Lattice-based crypto, part 2:
Protocols and structured lattices

Alice Pellet--Mary

CNRS and university of Bordeaux, France

Summer school in post-quantum cryptography 2022

1-5 August 2022, Budapest

Plan of the talks

Cryptographic primitives

public key encryption

signatures

Cryptographic problems based on lattices

Ring-LWE

LWE

NTRU

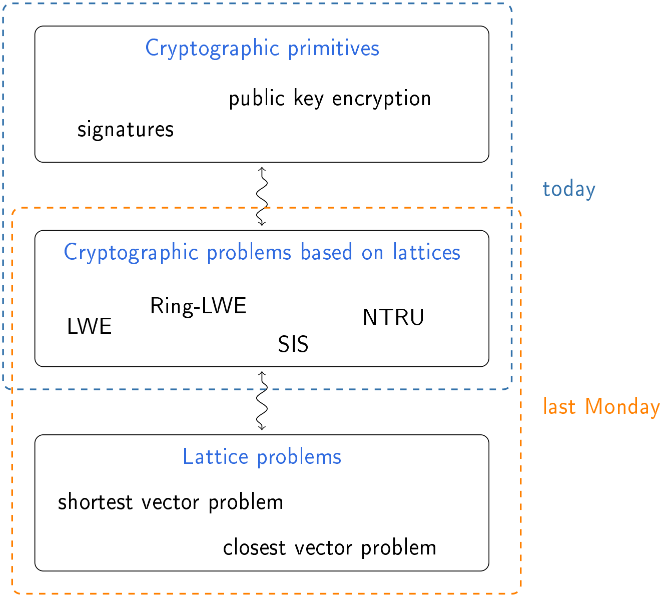
SIS

Lattice problems

shortest vector problem

closest vector problem

Plan of the talks



Outline of the talk

1. Public Key encryption from LWE
2. Trapdoors and signatures
3. Structured lattices

Reminder

What we have seen: LWE and SIS problems

- average case problems
- expressed using simple linear algebra
- best known algorithm takes time $2^{\Omega(n)}$ (if well chosen parameters)
  - even quantumly
  - e.g., $q = \mathrm{poly}(n)$ and $B = \Theta(n)$
- practical hardness quite well understood

Disclaimer

Monday we have seen:

- that LWE/SIS is as hard as worst-case lattice problems
  (i.e., if we can solve LWE/SIS with good proba, we can solve some lattice problem over all lattices)

Disclaimer

Monday we have seen:

- that LWE/SIS is as hard as worst-case lattice problems
  (i.e., if we can solve LWE/SIS with good proba, we can solve some lattice problem over all lattices)

Today we will see:

- cryptographic schemes based on LWE and SIS

Disclaimer

Monday we have seen:

- that LWE/SIS is as hard as worst-case lattice problems
  (i.e., if we can solve LWE/SIS with good proba, we can solve some lattice problem over all lattices)

Today we will see:

- cryptographic schemes based on LWE and SIS

But...

- for practical constructions, we choose parameters for which the reductions to worst-case problem do not hold
  - e.g., binary noise, small modulus q, ...

Disclaimer

Monday we have seen:

- that LWE/SIS is as hard as worst-case lattice problems
  (i.e., if we can solve LWE/SIS with good proba, we can solve some lattice problem over all lattices)

Today we will see:

- cryptographic schemes based on LWE and SIS

But...

- for practical constructions, we choose parameters for which the reductions to worst-case problem do not hold
  - e.g., binary noise, small modulus q, ...
- reductions are used to show that there is no fundamental flaw in the design
  - taking larger parameters, we can prove that the schemes are as secure as worst case lattice problems

Outline of the talk

1. Public Key encryption from LWE

2. Trapdoors and signatures

3. Structured lattices

Decision-LWE

χ_B: distribution over $\{-B, \cdots, B\}$

Reminder: decision-LWE

Sample $A \leftarrow \mathrm{Uniform}(\mathbb{Z}_q^{n \times m})$ and s, $e \leftarrow \chi_B^n \times \chi_B^m$

Given A and b, where

$$b := A s + e \bmod q \quad \text{or} \quad b \leftarrow \mathrm{Uniform}(\mathbb{Z}_q^n)$$

Guess whether b is uniform or not.

Decision-LWE

χ_B: distribution over $\{-B, \cdots, B\}$

Reminder: decision-LWE

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

Given $\boxed{A}$ and $\boxed{b}$, where

$$\boxed{b} := \boxed{A}\,\boxed{s} + \boxed{e} \bmod q \quad \text{or} \quad \boxed{b} \leftarrow \text{Uniform}(\mathbb{Z}_q^n)$$

Guess whether $\boxed{b}$ is uniform or not.

- assumed to be hard even with a quantum computer
  (for well chosen parameters)

LWE-based encryption scheme [LP11]

Parameters: $n, q \in \mathbb{Z}_{>0}$ and χ_B distribution over $\{-B, \cdots, B\}$

[LP11] Lindner and Peikert. Better key sizes (and attacks) for LWE-based encryption. CT-RSA.

LWE-based encryption scheme [LP11]

Parameters: $n, q \in \mathbb{Z}_{>0}$ and χ_B distribution over $\{-B, \cdots, B\}$

KeyGen: Sample $\boxed{A} \leftarrow \text{Uniform}(\mathbb{Z}_q^{n \times n})$ and $\boxed{s}, \boxed{e} \leftarrow \chi_B^n$

Return $pk = (\boxed{A}, \boxed{b} = \boxed{A}\boxed{s} + \boxed{e} \bmod q)$ and $sk = \boxed{s}$

[LP11] Lindner and Peikert. Better key sizes (and attacks) for LWE-based encryption. CT-RSA.

LWE-based encryption scheme [LP11]

Parameters: $n, q \in \mathbb{Z}_{>0}$ and χ_B distribution over $\{-B, \cdots, B\}$

KeyGen: Sample $A \leftarrow \mathrm{Uniform}(\mathbb{Z}_q^{n\times n})$ and s, $e \leftarrow \chi_B^n$

Return $pk = (A, b = A s + e \bmod q)$ and $sk = s$

Encrypt: message $m \in \{0, 1\}$

sample $\tilde{s}^T, \tilde{e}^T \leftarrow \chi_B^n$ and $e' \leftarrow \chi_B$

return $c = (\tilde{s}^T A + \tilde{e}^T, \tilde{s}^T b + e' + m \cdot \lfloor q/2 \rceil)$

(all mod q)

[LP11] Lindner and Peikert. Better key sizes (and attacks) for LWE-based encryption. CT-RSA.

LWE-based encryption scheme [LP11]

Parameters: $n, q \in \mathbb{Z}_{>0}$ and χ_B distribution over $\{-B, \cdots, B\}$

KeyGen: Sample $A \leftarrow \text{Uniform}(\mathbb{Z}_q^{n\times n})$ and s, $e \leftarrow \chi_B^n$

Return $pk = (A, b = A s + e \bmod q)$ and $sk = s$

Encrypt: message $m \in \{0,1\}$

sample $\tilde{s}^T, \tilde{e}^T \leftarrow \chi_B^n$ and $e' \leftarrow \chi_B$

return $c = (\tilde{s}^T A + \tilde{e}^T, \tilde{s}^T b + e' + m \cdot \lfloor q/2 \rceil)$

(all mod q)

Decrypt: $c = (c_1{}^T, c_2)$

compute $x = c_1{}^T s - c_2 \bmod q$ ($x \in [0, q]$)

return 1 if x is in $[q/4, 3q/4]$ and 0 otherwise

[LP11] Lindner and Peikert. Better key sizes (and attacks) for LWE-based encryption. CT-RSA.

Correctness

Theorem

If $q \geq 8 \cdot n \cdot B^2 + 4 \cdot B$, then the scheme is correct.

Correctness: for any message m and any $(pk, sk) \leftarrow KeyGen$, it holds that

$$\mathrm{Dec}(sk, \mathrm{Enc}(pk, m)) = m.$$

Correctness

Theorem

If $q \geq 8 \cdot n \cdot B^2 + 4 \cdot B$, then the scheme is correct.

Correctness: for any message m and any $(pk, sk) \leftarrow KeyGen$, it holds that

$$\mathrm{Dec}(sk, \mathrm{Enc}(pk, m)) = m.$$

Proof: on the board

Correctness

Theorem

If $q \geq 8 \cdot n \cdot B^2 + 4 \cdot B$, then the scheme is correct.

Correctness: for any message m and any $(pk, sk) \leftarrow KeyGen$, it holds that

$$\mathrm{Dec}(sk, \mathrm{Enc}(pk, m)) = m.$$

Proof: on the board

Decryption failures: if χ_B is a Gaussian distribution, the scheme might fail with very small probability (χ_B might output something $\geq B$)

Security: high level

Public information:

$\boxed{A}$

$\boxed{b} = \boxed{A}\boxed{s} + \boxed{e}$

$\boxed{c_1{}^T} = \boxed{\tilde{s}^T}\boxed{A} + \boxed{\tilde{e}^T}$

$\boxed{c_2} = \boxed{\tilde{s}^T}\boxed{b} + \boxed{e'} + m \cdot \lfloor q/2 \rceil$

Security: high level

Public information:

$\boxed{A}$

$\boxed{b} = \boxed{A}\boxed{s} + \boxed{e}$

$\boxed{c_1{}^T} = \boxed{\tilde{s}^T}\boxed{A} + \boxed{\tilde{e}^T}$

$\boxed{c_2} = \boxed{\tilde{s}^T}\boxed{b} + \boxed{e'} + m \cdot \lfloor q/2 \rceil$

Decision-LWE: $\boxed{b} \approx \boxed{b}$

Security: high level

Public information:

$$\boxed{A}$$

$$\boxed{b} = \boxed{A}\boxed{s} + \boxed{e}$$

$$\boxed{{c_1}^T} = \boxed{\tilde{s}^T}\boxed{A} + \boxed{\tilde{e}^T}$$

$$\boxed{c_2} = \boxed{\tilde{s}^T}\boxed{b} + \boxed{e'} + m \cdot \lfloor q/2 \rceil$$

Decision-LWE: $\boxed{b} \approx \boxed{b}$

Security: high level

Public information:

$\boxed{A}$

$\boxed{b} = \boxed{A}\boxed{s} + \boxed{e}$

$\boxed{c_1{}^T} = \boxed{\tilde{s}^T}\boxed{A} + \boxed{\tilde{e}^T}$

$\boxed{c_2} = \boxed{\tilde{s}^T}\boxed{b} + \boxed{e'} + m \cdot \lfloor q/2 \rceil$

Decision-LWE: $\boxed{b} \approx \boxed{b}$

Decision-LWE:

$\boxed{\tilde{s}^T}\boxed{A \mid b} + \boxed{\tilde{e}^T \mid e'} \approx \boxed{c_1{}^T \mid c}$

Security: high level

Public information:

$\boxed{A}$

$\boxed{b} = \boxed{A}\boxed{s} + \boxed{e}$

$\boxed{{c_1}^T} = \boxed{\tilde{s}^T}\boxed{A} + \boxed{\tilde{e}^T}$

$\boxed{c_2} = \boxed{c} + m \cdot \lfloor q/2 \rceil$

Decision-LWE: $\boxed{b} \approx \boxed{b}$

Decision-LWE:

$\boxed{\tilde{s}^T}\boxed{A \mid b} + \boxed{\tilde{e}^T \mid e'} \approx \boxed{{c_1}^T \mid c}$

Outline of the talk

1. Public Key encryption from LWE
2. Trapdoors and signatures
3. Structured lattices

Trapdoors

Two (related) notions of trapdoors for lattices:

- short basis of $\mathcal{L}$
- gadget-based

Trapdoors

Two (related) notions of trapdoors for lattices:

- short basis of $\mathcal{L}$
- gadget-based

Short basis

Idea: construct a lattice $\mathcal{L}$ with a good basis B_0 and a bad basis B_1

- given B_1, CVP is hard
- given B_0, CVP is easy

[Ajt99] Ajtai. Generating hard instances of the short basis problem. ICALP.

Short basis

Idea: construct a lattice $\mathcal{L}$ with a good basis B_0 and a bad basis B_1

- given B_1, CVP is hard
- given B_0, CVP is easy

Lemma [Ajt99]

One can efficiently create a uniform SIS lattice $\mathcal{L}$ together with a short basis of it.

[Ajt99] Ajtai. Generating hard instances of the short basis problem. ICALP.

Short basis

Idea: construct a lattice $\mathcal{L}$ with a good basis B_0 and a bad basis B_1

- given B_1, CVP is hard
- given B_0, CVP is easy

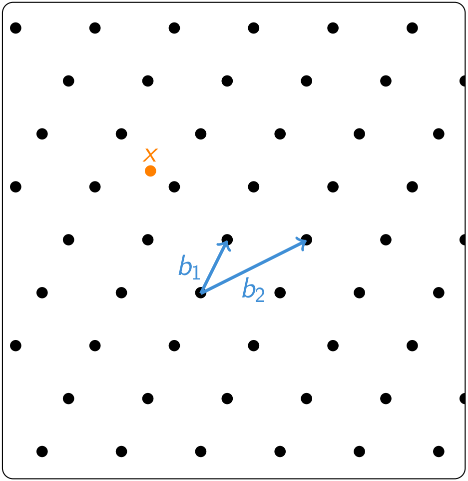
Lemma [Ajt99]

One can efficiently create a uniform SIS lattice $\mathcal{L}$ together with a short basis of it.

- CVP in $\mathcal{L}$ is hard if SIS is hard (if $\mathcal{L}$ represented by its HNF)
- the short basis enables to solve CVP efficiently

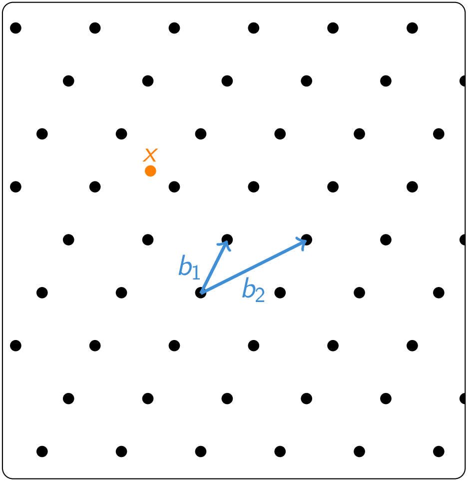
[Ajt99] Ajtai. Generating hard instances of the short basis problem. ICALP.

Solving CVP with a short basis



Input: $x = 3.7 \cdot b_1 - 1.4 \cdot b_2$

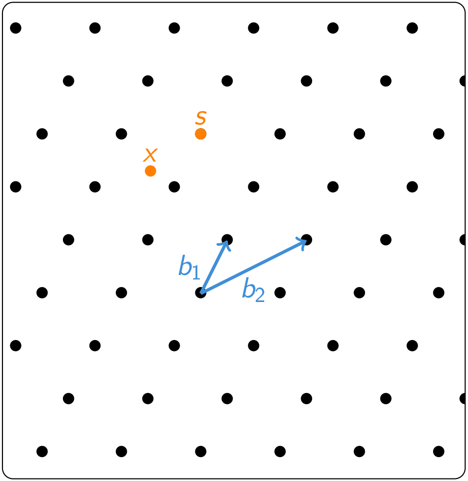
Solving CVP with a short basis



Input: $x = 3.7 \cdot b_1 - 1.4 \cdot b_2$

Algo: round each coordinate

Solving CVP with a short basis

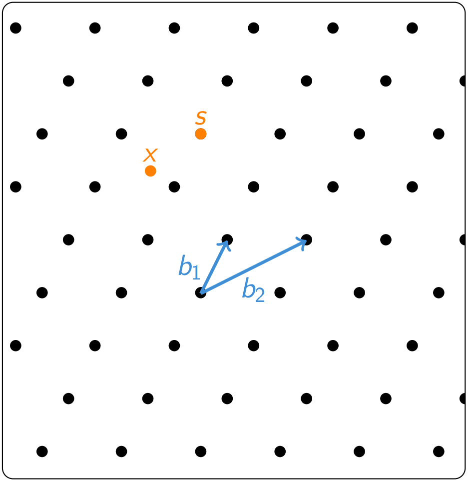


Input: $x = 3.7 \cdot b_1 - 1.4 \cdot b_2$

Algo: round each coordinate

Output: $s = 4 \cdot b_1 - 1 \cdot b_2$

Solving CVP with a short basis



Input: $x = 3.7 \cdot b_1 - 1.4 \cdot b_2$

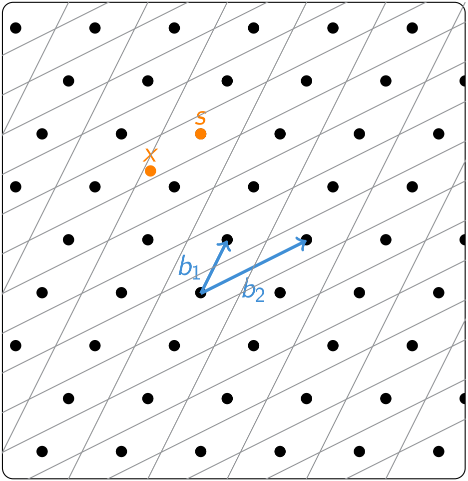
Algo: round each coordinate

Output: $s = 4 \cdot b_1 - 1 \cdot b_2$

The smaller the basis, the closer the solution

(called Babai's round-off algorithm)

Solving CVP with a short basis



Input: $x = 3.7 \cdot b_1 - 1.4 \cdot b_2$

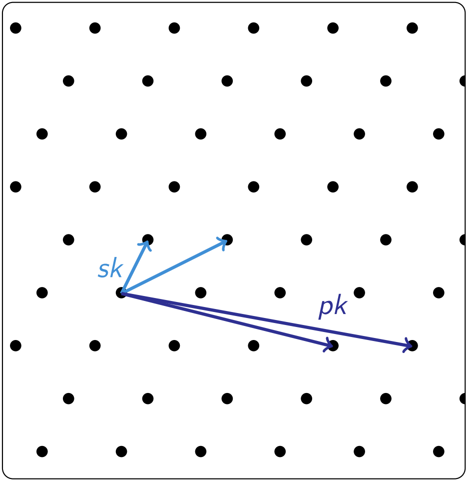
Algo: round each coordinate

Output: $s = 4 \cdot b_1 - 1 \cdot b_2$

The smaller the basis, the closer the solution

(called Babai's round-off algorithm)

Signing with a trapdoor (hash-and-sign) [GGH97]

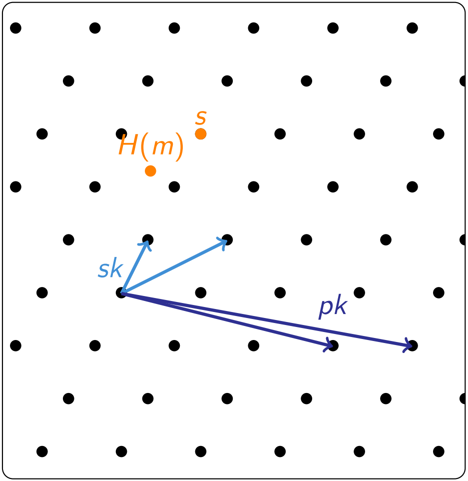


KeyGen:

- pk = bad basis of $\mathcal{L}$
- sk = short basis of $\mathcal{L}$

[GGH97] Goldreich, Goldwasser, and Halevi. Public-key cryptosystems from lattice reduction problems. CRYPTO

Signing with a trapdoor (hash-and-sign) [GGH97]



KeyGen:

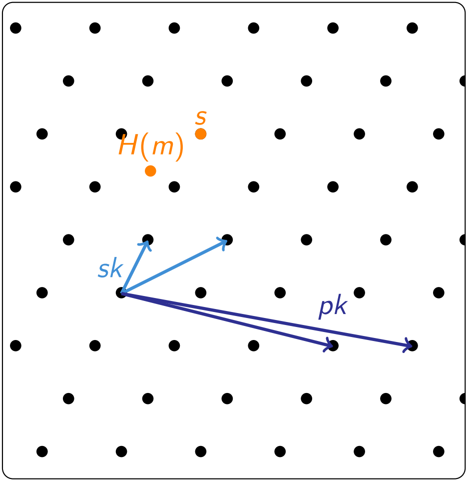
- pk = bad basis of $\mathcal{L}$
- sk = short basis of $\mathcal{L}$

Sign(m, sk):

- $x = H(m)$ (hash the message)
- output $s \in \mathcal{L}$ close to x

[GGH97] Goldreich, Goldwasser, and Halevi. Public-key cryptosystems from lattice reduction problems. CRYPTO

Signing with a trapdoor (hash-and-sign) [GGH97]



KeyGen:

- pk = bad basis of $\mathcal{L}$
- sk = short basis of $\mathcal{L}$

Sign(m, sk):

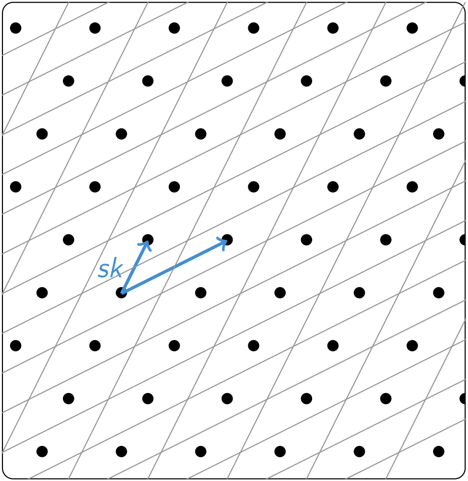
- $x = H(m)$ (hash the message)
- output $s \in \mathcal{L}$ close to x

Verify(s, pk):

- check that $s \in \mathcal{L}$
- check that $H(m) - s$ is small

[GGH97] Goldreich, Goldwasser, and Halevi. Public-key cryptosystems from lattice reduction problems. CRYPTO

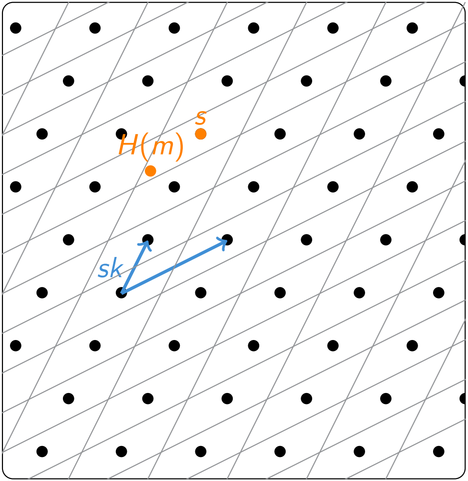
Attack on the signature scheme [NR06]



Parallelepiped attack:

[NR06] Nguyen and Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. J. Cryptology

Attack on the signature scheme [NR06]

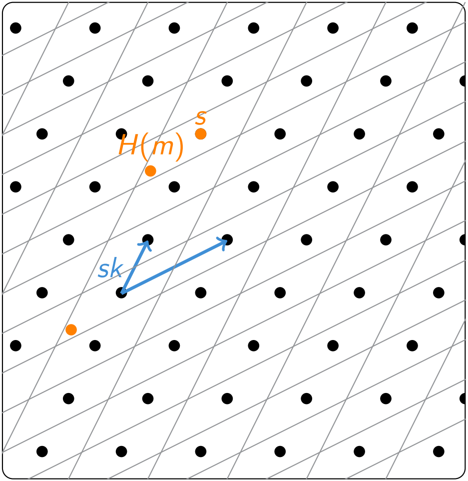


Parallelepiped attack:

- ask for a signature s on m

[NR06] Nguyen and Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. J. Cryptology

Attack on the signature scheme [NR06]

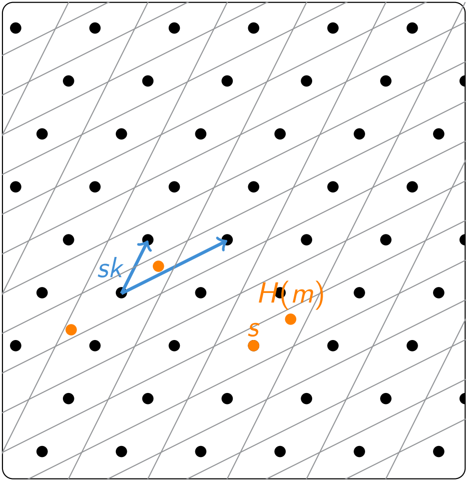


Parallelepiped attack:

- ask for a signature s on m
- plot $H(m) - s$

[NR06] Nguyen and Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. J. Cryptology

Attack on the signature scheme [NR06]

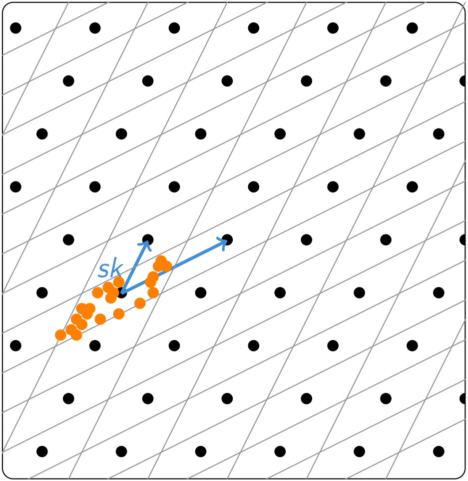


Parallelepiped attack:

- ask for a signature s on m
- plot $H(m) - s$
- repeat

[NR06] Nguyen and Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. J. Cryptology

Attack on the signature scheme [NR06]

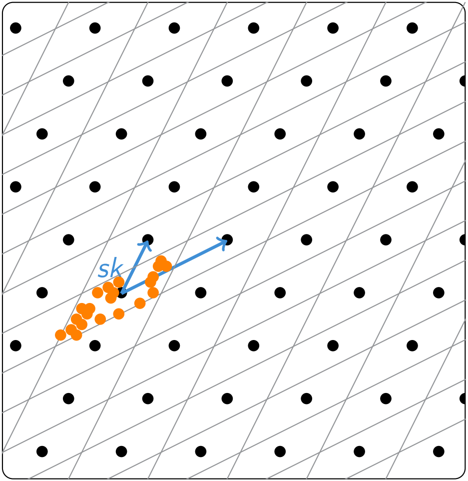


Parallelepiped attack:

- ask for a signature s on m
- plot $H(m) - s$
- repeat

[NR06] Nguyen and Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. J. Cryptology

Attack on the signature scheme [NR06]



Parallelepiped attack:

- ask for a signature s on m
- plot $H(m) - s$
- repeat

From the shape of the parallelepiped, one can recover the short basis

[NR06] Nguyen and Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. J. Cryptology

Preventing the attack [GPV08]

Idea: do not solve CVP deterministically but randomly

[GPV08] Gentry, Peikert, and Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. STOC

Preventing the attack [GPV08]

Idea: do not solve CVP deterministically but randomly

- using the short basis one can sample s from a Gaussian distribution
  - s is still in $\mathcal{L}$
  - centered in $H(m) \Rightarrow s$ close to $H(m)$
- the distribution of $H(m) - s$ becomes independent of sk

[GPV08] Gentry, Peikert, and Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. STOC

Preventing the attack [GPV08]

Idea: do not solve CVP deterministically but randomly

- using the short basis one can sample s from a Gaussian distribution
  - s is still in $\mathcal{L}$
  - centered in $H(m) \Rightarrow s$ close to $H(m)$
- the distribution of $H(m) - s$ becomes independent of sk

Lemma [GPV09]

Assuming that the SIS problem is hard, then the signature scheme is unforgeable under chosen-message attack.

[GPV08] Gentry, Peikert, and Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. STOC

Advanced constructions

One can construct many advanced primitives from lattices:

- (fully) homomorphic encryption
- identity based encryption
- functional encryption for linear functions
- ...

Outline of the talk

Number fields

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

Number fields

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

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

Number fields

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

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

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

Number fields

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

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

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

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

Embeddings

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

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

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

Embeddings

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

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

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

- both embeddings induce a (different) geometry on K

Embeddings

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

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

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

- both embeddings induce a (different) geometry on K

Which embedding should we choose?

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

Embeddings

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

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

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

- both embeddings induce a (different) geometry on K

Which embedding should we choose?

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

Ideals

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

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

Ideals

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

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

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

Ideals

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

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

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

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

Ideals

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

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

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

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

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

Ideal lattices

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

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

Ideal lattices

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

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

$\Sigma(\mathcal{O}_K)$ is a lattice of rank d in $\mathbb{Z}^d$ with basis $(\Sigma(X^i))_{0 \leq i < d}$

Ideal lattices

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

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

$\Sigma(\mathcal{O}_K)$ is a lattice of rank d in $\mathbb{Z}^d$ with basis $(\Sigma(X^i))_{0 \leq i < d}$

$\langle g \rangle$ is a lattice:

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

Ideal lattices

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

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

$\Sigma(\mathcal{O}_K)$ is a lattice of rank d in $\mathbb{Z}^d$ with basis $(\Sigma(X^i))_{0 \leq i < d}$

$\langle g \rangle$ is a lattice:

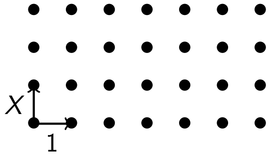
- $\langle g \rangle = g \cdot \mathcal{O}_K = g \cdot 1 \cdot \mathbb{Z} + g \cdot X \cdot \mathbb{Z} + \cdots + g \cdot X^{d-1} \cdot \mathbb{Z}$
- $\Sigma(\langle g \rangle) = \Sigma(g) \cdot \mathbb{Z} + \cdots + \Sigma(g \cdot X^{d-1}) \cdot \mathbb{Z}$

$\Sigma(\langle g \rangle)$ is a lattice of rank d in $\mathbb{Z}^d$ with basis $(\Sigma(g \cdot X^i))_{0 \leq i < d}$

(this is also true for non principal ideals)

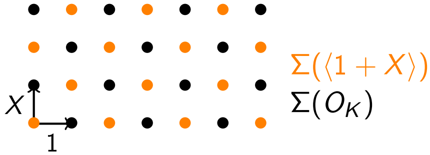
(we can replace Σ by σ and $\mathbb{Z}^d$ by $\mathbb{C}^d$)

Ideal lattices (2)

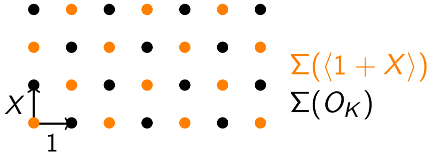


$\Sigma(O_K)$

Ideal lattices (2)

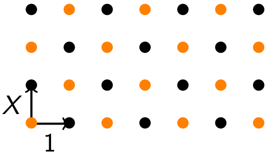


Ideal lattices (2)



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

Ideal lattices (2)



$\Sigma(\langle 1+X \rangle)$

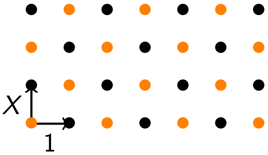
$\Sigma(O_K)$

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

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

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

Ideal lattices (2)



$\Sigma(\langle 1+X \rangle)$

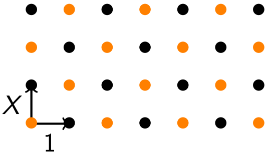
$\Sigma(O_K)$

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

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

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

Ideal lattices (2)



$\Sigma(\langle 1+X \rangle)$

$\Sigma(O_K)$

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

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

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

Module lattices

(Free) module:

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

Module lattices

(Free) module:

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

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

$\Sigma(M)$ is a lattice:

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

Module lattices

(Free) module:

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

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

$\Sigma(M)$ is a lattice:

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

Modules vs ideals

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

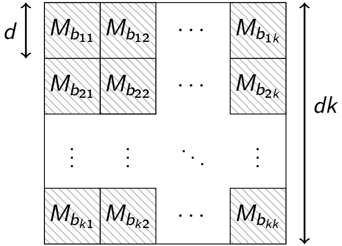
Modules vs ideals

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

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

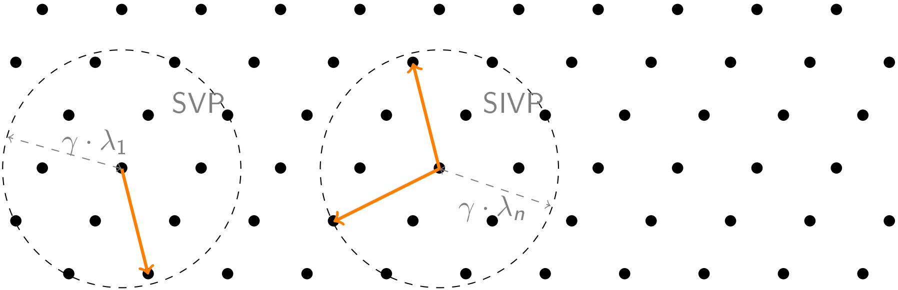
$$M_a = \begin{pmatrix} a_1 & -a_d & \cdots & -a_2 \\ a_2 & a_1 & \cdots & -a_3 \\ \vdots & \ddots & \ddots & \vdots \\ a_d & a_{d-1} & \cdots & a_1 \end{pmatrix}$$

basis of a
principal ideal lattice



basis of a free module lattice
of rank k

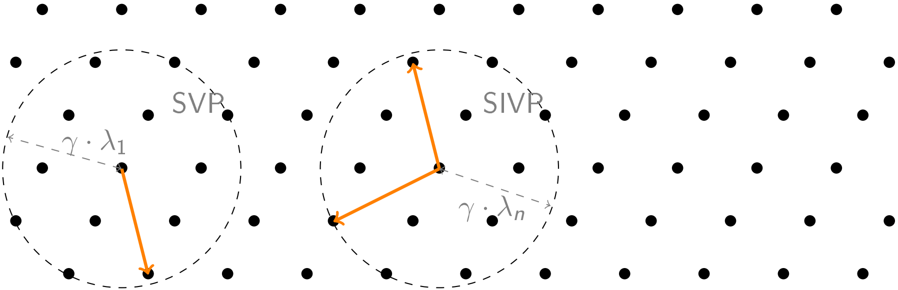
Algorithmic problems



γ-SVP
shortest vector problem

γ-SIVP
shortest independent vector problem

Algorithmic problems



γ-SVP
shortest vector problem

γ-SIVP
shortest independent vector problem

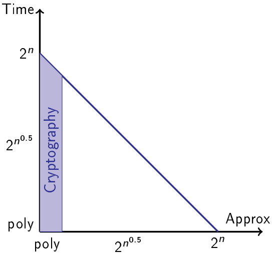
Notations:

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

(worst-case: we want algorithms for all ideal/module lattices)

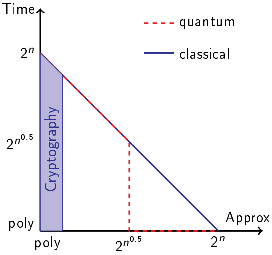
Hardness of SVP

Asymptotics:



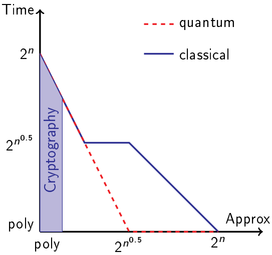
SVP and mod-SVP$_k$

($k \geq 2$)



id-SVP [CDW17]

(in cyclotomic fields)



id-SVP [PHS19,BR20]

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

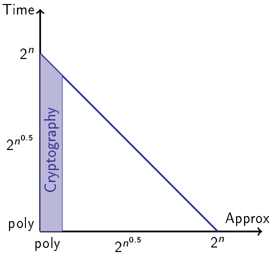
[CDW17] Cramer, Ducas, Wesolowski. Short stickelberger class relations and application to ideal-SVP. Eurocrypt.

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

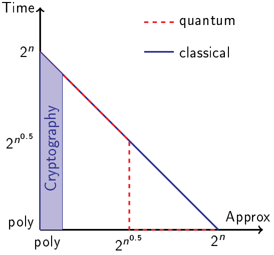
[BR20] Bernard, Roux-Langlois. Twisted-PHS: using the product formula to solve approx-SVP in ideal lattices. AC.

Hardness of SVP

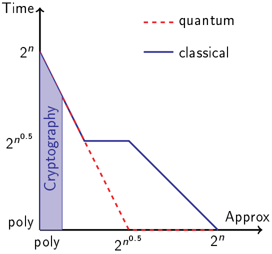
Asymptotics:



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



id-SVP [CDW17]
(in cyclotomic fields)



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

Practice: Darmstadt challenge[1]

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

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

RLWE and mod-LWE

Ring and Module-LWE

(search) mod-LWE$_k$

Parameters: q and B

Problem: Sample

- $A \leftarrow \text{Uniform}((\mathcal{O}_K/(q\mathcal{O}_K))^{m\times k})$
- $s, e \in \mathcal{O}_K^k \times \mathcal{O}_K^m$ with coefficients in $\{-B, \cdots, B\}$

Given A and $b = A \cdot s + e \bmod q$, recover s

(size of s and e can be defined using Σ or σ)

Ring and Module-LWE

(search) mod-LWE$_k$

Parameters: q and B

Problem: Sample

- $A \leftarrow \mathrm{Uniform}((\mathcal{O}_K/(q\mathcal{O}_K))^{m\times k})$
- $s, e \in \mathcal{O}_K^k \times \mathcal{O}_K^m$ with coefficients in $\{-B, \cdots, B\}$

Given A and $b = A \cdot s + e \bmod q$, recover s

(size of s and e can be defined using Σ or σ)

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

mod-LWE vs mod-SIVP

$$\text{mod-SVP}_m \quad \geq \quad \text{mod-LWE}_k \quad \geq \quad \text{mod-SIVP}_k$$

quantumly!

mod-LWE vs mod-SIVP

$$\text{mod-SVP}_m \quad \geq \quad \text{mod-LWE}_k \quad \geq \quad \text{mod-SIVP}_k$$

quantumly!

How large should m be?

- as small as possible
- but so that the closest point to b is As

mod-LWE vs mod-SIVP

$$\text{mod-SVP}_m \quad \geq \quad \text{mod-LWE}_k \quad \underset{\text{quantumly!}}{\geq} \quad \text{mod-SIVP}_k$$

How large should m be?

- as small as possible
- but so that the closest point to b is As
- $m = k$ is not sufficient

mod-LWE vs mod-SIVP

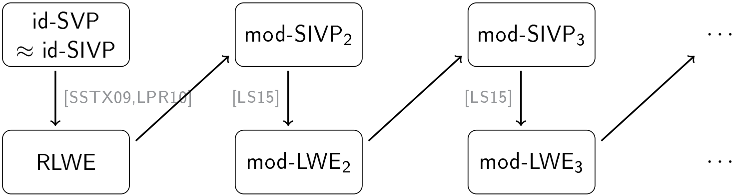
$$\text{mod-SVP}_m \quad \geq \quad \text{mod-LWE}_k \quad \geq \quad \text{mod-SIVP}_k$$

quantumly!

How large should m be?

- as small as possible
- but so that the closest point to b is As
- $m = k$ is not sufficient
- $m = k + 1$ might be sufficient depending on B and q
  - we need roughly $m = k \cdot \frac{\log(q)}{\log(q/B)}$
  - for $k = 1$, $m = 2$ is possible if $B \lesssim \sqrt{q}$

Reductions



⚠ Arrows may not all compose (different parameters) ⚠

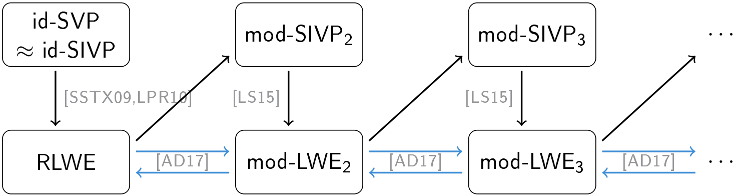
- References are for the first reductions. Better, more recent reductions may exist.
- reductions may be quantum
- reductions hold for σ and Gaussian noise

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

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

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

Reductions

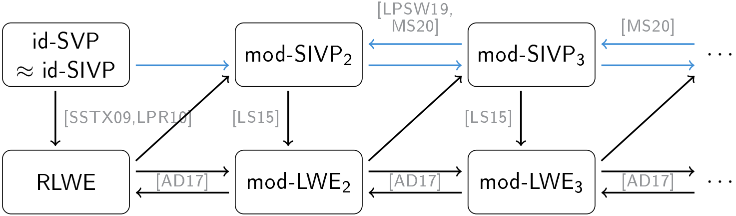


⚠ Arrows may not all compose (different parameters) ⚠

- References are for the first reductions. Better, more recent reductions may exist.
- reductions may be quantum
- reductions hold for σ and Gaussian noise

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

Reductions



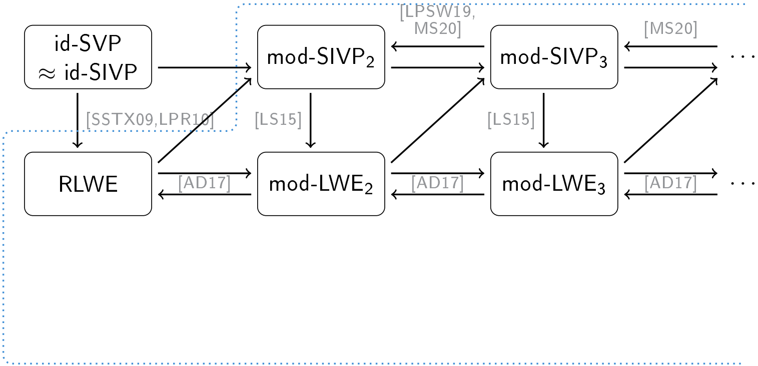
⚠ Arrows may not all compose (different parameters) ⚠

- References are for the first reductions. Better, more recent reductions may exist.
- reductions may be quantum
- reductions hold for σ and Gaussian noise

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

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

Reductions



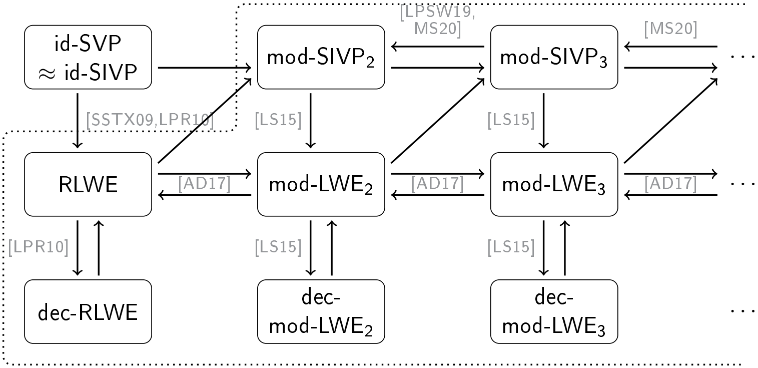
⚠ Arrows may not all compose (different parameters) ⚠

- References are for the first reductions. Better, more recent reductions may exist.
- reductions may be quantum
- reductions hold for σ and Gaussian noise

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

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

Reductions



⚠ Arrows may not all compose (different parameters) ⚠

- References are for the first reductions. Better, more recent reductions may exist.
- reductions may be quantum
- reductions hold for σ and Gaussian noise

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

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

NTRU

NTRU [HPS98]

(search) NTRU

Parameters: $q \geq B > 1$

Objective: Sample $f, g \in \mathcal{O}_K$ with coefficients in $\{-B, \cdots, B\}$.
Given $h = f \cdot g^{-1}$, recover (f, g)

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

NTRU [HPS98]

(search) NTRU

Parameters: $q \geq B > 1$

Objective: Sample $f, g \in \mathcal{O}_K$ with coefficients in $\{-B, \cdots, B\}$.
Given $h = f \cdot g^{-1}$, recover (f, g)

dec-NTRU

Parameters: q, B

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

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

NTRU [HPS98]

(search) NTRU

Parameters: $q \geq B > 1$

Objective: Sample $f, g \in \mathcal{O}_K$ with coefficients in $\{-B, \cdots, B\}$.
Given $h = f \cdot g^{-1}$, recover (f, g)

dec-NTRU

Parameters: q, B

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

Exercise: why is it unsafe to take $h = f$ or $h = g^{-1} \bmod q$?

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

NTRU [HPS98]

(search) NTRU

Parameters: $q \geq B > 1$

Objective: Sample $f, g \in \mathcal{O}_K$ with coefficients in $\{-B, \cdots, B\}$.
Given $h = f \cdot g^{-1}$, recover (f, g)

dec-NTRU

Parameters: q, B

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

Exercise: why is it unsafe to take $h = f$ or $h = g^{-1} \bmod q$?

- f is small, easy to distinguish from Uniform$(\mathcal{O}_K/(q\mathcal{O}_K))$ (which is likely $\approx q$)
- if $h = g^{-1}$, one can compute $h^{-1} = g \bmod q$ and same situation as above

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

Two regimes of NTRU

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

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

Two regimes of NTRU

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

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

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

[SS11] Stehlé and Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. Eurocrypt.
[WW18] Wang and Wang. Provably secure NTRUEncrypt over any cyclotomic field. SAC.

Two regimes of NTRU

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

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

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

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

[SS11] Stehlé and Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. Eurocrypt.
[WW18] Wang and Wang. Provably secure NTRUEncrypt over any cyclotomic field. SAC.

Two regimes of NTRU

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

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

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

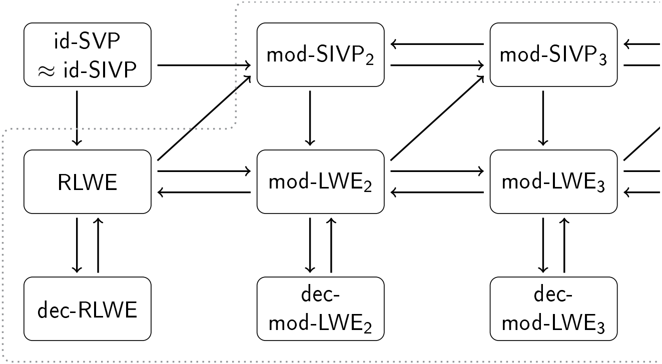
- h is not statistically close to uniform mod q
- NTRU is a special case of unique-SVP

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

[SS11] Stehlé and Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. Eurocrypt.

[WW18] Wang and Wang. Provably secure NTRUEncrypt over any cyclotomic field. SAC.

Reductions

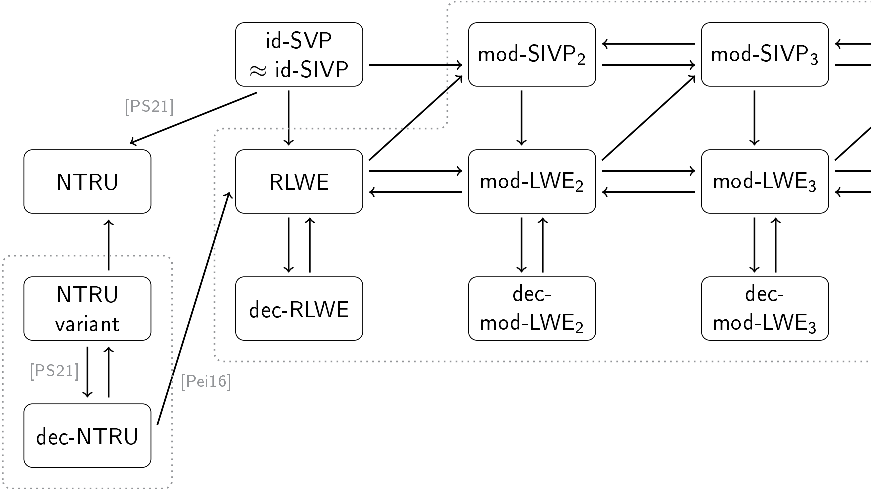


⚠ Arrows may not all compose (different parameters) ⚠

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

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

Reductions

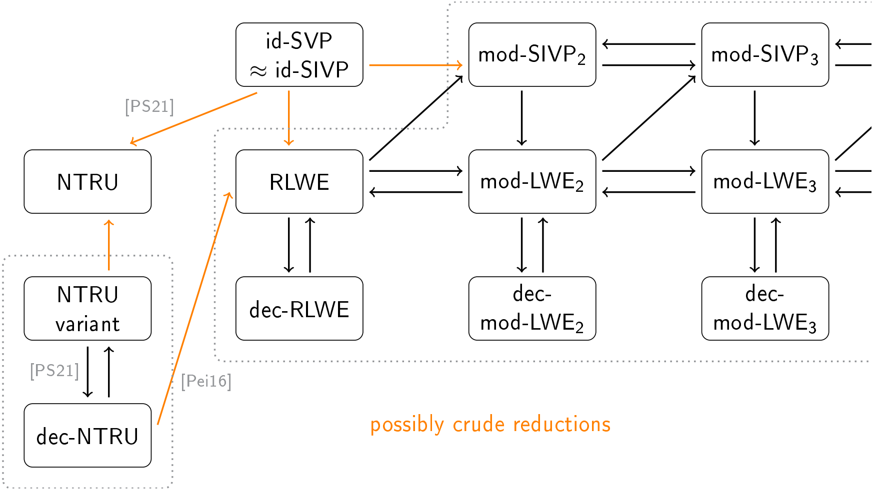


⚠ Arrows may not all compose (different parameters) ⚠

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

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

Reductions



⚠ Arrows may not all compose (different parameters) ⚠

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

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

Take-away from this section

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

Take-away from this section

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

Breaking id-SVP does not break:

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

Take-away from this section

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

Breaking id-SVP does not break:

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

Breaking id-SVP do break:

- some early FHE schemes
- the PV-Knap problem [HPS+14,BSS22]

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

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

Conclusion

Conclusion on lattice-based crypto

Advantages:

- many reductions (worst-case to average-case, search to decision, ...)
  - some parameters might still be broken
  - bug gives confidence that there are no major flaws in the problems

Conclusion on lattice-based crypto

Advantages:

- many reductions (worst-case to average-case, search to decision, ...)
  - some parameters might still be broken
  - bug gives confidence that there are no major flaws in the problems
- complexity of the best algorithms is quite well understood
  - LWE estimator: `https://github.com/malb/lattice-estimator`

Conclusion on lattice-based crypto

Advantages:

- many reductions (worst-case to average-case, search to decision, ...)
  - some parameters might still be broken
  - bug gives confidence that there are no major flaws in the problems
- complexity of the best algorithms is quite well understood
  - LWE estimator: `https://github.com/malb/lattice-estimator`
- quite efficient if using structured lattices

Conclusion on lattice-based crypto

Advantages:

- many reductions (worst-case to average-case, search to decision, . . .)
  - some parameters might still be broken
  - bug gives confidence that there are no major flaws in the problems
- complexity of the best algorithms is quite well understood
  - LWE estimator: `https://github.com/malb/lattice-estimator`
- quite efficient if using structured lattices
- can be used in many constructions

Conclusion on lattice-based crypto

Advantages:

- many reductions (worst-case to average-case, search to decision, ...)
  - some parameters might still be broken
  - bug gives confidence that there are no major flaws in the problems
- complexity of the best algorithms is quite well understood
  - LWE estimator: `https://github.com/malb/lattice-estimator`
- quite efficient if using structured lattices
- can be used in many constructions

Drawbacks:

- big keysizes and ciphertexts/signatures

Conclusion on lattice-based crypto

Advantages:

- many reductions (worst-case to average-case, search to decision, ...)
  - some parameters might still be broken
  - bug gives confidence that there are no major flaws in the problems
- complexity of the best algorithms is quite well understood
  - LWE estimator: `https://github.com/malb/lattice-estimator`
- quite efficient if using structured lattices
- can be used in many constructions

Drawbacks:

- big keysizes and ciphertexts/signatures
- structured lattice problems are still young
  - more cryptanalysis is needed

Conclusion on lattice-based crypto

Advantages:

- many reductions (worst-case to average-case, search to decision, . . .)
  - some parameters might still be broken
  - bug gives confidence that there are no major flaws in the problems
- complexity of the best algorithms is quite well understood
  - LWE estimator: `https://github.com/malb/lattice-estimator`
- quite efficient if using structured lattices
- can be used in many constructions

Drawbacks:

- big keysizes and ciphertexts/signatures
- structured lattice problems are still young
  - more cryptanalysis is needed

Thank you