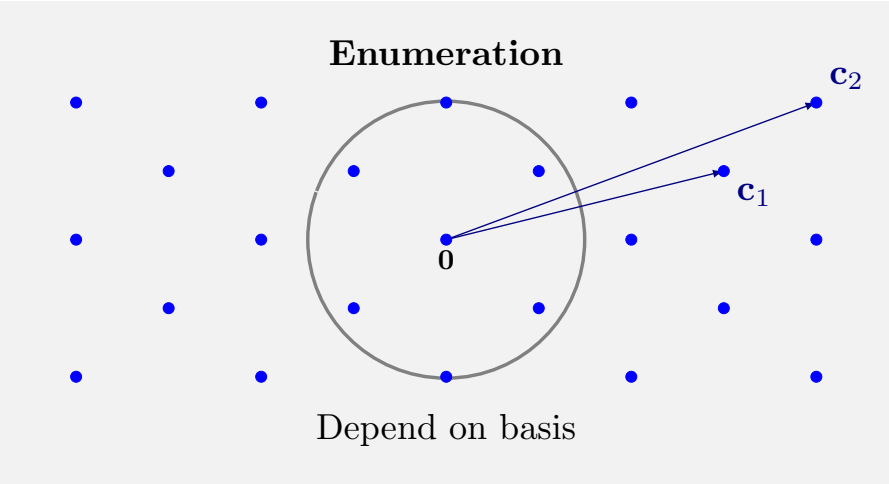




The two practical SVP solver families		
	Sieve (heuristic) [BDGL16; Laa15]	Enumeration [Kan83; FP83; HS07; GNR10; ANS18]
Space	$2^{0.208k+o(k)}$	$\mathrm{poly}(k)$
Time	$2^{0.292k+o(k)}$	$k^{k/(2e)+o(k)}$ $(\approx k^{0.184k})$
Quantum acceleration		
Space	$2^{0.265k+o(k)}$	$\mathrm{poly}(k)$
Time	$2^{0.265k+o(k)}$	$k^{k/(4e)+o(k)}$ $(\approx k^{0.091k})$

Performance of sieve/enuemration-based (SD)BKZ





Performances of sieve/enumeration-based (SD)BKZ [HPS11; MW16; Neu17]		
	Sieve-based	Enumeration-based
RHF	$k^{1/(2k)}$	$k^{1/(2k)}$
Time	$2^{0.292k+o(k)}$	$k^{k/(2e)+o(k)}$ $(\approx k^{0.184k})$
Quantum acceleration		
Time	$2^{0.265k+o(k)}$	$k^{k/(4e)+o(k)}$ $(\approx k^{0.091k})$
Space	$2^{0.265k+o(k)}$	$\mathrm{poly}(k)$

Performance of sieve/enuemration-based (SD)BKZ

1. To solve ApproxSVP for breaking (certain) NIST candidates, one needs to achieve RHF $k^{1/(2k)} \approx 1.006$ for $k \approx 500$.
   $\Rightarrow$ Sieve requires a **large space** $> 2^{100}$.

Performances of sieve/enumeration-based (SD)BKZ [HPS11; MW16; Neu17]		
	Sieve-based	Enumeration-based
RHF	$k^{1/(2k)}$	$k^{1/(2k)}$
Time	$2^{0.292k+o(k)}$	$k^{k/(2e)+o(k)}$ $(\approx k^{0.184k})$
Quantum acceleration		
Time	$2^{0.265k+o(k)}$	$k^{k/(4e)+o(k)}$ $(\approx k^{0.091k})$
Space	$2^{0.265k+o(k)}$	$\mathrm{poly}(k)$

Performance of sieve/enuemration-based (SD)BKZ

1. To solve ApproxSVP for breaking (certain) NIST candidates, one needs to achieve RHF $k^{1/(2k)} \approx 1.006$ for $k \approx 500$.
   $\Rightarrow$ Sieve requires a **large space** $> 2^{100}$.
2. Classical **cross-over point**: ≈ 70 by G6K [ADH+19, Fig. 3(a)].

Performances of sieve/enumeration-based (SD)BKZ [HPS11; MW16; Neu17]		
	Sieve-based	Enumeration-based
RHF	$k^{1/(2k)}$	$k^{1/(2k)}$
Time	$2^{0.292k+o(k)}$	$k^{k/(2e)+o(k)}$ $(\approx k^{0.184k})$
Quantum acceleration		
Time	$2^{0.265k+o(k)}$	$k^{k/(4e)+o(k)}$ $(\approx k^{0.091k})$
Space	$2^{0.265k+o(k)}$	$\mathrm{poly}(k)$

Performance of sieve/enuemration-based (SD)BKZ

1. To solve ApproxSVP for breaking (certain) NIST candidates, one needs to achieve RHF $k^{1/(2k)} \approx 1.006$ for $k \approx 500$.
   $\Rightarrow$ Sieve requires a **large space** $> 2^{100}$.
2. Classical **cross-over point**: ≈ 70 by G6K [ADH+19, Fig. 3(a)].

$\Rightarrow$ Can we improve enumeration-based SVP solver [Kan83; FP83]?

Performances of sieve/enumeration-based (SD)BKZ [HPS11; MW16; Neu17]		
	Sieve-based	Enumeration-based
RHF	$k^{1/(2k)}$	$k^{1/(2k)}$
Time	$2^{0.292k+o(k)}$	$k^{k/(2e)+o(k)}$ $(\approx k^{0.184k})$
Quantum acceleration		
Time	$2^{0.265k+o(k)}$	$k^{k/(4e)+o(k)}$ $(\approx k^{0.091k})$
Space	$2^{0.265k+o(k)}$	$\mathrm{poly}(k)$

Performance of sieve/enuemration-based (SD)BKZ

1. To solve ApproxSVP for breaking (certain) NIST candidates, one needs to achieve RHF $k^{1/(2k)} \approx 1.006$ for $k \approx 500$.
   $\Rightarrow$ Sieve requires a **large space** $> 2^{100}$.
2. Classical **cross-over point**: ≈ 70 by G6K [ADH+19, Fig. 3(a)].

$\Rightarrow$ Can we improve enumeration-based SVP solver [Kan83; FP83]?

$\Rightarrow$ **Can we improve enumeration-based lattice reduction?**

Performances of sieve/enumeration-based (SD)BKZ [HPS11; MW16; Neu17]		
	Sieve-based	Enumeration-based
RHF	$k^{1/(2k)}$	$k^{1/(2k)}$
Time	$2^{0.292k+o(k)}$	$k^{k/(2e)+o(k)}$ $(\approx k^{0.184k})$
Quantum acceleration		
Time	$2^{0.265k+o(k)}$	$k^{k/(4e)+o(k)}$ $(\approx k^{0.091k})$
Space	$2^{0.265k+o(k)}$	$\mathrm{poly}(k)$

Performance of sieve-based (SD)BKZ and FastEnum

1. To solve ApproxSVP for breaking (certain) NIST candidates, one needs to achieve RHF $k^{1/(2k)} \approx 1.006$ for $k \approx 500$.
   $\Rightarrow$ Sieve requires a **large space** $> 2^{100}$.
2. Classical **cross-over point**: ≈ 70 by G6K [ADH+19, Fig. 3(a)].

$\Rightarrow$ Can we improve enumeration-based SVP solver [Kan83; FP83]?

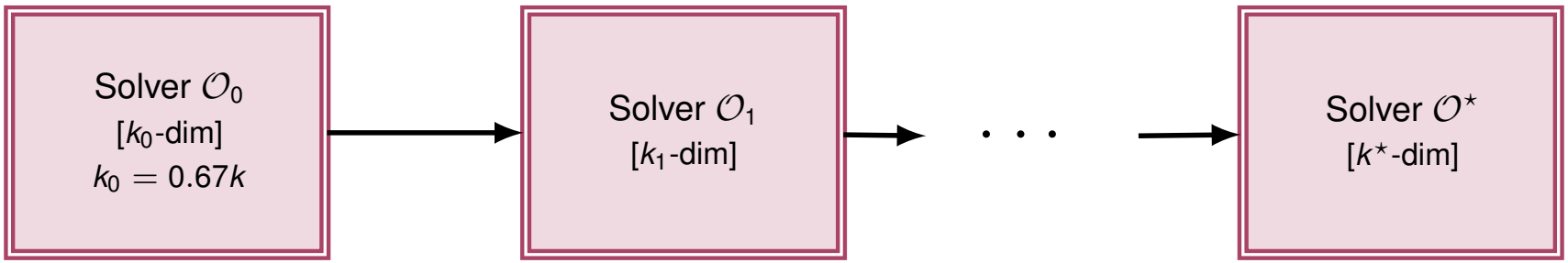
$\Rightarrow$ **Can we improve enumeration-based lattice reduction?**

Performances of sieve-based (SD)BKZ and FastEnum [ABF+20]

	Sieve-based (SD)BKZ	FastEnum [ABF+20]
RHF	$k^{1/(2k)}$	$k^{1/(2k)}$
Time	$2^{0.292k+o(k)}$	$k^{k/8+o(k)}$ $(\approx k^{0.125k+o(k)})$
Quantum acceleration		
Time	$2^{0.265k+o(k)}$	$k^{k/16+o(k)}$ $(\approx k^{0.062k})$
Space	$2^{0.265k+o(k)}$	$\mathrm{poly}(k)$

The idea

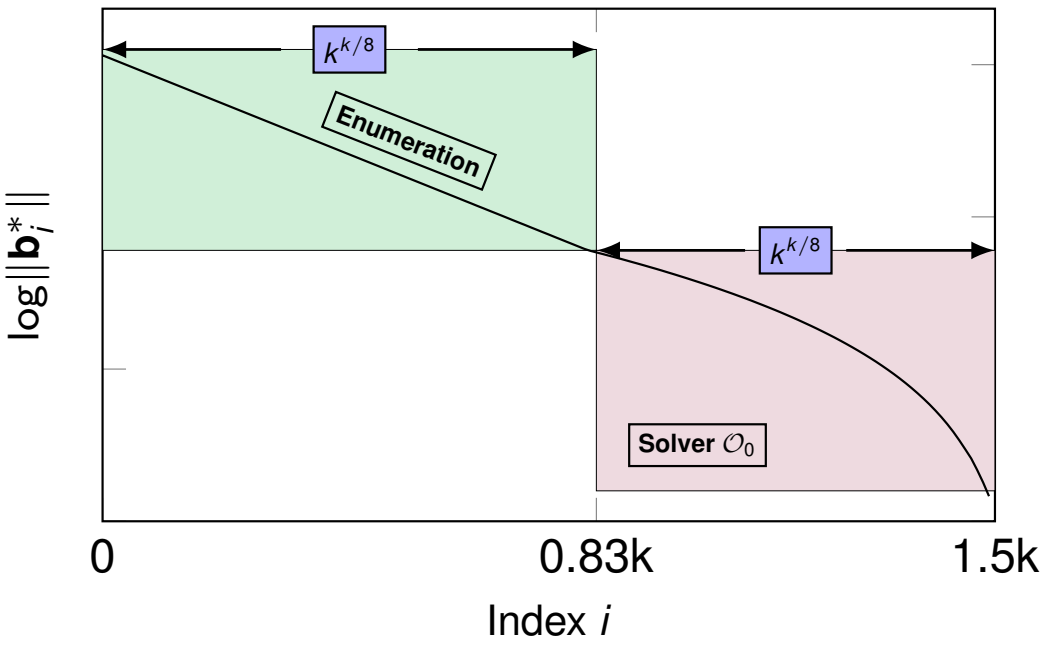
- Start from a smaller $k_0 = k \cdot 2e/8 (\approx 0.67k)$ as $k_0^{k_0/(2e)} \leq k^{k/8}$.
- k_0-dim SVP (by Minkowski's theorem)
  $\Rightarrow$ For k_0-dim lattice, reach HF: $\sqrt{k_0}$ and RHF: $\sqrt{k_0}^{1/(k_0-1)} \approx k^{1/(1.36 \cdot k)}$.

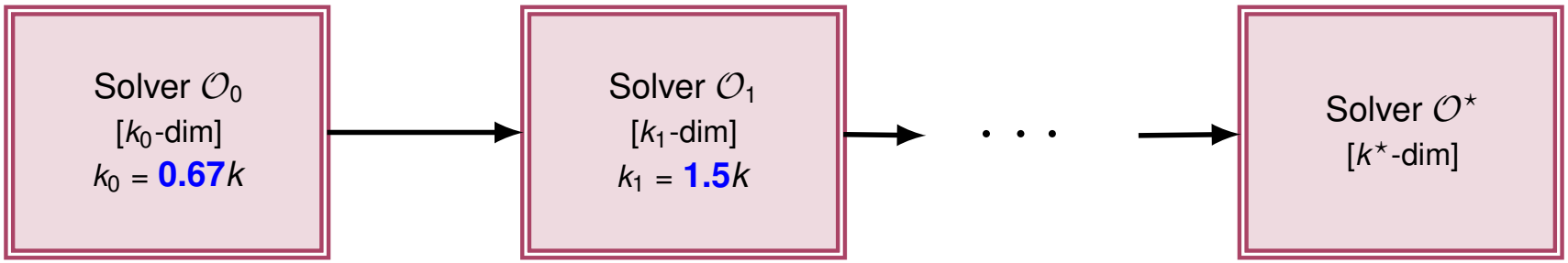


RHF: $k^{1/(1.36 \cdot k)}$ Smaller and smaller RHF Target RHF: $k^{1/(2 \cdot k)}$

The idea

Solver $\mathcal{O}_1$ reaching a smaller RHF.

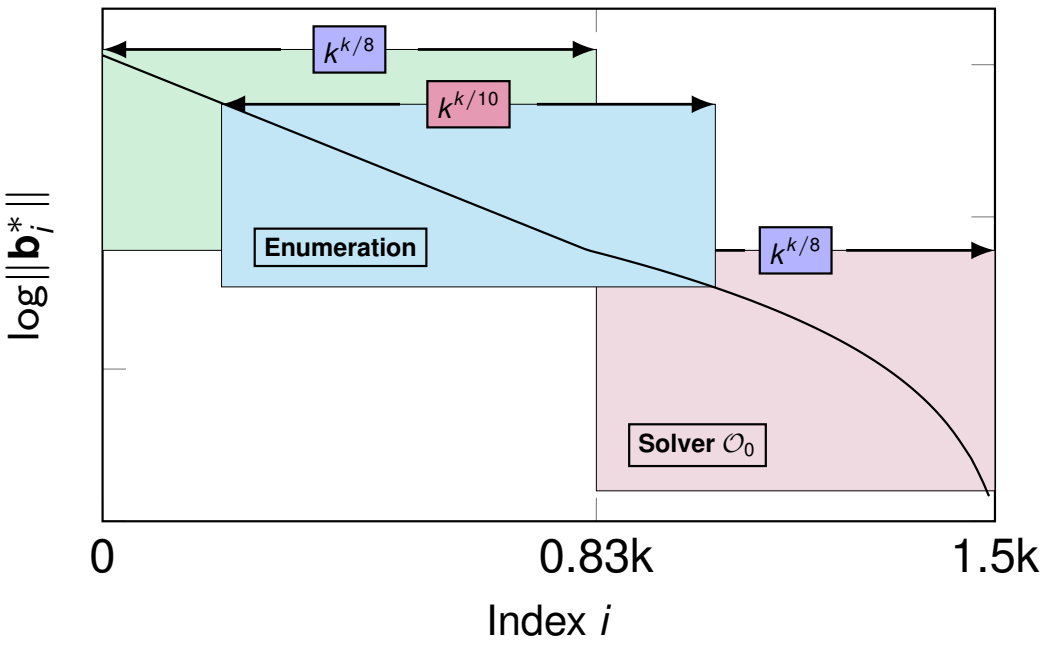


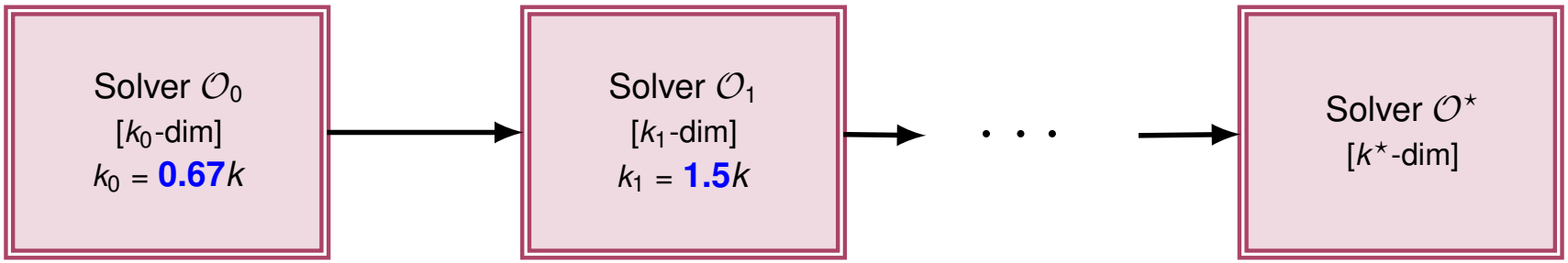


RHF: $k^{1/(1.36\cdot k)}$ RHF: $k^{1/(1.50\cdot k)}$ Target RHF: $k^{1/(2\cdot k)}$

The idea ($k^{k/10}$?)

Solver $\mathcal{O}_1$ reaching a smaller RHF.





RHF: $k^{1/(1.36\cdot k)}$

RHF: $k^{1/(1.50\cdot k)}$

Target RHF: $k^{1/(2\cdot k)}$

New cross-over points

- Suppose we take the following numbers (in the quantum setting):
  1. [ABF+20]: $\log(T_{enum}(k)) = (k \log k/8 - 0.547k + 10.4)/2$;
  2. [ABLR20]: $\log(T_{enum}(k)) = (k \log k/8 - 0.654k + 25.84)/2$;
  3. [Laa15; ADPS16]: $\log(T_{sieve}(k)) = 0.265k + o(k)$.

     (Notice that $o(k)$ is omitted for sieve!)

New cross-over points

- Suppose we take the following numbers (in the quantum setting):
  1. [ABF+20]: $\log(T_{enum}(k)) = (k \log k/8 - 0.547k + 10.4)/2$;
  2. [ABLR20]: $\log(T_{enum}(k)) = (k \log k/8 - 0.654k + 25.84)/2$;
  3. [Laa15; ADPS16]: $\log(T_{sieve}(k)) = 0.265k + o(k)$.

  (Notice that $o(k)$ is omitted for sieve!)

Cross-over points basing on the numbers above		
	1 & 3	2 & 3
Maximal k s.t. $T_{enum}(k) < T_{sieve}(k)$	329	547

New cross-over points

- Suppose we take the following numbers (in the quantum setting):
  1. [ABF+20]: $\log(T_{enum}(k)) = (k \log k/8 - 0.547k + 10.4)/2$;
  2. [ABLR20]: $\log(T_{enum}(k)) = (k \log k/8 - 0.654k + 25.84)/2$;
  3. [Laa15; ADPS16]: $\log(T_{sieve}(k)) = 0.265k + o(k)$.

  (Notice that $o(k)$ is omitted for sieve!)

Cross-over points basing on the numbers above		
	1 & 3	2 & 3
Maximal k s.t. $T_{enum}(k) < T_{sieve}(k)$	329	547

Examples of k in NIST candidates [ABLR20]			
Candidate	Kyber-512	Frodo640	NTRU ntruhrss701
k	380	498	470
Candidate	LightSaber	Falcon	Dilithium III
k	428	388	475

New cross-over points

- Suppose we take the following numbers (in the quantum setting):
  1. [ABF+20]: $\log(T_{enum}(k)) = (k \log k/8 - 0.547k + 10.4)/2$;
  2. [ABLR20]: $\log(T_{enum}(k)) = (k \log k/8 - 0.654k + 25.84)/2$;
  3. [Laa15; ADPS16]: $\log(T_{sieve}(k)) = 0.265k + \#\mathcal{P}(k)$.
  4. [CL21]: $\log(T_{sieve}(k)) = 0.257k + \#\mathcal{P}(k)$.

Cross-over points basing on the numbers above			
	1 & 3	2 & 3	2 & 4
Maximal k s.t. $T_{enum}(k) < T_{sieve}(k)$	329	547	484

Examples of k in NIST candidates [ABLR20]			
Candidate	Kyber-512	Frodo640	NTRU ntruhrss701
k	380	498	470
Candidate	LightSaber	Falcon	Dilithium III
k	428	388	475

New cross-over points

- Suppose we take the following numbers (in the quantum setting):
  1. [ABF+20]: $\log(T_{enum}(k)) = (k \log k/8 - 0.547k + 10.4)/2$;
  2. [ABLR20]: $\log(T_{enum}(k)) = (k \log k/8 - 0.654k + 25.84)/2$;
  3. [Laa15; ADPS16]: $\log(T_{sieve}(k)) = 0.265k + o(k)$.
  4. [CL21]: $\log(T_{sieve}(k)) = 0.257k + o(k)$.

$\Rightarrow$ What should the $o(k)$ concretely be in the quantum setting?

Cross-over points basing on the numbers above			
	1 & 3	2 & 3	2 & 4
Maximal k s.t. $T_{enum}(k) < T_{sieve}(k)$	329	547	484

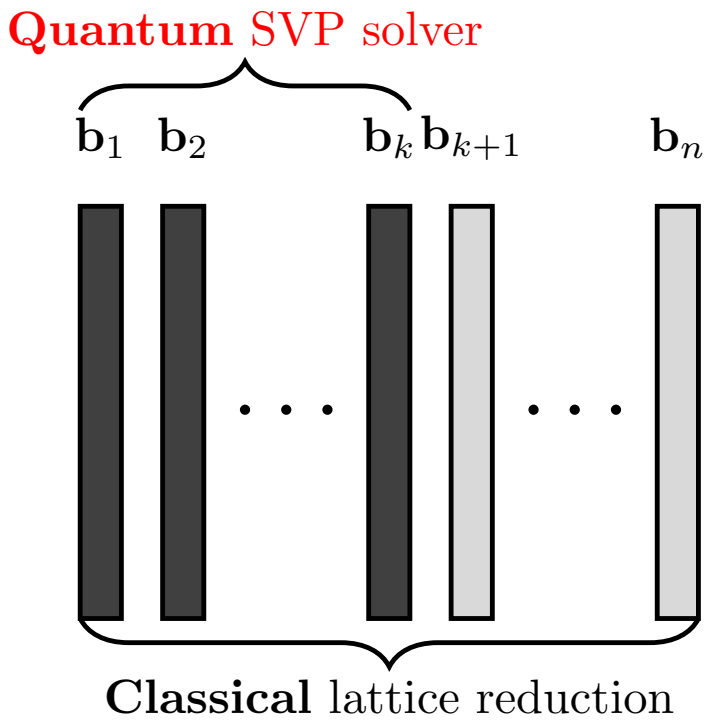
Examples of k in NIST candidates [ABLR20]			
Candidate	Kyber-512	Frodo640	NTRU ntruhrss701
k	380	498	470
Candidate	LightSaber	Falcon	Dilithium III
k	428	388	475

Concluding remarks of Part I

- Enumeration and Sieve are the two most efficient SVP candidates for lattice reduction.
- The current cross-over point between enumeration-based and sieve-based lattice reduction algorithms is:

  $\Rightarrow$ **unknown** ($o(k)$ is unknown for quantum sieve).
- Open: enumeration is relevant for cryptanalysis or not.

Have we fully made use of the quantum computation?



- **Quantum** SVP solver: Quantum manipulation of classical data;
- Lattice reduction: ApproxSVP $\leq$ SVP.

Part II: **The Learning With Errors problem and (Extended-)Dihedral Coset Problem.**

(Recall: ApproxSVP is equivalent to LWE.)

LWE and DCP

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

LWE: Given

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

where $\forall i, \mathbf{a}_i \in_R \mathbb{Z}_q^n$, $e_i \hookleftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$,
$|e_i|/q \approx \alpha = 1/\mathrm{poly}(n)$, find $\mathbf{s}$.

LWE and DCP

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

LWE: Given

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

where $\forall i, \mathbf{a}_i \in_R \mathbb{Z}_q^n$, $e_i \hookleftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$, $|e_i|/q \approx \alpha = 1/\mathrm{poly}(n)$, find $\mathbf{s}$.

DCP: Given

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

where $\forall i, x_i \in_R \mathbb{Z}_N$, find s.

LWE and DCP

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

LWE: Given

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

where $\forall i, \mathbf{a}_i \in_R \mathbb{Z}_q^n$, $e_i \hookleftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$, $|e_i|/q \approx \alpha = 1/\mathrm{poly}(n)$, find $\mathbf{s}$.

$\leq$ [Reg02]

DCP: Given

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

where $\forall i, x_i \in_R \mathbb{Z}_N$, find s.

LWE and DCP

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

LWE: Given

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

where $\forall i, \mathbf{a}_i \in_R \mathbb{Z}_q^n$, $e_i \hookleftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$, $|e_i|/q \approx \alpha = 1/\mathrm{poly}(n)$, find $\mathbf{s}$.

$\leq$ [Reg02]

DCP: Given

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

where $\forall i, x_i \in_R \mathbb{Z}_N$, find s.

Not better than lattice reduction

LWE and DCP

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

LWE: Given

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

where $\forall i, \mathbf{a}_i \in_R \mathbb{Z}_q^n$, $e_i \hookleftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$, $|e_i|/q \approx \alpha = 1/\mathrm{poly}(n)$, find $\mathbf{s}$.

$\leq$ [Reg02]

DCP: Given

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

where $\forall i, x_i \in_R \mathbb{Z}_N$, find s.

Not better than lattice reduction

Lattice reduction (sieve-based):

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

Kuperberg [Kup13]:

$$2^{\mathcal{O}(\log \ell + n \log q / \log \ell)} \left(= 2^{\mathcal{O}(n)}\right)$$

The reduction produces $\ell = \mathrm{poly}(n)$, $N = 2^{n \log n}$ [BKSW18]

(Originally, [Reg02] produces $\ell = \mathrm{poly}(n)$, $N = 2^{n^2}$.)

LWE and DCP

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

LWE: Given

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

where $\forall i, \mathbf{a}_i \in_R \mathbb{Z}_q^n$, $e_i \hookleftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$, $|e_i|/q \approx \alpha = 1/\mathrm{poly}(n)$, find $\mathbf{s}$.

$\leq$ [Reg02]

$\geq$?

DCP: Given

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

where $\forall i, x_i \in_R \mathbb{Z}_N$, find s.

Can we do the reverse reduction? (We only know DCP $\leq$ SubsetSum$_{\approx 1}$)

Lattice reduction (sieve-based):

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

Kuperberg [Kup13]:

$$2^{\mathcal{O}(\log \ell + n \log q / \log \ell)} \left(= 2^{\mathcal{O}(n)}\right)$$

The reduction produces $\ell = \mathrm{poly}(n)$, $N = 2^{n \log n}$ [BKSW18]

(Originally, [Reg02] produces $\ell = \mathrm{poly}(n)$, $N = 2^{n^2}$.)

Extended DCP

EDCP	DCP
for an integer M	
$\sum_{j=0}^{M-1} \lvert j, \mathbf{x} + j \cdot \mathbf{s} \rangle$	$\lvert 0, x \rangle + \lvert 1, x + s \rangle$

What if you are given:

$$\lvert 0, x \rangle + \lvert 1, x + s \rangle + \lvert 2, x + 2 \cdot s \rangle + \lvert 3, x + 3 \cdot s \rangle + \cdots ?$$

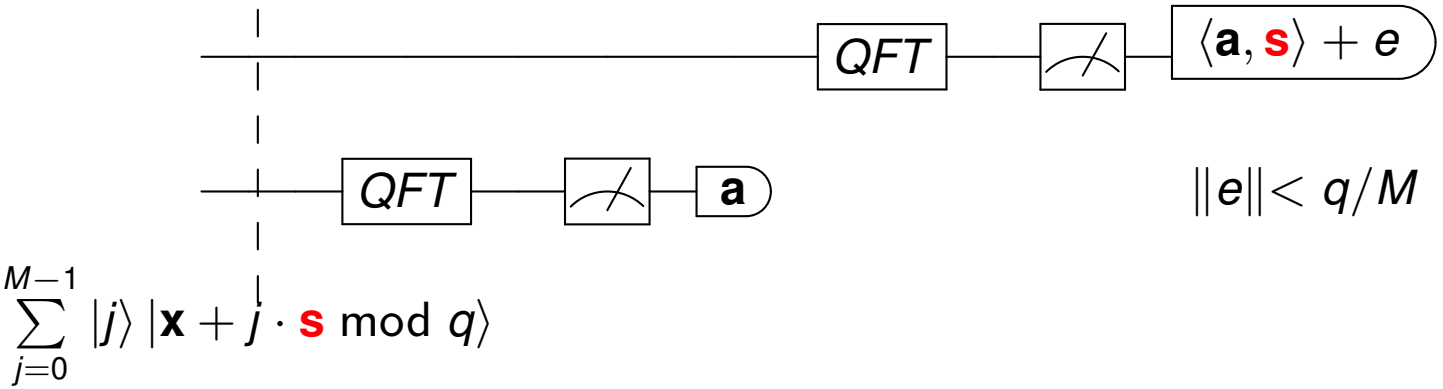
Extended DCP

EDCP	DCP
for an integer M	
$\sum_{j=0}^{M-1} \lvert j, \mathbf{x} + j \cdot \mathbf{s} \rangle$	$\lvert 0, x \rangle + \lvert 1, x + s \rangle$

Main result in [BKSW18]:

$$\boxed{\text{LWE} \iff \text{EDCP} \leq \text{DCP}}$$

EDCP $\leq$ LWE



- This actually generalizes the Shor's period-finding algorithm.
  1. Given f a periodic function, we can prepare EDCP sample with $M = q$;
  2. This produce LWE sample with noise $e = 0$.

LWE and EDCP

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

LWE: Given

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

where $\forall i, \mathbf{a}_i \in_R \mathbb{Z}_q^n$, $e_i \hookleftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$ with $\alpha = 1/\mathrm{poly}(n)$, find $\mathbf{s}$.

$\Longleftrightarrow$ [BKSW18]

EDCP: Given

$$\sum_{j=0}^{M-1} |j\rangle\, |\mathbf{x}_1 + j \cdot \mathbf{s} \bmod q\rangle$$
$$\vdots$$
$$\sum_{j=0}^{M-1} |j\rangle\, |\mathbf{x}_l + j \cdot \mathbf{s} \bmod q\rangle$$

where $\forall i, \mathbf{x}_i \in \mathbb{Z}_q^n$, find $\mathbf{s}$.

Asymtotically same as solving DCP

Lattice reduction (sieve-based):

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

Kuperberg [Kup13; Pei20]:

$$2^{\mathcal{O}(\log \ell + n \log q / \log \ell)} \left(= 2^{\mathcal{O}(n)}\right)$$

The reduction produces $\ell = \mathrm{poly}(n)$

LWE and EDCP

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

LWE: Given

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

where $\forall i, \mathbf{a}_i \in_R \mathbb{Z}_q^n$, $e_i \hookleftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$ with $\alpha = 1/\mathrm{poly}(n)$, find $\mathbf{s}$.

$\Longleftrightarrow$ [BKSW18]

EDCP: Given

$$\sum_{j=0}^{M-1} |j\rangle |\mathbf{x}_1 + j \cdot \mathbf{s} \bmod q\rangle$$
$$\vdots$$
$$\sum_{j=0}^{M-1} |j\rangle |\mathbf{x}_l + j \cdot \mathbf{s} \bmod q\rangle$$

where $\forall i, \mathbf{x}_i \in \mathbb{Z}_q^n$, find $\mathbf{s}$.

$\Rightarrow$ The best known hidden constant is 0.265 with lattice reduction.

Lattice reduction (sieve-based):

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

Kuperberg [Kup13; Pei20]:

$$2^{\mathcal{O}(\log \ell + n \log q / \log \ell)} \left(= 2^{\mathcal{O}(n)}\right)$$

The reduction produces $\ell = \mathrm{poly}(n)$

LWE and EDCP

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

LWE: Given

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

where $\forall i, \mathbf{a}_i \in_R \mathbb{Z}_q^n$, $e_i \hookleftarrow \mathcal{D}_{\mathbb{Z},\alpha q}$ with $\alpha = 1/\mathrm{poly}(n)$, find $\mathbf{s}$.

$\Longleftrightarrow$ [BKSW18]

EDCP: Given

$$\sum_{j=0}^{M-1} |j\rangle\,|\mathbf{x}_1 + j \cdot \mathbf{s} \bmod q\rangle$$
$$\vdots$$
$$\sum_{j=0}^{M-1} |j\rangle\,|\mathbf{x}_l + j \cdot \mathbf{s} \bmod q\rangle$$

where $\forall i, \mathbf{x}_i \in \mathbb{Z}_q^n$, find $\mathbf{s}$.

Q: Find separation between DCP and EDCP or prove they are equivalent.

Lattice reduction (sieve-based):

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

Kuperberg [Kup13; Pei20]:

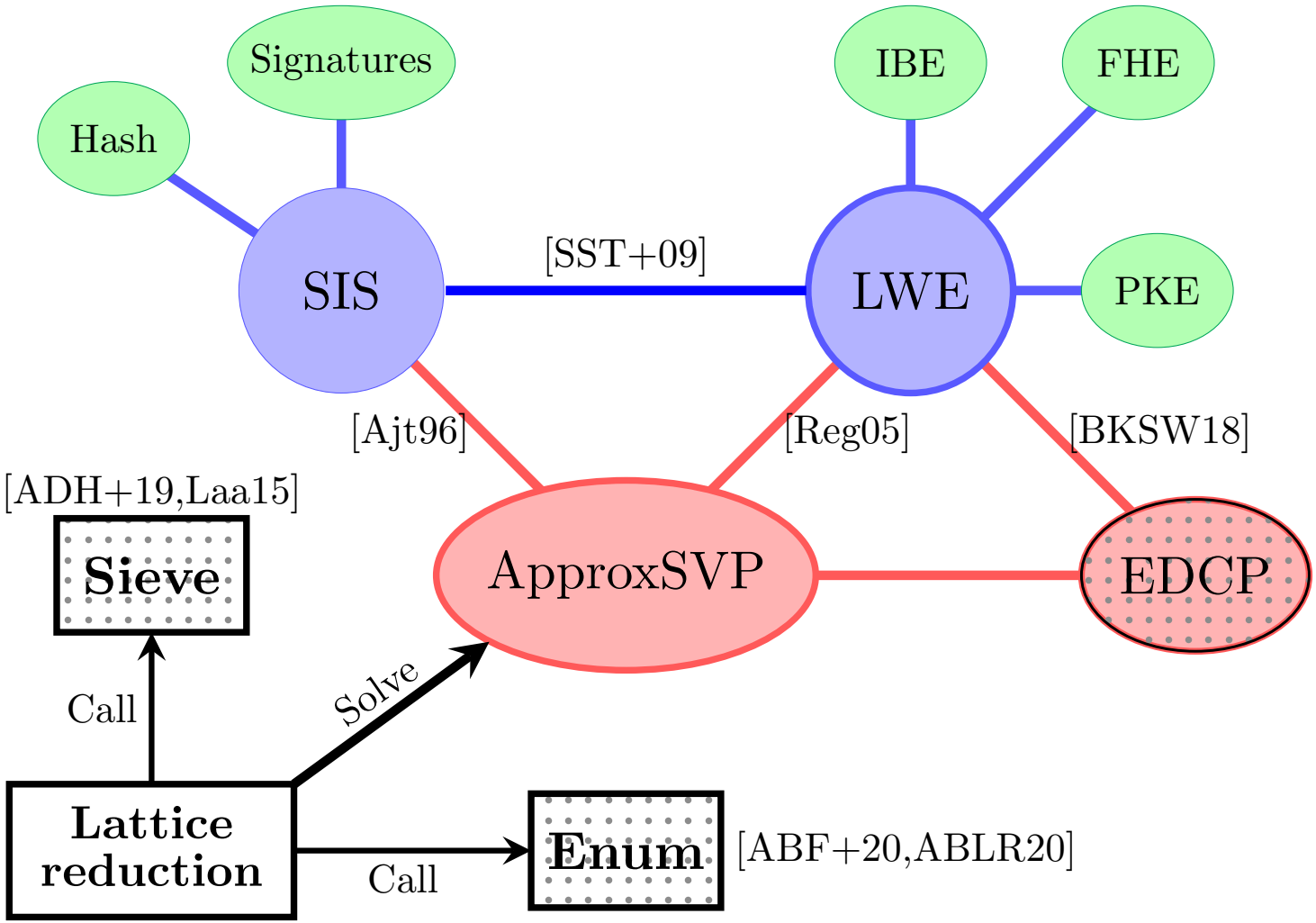
$$2^{\mathcal{O}(\log \ell + n \log q / \log \ell)} \left(= 2^{\mathcal{O}(n)}\right)$$

The reduction produces $\ell = \mathrm{poly}(n)$

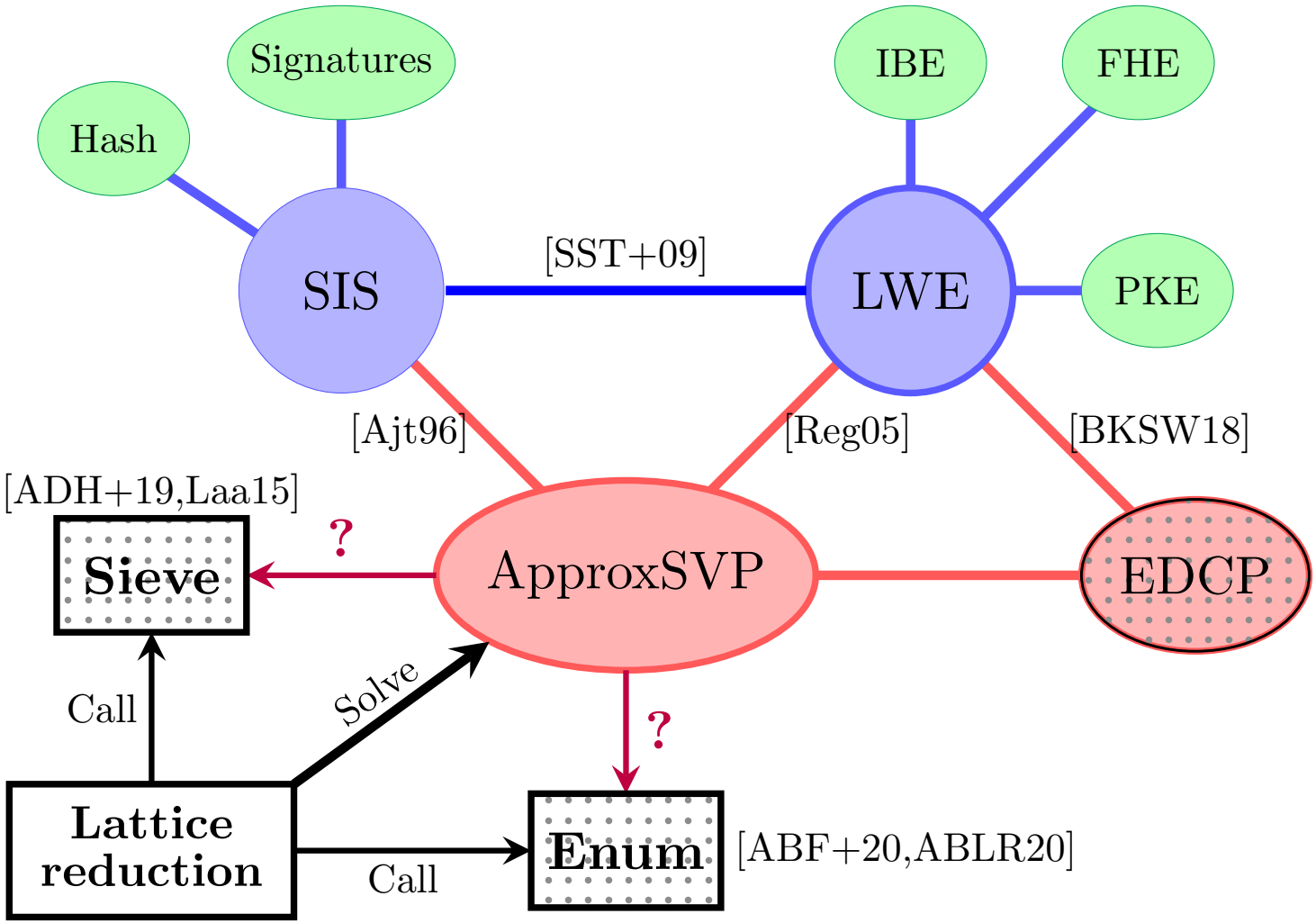
Concluding remarks of Part II

- LWE (therefore ApproxSVP) is equivalent to EDCP;
- To study quantum algorithms for ApproxSVP, may study EDCP directly.

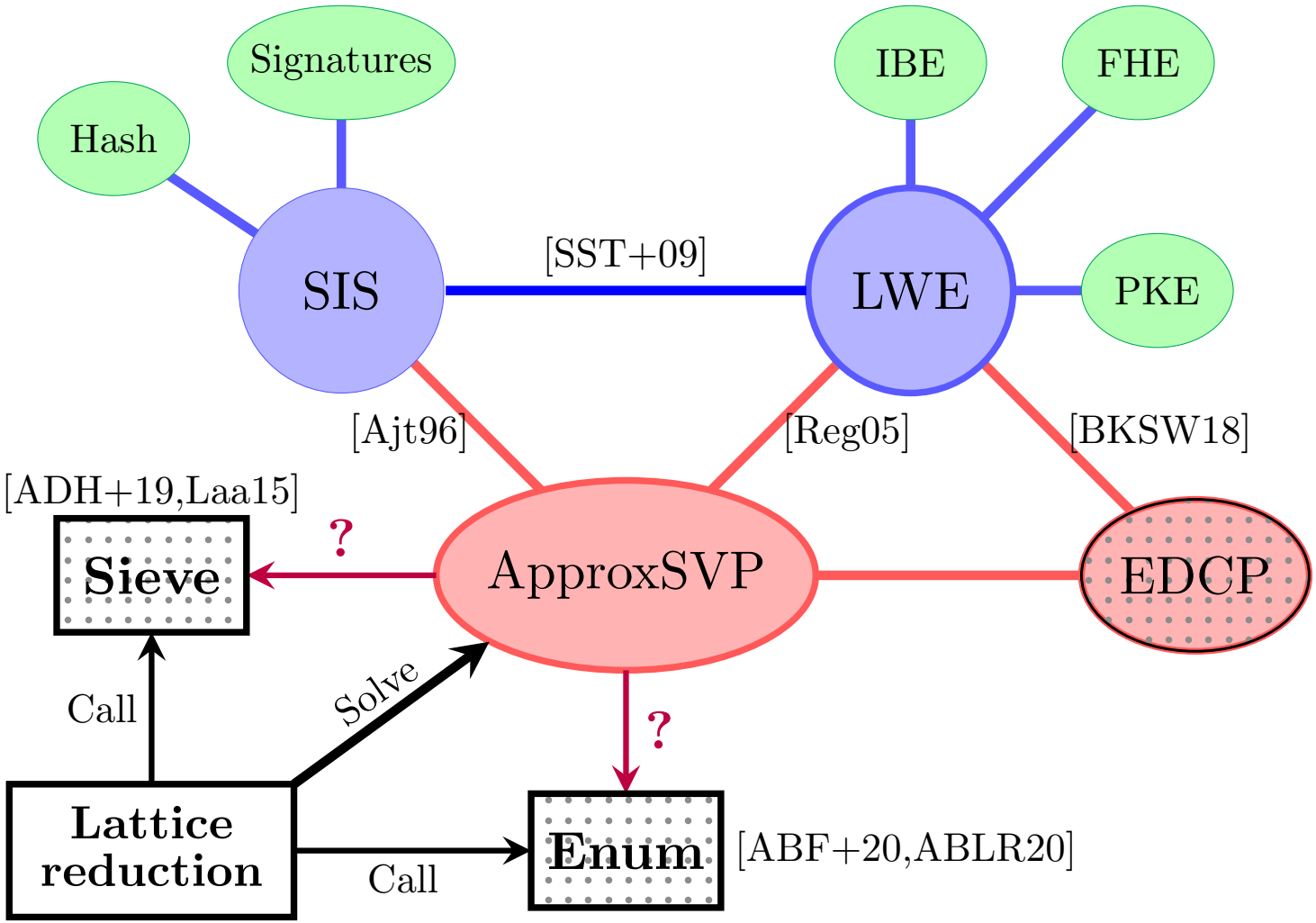
Conclusion


Signatures
IBE
FHE
Hash
SIS
[SST+09]
LWE
PKE
[Ajt96]
[Reg05]
[BKSW18]
[ADH+19,Laa15]
Sieve
ApproxSVP
EDCP
Call
Solve
Lattice reduction
Call
Enum
[ABF+20,ABLR20]

Conclusion


Signatures
IBE
FHE
Hash
SIS
[SST+09]
LWE
PKE
[Ajt96]
[Reg05]
[BKSW18]
[ADH+19,Laa15]
?
Sieve
ApproxSVP
EDCP
Call
Solve
?
Lattice reduction
Call
Enum
[ABF+20,ABLR20]

Conclusion



Thank you!

References I

[ABF+20] Martin R. Albrecht, Shi Bai, Pierre-Alain Fouque, Paul Kirchner, Damien Stehlé, and Weiqiang Wen, Faster enumeration-based lattice reduction: Root hermite factor $k^{1/(2k)}$ time $k^{k/8+o(k)}$, Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II, 2020, pp. 186–212.

[ABLR20] Martin R. Albrecht, Shi Bai, Jianwei Li, and Joe Rowell, Lattice reduction with approximate enumeration oracles: Practical algorithms and concrete performance, Cryptology ePrint Archive, Report 2020/1260, 2020, `https://eprint.iacr.org/2020/1260`.

[ADH+19] Martin R. Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn W. Postlethwaite, and Marc Stevens, The general sieve kernel and new records in lattice reduction, 2019, pp. 717–746.

[ADPS16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe, Post-quantum key exchange - A new hope, 2016, pp. 327–343.

[ADRS15] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz, Solving the shortest vector problem in 2^n time using discrete Gaussian sampling: Extended abstract, 2015, pp. 733–742.

[AKS01] Miklós Ajtai, Ravi Kumar, and D. Sivakumar, A sieve algorithm for the shortest lattice vector problem, 2001, pp. 601–610.

[ANS18] Yoshinori Aono, Phong Q. Nguyen, and Yixin Shen, Quantum lattice enumeration and tweaking discrete pruning, 2018, pp. 405–434.

[BDGL16] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven, New directions in nearest neighbor searching with applications to lattice sieving, 2016, pp. 10–24.

[BKSW18] Zvika Brakerski, Elena Kirshanova, Damien Stehlé, and Weiqiang Wen, Learning with errors and extrapolated dihedral cosets, 2018, pp. 702–727.

[CL21] André Chailloux and Johanna Loyer, Lattice sieving via quantum random walks, Cryptology ePrint Archive, Report 2021/570, 2021, `https://eprint.iacr.org/2021/570`.

[FP83] Ulrich Fincke and Michael Pohst, A procedure for determining algebraic integers of given norm, EUROCAL (J. A. van Hulzen, ed.), LNCS, vol. 162, Springer, 1983, pp. 194–202.

[GN08] Nicolas Gama and Phong Q. Nguyen, Finding short lattice vectors within Mordell's inequality, 2008, pp. 207–216.

[GNR10] Nicolas Gama, Phong Q. Nguyen, and Oded Regev, Lattice enumeration using extreme pruning, 2010, pp. 257–278.

References II

[HPS11] Guillaume Hanrot, Xavier Pujol, and Damien Stehlé, Analyzing blockwise lattice algorithms using dynamical systems, 2011, pp. 447–464.

[HS07] Guillaume Hanrot and Damien Stehlé, Improved analysis of kannan's shortest lattice vector algorithm, 2007, pp. 170–186.

[Kan83] Ravi Kannan, Improved algorithms for integer programming and related lattice problems, 1983, pp. 193–206.

[Kup13] Greg Kuperberg, Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem, 8th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2013, May 21-23, 2013, Guelph, Canada, 2013, pp. 20–34.

[Laa15] Thijs Laarhoven, Search problems in cryptography, Ph.D. thesis, Eindhoven University of Technology, 2015.

[MW16] Daniele Micciancio and Michael Walter, Practical, predictable lattice basis reduction, 2016, pp. 820–849.

[Neu17] Arnold Neumaier, Bounding basis reduction properties, Des. Codes Cryptogr. **84** (2017), no. 1-2, 237–259.

[Pei20] Chris Peikert, He gives C-sieves on the CSIDH, 2020, pp. 463–492.

[PS09] Xavier Pujol and Damien Stehle, Solving the shortest lattice vector problem in time 2^2.465n, Cryptology ePrint Archive, Report 2009/605, 2009, `https://eprint.iacr.org/2009/605`.

[SE94] Claus-Peter Schnorr and Michael Euchner, Lattice basis reduction: Improved practical algorithms and solving subset sum problems, Math. Program. **66** (1994), 181–199.

[Wal20] Michael Walter, The convergence of slide-type reductions, Cryptology ePrint Archive, Report 2020/1409, 2020, `https://eprint.iacr.org/2020/1409`.