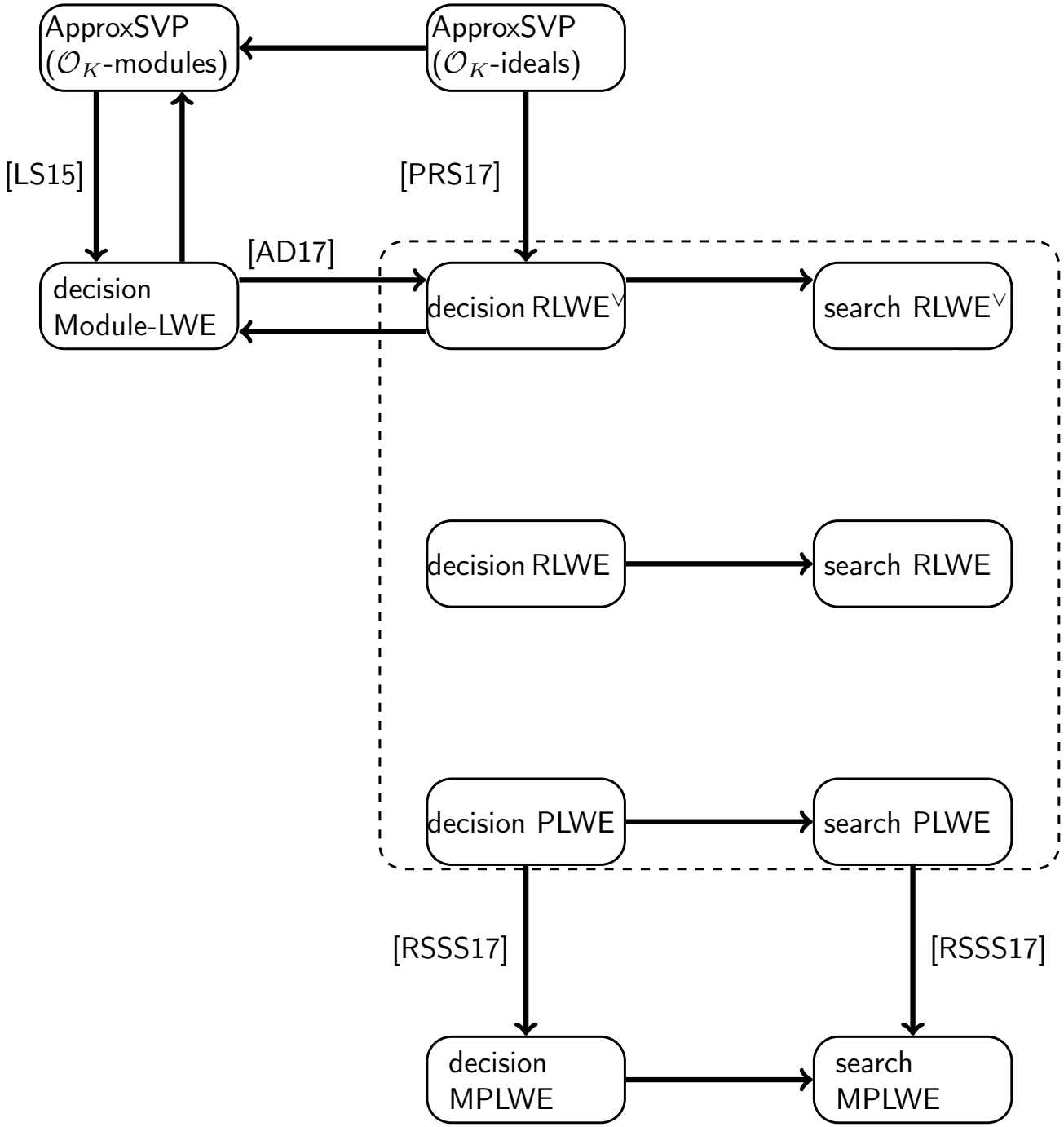
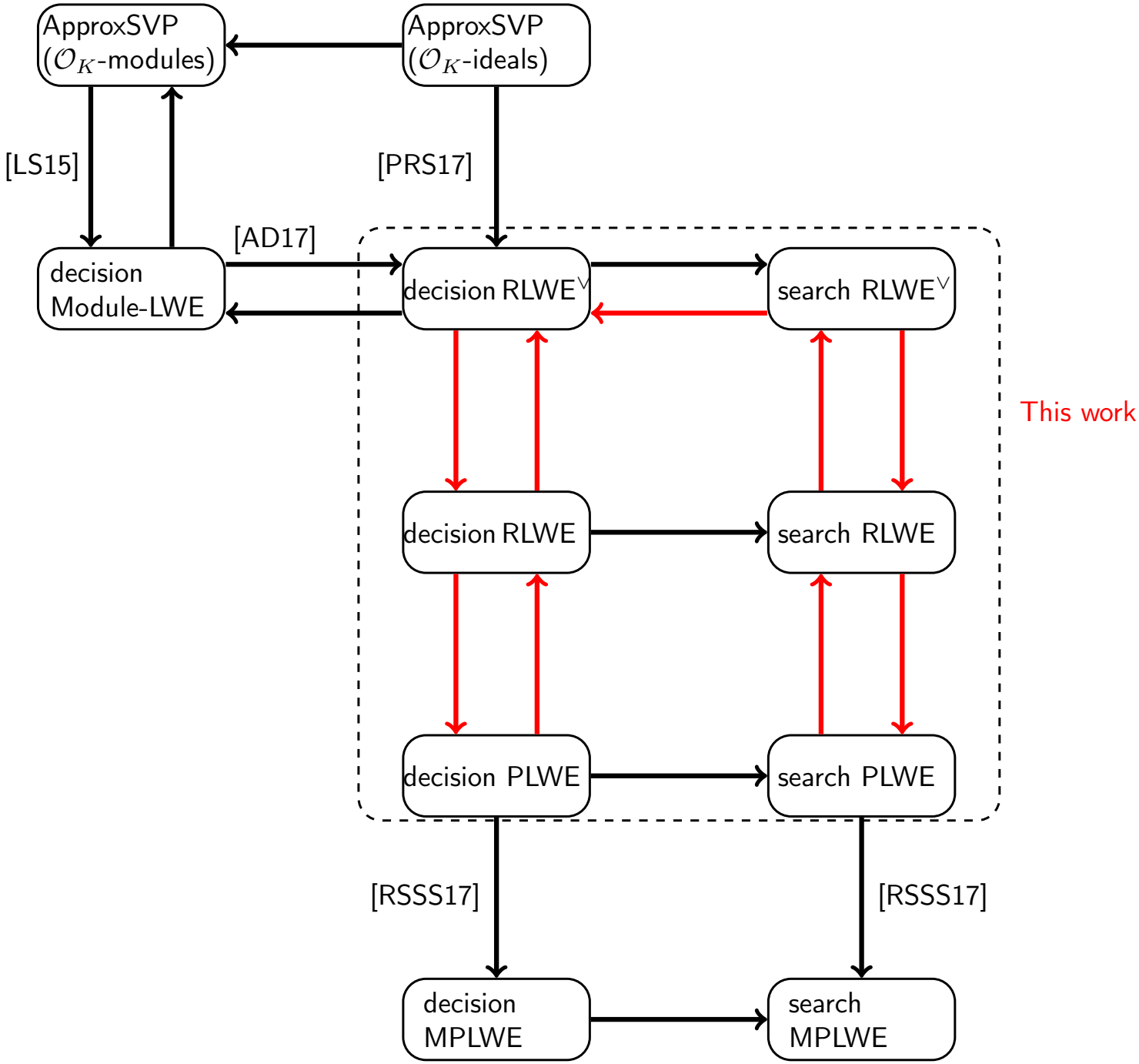
On the Ring-LWE and Polynomial-LWE problems

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


ApproxSVP
($\mathcal{O}_K$-modules)
ApproxSVP
($\mathcal{O}_K$-ideals)
[LS15]
[PRS17]
[AD17]
decision
Module-LWE
decision RLWE$^\vee$
search RLWE$^\vee$
decision RLWE
search RLWE
decision PLWE
search PLWE
[RSSS17]
[RSSS17]
decision
MPLWE
search
MPLWE


ApproxSVP
($\mathcal{O}_K$-modules)
ApproxSVP
($\mathcal{O}_K$-ideals)
[LS15]
[PRS17]
[AD17]
decision
Module-LWE
decision RLWE$^\vee$
search RLWE$^\vee$
This work
decision RLWE
search RLWE
decision PLWE
search PLWE
[RSSS17]
[RSSS17]
decision
MPLWE
search
MPLWE

"On variants of Polynomial-LWE and Ring-LWE"
(joint work with **M. Rosça** and **D. Stehlé**, submitted)

Results:

(A) The 3 settings are essentially† the same

(B) Search = Decision in all settings.

†: 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

An encryption scheme [Regev'05]

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

Alice	Evil	Bruno
$\mathbf{s} \in \mathbb{Z}_q^n$		$\mu \in \{0,1\}$
$\mathbf{A} \in \mathcal{M}_{m \times n}(\mathbb{Z}_q),\ e_i \hookleftarrow \chi$	$\longrightarrow \left(\mathbf{A}, \mathbf{b} \right)$	
$\mathbf{b} = \mathbf{A}\,\mathbf{s} + \mathbf{e} \bmod q$		

An encryption scheme [Regev'05]

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

Alice	Evil	Bruno
$\mathbf{s} \in \mathbb{Z}_q^n$		$\mu \in \{0,1\}$
$\mathbf{A} \in \mathcal{M}_{m \times n}(\mathbb{Z}_q),\ e_i \hookleftarrow \chi$	$\longrightarrow \left(\mathbf{A}, \mathbf{b} \right)$	
$\mathbf{b} = \mathbf{A}\,\mathbf{s} + \mathbf{e} \bmod q$		
$e' = b' - \langle \mathbf{a}', \mathbf{s} \rangle \bmod q$	$\longleftarrow \quad (\mathbf{a}', b')$	$\leftarrow \mathsf{E}_{\mathbf{A},\mathbf{b}}(\mu) = (\sum_{i \in \mathcal{I}} \mathbf{a}_i, \sum_{i \in \mathcal{I}} b_i + \mu \lfloor \frac{q}{2} \rfloor)$

An encryption scheme [Regev'05]

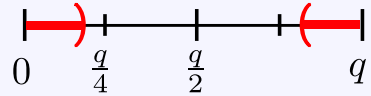
n "security parameter", q prime, $n \leq m \leq poly(n)$, χ distribution over $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$.

Alice	Evil	Bruno
$\mathbf{s} \in \mathbb{Z}_q^n$		$\mu \in \{0,1\}$
$\mathbf{A} \in \mathcal{M}_{m\times n}(\mathbb{Z}_q),\ e_i \hookleftarrow \chi$	$\longrightarrow \left(\mathbf{A}, \mathbf{b} \right)$	
$\mathbf{b} = \mathbf{A}\,\mathbf{s} + \mathbf{e} \bmod q$		
$e' = b' - \langle \mathbf{a}', \mathbf{s} \rangle \bmod q$	$\longleftarrow (\mathbf{a}', b')$	$\leftarrow \mathsf{E}_{\mathbf{A},\mathbf{b}}(\mu) = (\sum_{i\in\mathcal{I}} \mathbf{a}_i, \sum_{i\in\mathcal{I}} b_i + \mu\lfloor \frac{q}{2} \rfloor)$

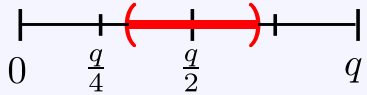
$$\mathsf{Dec}_{\mathbf{s}}(\mathbf{a}', b') = \begin{cases} 0 \text{ if } e' \sim 0 \\ 1 \text{ if } e' \sim \frac{q}{2} \end{cases}$$

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

$\mu = 0$



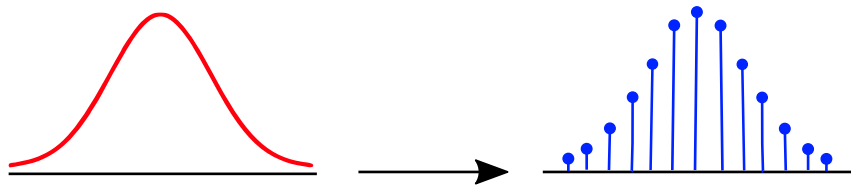
$\mu = 1$



Learning With Errors [R'05]

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

$\chi \to D_r$ **discrete Gaussian distribution**



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

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

Search-LWE$_{q,r}$:

$$\text{From } \left(\begin{array}{c} m \updownarrow \\ \overbrace{\longleftrightarrow}^{n} \end{array} \boxed{\mathbf{A}} \;,\; \boxed{\mathbf{b}} = \boxed{\mathbf{A}}\,\boxed{\mathbf{s}} + \boxed{\mathbf{e}} \right), \text{ find } \boxed{\mathbf{s}}$$

Hardness [R'05]

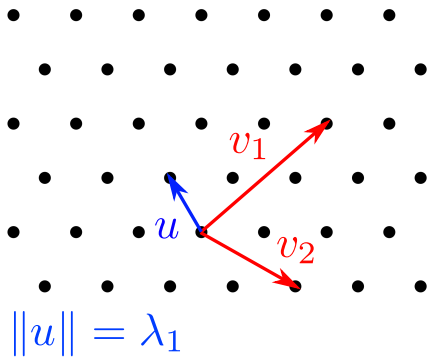
Decision-LWE$_{q,D_r}$**:** Given $(\mathbf{a}_i, b_i)_{i \leq m}$ either from $A_{\mathbf{s},D_r}$ or $\mathcal{U}(\mathbb{Z}_q^n \times \mathbb{Z}_q)$, decide which one was given.

Lattice $\mathcal{L} = \mathbf{A}\mathbb{Z}^n$, $\lambda_1 =$ length of a shortest vector in $\mathcal{L} \setminus \{0\}$.

ApproxSVP$_\gamma$: Given $d > 0$, decide if $\lambda_1 \leq d$ or $\lambda_1 > d\gamma$.

For general lattices:

time	$poly(n)$	$2^{O(n)}$
γ	$2^{\widetilde{O}(n)}$	$poly(n)$



Hardness [R'05]

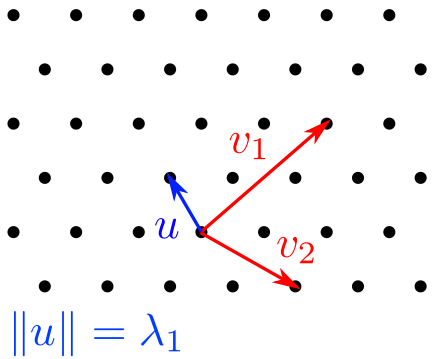
Decision-LWE$_{q,D_r}$**:** Given $(\mathbf{a}_i, b_i)_{i \leq m}$ either from $A_{\mathbf{s},D_r}$ or $\mathcal{U}(\mathbb{Z}_q^n \times \mathbb{Z}_q)$, decide which one was given.

Lattice $\mathcal{L} = \mathbf{A}\mathbb{Z}^n$, $\lambda_1 =$ length of a shortest vector in $\mathcal{L} \setminus \{0\}$.

ApproxSVP$_\gamma$: Given $d > 0$, decide if $\lambda_1 \leq d$ or $\lambda_1 > d\gamma$.

For general lattices:

time	$poly(n)$	$2^{O(n)}$
γ	$2^{\widetilde{O}(n)}$	$poly(n)$



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

LWE in practice

Perks:

- ✓ simple description, simple operations
- ✓ flexible parameters, many possibilities
- ✓ **post-quantum**

Drawbacks:

- ✗ key-size
- ✗ speed (compared to other)

Frodo† (NIST competitor)	VS	Current crypto RSA 3072-bits	Current crypto ECDH nistp256
Public key ~ 11 KBytes		~ 400 bytes	32 bytes
Handshake ~ 2.5ms		~ 5 ms	~ 1.3 ms

†: [BCD++'17]

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

Add structure: ideal lattices

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

Good example: $f = X^n + 1, n = 2^d$.

polynomials

$$s = \sum s_i X^i \in R_q = R/qR$$

Product: $a \cdot s \bmod f$

vectors/matrices

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

Mult. by a = use **Toeplitz matrix**

$$T_f(a) = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ -a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & & \ddots & \vdots \\ -a_1 & -a_2 & \cdots & a_0 \end{bmatrix}$$

Add structure: ideal lattices

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

Good example: $f = X^n + 1, n = 2^d$.

polynomials

$s = \sum s_i X^i \in R_q = R/qR$

Product: $a \cdot s \bmod f$

vectors/matrices

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

Mult. by a = use **Toeplitz matrix**

$$T_f(a) = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ -a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & & \ddots & \vdots \\ -a_1 & -a_2 & \cdots & a_0 \end{bmatrix}$$

Noise: $e = \sum e_i X^i, e_i \hookleftarrow D_{r_i}$.

$\mathbf{e} = (e_0, \ldots, e_{n-1}) \in \mathbb{R}^n$

Sample: $(a, b = a \cdot s + e \bmod qR)$

$(\mathbf{a}, b = T_f(a) \cdot \mathbf{s}^\top + \mathbf{e} \bmod q)$

Classic LWE

$$\mathbf{b} = \underbrace{\mathbf{A}}_{n}\ \mathbf{s} + \mathbf{e}\ \Big\}k$$

Polynomial-LWE (PLWE)

$$\Big\}k'n\quad \mathbf{b} = \underbrace{\begin{matrix} T_f(a_1) \\ \hline T_f(a_2) \\ \hline T_f(a_{k'}) \end{matrix}}_{n}\ \mathbf{s} + \begin{matrix} \mathbf{e}_1 \\ \hline \mathbf{e}_2 \\ \hline \mathbf{e}_{k'} \end{matrix}$$

1 PLWE sample = n correlated LWE samples.

PLWE and its hardness [SSTX'09]

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

$\vec{r} = \mathsf{diag}(r_i)_{i \leq n}, r_i \geq 0$
$D_{\vec{r}}$ n-dimensional **Gaussian**.

PLWE$_{q,\vec{r},f}$ distribution: Fix $s \in R_q$

$$\mathcal{B}_{s,D_{\vec{r}}} : \begin{cases} a \hookleftarrow \mathcal{U}(R_q) \\ e \hookleftarrow D_{\vec{r}} \\ \text{outputs } (a, b = (a \cdot s + e) \bmod qR) \end{cases}$$

Search-PLWE$_{q,\vec{r},f}$ and **Decision-PLWE$_{q,\vec{r},f}$** defined as before.

PLWE and its hardness [SSTX'09]

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

$\vec{r} = \mathsf{diag}(r_i)_{i \leq n}, r_i \geq 0$
$D_{\vec{r}}$ n-dimensional **Gaussian**.

PLWE$_{q,\vec{r},f}$ distribution: Fix $s \in R_q$

$$\mathcal{B}_{s,D_{\vec{r}}} : \begin{cases} a \hookleftarrow \mathcal{U}(R_q) \\ e \hookleftarrow D_{\vec{r}} \\ \text{outputs } (a, b = (a \cdot s + e) \bmod qR) \end{cases}$$

Search-PLWE$_{q,\vec{r},f}$ and **Decision-PLWE$_{q,\vec{r},f}$** defined as before.

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

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

Practice vs. Theory

Perks:

- ✓ fast and compact operations
- ✓ still post-quantum

New Hope[†]
(NIST competitor)

Public key: ~ 2 KBytes
Handshake: ~ 0.3 ms

Theoretical limitations:

- ✗ γ depends on f's "expansion factor"
- ✗ Working with R relies too much on f

$\rightarrow$ Restricts "good f's"

$\rightarrow$ Difficult proofs, lacks tools and flexibility

†: [ADPS'15]

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.

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.

The space $H = \{(v_1, \ldots, v_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} \ : \ \forall\ i \geq 1, v_{i+s_1+s_2} = \overline{v_{i+s_1}}\}$.

Two representations

Coefficient embedding

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

Minkowski embedding

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

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

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 $b_i \in \mathcal{O}_K$ $(b_i \neq 0)$.

Dual (lattice): $\mathcal{O}_K^\vee = \{\mathbf{y} \in H : \forall\, \mathbf{x} \in \mathcal{O}_K, \langle \mathbf{y}, \mathbf{x} \rangle \in \mathbb{Z}\}$.

- ✓ $\mathcal{O}_K$ is a **regularization** of $R = \mathbb{Z}[X]/f$
  - $R \subsetneq \mathcal{O}_K$ in general
- ✓ $\mathcal{O}_K$ is **intrinsic** to K: its structure **does not depend** on 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**.

RLWE [LPR'10]

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

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

RLWE$^{\vee}_{q,\vec{r}}$ distribution: Fix $s \in \mathcal{O}^{\vee}_{K,q} := \mathcal{O}^{\vee}_K / q\mathcal{O}^{\vee}_K$

$$\mathcal{A}^{\vee}_{s,D_{\vec{r}}} : \begin{cases} a \hookleftarrow \mathcal{U}(\mathcal{O}_{K,q}) \\ e \hookleftarrow D^H_{\vec{r}} \\ \text{outputs } (a, b = (as + e) \bmod q\mathcal{O}^{\vee}_K) \end{cases}$$

Search-RLWE$^{\vee}_{q,\vec{r}}$ and **Decision-RLWE$^{\vee}_{q,\vec{r}}$** defined as before.

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

✓ "Canonical" objects

↓

✓ Easier proofs/noise management

↓

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

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

What is left?

- Using **RLWE**$^\vee$ variants → Need to deal with $\mathcal{O}_K^\vee$
- $\mathbb{Z}$-basis of $\mathcal{O}_K$? → long precomputations for some f's, **non-uniform** reductions
- In practice, f stays cyclotomic. → 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$^\vee$**?

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

New Results!

(C) Are there "weaker" fields for **ApproxSVP**? For Ring-based **LWE**?
"Ill-defined": [EHL'14, ELOS'15, CLS'15, HCS'16]

(D) Are there other (better?) structures than ideal lattices for LWE?
Adressed in [LS'15, AD'17, RSSS'17]

1. LWE and Cryptography
2. Ring-based LWE
3. Reductions between Ring-based LWE's
   - Controlled RLWE$^\vee$ to RLWE
   - From $\mathcal{O}_K$ to R with the conductor
   - Large families of nice polynomials
4. Search to Decision

Transforming samples [LPR'10, LPR'13]

Goal: map $\mathcal{A}^{\vee}_{s,\Sigma}$ to $\mathcal{A}_{s',\Sigma'}$ and "uniform" to "uniform"

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

Transforming samples [LPR'10, LPR'13]

Goal: map $\mathcal{A}^{\vee}_{s,\Sigma}$ to $\mathcal{A}_{s',\Sigma'}$ and "uniform" to "uniform"

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

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 $(a,b) \hookleftarrow \mathcal{A}^{\vee}_{s,\Sigma}$:

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

$\Sigma' = \text{diag}\left[\,|\sigma_i(\mathbf{t})|\,\right] \cdot \Sigma \cdot \text{diag}\left[\,|\sigma_i(\mathbf{t})|\,\right]$

If $(a,b) \hookleftarrow$ uniform:

$[\times \mathbf{t}]$ isomorphism $\Rightarrow (a, \mathbf{t}b)$ uniform

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 $\mathbf{RLWE}^{\vee}_{q,\Sigma}$

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

Ingredients and tools

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

- **Idea:** use **Gaussian sampling** in $(\mathcal{O}_K^\vee)^{-1}$.
- **Main difficulty:** achieving a small enough standard deviation
  - Require factorization of $q\mathcal{O}_K$ in prime ideals in $\mathcal{O}_K$ (non-uniform reduction)

Ingredients and tools

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

- **Idea:** use **Gaussian sampling** in $(\mathcal{O}_K^\vee)^{-1}$.
- **Main difficulty:** achieving a small enough standard deviation
  - Require factorization of $q\mathcal{O}_K$ in prime ideals in $\mathcal{O}_K$ (non-uniform reduction)
- Tools:
  - Inclusion/exclusion
  - Case disjonction on factors' size (norm)
  - "Smoothness parameters" of lattices
  - Tail bounds on Gaussian distributions

1. LWE and Cryptography
2. Ring-based LWE
3. Reductions between Ring-based LWE's
   - Controlled RLWE$^\vee$ to RLWE
   - From $\mathcal{O}_K$ to R with the conductor
   - Large families of nice polynomials
4. Search to Decision

Mapping RLWE to PLWE-like

Goal: map $\mathcal{A}_{s,\Sigma}$ to $\mathcal{B}_{s',\Sigma'}$ and "uniform" to "uniform"

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

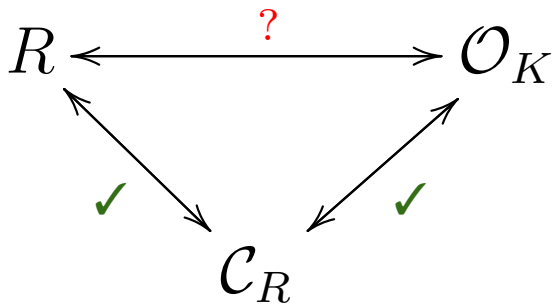
Result: We can find $[\times \mathbf{t}] : \mathcal{O}_{K,q} \simeq R_q$, such that $\|\sigma(\mathbf{t})\| \leq poly(n)$, for some $\mathbf{t}$ in **the conductor ideal** $\mathcal{C}_R = \{\mathbf{t} \in K \ : \ \mathbf{t}\mathcal{O}_K \subset R\}$.

Mapping RLWE to PLWE-like

Goal: map $\mathcal{A}_{s,\Sigma}$ to $\mathcal{B}_{s',\Sigma'}$ and "uniform" to "uniform"

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

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 $q \nmid \Delta(f)$, 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

"Minkowski noise"

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

If $(a, b) \hookleftarrow \mathcal{A}_{s,\Sigma}$:

$\mathbf{t}^2 b = (\mathbf{t}a)(\mathbf{t}s) + \mathbf{t}^2 e$

If $(a, b) \hookleftarrow$ uniform:

$[\times \mathbf{t}]$ isomorphism $\Rightarrow (\mathbf{t}a, \mathbf{t}^2 b)$ uniform

$e' = \mathbf{t}^2 e \hookleftarrow D^H_{\Sigma_{\mathbf{t}}}$, where $\Sigma_{\mathbf{t}} = \mathrm{diag}[\,|\sigma_i(\mathbf{t})|^2\,] \cdot \Sigma \cdot \mathrm{diag}[\,|\sigma_i(\mathbf{t})|^2\,]$.

e' lives in H, while **PLWE**$_f$ asks for "Coefficient" representation.

"Minkowski" vs "Coefficient"

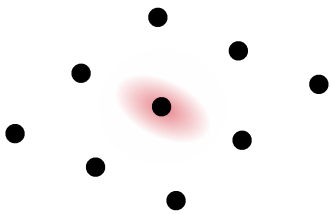
Relation between embeddings:

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

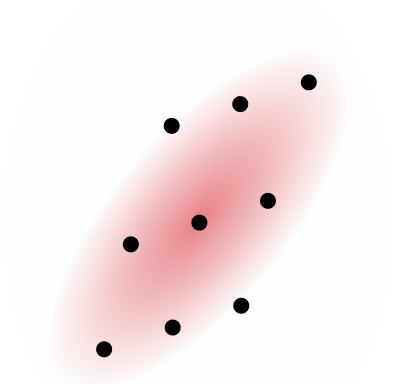
New noise: $\mathbf{V}_f{}^{-1}\sigma(e') \hookleftarrow D_{\Sigma'}$, with $\Sigma' = \mathbf{V}_f{}^{-\top}\Sigma_{\mathbf{t}}\,\mathbf{V}_f^{-1}$

Possible situations

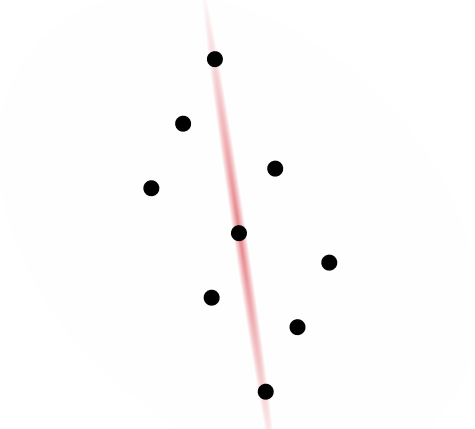
$\mathbf{V}_f^{-1}$ reasonable



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



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

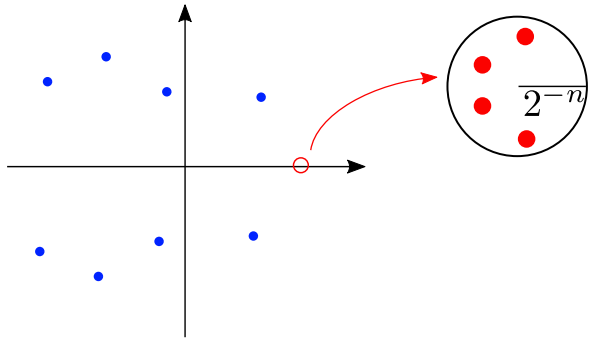


Inverse Vandermondes and roots separation

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

Main difficulties:

- Δ_j can be exponentially small [BM'04]



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

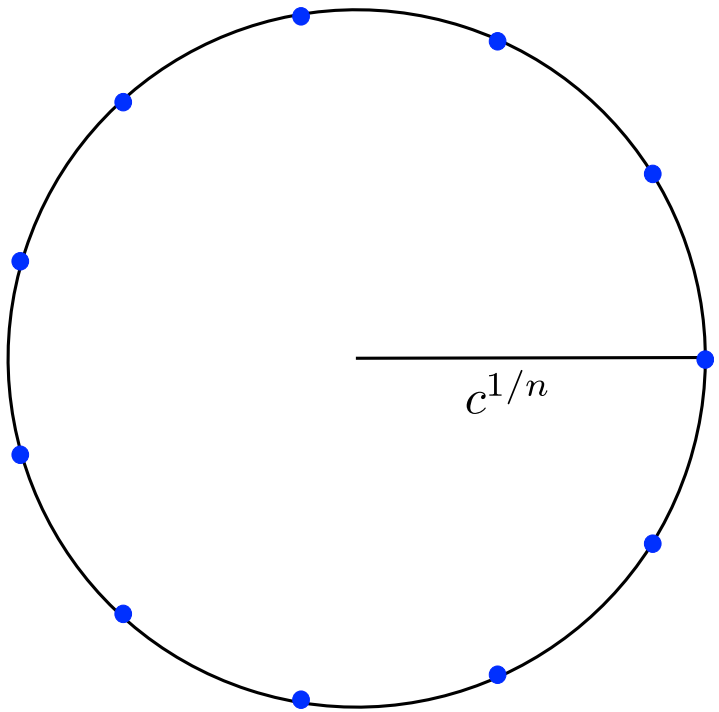
- Bound for a large class of polynomials

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 $\alpha_j = c^{1/n}\mathsf{e}^{2i\pi\frac{j}{n}}$.

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



Perturbations of a good situation

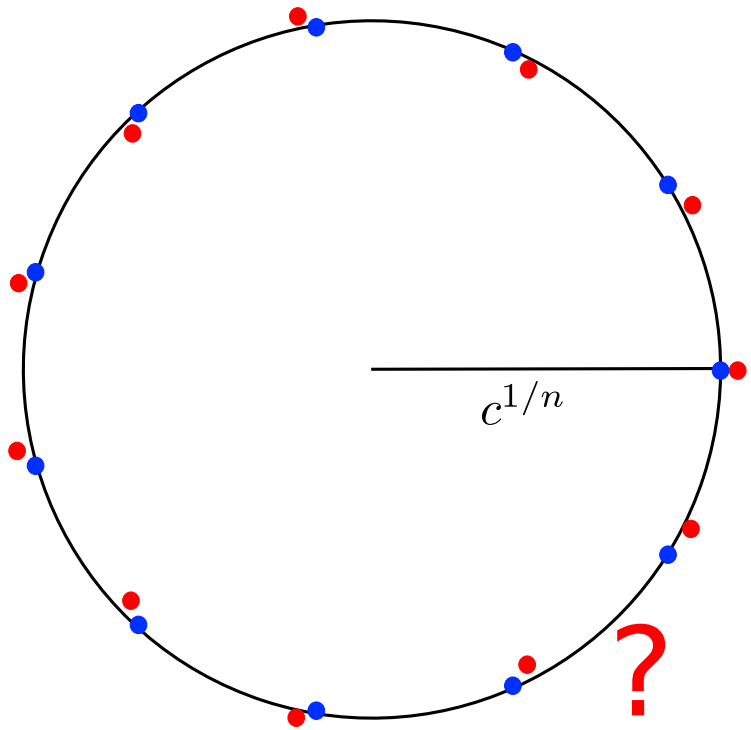
(1) $f := X^n - c \in \mathbb{Z}[X]$, with $\alpha_j = c^{1/n} \mathrm{e}^{2i\pi \frac{j}{n}}$.

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

(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.



Perturbations of a good situation

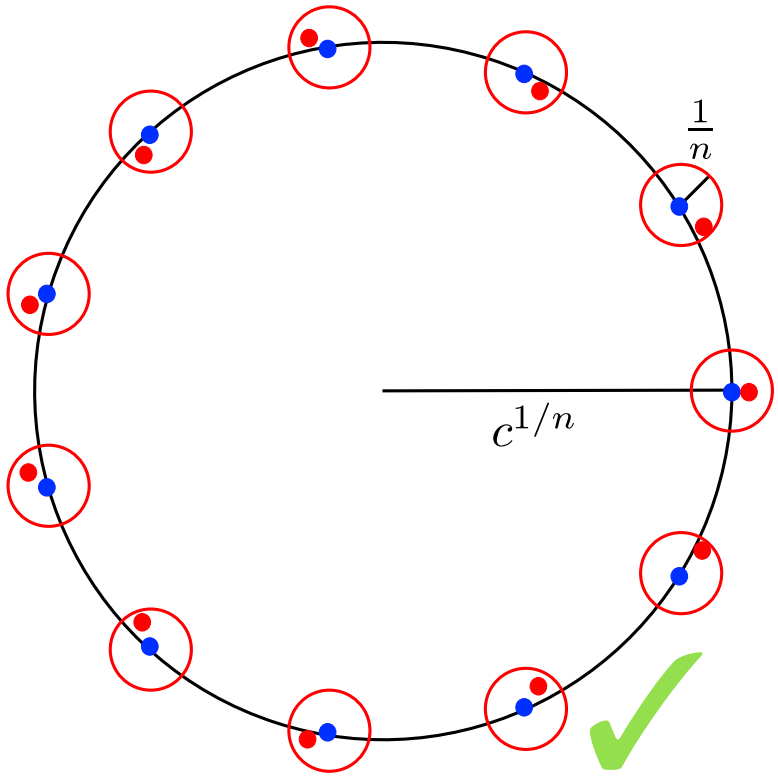
(1) $f := X^n - c \in \mathbb{Z}[X]$, with $\alpha_j = c^{1/n} \mathrm{e}^{2i\pi \frac{j}{n}}$.

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

(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)

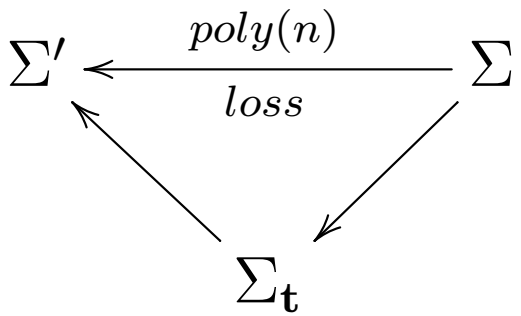
If $|P(z)| < |f(z)|$ on a circle, then f and $f + P$ have the same numbers of zeros inside this circle.

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:

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



Ingredients and tools

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

- **Idea:** If β_i's are close to α_i's, then $\|\mathbf{V}_g^{-1}\| \sim \|\mathbf{V}_f^{-1}\|$.
- **Main difficulty:** lower bound on $|\Delta_j| = \prod_{j \neq k} |\beta_k - \beta_j|$.

Ingredients and tools

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

- **Idea:** If β_i's are close to α_i's, then $\|\mathbf{V}_g^{-1}\| \sim \|\mathbf{V}_f^{-1}\|$.
- **Main difficulty:** lower bound on $|\Delta_j| = \prod_{j \neq k} |\beta_k - \beta_j|$.
- Steps:
  - Bound $|P(z)|, |f(z)|$ on $D(\alpha_i, \frac{1}{n}) \Rightarrow$ conditions on $c, \|P\|_1$.
  - Assume conditions are met.
    Rouché's theorem implies $|\Delta_j| \geq \prod \left(\underbrace{|\alpha_k - \alpha_j|}_{\text{well-known}} - \frac{2}{n} \right)$
  - Irreducibility when c is a large enough prime

Main idea

Given: $\left(\mathbf{A}, \mathbf{b} = \mathbf{A}\,\mathbf{s} + \mathbf{e} \right)$, find good approx. of all $\sigma_i(e)$'s

$$\mathbf{e} = \begin{array}{|c|}\hline e_1 \\ \hline \vdots \\ \hline e_k \\ \hline \end{array} \quad \xrightarrow{\sigma} \quad \sigma(\mathbf{e}) = \begin{array}{|c|c|c|}\hline \sigma_1(e_1) & \dots & \sigma_n(e_1) \\ \hline \vdots & & \vdots \\ \hline \sigma_1(e_k) & \dots & \sigma_n(e_k) \\ \hline \end{array}$$

$$\overbrace{\left[\tilde{z}_1\right]}, \ \dots \ , \overbrace{\left[\tilde{z}_n\right]}$$

Main idea

Given: $\left(\mathbf{A}, \mathbf{b} = \mathbf{A}\ \mathbf{s} + \mathbf{e} \right)$, find good approx. of all $\sigma_i(e)$'s

$$\mathbf{e} = \begin{array}{|c|}\hline e_1 \\ \hline \vdots \\ \hline e_k \\ \hline \end{array} \quad \xrightarrow{\sigma} \quad \sigma(\mathbf{e}) = \begin{array}{|c|c|}\hline \sigma_1(e_1) & \sigma_n(e_1) \\ \vdots & \vdots \\ \sigma_1(e_k) & \sigma_n(e_k) \\ \hline \end{array} \quad \begin{matrix} \wr & \wr \\ \left[\tilde{z}_1\right], & \left[\tilde{z}_n\right] \end{matrix}$$

Round $\sigma\left(\mathbf{A}\ \mathbf{s} + \mathbf{e} \right) - \left[\tilde{z}_1 \,|\, \ldots \,|\, \tilde{z}_n \right] \rightarrow \sigma\left(\mathbf{A}\ \mathbf{s} \right)$

Invert a_i's to obtain $\mathbf{A}^{-1}$, then $\sigma\left(\mathbf{A}^{-1} \right) \cdot \sigma\left(\mathbf{A}\ \mathbf{s} \right) = \sigma\left(\mathbf{s} \right)$

Oracle Hidden Center Problem

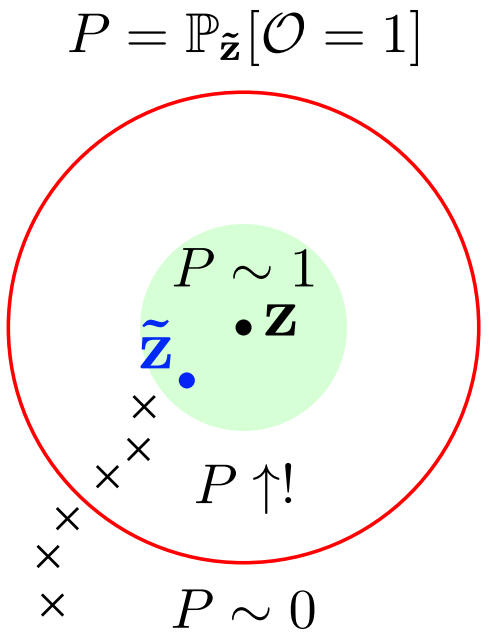
Input: Samples $(a_i, b_i = a_i s + e_i)_{i \leq k}$ from $\mathcal{A}_{s,\vec{r}}$
An oracle $\mathcal{O}$ for **Decision-RLWE**.

Want: A good approximation of $\mathbf{z} = (\sigma_1(e_1), \ldots, \sigma_1(e_k))$

Theorem ([PRS'17])

A good approximation of $\mathbf{z}$ *can be found in* $poly(n)$ *time by solving the* Oracle Hidden Center Problem.

Goal: Build a solver $\mathcal{O}_{\mathbf{z}}$ for **OHCP**$_{\mathbf{z}}$ from $\mathcal{O}$.



Description of the solver

$\mathcal{O}_{\mathbf{z}}$ creates new samples, feed them to $\mathcal{O}$.

Input: $\tilde{\mathbf{z}} = (\tilde{z}_1, \ldots, \tilde{z}_k) \in \mathbb{R}_+^n, \alpha > 0, \delta > 0$

Output: 1 if $\mathcal{O}$ accepts the sample, 0 else.

1. $s' \hookleftarrow \mathcal{U}(\mathcal{O}_{K,q})$
2. $t_1, \ldots, t_k \hookleftarrow D_{\tilde{O}(2^\alpha)}$
   $e' \hookleftarrow D_\delta$
3. $a' = \langle \mathbf{t}, \mathbf{a} \rangle$
   $b' = \langle \mathbf{b}, \mathbf{t} - \tilde{\mathbf{z}} \rangle + a's' + e'$.
4. Outputs $\mathcal{O}(a', b')$.

Description of the solver

$\mathcal{O}_{\mathbf{z}}$ creates new samples, feed them to $\mathcal{O}$.

Input: $\tilde{\mathbf{z}} = (\tilde{z}_1, \dots, \tilde{z}_k) \in \mathbb{R}_+^n, \alpha > 0, \delta > 0$

Output: 1 if $\mathcal{O}$ accepts the sample, 0 else.

1. $s' \hookleftarrow \mathcal{U}(\mathcal{O}_{K,q})$
2. $t_1, \dots, t_k \hookleftarrow D_{\widetilde{O}(2^\alpha)}$
   $e' \hookleftarrow D_\delta$
3. $a' = \langle \mathbf{t}, \mathbf{a} \rangle$
   $b' = \langle \mathbf{b}, \mathbf{t} - \tilde{\mathbf{z}} \rangle + a's' + e'$.
4. Outputs $\mathcal{O}(a', b')$.

$$b' = a'(s + s') + \underbrace{\langle \mathbf{t} - \tilde{\mathbf{z}}, \mathbf{e} \rangle + e'}_{\textbf{controlled Gaussian}}$$

$$a' = \sum_{i \leq k} a_i t_i$$

(a', b') is a valid **RLWE**-like sample

$\Leftrightarrow$

$a' \approx$ uniform

Description of the solver

$\mathcal{O}_{\mathbf{z}}$ creates new samples, feed them to $\mathcal{O}$.

Input: $\tilde{\mathbf{z}} = (\tilde{z}_1, \dots, \tilde{z}_k) \in \mathbb{R}_+^n, \alpha > 0, \delta > 0$

Output: 1 if $\mathcal{O}$ accepts the sample, 0 else.

1. $s' \hookleftarrow \mathcal{U}(\mathcal{O}_{K,q})$
2. $t_1, \dots, t_k \hookleftarrow D_{\widetilde{O}(2^\alpha)}$
   $e' \hookleftarrow D_\delta$
3. $a' = \langle \mathbf{t}, \mathbf{a} \rangle$
   $b' = \langle \mathbf{b}, \mathbf{t} - \tilde{\mathbf{z}} \rangle + a's' + e'.$
4. Outputs $\mathcal{O}(a', b')$.

$$b' = a'(s + s') + \underbrace{\langle \mathbf{t} - \tilde{\mathbf{z}}, \mathbf{e} \rangle + e'}_{\textbf{controlled Gaussian}}$$

$$a' = \sum_{i \leq k} a_i t_i$$

(a', b') is a valid **RLWE**-like sample

$\Leftrightarrow$

$a' \approx$ uniform

Result: (Leftover Hash Lemma)
The distribution of $(a_1, \dots, a_k, a')$ is statistically indistinguishable from uniform.

A ring-based Leftover Hash Lemma

Result: (Leftover Hash Lemma)
The distribution of $(a_1, \ldots, a_k, a')$ is statistically indistinguishable from uniform.

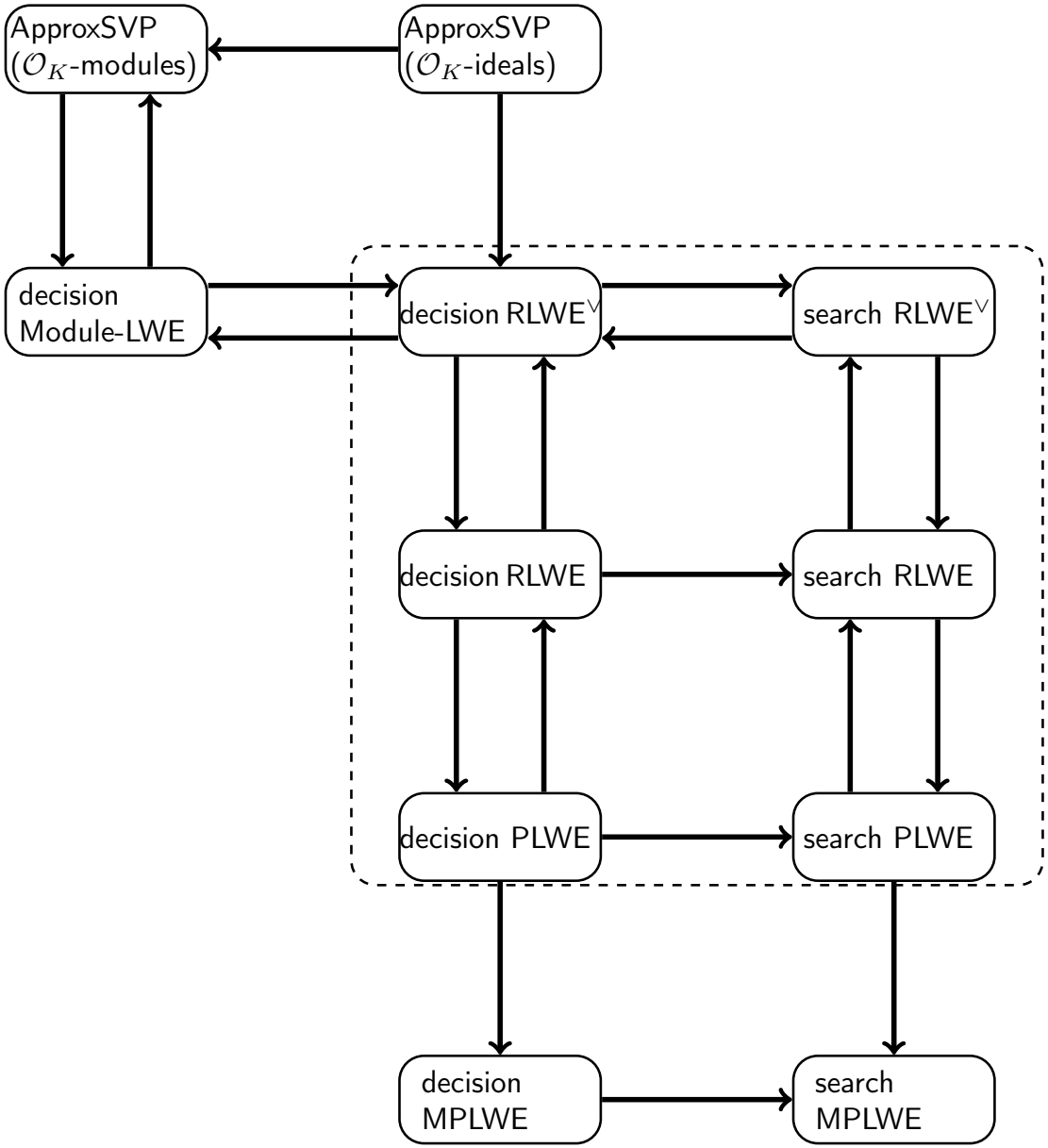
- **Idea:** Adapting Minkowski-Hlawka theorem to the ring context.
- **Main difficulty:** Lower bound on $\lambda_1(\mathbf{a}^{\perp})$.
- Tools:
  - Duality for q-ary module lattices
  - Understand solutions of $a \cdot x = b$ in the ring $\mathcal{O}_{K,q}$
  - Bound number of lattice points in a ball
  - "Smoothness parameters" for lattices

Open Problems

(A) Make reductions uniform.

(B) $\|V_f^{-1}\| \leq \widetilde{O}(n^{3.5})$ in proof vs. $\|V_f^{-1}\| \sim 1$ in practice. Improvement?

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


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 :)