On the Ring-LWE and Polynomial-LWE problems

Miruna Roșca, Damien Stehlé, **Alexandre Wallet**

About today's talk

It's post-quantum (public-key) crypto time!

- Cryptography = building **secure** schemes
- Theoretical security = **reduction** from **hard**† **algorithmic problems**
- Classical **public-key** crypto (RSA, DLog) broken by quantum computers.

$\Rightarrow$ We need **quantum hard**† **problems**.

This talk is about:

- Lattice-based cryptography (a post-quantum assumption)
- Reductions between hard† problems related to lattices
- Theoretical stuff, but impacts the understanding of practical schemes

$\dagger$: at least conjecturally

About today's talk

It's post-quantum (public-key) crypto time!

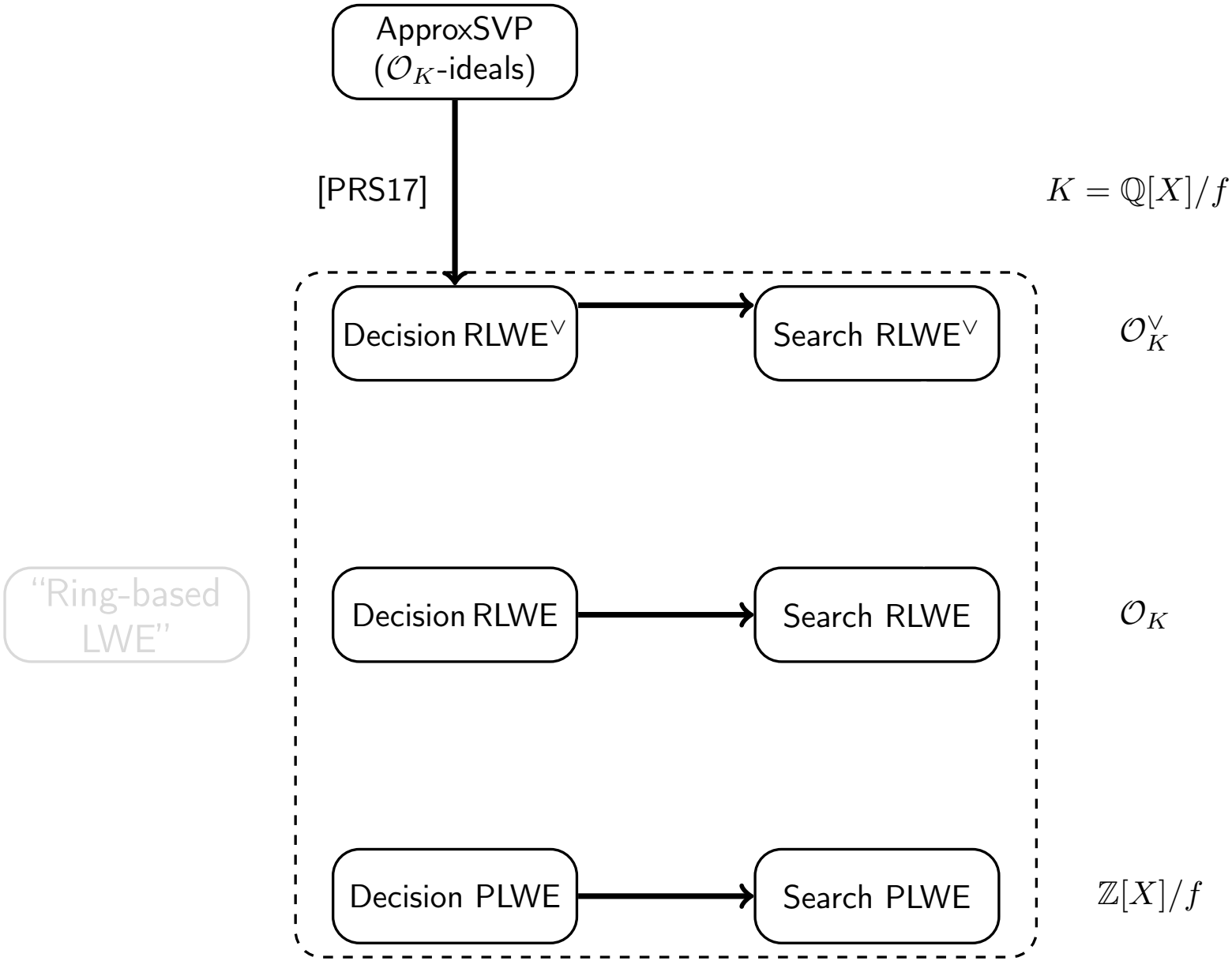
- Cryptography = building **secure** schemes
- Theoretical security = **reduction** from **hard**† **algorithmic problems**
- Classical **public-key** crypto (RSA, DLog) broken by quantum computers.

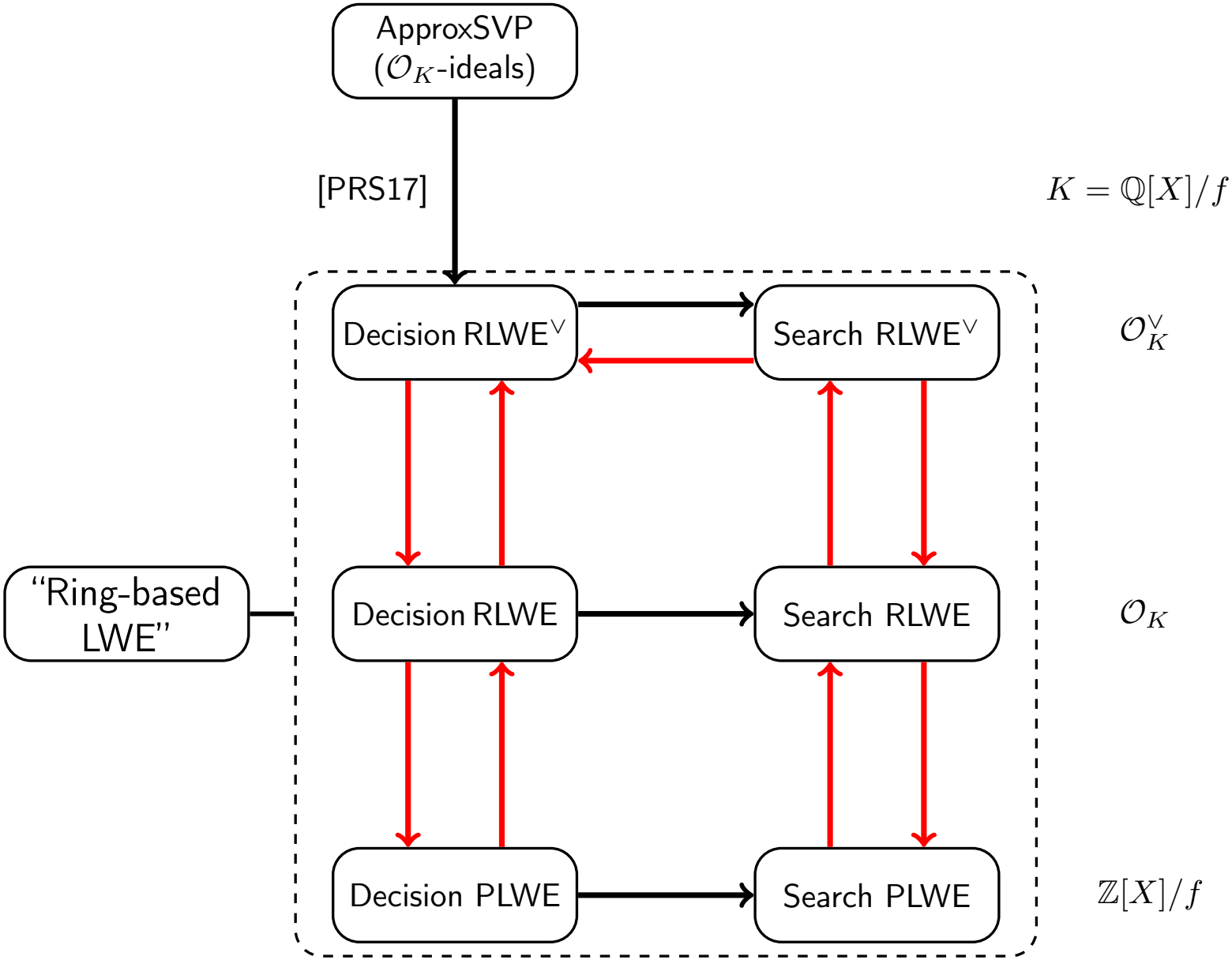
$\Rightarrow$ We need **quantum hard**† **problems**.

This talk is about:

- Lattice-based cryptography (a post-quantum assumption)
- Reductions between hard† problems related to lattices
- Theoretical stuff, but impacts the understanding of practical schemes

$\dagger$: at least conjecturally


ApproxSVP
($\mathcal{O}_K$-ideals)
[PRS17]
$K = \mathbb{Q}[X]/f$
Decision RLWE$^\vee$
Search RLWE$^\vee$
$\mathcal{O}_K^\vee$
"Ring-based LWE"
Decision RLWE
Search RLWE
$\mathcal{O}_K$
Decision PLWE
Search PLWE
$\mathbb{Z}[X]/f$


ApproxSVP
($\mathcal{O}_K$-ideals)
[PRS17]
$K = \mathbb{Q}[X]/f$
Decision RLWE$^\vee$
Search RLWE$^\vee$
$\mathcal{O}_K^\vee$
"Ring-based LWE"
Decision RLWE
Search RLWE
$\mathcal{O}_K$
Decision PLWE
Search PLWE
$\mathbb{Z}[X]/f$

"On variants of Polynomial-LWE and Ring-LWE"
(EUROCRYPT 2018)

Results:

(A) The 3 settings are essentially† the same

(B) Search = Decision in all settings.

Not described: Worst-case hardness for Polynomial-LWE.

†: for a large number of "reasonable" polynomials, up to polynomial factors on noise, assuming some information about the field are known.

1. LWE and Cryptography
   - Regev's encryption scheme
   - Learning With Errors (LWE) and its hardness
2. Ring-based LWE
3. Reductions between Ring-based LWE's
4. Search to Decision
5. Open problems

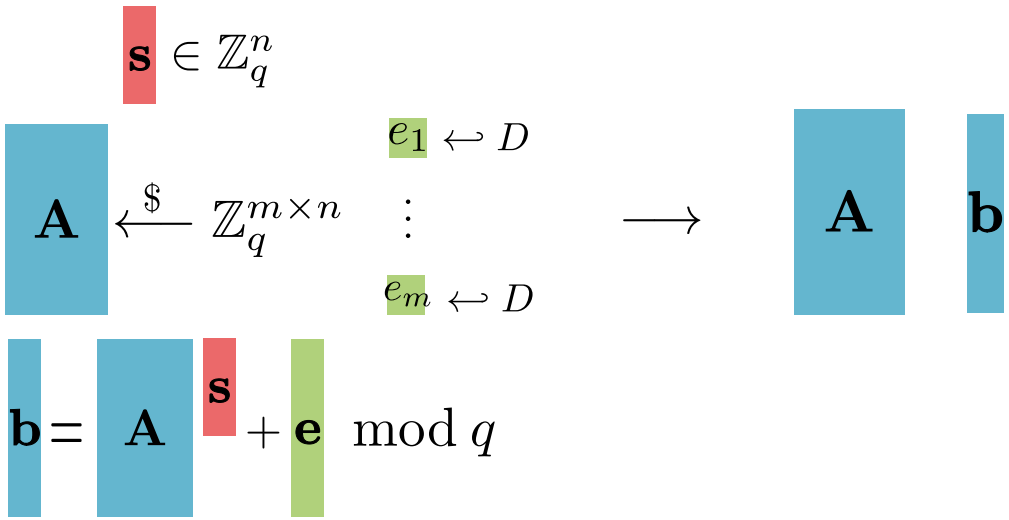
An encryption scheme [Regev'05]

n "security parameter", q prime, $n \leq m \leq poly(n)$, D distribution over $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$.

Alice

Eve

Bruno



An encryption scheme [Regev'05]

n "security parameter", q prime, $n \leq m \leq poly(n)$, D distribution over $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$.

Alice | Eve | Bruno

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

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

$e_1 \hookleftarrow D$ ⋮ $e_m \hookleftarrow D$

$\longrightarrow$ $\mathbf{A}$ $\mathbf{b}$

$\mu \in \{0,1\}$

$\mathbf{b} = \mathbf{A}\,\mathbf{s} + \mathbf{e} \bmod q$

$\mathbf{c} \xleftarrow{\$} \{0,1\}^m$

$e' = b' - \langle \mathbf{a}', \mathbf{s} \rangle \bmod q$ $\longleftarrow$ $(\mathbf{a}', b')$ $\longleftarrow$ $\mathsf{E}_{\mathbf{A},\mathbf{b}} = (\mathbf{c}^\top \mathbf{A}, \mathbf{c}^\top \mathbf{b} + \mu \lceil \frac{q}{2} \rceil)$

An encryption scheme [Regev'05]

n "security parameter", q prime, $n \leq m \leq poly(n)$, D distribution over $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$.

Alice | Eve | Bruno

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

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

$e_1 \hookleftarrow D$ ⋮ $e_m \hookleftarrow D$

$\longrightarrow$ $\mathbf{A}$ $\mathbf{b}$

$\mu \in \{0,1\}$

$\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$

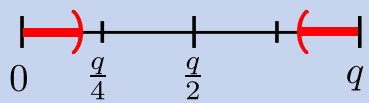
$\mathbf{c} \xleftarrow{\$} \{0,1\}^m$

$e' = b' - \langle \mathbf{a}', \mathbf{s} \rangle \bmod q$ $\longleftarrow$ $(\mathbf{a}', b')$ $\longleftarrow$ $\mathsf{E}_{\mathbf{A},\mathbf{b}} = (\mathbf{c}^\top \mathbf{A}, \mathbf{c}^\top \mathbf{b} + \mu\lceil \frac{q}{2} \rceil)$

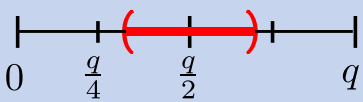
$$\mathsf{Dec}_{\mathbf{s}}(\mathbf{a}', b') = \begin{cases} 0 \text{ if } e' \sim 0 \\ 1 \text{ if } e' \sim \frac{q}{2} \end{cases}$$

Correctness: q, m, χ chosen s.t. $e' = \sum e_i \leq \frac{q}{4}$ whp.

$\mu = 0$



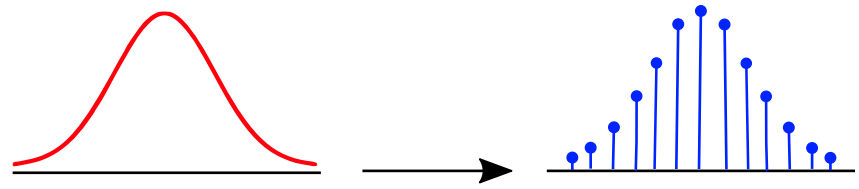
$\mu = 1$



Learning With Errors [Regev'05]

$n \in \mathbb{N}^*$, $q \leq poly(n)$ a prime
$\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$.

$D \to D_\sigma$ **discrete Gaussian distribution**



LWE distribution: Fix $\mathbf{s} \in \mathbb{Z}_q^n$.

$$A_{\mathbf{s},\sigma,q} : \begin{cases} \mathbf{a} \hookleftarrow \mathcal{U}(\mathbb{Z}_q^n) \\ e \hookleftarrow D_\sigma \\ \text{outputs } (\mathbf{a}, b = (\langle \mathbf{a}, \mathbf{s} \rangle + e) \bmod q) \end{cases}$$

Search

Given $\left(\mathbf{A}, \mathbf{b} = \mathbf{A}\,\mathbf{s} + \mathbf{e} \bmod q \right)$

Find $\mathbf{s}$

Decision

Distinguish

$\left(\mathbf{A}, \mathbf{b} \right)$ and $\left(\mathbf{A}, \mathbf{u} \right)$

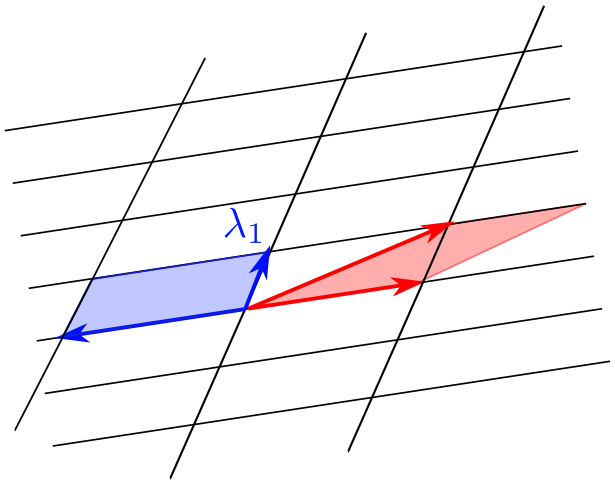
$\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^m$

LWE hardness and lattices [Regev'05]

Euclidean lattice:

$$\mathcal{L}(\mathbf{B}) := \mathbf{B} \cdot \mathbb{Z}^n = \left\{ \mathbf{B}\,\mathbf{v} \;:\; \mathbf{v} \in \mathbb{Z}^n \right\}$$

λ_1 length of a shortest (non-0) vector



ApproxSVP$_\gamma$: Given $\mathbf{B}$, compute λ_1 up to a factor γ.

For $\gamma = \text{poly}(n)$, best known algo runs in time $2^{O(n)}$ (classic, **quantum**).

break Regev's encryption $\xrightarrow{classical}$ solve **Decision-LWE** $=$ solve **Search-LWE** $\xrightarrow{quantum}$ solve **ApproxSVP**$_{\text{poly}(n)}$

Practical limitations of LWE: public data size, speed.

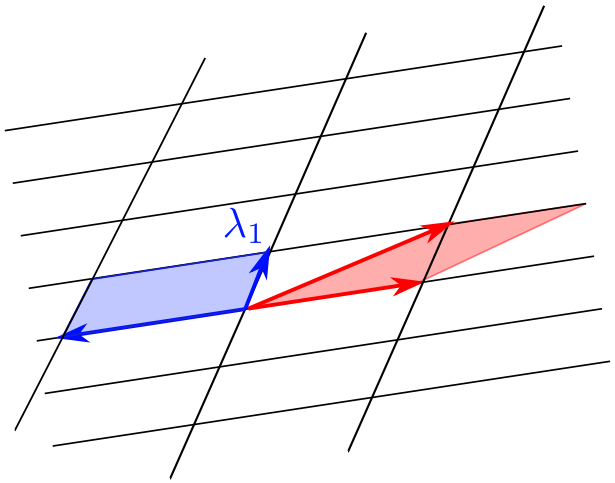
A solution: use **structured** matrices/lattices.

LWE hardness and lattices [Regev'05]

Euclidean lattice:

$$\mathcal{L}(\mathbf{B}) := \mathbf{B} \cdot \mathbb{Z}^n = \left\{ \mathbf{B}\,\mathbf{v} \;:\; \mathbf{v} \in \mathbb{Z}^n \right\}$$

λ_1 length of a shortest (non-0) vector



ApproxSVP$_\gamma$: Given $\mathbf{B}$, compute λ_1 up to a factor γ.

For $\gamma = \text{poly}(n)$, best known algo runs in time $2^{O(n)}$ (classic, **quantum**).

break Regev's encryption $\xRightarrow{classical}$ solve **Decision-LWE** $=$ solve **Search-LWE** $\xRightarrow{quantum}$ solve **ApproxSVP**$_{\text{poly}(n)}$

Practical limitations of LWE: public data size, speed.

A solution: use **structured** matrices/lattices.

1. LWE and Cryptography

2. Ring-based LWE
   - Polynomial-LWE: ideal lattices
   - Ring-LWE: more algebraic number theory

3. Reductions between Ring-based LWE's

4. Search to Decision

5. Open problems

Polynomial-LWE (PLWE) [SSTX09]

Change $\mathbb{Z}_q^n$ to $R_q := \mathbb{Z}_q[X]/f$. Good example: $f = X^n + 1$, with $n = 2^d$.

polynomials

$s = \sum s_i X^i \in R_q$

Produit: $a \cdot s \bmod f$

integer vectors/matrices

$\mathbf{s} = (s_0, \ldots, s_{n-1})^\top \in \mathbb{Z}_q^n$

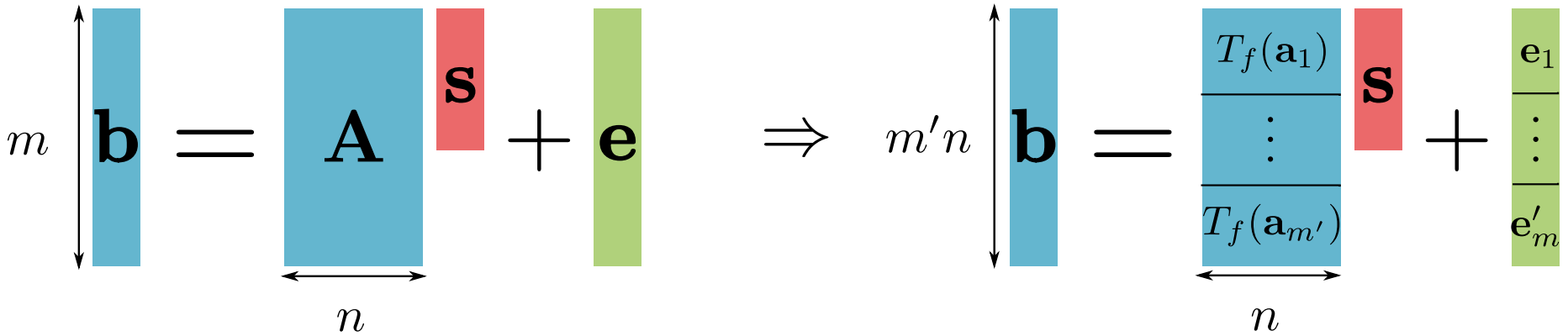
Mult. by a with **structured matrix**

$$T_f(\mathbf{a}) = \begin{bmatrix} a_0 & -a_1 & \cdots & -a_{n-1} \\ a_1 & a_0 & \cdots & -a_{n-2} \\ \vdots & & \ddots & \vdots \\ a_{n-1} & a_{n-2} & \cdots & a_0 \end{bmatrix}$$

$$\text{New Public key} = \left(\begin{array}{c} T_f(\mathbf{a}_1) \\ \hline \vdots \\ \hline T_f(\mathbf{a}_k) \end{array} , \mathbf{b} = \begin{array}{c} T_f(\mathbf{a}_1) \\ \hline \vdots \\ \hline T_f(\mathbf{a}_k) \end{array} \mathbf{s} + \begin{array}{c} \mathbf{e}_1 \\ \hline \vdots \\ \hline \mathbf{e}_k \end{array} \bmod q \right)$$

Plain LWE

Polynomial-LWE (PLWE)



1 PLWE sample = n correlated LWE samples.

PLWE and its hardness [SSTX'09]

$R = \mathbb{Z}[X]/f$
f monic, irreducible, degree n.

Σ: any pos.def.matrix
D_Σ n-dimensional **Gaussian**.

PLWE distribution: Fix $s \in R_q$

$$\mathsf{PLWE}_{q,\Sigma,f,s} : \begin{cases} a \hookleftarrow \mathcal{U}(R_q) \\ e \hookleftarrow D_\Sigma \\ \text{outputs } (a, b = (a \cdot s + e) \bmod qR) \end{cases}$$

Solve **Search-PLWE** $\Rightarrow$ solve **ApproxSVP**$_\gamma$ in **ideal lattices** for $\gamma \leq poly(n)$.

ideal lattice? Ex: $aR = \{\text{multiples of } a \text{ in } R\} \longmapsto T_f(a) \cdot \mathbb{Z}^n$

PLWE and its hardness [SSTX'09]

$R = \mathbb{Z}[X]/f$
f monic, irreducible, degree n.

Σ: any pos.def.matrix
D_Σ n-dimensional **Gaussian**.

PLWE distribution: Fix $s \in R_q$

$$\mathsf{PLWE}_{q,\Sigma,f,s} : \begin{cases} a \hookleftarrow \mathcal{U}(R_q) \\ e \hookleftarrow D_\Sigma \\ \text{outputs } (a, b = (a \cdot s + e) \bmod qR) \end{cases}$$

Solve **Search-PLWE** $\Rightarrow$ solve **ApproxSVP**$_\gamma$ in **ideal lattices** for $\gamma \leq poly(n)$.

ideal lattice? Ex: $aR = \{\text{multiples of } a \text{ in } R\} \longmapsto T_f(a) \cdot \mathbb{Z}^n$

Practice vs. Theory

Perks:

- ✓ fast and compact operations
- ✓ **post-quantum** scheme

New Hope
(NIST competitor)

Public key: ~ 2 KBytes
Handshake: ~ 0.3 ms

Theoretical limitations:

- ✗ γ depends on f's "expansion factor" $\rightarrow$ Restricts "good f's"
- ✗ Working with R relies too much on f $\rightarrow$ Lack of generality/flexibility

Number fields and rings

$R = \mathbb{Z}[X]/f$ is a **number ring**. Lives in $K = \mathbb{Q}[X]/f$, a **number field**.

Structure: $K = \mathrm{Span}_{\mathbb{Q}}(1, X, \ldots, X^{n-1})$ where $n = \deg f$

Field embeddings: $\sigma_j(a) = \sum a_i {\alpha_j}^i \in \mathbb{C}$ where $f = \prod_{i \leq n}(X - \alpha_j)$.

f has s_1 real roots and $2s_2$ (conjugate) complex roots.

Two representations

Coefficient embedding

$$a \longmapsto \mathbf{a} = (a_0, \ldots, a_{n-1})^\top \in \mathbb{Q}^n$$

"Canonical" embedding

$$a \longmapsto \sigma(a) = (\sigma_1(a), \ldots, \sigma_n(a))^\top \in H$$

$$\sigma(ab) = (\sigma_i(a)\sigma_i(b))_{i \leq n}$$

H is a $\mathbb{R}$-inner-product space of dimension n in $\mathbb{C}^n$

"canonical norm" $\neq$ "coefficient norm"

Number fields and rings

$R = \mathbb{Z}[X]/f$ is a **number ring**. Lives in $K = \mathbb{Q}[X]/f$, a **number field**.

Structure: $K = \mathrm{Span}_{\mathbb{Q}}(1, X, \ldots, X^{n-1})$ where $n = \deg f$

Field embeddings: $\sigma_j(a) = \sum a_i {\alpha_j}^i \in \mathbb{C}$ where $f = \prod_{i \le n}(X - \alpha_j)$.

f has s_1 real roots and $2s_2$ (conjugate) complex roots.

Two representations

Coefficient embedding

$$a \longmapsto \mathbf{a} = (a_0, \ldots, a_{n-1})^\top \in \mathbb{Q}^n$$

"Canonical" embedding

$$a \longmapsto \sigma(a) = (\sigma_1(a), \ldots, \sigma_n(a))^\top \in H$$

$$\sigma(ab) = (\sigma_i(a)\sigma_i(b))_{i \le n}$$

H is a $\mathbb{R}$-inner-product space of dimension n in $\mathbb{C}^n$

"canonical norm" $\neq$ "coefficient norm"

The ring of algebraic integers

$$\mathcal{O}_K = \{x \in K \text{ roots of monic polynomials in } \mathbb{Z}[X]\}$$

It is a lattice: $\mathcal{O}_K = \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n$ for some $b_i \in \mathcal{O}_K$ $(b_i \neq 0)$.

(As any lattice, it has a dual $\mathcal{O}_K^\vee$.)

$\mathcal{O}_K$: **regularization** of $\mathbb{Z}[X]/f$
(in general, $R \subsetneq \mathcal{O}_K$)

$\mathcal{O}_K$: **intrinsic** to K.
Structure **independent** from f

It may not be possible to take $1, X, \ldots, X^{n-1}$ as a basis

Computing a $\mathbb{Z}$-basis for $\mathcal{O}_K$ is usually **hard**.

Ring-LWE (RLWE) [LPR10]

New ring choice: $\mathcal{O}_{K,q} = \mathcal{O}_K / q\mathcal{O}_K$.

$\alpha_1, \ldots, \alpha_n \in \mathbb{C}$: roots of f.

algebraic integers

$s \in \mathcal{O}_{K,q}^\vee$

Product: $a \cdot s$

complex vectors/matrices

$\sigma(s) = (s(\alpha_1), \ldots, s(\alpha_n)) \in \mathbb{C}^n$

Mult. by a **coordinate-wise**

$\sigma(as) = (a(\alpha_1)s(\alpha_1), \ldots, a(\alpha_n)s(\alpha_n))$

$D(a) := \mathrm{Diag}(a(\alpha_1), \ldots, a(\alpha_n))$.

$$\text{New Public key} = \left(\begin{bmatrix} \mathrm{D}(a_1) \\ \vdots \\ \mathrm{D}(a_k) \end{bmatrix}, \mathbf{b} = \begin{bmatrix} \mathrm{D}(a_1) \\ \vdots \\ \mathrm{D}(a_k) \end{bmatrix} \mathbf{s} + \begin{bmatrix} \mathbf{e}_1 \\ \vdots \\ \mathbf{e}_k \end{bmatrix} \bmod q \right)$$

RLWE [LPR'10]

$R \rightsquigarrow \mathcal{O}_K$, **use canonical embedding.**
Assume a $\mathbb{Z}$-basis of $\mathcal{O}_K$ is known.

$$H = \mathsf{Span}_{\mathbb{R}}(\mathbf{v}_1, \ldots, \mathbf{v}_n)$$
$$D_\Sigma^H : e_i \hookleftarrow D_\Sigma, \text{ outputs } e = \sum e_i \mathbf{v}_i \in H.$$

$\mathsf{RLWE}^\vee_{q,\Sigma,s}$ distribution: Fix $s \in \mathcal{O}^\vee_{K,q} := \mathcal{O}^\vee_K / q\mathcal{O}^\vee_K$

$$\mathsf{RLWE}^\vee_{q,\Sigma,s} : \begin{cases} a \hookleftarrow \mathcal{U}(\mathcal{O}_{K,q}) \\ e \hookleftarrow D_\Sigma^H \\ \text{outputs } (a, b = (as + e) \bmod q\mathcal{O}^\vee_K) \end{cases}$$

"Primal" variant: $\mathsf{RLWE}_{q,\Sigma,s}$ with $s \in \mathcal{O}_{K,q} := \mathcal{O}_K / q\mathcal{O}_K$.

- the dual appears "naturally" in the reduction
- for some rings, describing the dual is easy
- (but then, so is getting to "primal" version)

✓ "Canonical" objects
✓ Flexible (theoretical) tools
✓ More general proofs

↓

[LPR'10] **Decision-RLWE$^\vee$** $=$ **Search-RLWE$^\vee$** for Galois fields

[PRS'17] **Decision** $\Rightarrow$ **ApproxSVP** for **RLWE$^\vee$, RLWE, PLWE**

Situation?

- Using **RLWE$^\vee$** variants $\rightarrow$ Deal with $\mathcal{O}_K^\vee$ and floating point numbers
- $\mathbb{Z}$-basis of $\mathcal{O}_K$? $\rightarrow$ long precomputations, **non-uniform** reductions

In practice (NewHope), $f = X^{2^d} - 1$, $\mathcal{O}_K = \mathbb{Z}[X]/f$ and coeff. embedding.

What if cyclotomic fields are "weak"?

✓ "Canonical" objects
✓ Flexible (theoretical) tools
✓ More general proofs

↓

[LPR'10] **Decision-RLWE$^\vee$** $=$ **Search-RLWE$^\vee$** for Galois fields

[PRS'17] **Decision** $\Rightarrow$ **ApproxSVP** for **RLWE$^\vee$, RLWE, PLWE**

Situation?

- Using **RLWE$^\vee$** variants $\rightarrow$ Deal with $\mathcal{O}_K^\vee$ and floating point numbers
- $\mathbb{Z}$-basis of $\mathcal{O}_K$? $\rightarrow$ long precomputations, **non-uniform** reductions

In practice (NewHope), $f = X^{2^d} - 1$, $\mathcal{O}_K = \mathbb{Z}[X]/f$ and coeff. embedding.

What if cyclotomic fields are "weak"?

Situation and problems

(A) Relations between **PLWE, RLWE, RLWE$^\vee$**?

(B) Are **Decision** and **Search** equivalent in Ring-based **LWE**?

(C) Are there "weaker" fields for **ApproxSVP**? For Ring-based **LWE**?

(D) Are there other (better?) structures than ideal lattices for LWE?

Situation and problems

(A) Relations between **PLWE, RLWE, RLWE$^\vee$**?

Today

(B) Are **Decision** and **Search** equivalent in Ring-based LWE?

(C) Are there "weaker" fields for **ApproxSVP**? For Ring-based **LWE**?

Ideal-ApproxSVP seems a bit weaker than expected [PHS19]
Ring-LWE: short answer, we don't know yet.

(D) Are there other (better?) structures than ideal lattices for LWE?

Short: yes [LS15,RSSS18].

Transforming samples [LPR'10, LPR'13]

Goal: map $\mathrm{RLWE}^{\vee}_{s,\Sigma}$ samples to $\mathrm{RLWE}_{s',\Sigma'}$ samples

Want: $\theta : \begin{array}{ccc} \mathcal{O}_{K,q} \times \mathcal{O}^{\vee}_{K,q} & \longrightarrow & \mathcal{O}_{K,q} \times \mathcal{O}_{K,q} \\ (a, b) & \longmapsto & (a', b') \end{array}$

Assume $\exists\, \mathbf{t} \in \mathcal{O}_K$ such that $[\times \mathbf{t}] : \mathcal{O}^{\vee}_{K,q} \simeq \mathcal{O}_{K,q}$. Let $\theta_{\mathbf{t}}(a, b) = (a, \mathbf{t}b \bmod q)$.

If $b = as + e$, then $\mathbf{t}b = a(\mathbf{t}s) + \mathbf{t}e$, with $\mathbf{t}e \hookleftarrow D^{H}_{\Sigma'}$

New noise parameter: $\Sigma' = \mathrm{diag}\left[\,|\sigma_i(\mathbf{t})|\,\right] \cdot \Sigma \cdot \mathrm{diag}\left[\,|\sigma_i(\mathbf{t})|\,\right]$

Questions:

1) Does such $\mathbf{t}$ exist? 2) How large is $\mathbf{t}e$?

Transforming samples [LPR'10, LPR'13]

Goal: map $\mathrm{RLWE}^{\vee}_{s,\Sigma}$ samples to $\mathrm{RLWE}_{s',\Sigma'}$ samples

$$\textbf{Want: } \theta : \begin{array}{ccc} \mathcal{O}_{K,q} \times \mathcal{O}^{\vee}_{K,q} & \longrightarrow & \mathcal{O}_{K,q} \times \mathcal{O}_{K,q} \\ (a, b) & \longmapsto & (a', b') \end{array}$$

Assume $\exists\ \mathbf{t} \in \mathcal{O}_K$ such that $[\times \mathbf{t}] : \mathcal{O}^{\vee}_{K,q} \simeq \mathcal{O}_{K,q}$. Let $\theta_{\mathbf{t}}(a, b) = (a, \mathbf{t}b \bmod q)$.

If $b = as + e$, then $\mathbf{t}b = a(\mathbf{t}s) + \mathbf{t}e$, with $\mathbf{t}e \hookleftarrow D^{H}_{\Sigma'}$

New noise parameter: $\Sigma' = \mathrm{diag}\left[\,|\sigma_i(\mathbf{t})|\,\right] \cdot \Sigma \cdot \mathrm{diag}\left[\,|\sigma_i(\mathbf{t})|\,\right]$

Questions:

1) Does such $\mathbf{t}$ exist? 2) How large is $\mathbf{t}e$?

From RLWE$^\vee$ to RLWE

[LPR'10] Compute $\mathbf{t}$ in $poly(n)$-time with CRT

✓ Existence ✗ Size

↓

Our result†**:** An adequate $\mathbf{t}$ with $\|\sigma(\mathbf{t})\| \leq poly(n)$ exists in an adequate lattice.

✓ Existence ✓ Size

Consequence: solving $\mathbf{RLWE}_{q,\Sigma'} \Rightarrow$ solving $\mathbf{RLWE}^\vee_{q,\Sigma}$

$$\Sigma' \xleftarrow[loss]{poly(n)} \Sigma$$

†: Improved in [PP'19] "Algebraically structured LWE: revisited"

Ingredients and tools

Our result: An adequate $\mathbf{t}$ with $\|\sigma(\mathbf{t})\| \leq poly(n)$ exists in an adequate lattice.

- **Idea:** sample **Gaussians** in $(\mathcal{O}_K^\vee)^{-1}$ (inverse of the dual)
- **Main difficulty:** achieving a small enough standard deviation
- Tools:
  - Inclusion/exclusion
  - Tail bounds on Gaussian distributions
  - Smoothing parameters of lattices
  - Case disjonction on factors' size (norm)

Mapping RLWE to PLWE-like

Goal: map $\mathrm{RLWE}_{s,\Sigma}$ samples to $\mathrm{PLWE}_{s',\Sigma'}$ samples

$$\textbf{Want: } \theta : \begin{array}{ccc} \mathcal{O}_{K,q} \times \mathcal{O}_{K,q} & \longrightarrow & R_q \times R_q \\ (a, b) & \longmapsto & (a', b') \end{array}$$

Result†**:** We can find $[\times \mathbf{t}] : \mathcal{O}_{K,q} \simeq R_q$, such that $\|\sigma(\mathbf{t})\| \leq poly(n)$, for some $\mathbf{t}$ in **the conductor ideal** $\mathcal{C}_R = \{\mathbf{t} \in K \ : \ \mathbf{t}\mathcal{O}_K \subset R\}$.

$\mathcal{C}_R$ "interpolates" between R and $\mathcal{O}_K$

Lemma: if $q \not| \Delta(f)$, then $R_q \simeq \mathcal{C}_R/q\mathcal{C}_R \simeq \mathcal{O}_{K,q}$.

- Control $\|\sigma(\mathbf{t})\|$ with the same technique as earlier

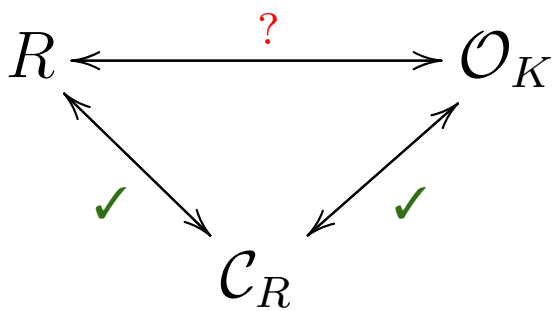
†: Improved in [PP19] "Algebraically structured LWE: revisited"

Mapping RLWE to PLWE-like

Goal: map $\mathrm{RLWE}_{s,\Sigma}$ samples to $\mathrm{PLWE}_{s',\Sigma'}$ samples

Want: $\theta : \begin{array}{ccc} \mathcal{O}_{K,q} \times \mathcal{O}_{K,q} & \longrightarrow & R_q \times R_q \\ (a, b) & \longmapsto & (a', b') \end{array}$

Result†**:** We can find $[\times \mathbf{t}] : \mathcal{O}_{K,q} \simeq R_q$, such that $\|\sigma(\mathbf{t})\| \leq poly(n)$, for some $\mathbf{t}$ in **the conductor ideal** $\mathcal{C}_R = \{\mathbf{t} \in K \ : \ \mathbf{t}\mathcal{O}_K \subset R\}$.



$\mathcal{C}_R$ "interpolates" between R and $\mathcal{O}_K$

Lemma: if $q \not| \Delta(f)$, then $R_q \simeq \mathcal{C}_R/q\mathcal{C}_R \simeq \mathcal{O}_{K,q}$.

- Control $\|\sigma(\mathbf{t})\|$ with the same technique as earlier

†: Improved in [PP19] "Algebraically structured LWE: revisited"

"Canonical noise"

Good candidate: $\theta_{\mathbf{t}}(a, b) = (\mathbf{t}a, \mathbf{t}^2 b \bmod q)$, for $\mathbf{t}$ as described.

If $b = as + e$, then $\mathbf{t}^2 b = (\mathbf{t}a)(\mathbf{t}s) + \mathbf{t}^2 e$, with $\mathbf{t}^2 e \hookleftarrow D^H_{\Sigma_{\mathbf{t}}}$

New noise parameter: $\Sigma_{\mathbf{t}} = \mathsf{diag}[\,|\sigma_i(\mathbf{t})|^2\,] \cdot \Sigma \cdot \mathsf{diag}[\,|\sigma_i(\mathbf{t})|^2\,]$

The catch:

$\mathbf{t}^2 e$ lives in H, while PLWE_f asks for **"coefficient"** representation.

“Canonical” vs “Coefficient”

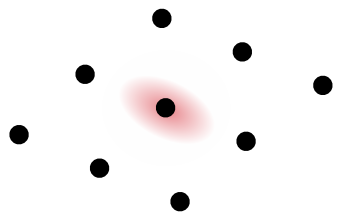
Relation between embeddings:

$$\sigma(a) = \mathbf{V}_f \cdot \mathbf{a}, \text{ with } \mathbf{V}_f = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & & \dots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{bmatrix}$$

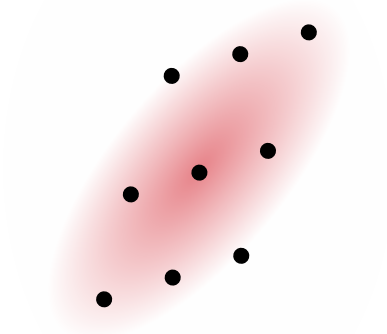
New noise: $\mathbf{V}_f{}^{-1}\sigma(\mathbf{t}^2 e) \hookleftarrow D_{\Sigma'}$, with $\Sigma' = \mathbf{V}_f{}^{-\top}\Sigma_{\mathbf{t}}\,\mathbf{V}_f^{-1}$

Possible situations

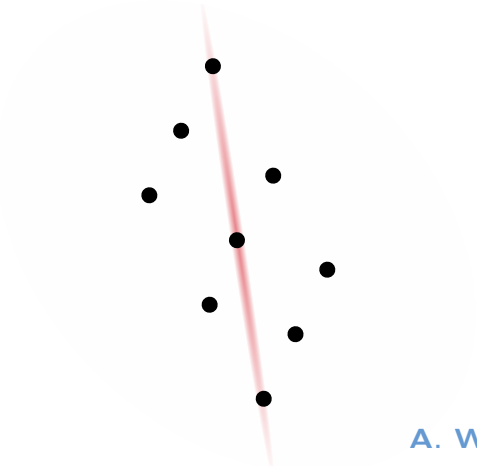
$\mathbf{V}_f^{-1}$ reasonable



$\mathbf{V}_f^{-1}$ too large



$\mathbf{V}_f^{-1}$ too skew

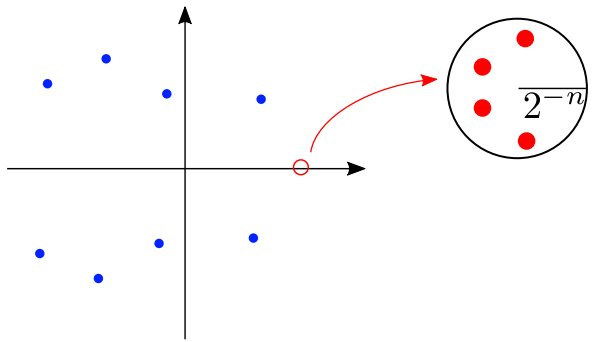


Inverse Vandermondes and roots separation

$$\mathbf{V}_f^{-1} = \left(\frac{S_{i,j}}{\Delta_j}\right)_{i,j}, \text{ where } \Delta_j = \prod_{k\neq j}(\alpha_k - \alpha_j).$$

Main difficulties:

- Δ_j can be exponentially small [BM'04]



$\min_j |\Delta_j| \leq \tilde{O}(2^{-n})$

- Bound for a large class of polynomials

Goal: A large family of irreducible polynomials in $\mathbb{Z}[X]$ with $\|\mathbf{V}_f^{-1}\| \leq poly(n)$.

Perturbations of a good situation

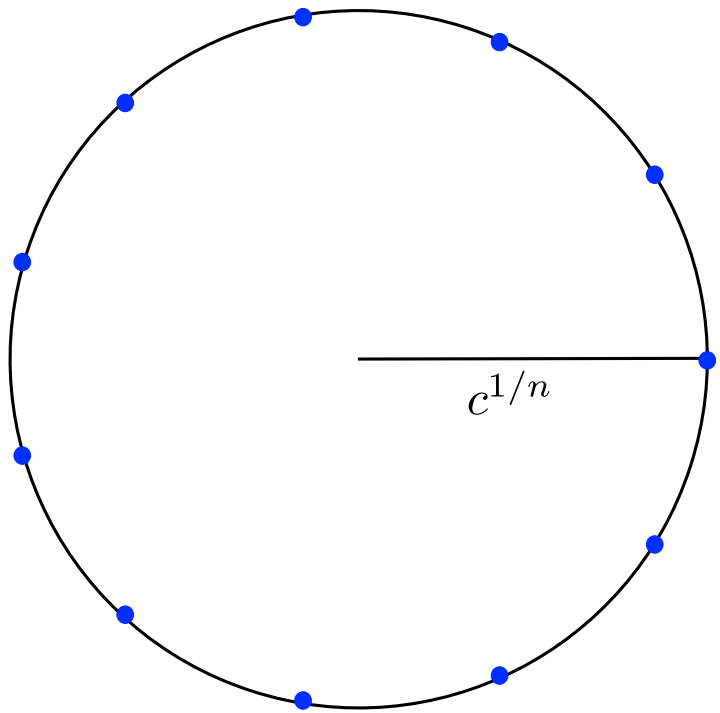
(1) $f := X^n - c \in \mathbb{Z}[X]$, with $\alpha_j = c^{1/n}\mathrm{e}^{2i\pi\frac{j}{n}}$.

$\|\mathbf{V}_f^{-1}\|_\infty = 1$.

(2) Let $P = \sum_{i=1}^{n/2} p_i X^i \in \mathbb{Z}[X]$.

Perturbation: $g := f + P = \prod_{i=1}^{n}(X - \beta_j)$

If "P small", β_i's should stay close to α_i's.



Theorem (Rouché):
If $|P(z)| < |f(z)|$ on a circle, then f and $f + P$ have the same numbers of zeros inside this circle.

Perturbations of a good situation

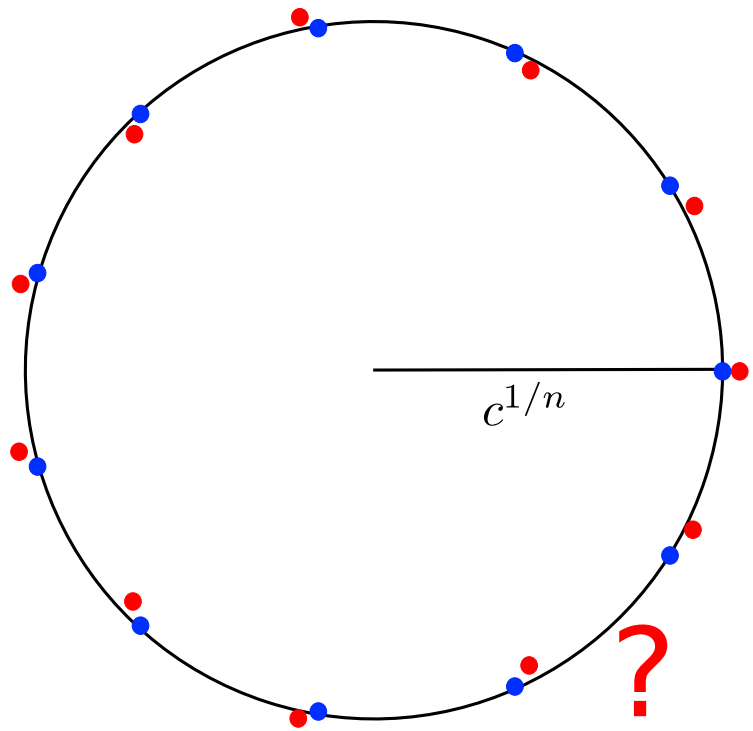
(1) $f := X^n - c \in \mathbb{Z}[X]$, with $\alpha_j = c^{1/n}\mathrm{e}^{2i\pi\frac{j}{n}}$.

$\|\mathbf{V}_f^{-1}\|_\infty = 1$.

(2) Let $P = \sum_{i=1}^{n/2} p_i X^i \in \mathbb{Z}[X]$.

Perturbation: $g := f + P = \prod_{i=1}^{n}(X - \beta_j)$

If "P small", β_i's should stay close to α_i's.



Theorem (Rouché):
If $|P(z)| < |f(z)|$ on a circle, then f and $f + P$ have the same numbers of zeros inside this circle.

Perturbations of a good situation

(1) $f := X^n - c \in \mathbb{Z}[X]$, with $\alpha_j = c^{1/n} \mathrm{e}^{2i\pi \frac{j}{n}}$.

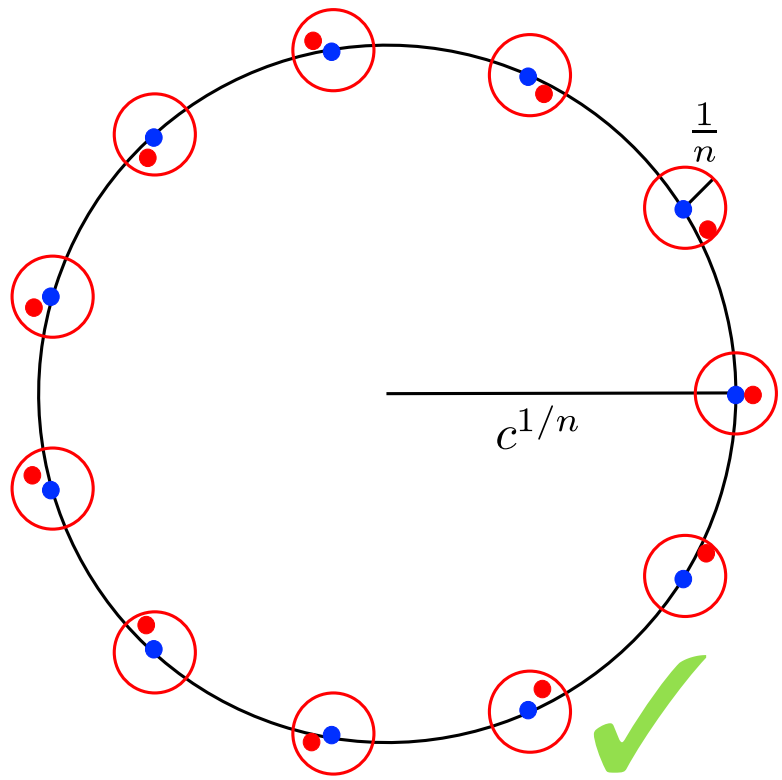
$\|\mathbf{V}_f^{-1}\|_\infty = 1$.

(2) Let $P = \sum_{i=1}^{n/2} p_i X^i \in \mathbb{Z}[X]$.

Perturbation: $g := f + P = \prod_{i=1}^{n}(X - \beta_j)$

If "P small", β_i's should stay close to α_i's.

Theorem (Rouché):
If $|P(z)| < |f(z)|$ on a circle, then f and $f + P$ have the same numbers of zeros inside this circle.

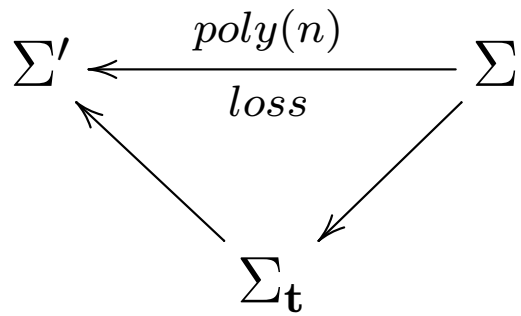


Completing the reduction

Result: We can exhibit exponentially many $f \in \mathbb{Z}[X]$, monic and irreducible, such that $\|\mathbf{V}_f^{-1}\| \leq poly(n)$.

For any such f, we have in K_f:

$$\text{solving } \mathbf{PLWE}_{q,\Sigma',f} \Rightarrow \text{solving } \mathbf{RLWE}_{q,\Sigma}$$



Search to Decision (shortest version)

Given: $\left(\mathbf{A}, \mathbf{b} = \mathbf{A}\,\mathbf{s} + \mathbf{e} \right)$ + disting. oracle, find $\mathbf{s}$.

Main steps:

Generate **RLWE**-like samples using Gaussians $t_i \hookleftarrow D_{\sigma,\mathcal{O}_K}$ $\longrightarrow$ Get good approximations of noise in poly time [PRS'17]

Difficulty: Find minimal σ s.t. linear combinations of t_i's look uniform.

Result: Leftover Hash Lemma over number rings.
$a_1, \ldots, a_m$: rows of $\mathbf{A}$. Standard dev. $\sigma \geq \widetilde{O}(\sqrt{n} \cdot \Delta_K^{1/n} \cdot q^{1/m})$.

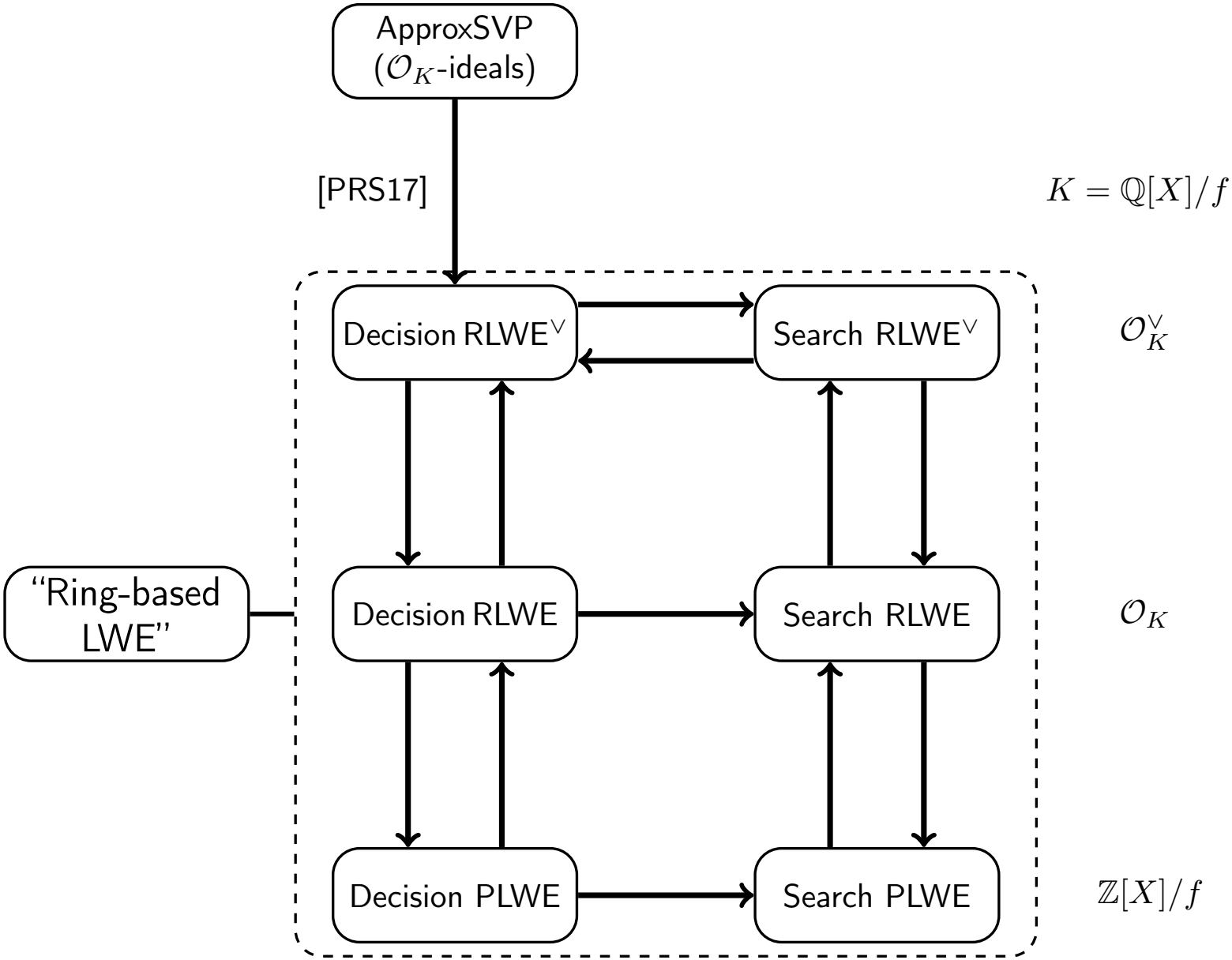
If $t_i \hookleftarrow D_{\sigma,\mathcal{O}_K}$, then $\sum_{i \leq m} a_i t_i$ is essentially uniform.

A ring-based Leftover Hash Lemma

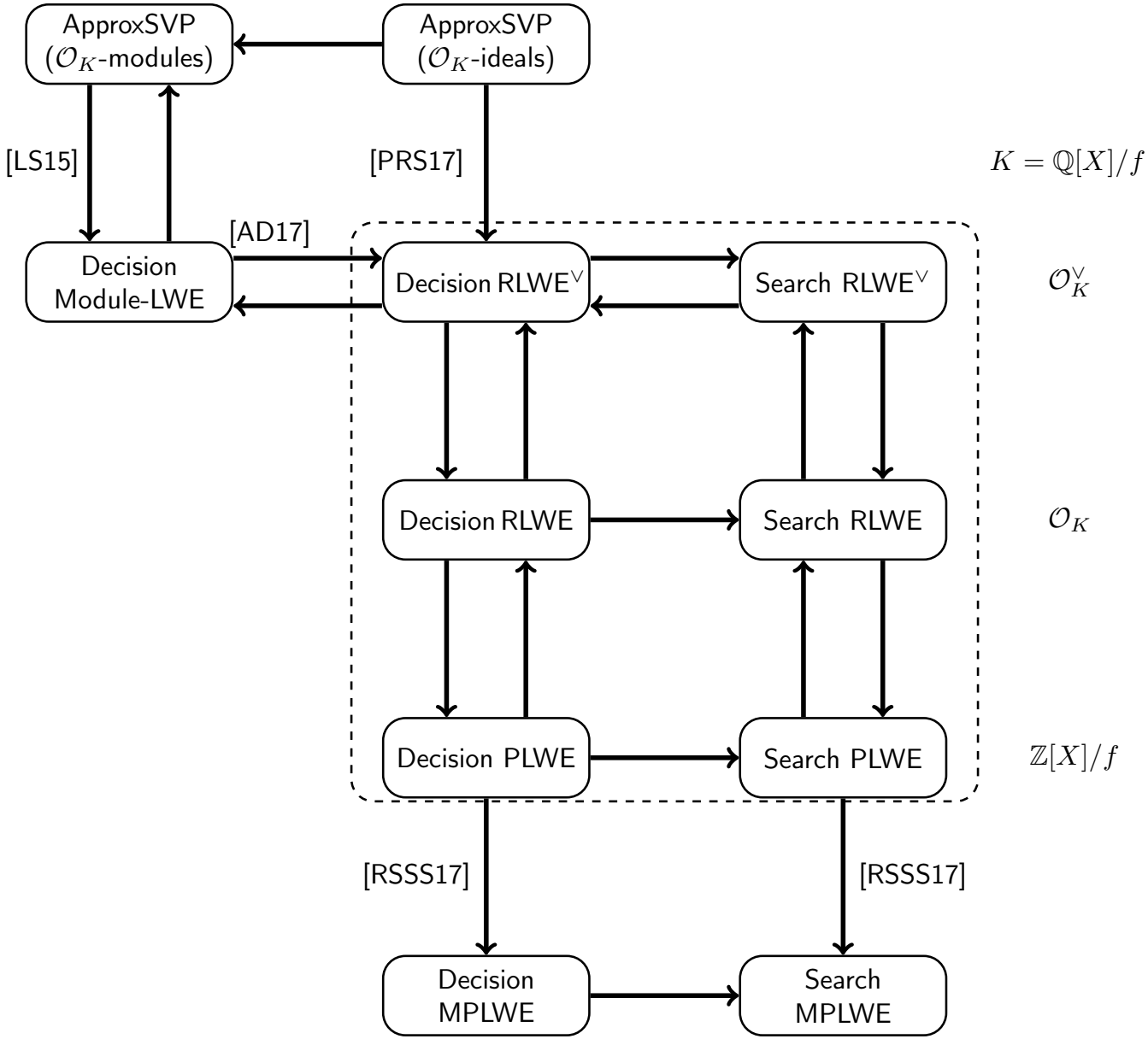
Result: (Leftover Hash Lemma)
$(a_1, \ldots, a_k, \sum_i a_i t_i)$ is statistically indistinguishable from a uniform tuple.

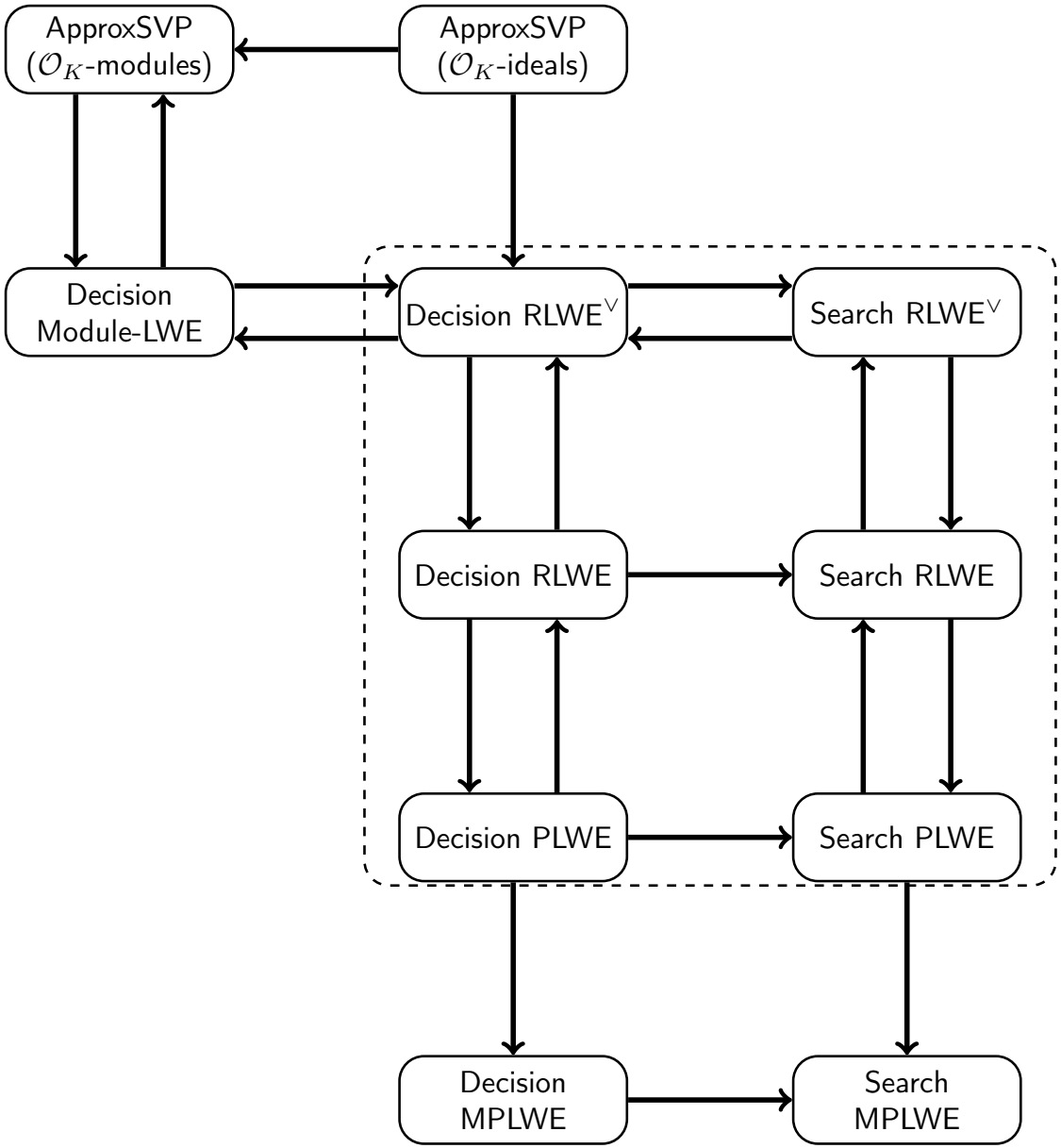
- **Idea:** Adapting [SS'11]'s result to a general context.
- **Main difficulty:** Lower bound on the shortest vectors of some q-ary lattice.
- Tools:
  - Smoothing parameters of q-ary lattices
  - Understand solutions of $a \cdot x = b$ in the ring $\mathcal{O}_{K,q}$
  - Duality for q-ary **module** lattices
  - Bound number of lattice points in a ball

Open Problems



Open Problems




ApproxSVP
($\mathcal{O}_K$-modules)
ApproxSVP
($\mathcal{O}_K$-ideals)
Decision
Module-LWE
Decision RLWE$^\vee$
Search RLWE$^\vee$
Decision RLWE
Search RLWE
Decision PLWE
Search PLWE
Decision
MPLWE
Search
MPLWE

Thank you :)