Technische Universiteit
Eindhoven
University of Technology

Lattice-based cryptography

Thijs Laarhoven

mail@thijs.com
http://www.thijs.com/

PQC Executive School
(July 1, 2019)

TU/e

Outline

Lattices

Lattice-based signatures

Lattice algorithms

Summary

References

Outline

Lattices

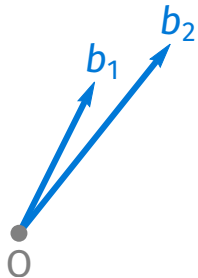
What is a lattice?

Lattices

What is a lattice?

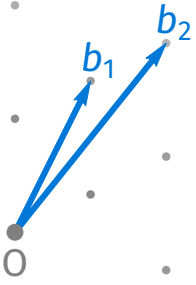
Lattices

What is a lattice?



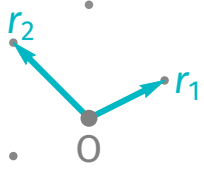
Lattices

What is a lattice?



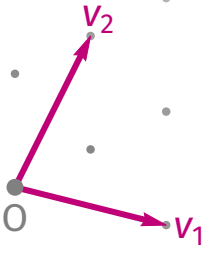
Lattices

Basis for the same lattice



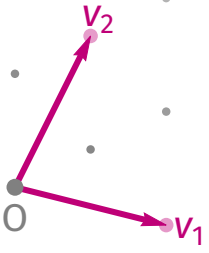
Lattices

Basis for a sublattice



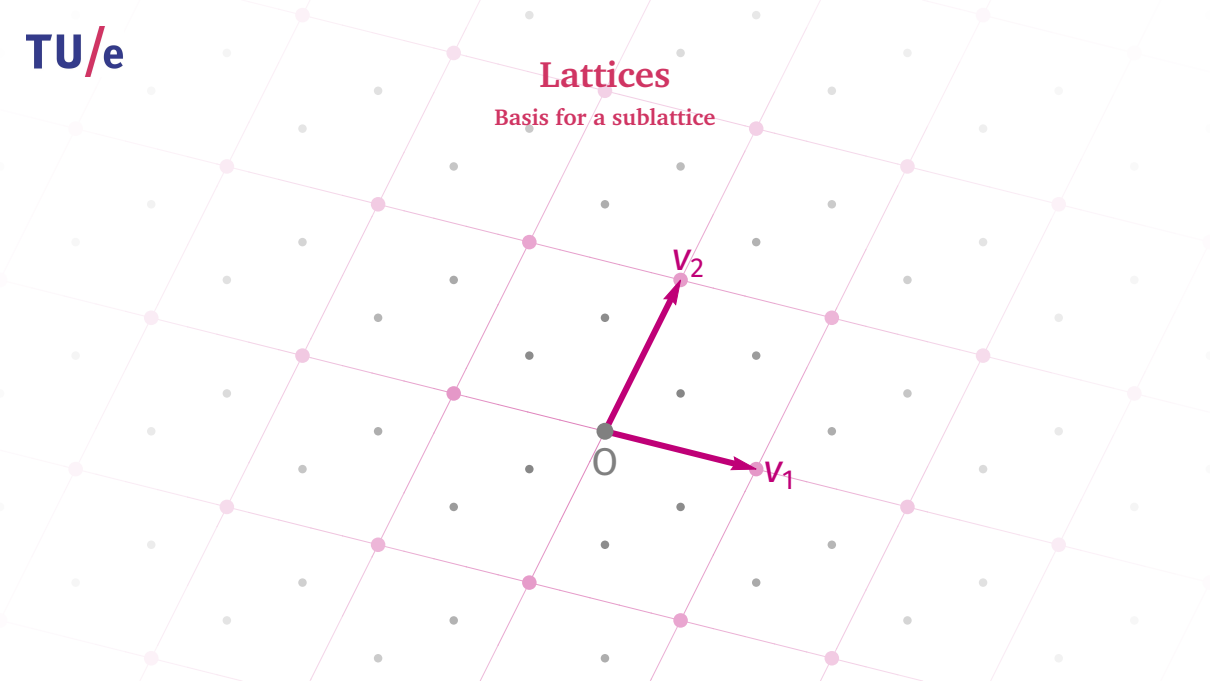
Lattices

Basis for a sublattice



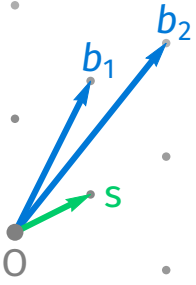
Lattices

Basis for a sublattice



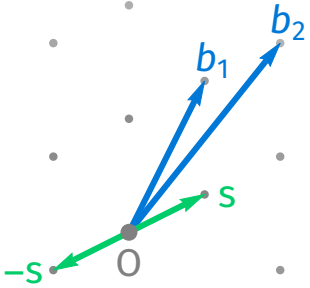
Lattices

Shortest Vector Problem (SVP)



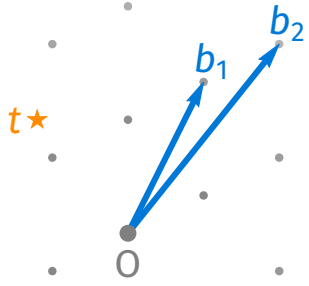
Lattices

Shortest Vector Problem (SVP)



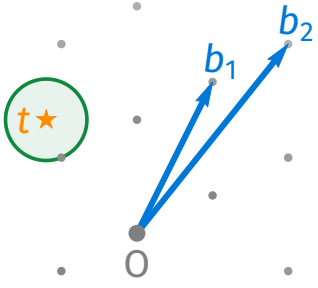
Lattices

Closest Vector Problem (CVP)



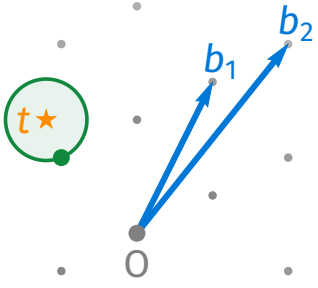
Lattices

Closest Vector Problem (CVP)



Lattices

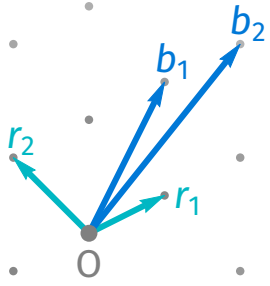
Closest Vector Problem (CVP)



TU/e

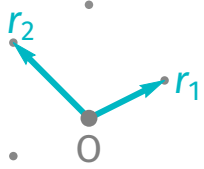
Lattices

Lattice basis reduction



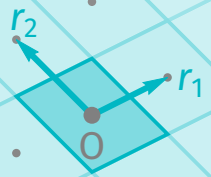
Lattices

Finding closest vectors (good basis)



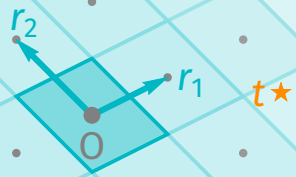
Lattices

Finding closest vectors (good basis)



Lattices

Finding closest vectors (good basis)



Lattices

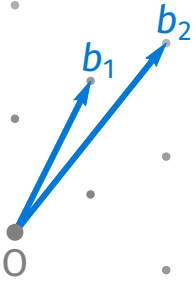
Finding closest vectors (good basis)

Lattices

Finding closest vectors (good basis)

Lattices

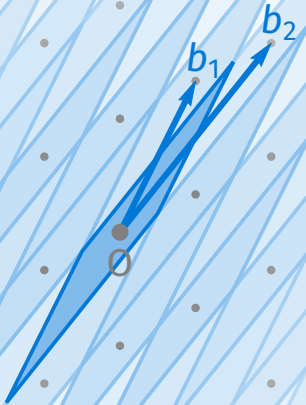
Finding closest vectors (bad basis)



TU/e

Lattices

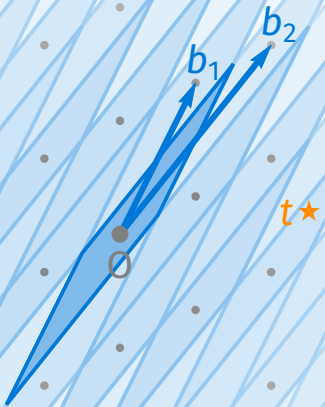
Finding closest vectors (bad basis)



TU/e

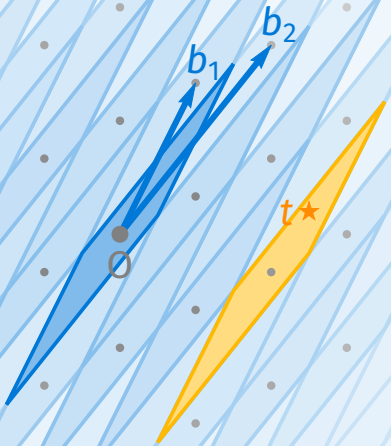
Lattices

Finding closest vectors (bad basis)



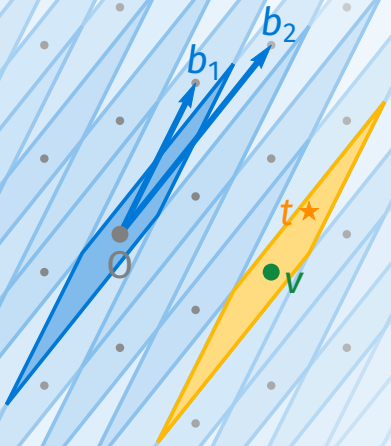
Lattices

Finding closest vectors (bad basis)



Lattices

Finding closest vectors (bad basis)



TU/e

Lattices

Lattice problems

Easy lattice problems:

- Given a good basis, finding a bad basis
- Given a good basis, finding short lattice vectors
- Given a good basis, finding close lattice vectors
- Given any basis, verifying membership of the lattice

TU/e

Lattices

Lattice problems

Easy lattice problems:

- Given a good basis, finding a bad basis
- Given a good basis, finding short lattice vectors
- Given a good basis, finding close lattice vectors
- Given any basis, verifying membership of the lattice

Hard lattice problems:

- Given a bad basis, finding a good basis
- Given a bad basis, finding short lattice vectors
- Given a bad basis, finding close lattice vectors

Outline

TU/e

Lattice-based signatures

Overview [GGH97]

Private key:

$\boldsymbol{R} = \{\boldsymbol{r}_1, \ldots, \boldsymbol{r}_n\}$

Public key:

$\boldsymbol{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$

Signing $\boldsymbol{m}$:

$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{s} = \boldsymbol{R}\lfloor \boldsymbol{R}^{-1}\boldsymbol{c} \rceil$

Verifying $\boldsymbol{s}$:

$\boldsymbol{s} \in \mathcal{L}$

$\|\boldsymbol{s} - H(\boldsymbol{m})\|$ small

Lattice-based signatures

Private key

Private key:

$\boldsymbol{R} = \{\boldsymbol{r}_1, \ldots, \boldsymbol{r}_n\}$

Public key:

$\boldsymbol{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$

Signing $\boldsymbol{m}$:

$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{s} = \boldsymbol{R}\lfloor \boldsymbol{R}^{-1}\boldsymbol{c} \rceil$

Verifying $\boldsymbol{s}$:

$\boldsymbol{s} \in \mathcal{L}$

$\|\boldsymbol{s} - H(\boldsymbol{m})\|$ small

Lattice-based signatures

Private key

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

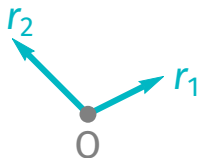
$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small



Lattice-based signatures

Private key

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

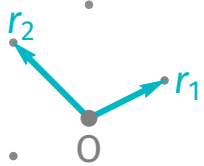
$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small



Lattice-based signatures

Public key

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

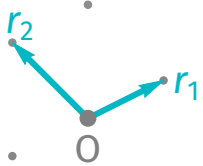
$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small



Lattice-based signatures

Public key

Private key:

$\boldsymbol{R} = \{\boldsymbol{r}_1, \ldots, \boldsymbol{r}_n\}$

Public key:

$\boldsymbol{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$

Signing $\boldsymbol{m}$:

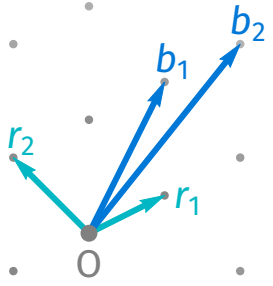
$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{s} = \boldsymbol{R}\lfloor \boldsymbol{R}^{-1}\boldsymbol{c} \rceil$

Verifying $\boldsymbol{s}$:

$\boldsymbol{s} \in \mathcal{L}$

$\|\boldsymbol{s} - H(\boldsymbol{m})\|$ small



Lattice-based signatures

Signing a message

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

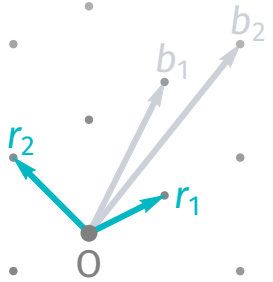
$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small



Lattice-based signatures

Signing a message

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

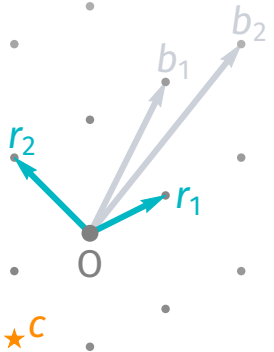
$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small



Lattice-based signatures

Signing a message

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

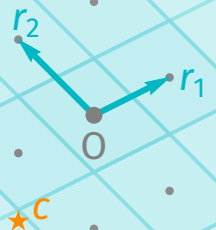
$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small



Lattice-based signatures

Signing a message

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

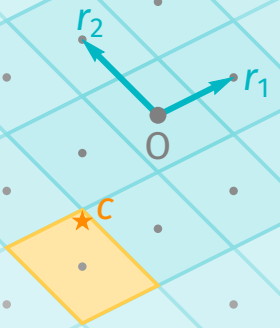
$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small



Lattice-based signatures

Signing a message

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

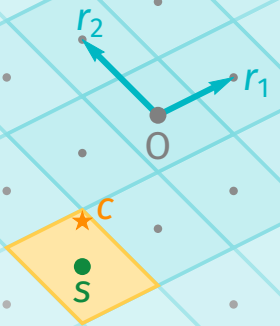
$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small



Lattice-based signatures

Verifying a signature

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$\boldsymbol{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$

Signing $\boldsymbol{m}$:

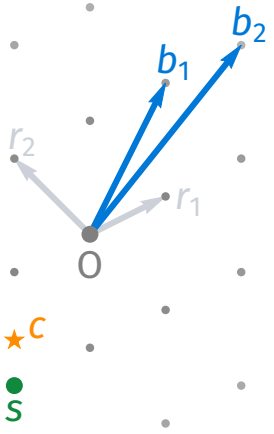
$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{s} = R\lfloor R^{-1}\boldsymbol{c} \rceil$

Verifying $\boldsymbol{s}$:

$\boldsymbol{s} \in \mathcal{L}$

$\|\boldsymbol{s} - H(\boldsymbol{m})\|$ small



Lattice-based signatures

Verifying a signature

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$\boldsymbol{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$

Signing $\boldsymbol{m}$:

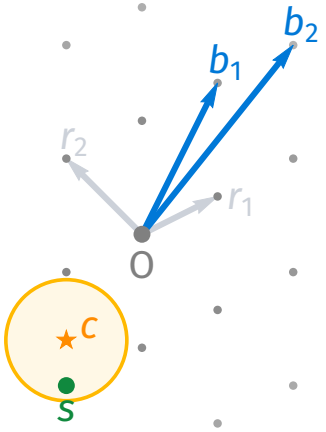
$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{s} = R\lfloor R^{-1}\boldsymbol{c} \rceil$

Verifying $\boldsymbol{s}$:

$\boldsymbol{s} \in \mathcal{L}$

$\|\boldsymbol{s} - H(\boldsymbol{m})\|$ small



TU/e

Lattice-based signatures

Overview

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

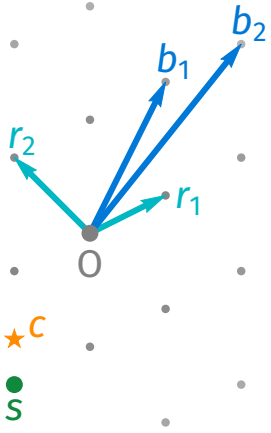
$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small



Lattice-based signatures

Attacking the scheme [NR06]

Private key:

$\boldsymbol{R} = \{\boldsymbol{r}_1, \ldots, \boldsymbol{r}_n\}$

Public key:

$\boldsymbol{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$

Signing $\boldsymbol{m}$:

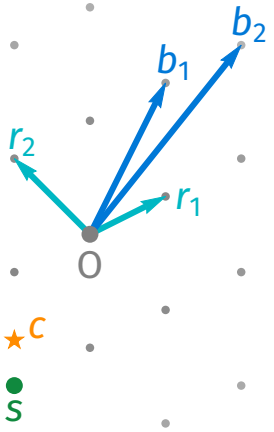
$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{s} = \boldsymbol{R}\lfloor \boldsymbol{R}^{-1}\boldsymbol{c} \rceil$

Verifying $\boldsymbol{s}$:

$\boldsymbol{s} \in \mathcal{L}$

$\|\boldsymbol{s} - H(\boldsymbol{m})\|$ small



Obtain error vectors:

$\boldsymbol{s} = \mathrm{Sign}(\boldsymbol{m})$

$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{e} = \boldsymbol{c} - \boldsymbol{s}$

Leaks $\boldsymbol{R} = \{\boldsymbol{r}_1, \ldots, \boldsymbol{r}_d\}$:

$\boldsymbol{e} \in \mathcal{D}(\boldsymbol{R})$

Can recover $\boldsymbol{R}$ via gradient descent

Lattice-based signatures

Obtain a signature

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small

Obtain error vectors:

$s = \text{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

Lattice-based signatures

Compute the error vector

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small

Obtain error vectors:

$s = \text{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

Lattice-based signatures

Store the error vector

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small

Obtain error vectors:

$s = \text{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

TU/e

Lattice-based signatures

Obtain a signature

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small

Obtain error vectors:

$s = \text{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

TU/e

Lattice-based signatures

Compute the error vector

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

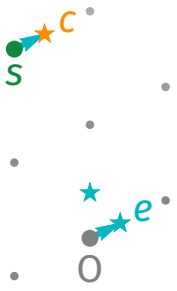
$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small



Obtain error vectors:

$s = \text{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

Lattice-based signatures

Store the error vector

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small

Obtain error vectors:

$s = \text{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

Lattice-based signatures

Obtain a signature

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

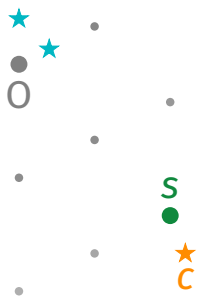
$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small



Obtain error vectors:

$s = \text{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

Lattice-based signatures

Compute the error vector

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

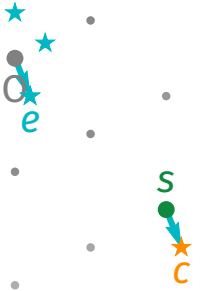
$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small



Obtain error vectors:

$s = \text{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

Lattice-based signatures

Store the error vector

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small

Obtain error vectors:

$s = \text{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

TU/e

Lattice-based signatures

Obtain many error vectors

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small

Obtain error vectors:

$s = \text{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

Lattice-based signatures

Obtain many error vectors

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small

Obtain error vectors:

$s = \text{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

Lattice-based signatures

Obtain many error vectors

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small

Obtain error vectors:

$s = \text{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

Lattice-based signatures

Obtain many error vectors

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small

Obtain error vectors:

$s = \text{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

Lattice-based signatures

Recover the private key

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

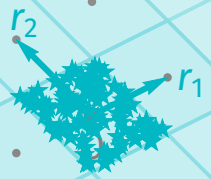
$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small



Obtain error vectors:

$s = \mathrm{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

Lattice-based signatures

Recover the private key

Private key:

$R = \{r_1, \ldots, r_n\}$

Public key:

$B = \{b_1, \ldots, b_n\}$

Signing m:

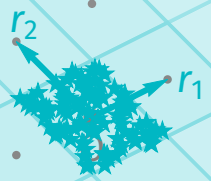
$c = H(m)$

$s = R\lfloor R^{-1}c \rceil$

Verifying s:

$s \in \mathcal{L}$

$\|s - H(m)\|$ small



Obtain error vectors:

$s = \mathrm{Sign}(m)$

$c = H(m)$

$e = c - s$

Leaks $R = \{r_1, \ldots, r_d\}$:

$e \in \mathcal{D}(R)$

Can recover R via gradient descent

Lattice-based signatures

Overview

Private key:

$\boldsymbol{R} = \{\boldsymbol{r}_1, \ldots, \boldsymbol{r}_n\}$

Public key:

$\boldsymbol{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$

Signing $\boldsymbol{m}$:

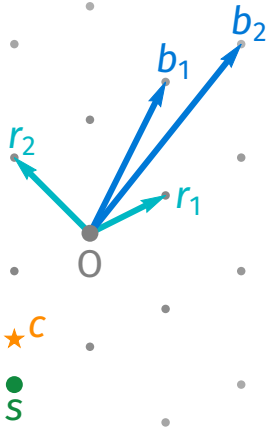
$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{s} = \boldsymbol{R}\lfloor \boldsymbol{R}^{-1}\boldsymbol{c} \rceil$

Verifying $\boldsymbol{s}$:

$\boldsymbol{s} \in \mathcal{L}$

$\|\boldsymbol{s} - H(\boldsymbol{m})\|$ small



Obtain error vectors:

$\boldsymbol{s} = \mathrm{Sign}(\boldsymbol{m})$

$\boldsymbol{c} = H(\boldsymbol{m})$

$\boldsymbol{e} = \boldsymbol{c} - \boldsymbol{s}$

Leaks $\boldsymbol{R} = \{\boldsymbol{r}_1, \ldots, \boldsymbol{r}_d\}$:

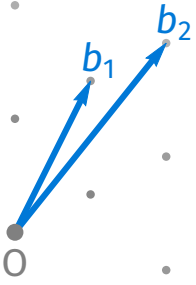
$\boldsymbol{e} \in \mathcal{D}(\boldsymbol{R})$

Can recover $\boldsymbol{R}$ via gradient descent

Outline

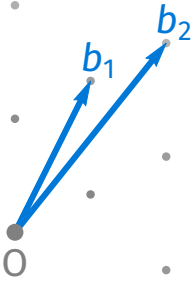
Lattice algorithms

Lattice enumeration [FP85]



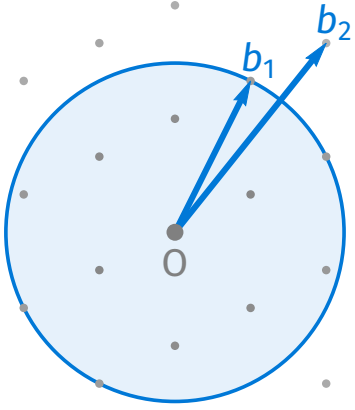
Lattice algorithms

Determine possible coefficients of b_2



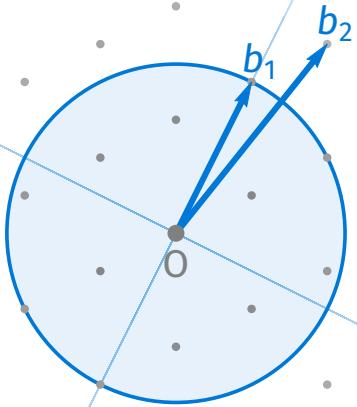
Lattice algorithms

Determine possible coefficients of b_2



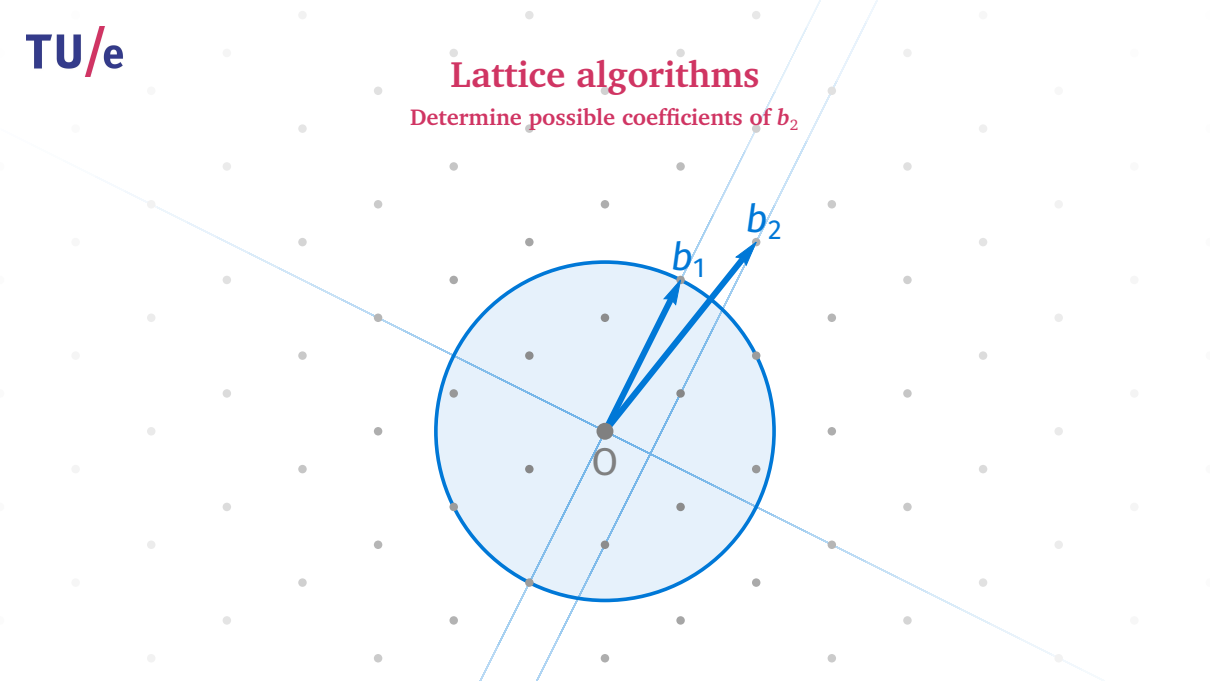
Lattice algorithms

Determine possible coefficients of b_2



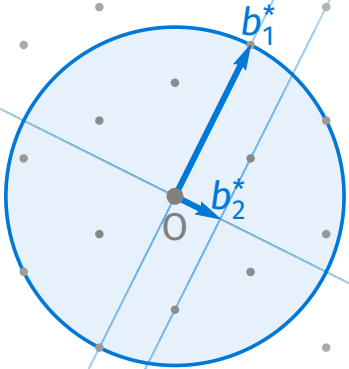
Lattice algorithms

Determine possible coefficients of b_2



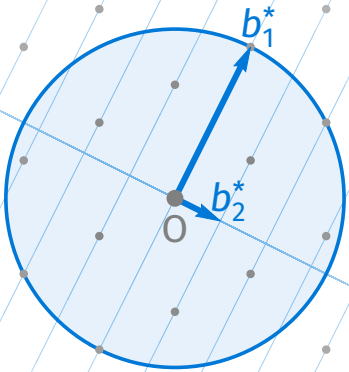
Lattice algorithms

Determine possible coefficients of b_2



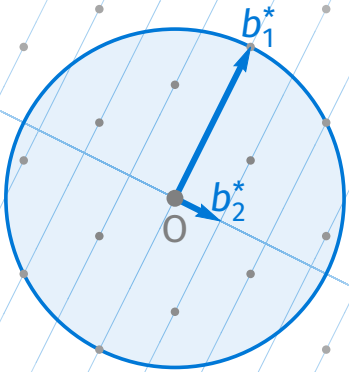
Lattice algorithms

Determine possible coefficients of b_2



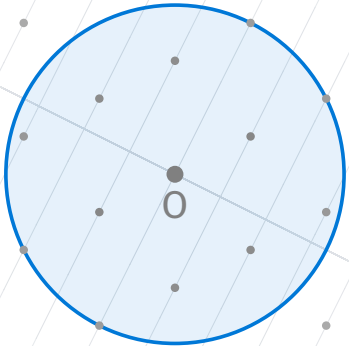
Lattice algorithms

Find short vectors for each coefficient of b_2



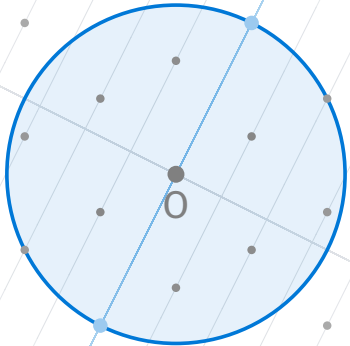
Lattice algorithms

Find short vectors for each coefficient of b_2



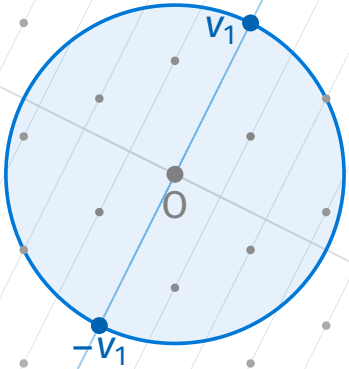
Lattice algorithms

Find short vectors for each coefficient of b_2



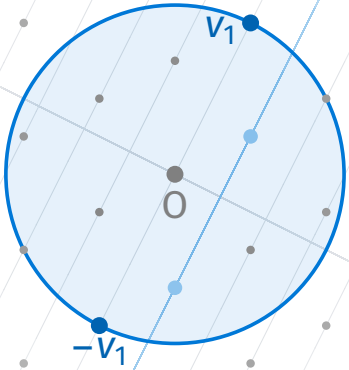
Lattice algorithms

Find short vectors for each coefficient of b_2



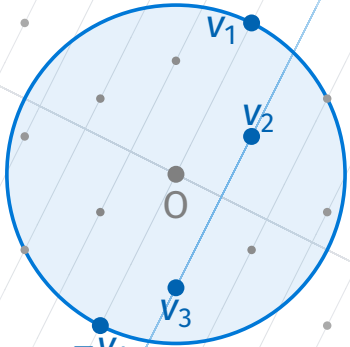
Lattice algorithms

Find short vectors for each coefficient of b_2



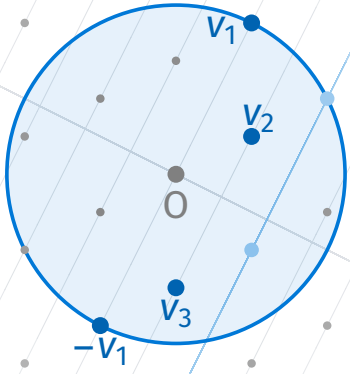
Lattice algorithms

Find short vectors for each coefficient of b_2



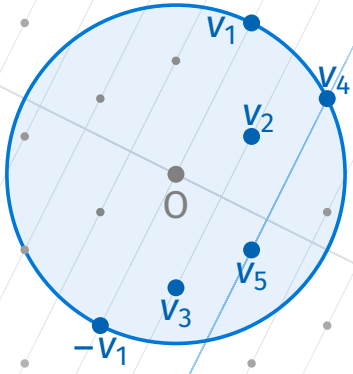
Lattice algorithms

Find short vectors for each coefficient of b_2



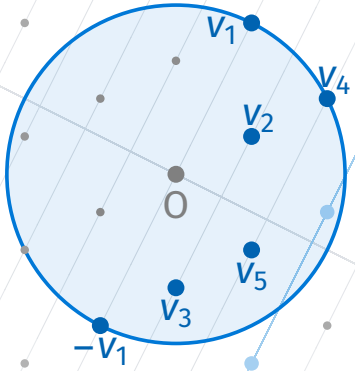
Lattice algorithms

Find short vectors for each coefficient of b_2



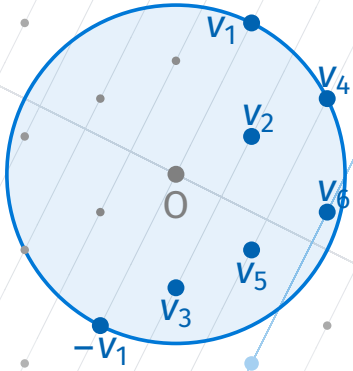
Lattice algorithms

Find short vectors for each coefficient of b_2



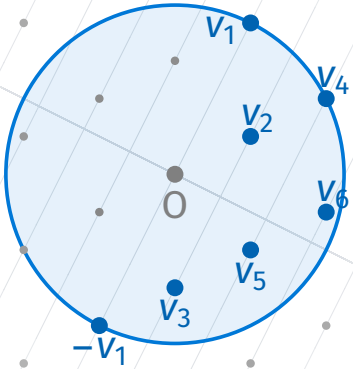
Lattice algorithms

Find short vectors for each coefficient of b_2



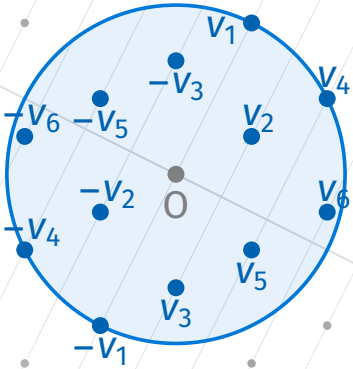
Lattice algorithms

Find short vectors for each coefficient of b_2



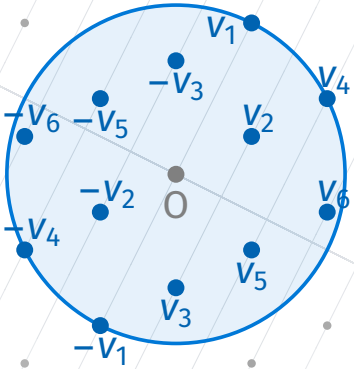
Lattice algorithms

Find short vectors for each coefficient of b_2



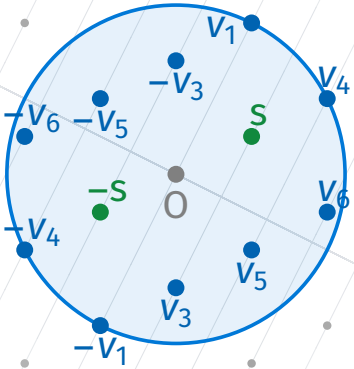
Lattice algorithms

Find a shortest vector among all found vectors



Lattice algorithms

Find a shortest vector among all found vectors



TU/e

Lattice algorithms

Lattice enumeration vs. lattice sieving

Lattice enumeration

- Brute-force all combinations of the basis vectors [FP85]
- Each coordinate $2^{O(n)}$ options $\implies$ $2^{O(n^2)}$ time complexity
- Balance preprocessing time with search time: $2^{O(n \log n)}$ time [Kan83]
- Requires almost no memory

TU/e

Lattice algorithms

Lattice enumeration vs. lattice sieving

Lattice enumeration

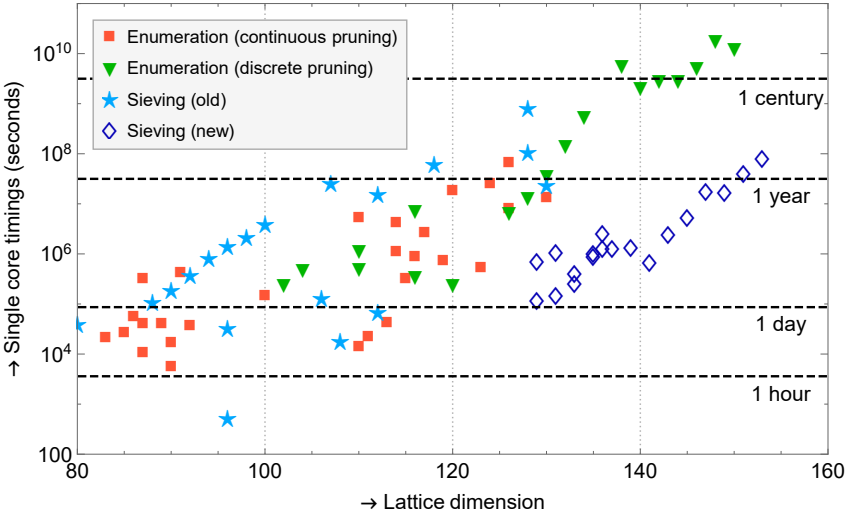
- Brute-force all combinations of the basis vectors [FP85]
- Each coordinate $2^{O(n)}$ options $\implies$ $2^{O(n^2)}$ time complexity
- Balance preprocessing time with search time: $2^{O(n \log n)}$ time [Kan83]
- Requires almost no memory

Lattice sieving

- Combine vectors in a huge list to find shorter vectors [AKS01]
- Generally requires $2^{O(n)}$ time and $2^{O(n)}$ space
- Current best asymptotics: $2^{0.292n}$ time and space [BDGL16]

Lattice algorithms

Practice [SVP]



TU/e

Lattice algorithms

Concrete estimates

Most common hardness estimates:

- Cost of finding nice basis (n) $\geq$ Cost of sieving/enumeration (β)
- Ignore space complexity, ignore $o(\beta)$ in time complexity
- Classical sieving: $2^{0.292\beta}$ time [BDGL16]
- Quantum sieving: $2^{0.265\beta}$ time [Laa16]
- "Paranoid bound": $2^{0.208\beta}$ time

Outline

TU/e

Summary

Lattice-based cryptography

- Main principle: hard to find good bases from bad bases
  - Private key: Good lattice basis
  - Public key: Bad lattice basis
- Signatures: Decode with good basis to nearby lattice point

Lattice-based cryptanalysis

- Two flavors, trading time for memory
  - Enumeration: Low memory, slower in high dimensions
  - Sieving: High memory, faster in practice
- Security estimates: solving SVP/CVP takes $\geq 2^{0.292n}$ time

TU/e

Summary

Lattice-based cryptography

- Main principle: hard to find good bases from bad bases
  - Private key: Good lattice basis
  - Public key: Bad lattice basis
- Signatures: Decode with good basis to nearby lattice point

Lattice-based cryptanalysis

- Two flavors, trading time for memory
  - Enumeration: Low memory, slower in high dimensions
  - Sieving: High memory, faster in practice
- Security estimates: solving SVP/CVP takes $\geq 2^{0.292n}$ time

Next talk: Key exchange, encryption, side-channel, attacks and more!

TU/e

References (clickable)

Lattice-based cryptography

- General: [MG02], [MR09], [Mic16], [Pei16], [NIST]
- Signatures: [GGH97], [NR06], [DN12]
- NTRU: [HPS98], [HHPW10], [SS11], [BCLV17]
- LWE: [Reg05], [Reg10], [BCD+16]
- Ring-LWE: [SSTX09], [LPR10], [LPR13]
- (Ring-)LWR: [BPR13], [AKPW13], [AKRV17], [BBF+17]

Lattice-based cryptanalysis

- General: [MG02], [MR09], [HPS11], [Mic16], [ACD+18], [SVP]
- Enumeration: [FP85], [Kan83], [GNR10], [AN17], [ANS18]
- Sieving: [AKS01], [LMP15], [BDGL16], [Laa16], [Duc18], [ADH+19]
- Basis reduction: [LLL82], [SE94], [CN11]