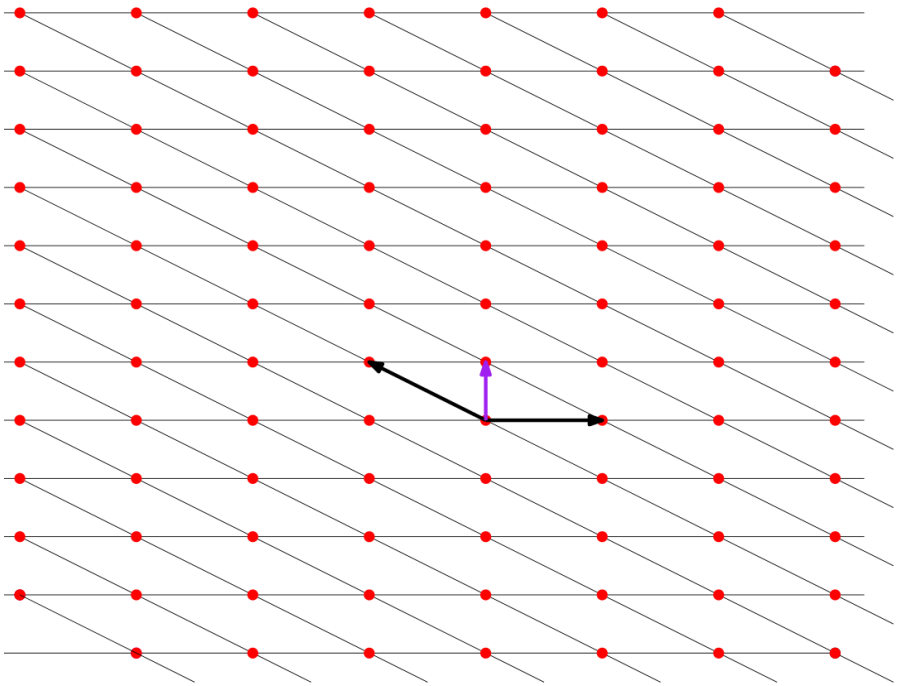
On the Ring-LWE and Polynomial-LWE problems

Miruna Rosca Damien Stehlé Alexandre Wallet

EUROCRYPT 2018

Lattices and hard problems



Lattice

Let $b_1, b_2, \ldots, b_n \in \mathbb{R}^n$ be some linearly independent vectors. The set

$$\mathcal{L}(\mathbf{B}) = \{x_1 b_1 + x_2 b_2 + \cdots + x_n b_n : x_i \in \mathbb{Z}\}$$

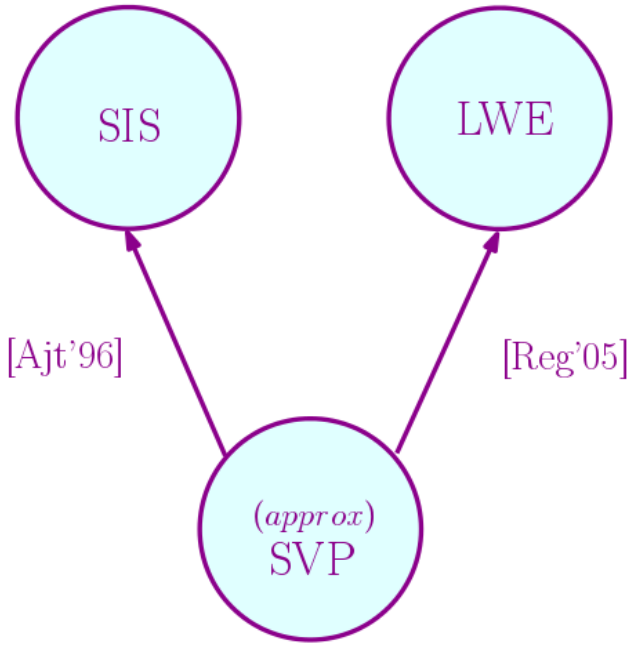
is called the lattice generated by them.

Approx SVP$_\gamma$

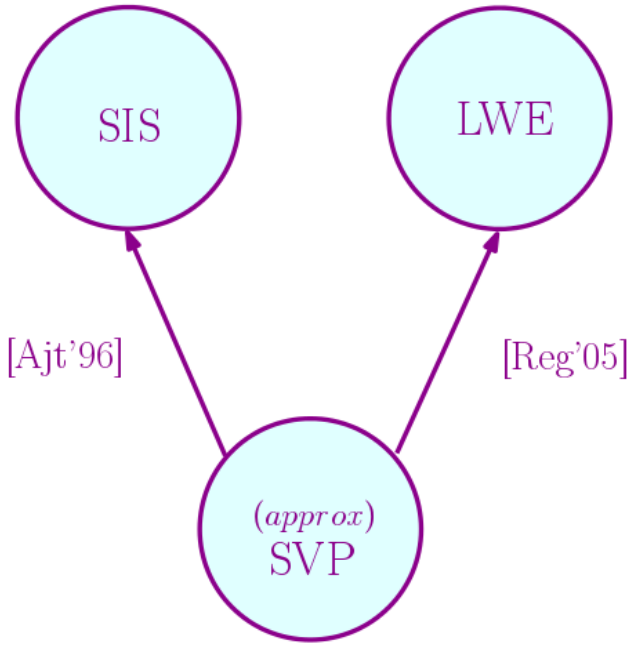
Find a nonzero $x \in \mathbb{Z}^n$ s.t.
$||\mathbf{B} \cdot x|| < \gamma \cdot \min(||\mathbf{B} \cdot y|| : y \in \mathbb{Z}^n)$.

* some of the figures borrowed from A. Wallet

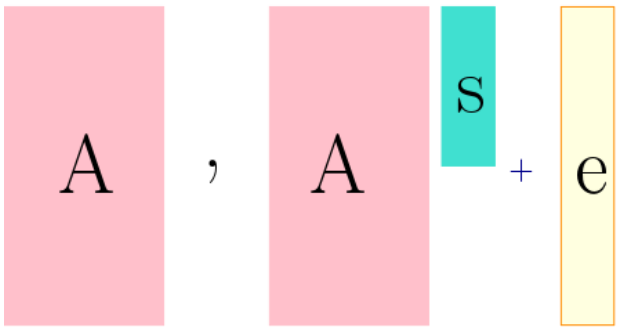
How to use lattices for crypto?



How to use lattices for crypto?

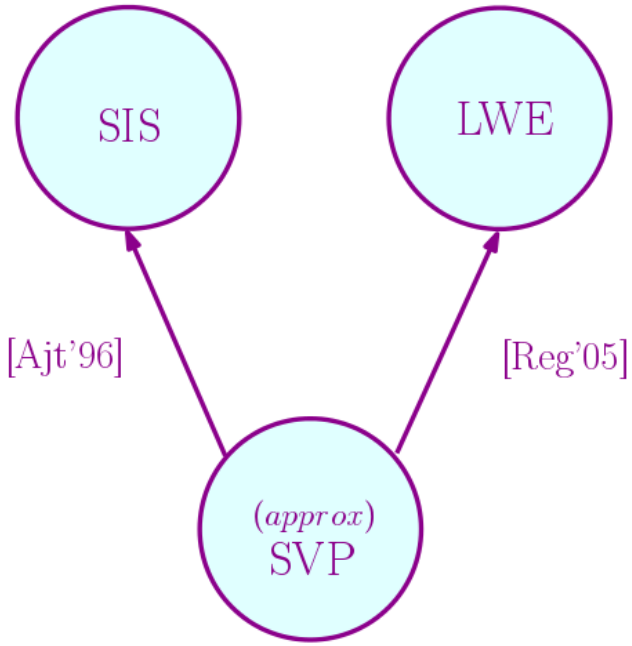


Learning with Errors:



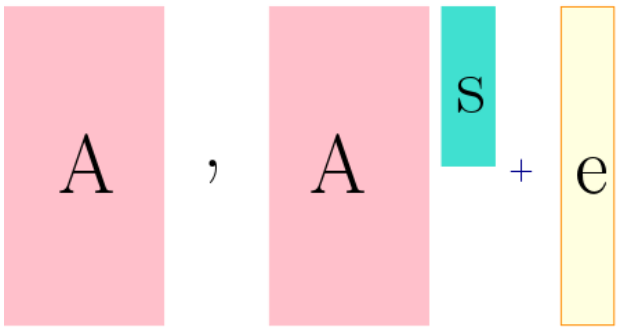
Search: Find **s**.
Decision: Distinguish this distribution from the uniform one.

How to use lattices for crypto?



efficiency?

Learning with Errors:



Search: Find **s**.
Decision: Distinguish this distribution from the uniform one.

More structure: PLWE, RLWE, RLWE$^\vee$ [SSTX09],[LPR10]

f monic, deg. n, irred.

$$R := \mathbb{Z}[x]/f$$

PLWE

$$s \in R_q := R/qR$$

$\mathcal{B}_{s,\Sigma}$ distribution

$a \hookleftarrow \mathcal{U}(R_q)$
$e \hookleftarrow \mathcal{D}_\Sigma$
$(a, b = a \cdot s + e \bmod qR)$

More structure: PLWE, RLWE, RLWE$^\vee$ [SSTX09],[LPR10]

f monic, deg. n, irred.

$$R := \mathbb{Z}[x]/f$$

$$K := \mathbb{Q}[x]/f$$

n field embeddings: σ_j

canonical embedding: $\sigma(a) = (\sigma_1(a), \ldots, \sigma_n(a))$

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

$$H = \text{Span}\{h_i\}_i$$

$$\mathcal{D}_\Sigma^H : \begin{cases} x \hookleftarrow \mathcal{D}_\Sigma \\ \text{output } \sum x_i \cdot h_i \end{cases}$$

$\mathcal{O}_K$ ring of integers of K, $\mathcal{O}_K^\vee$ the dual of $\mathcal{O}_K$

PLWE

$$s \in R_q := R/qR$$

$\mathcal{B}_{s,\Sigma}$ distribution

$a \hookleftarrow \mathcal{U}(R_q)$

$e \hookleftarrow \mathcal{D}_\Sigma$

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

More structure: PLWE, RLWE, RLWE$^\vee$ [SSTX09],[LPR10]

f monic, deg. n, irred.

$$R := \mathbb{Z}[x]/f$$

$$K := \mathbb{Q}[x]/f$$

n field embeddings: σ_j

canonical embedding: $\sigma(a) = (\sigma_1(a), \ldots, \sigma_n(a))$

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

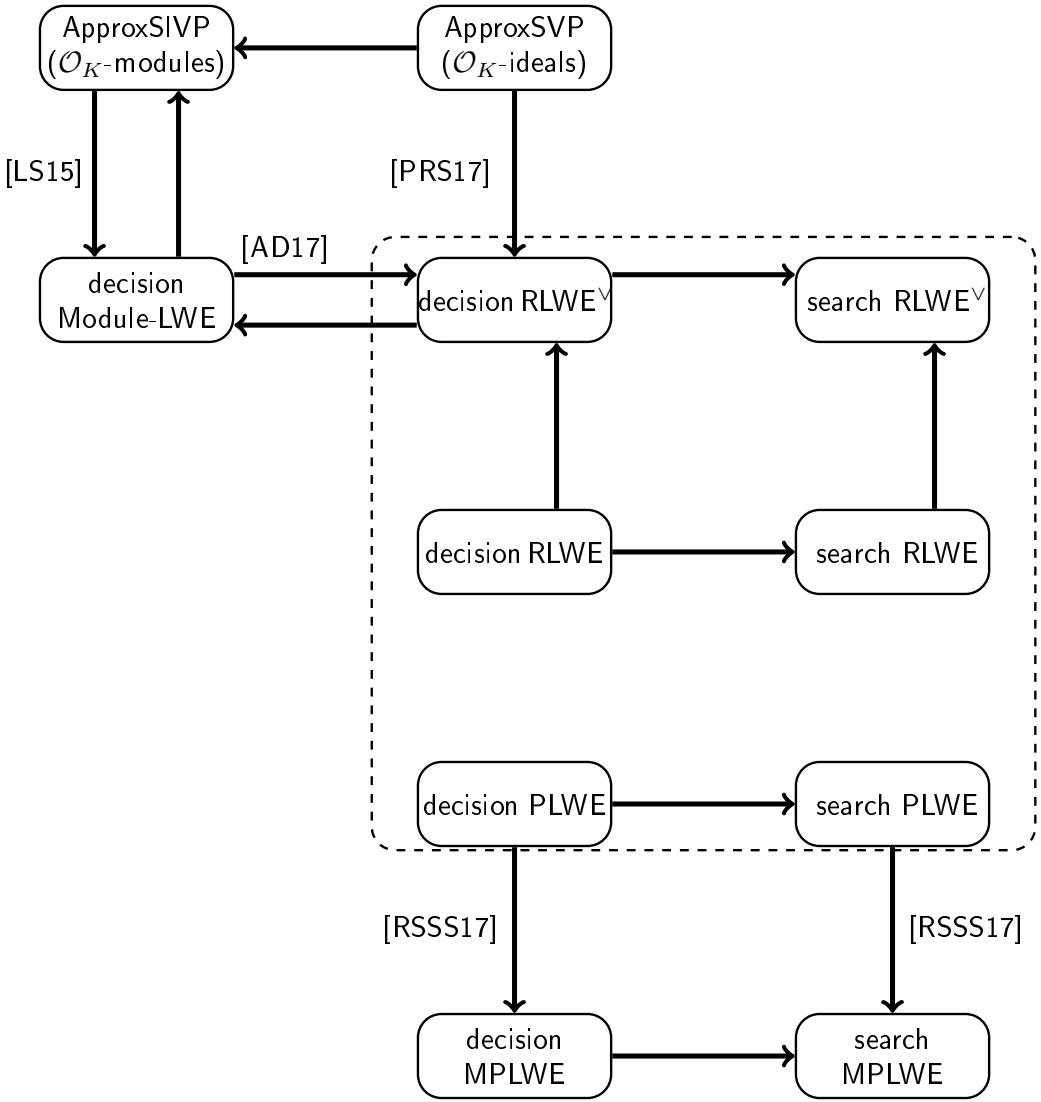
$$H = \mathsf{Span}\{h_i\}_i$$

$$\mathcal{D}_\Sigma^H : \begin{cases} x \hookleftarrow \mathcal{D}_\Sigma \\ \text{output } \sum x_i \cdot h_i \end{cases}$$

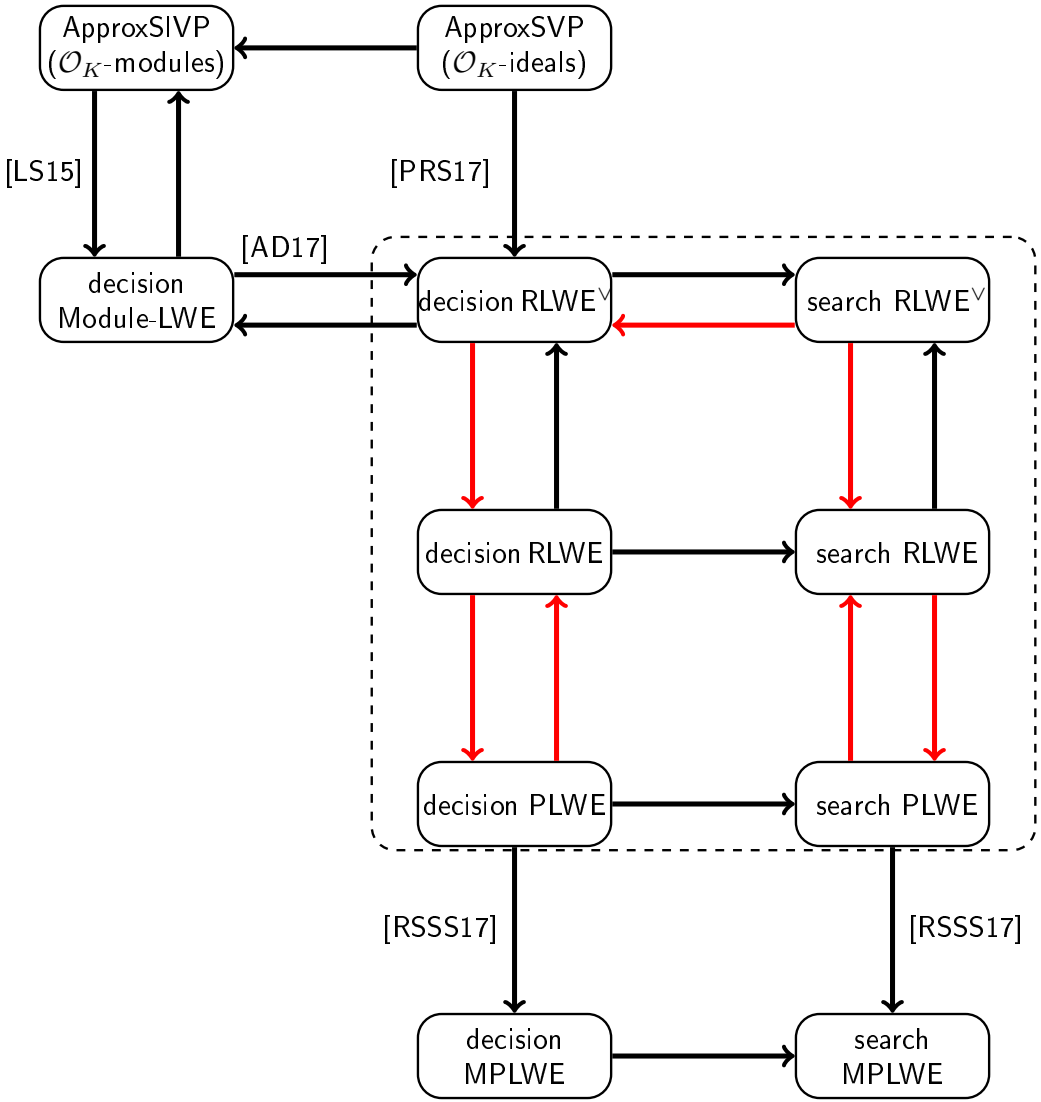
$\mathcal{O}_K$ ring of integers of K, $\mathcal{O}_K^\vee$ the dual of $\mathcal{O}_K$

PLWE	RLWE	RLWE$^\vee$
$s \in R_q := R/qR$	$s \in \mathcal{O}_{K,q} := \mathcal{O}_K/q\mathcal{O}_K$	$s \in \mathcal{O}^\vee_{K,q} := \mathcal{O}^\vee_K/q\mathcal{O}^\vee_K$
$\mathcal{B}_{s,\Sigma}$ distribution	$\mathcal{A}_{s,\Sigma}$ distribution	$\mathcal{A}^\vee_{s,\Sigma}$ distribution
$a \hookleftarrow \mathcal{U}(R_q)$ $e \hookleftarrow \mathcal{D}_\Sigma$ $(a, b = a \cdot s + e \bmod qR)$	$a \hookleftarrow \mathcal{U}(\mathcal{O}_{K,q})$ $e \hookleftarrow \mathcal{D}_\Sigma^H$ $(a, b = a \cdot s + e \bmod q\mathcal{O}_K)$	$a \hookleftarrow \mathcal{U}(\mathcal{O}_{K,q})$ $e \hookleftarrow \mathcal{D}_\Sigma^H$ $(a, b = a \cdot s + e \bmod q\mathcal{O}^\vee_K)$

State of the art and Contributions



State of the art and Contributions



From RLWE$^\vee$ to RLWE

Assume $\exists\ \mathbf{t} \in (\mathcal{O}_K^\vee)^{-1}$ such that $[\times \mathbf{t}] : \mathcal{O}_{K,q}^\vee \simeq \mathcal{O}_{K,q}$.

$$\theta_{\mathbf{t}} : \begin{array}{ccc} \mathcal{O}_{K,q} \times \mathcal{O}_{K,q}^\vee & \longrightarrow & \mathcal{O}_{K,q} \times \mathcal{O}_{K,q} \\ (a, b) & \longmapsto & (a, \mathbf{t}b \bmod q) \end{array}$$

From RLWE$^\vee$ to RLWE

Assume $\exists\ \mathbf{t} \in (\mathcal{O}_K^\vee)^{-1}$ such that $[\times \mathbf{t}] : \mathcal{O}_{K,q}^\vee \simeq \mathcal{O}_{K,q}$.

$$\theta_{\mathbf{t}} : \begin{array}{ccc} \mathcal{O}_{K,q} \times \mathcal{O}_{K,q}^\vee & \longrightarrow & \mathcal{O}_{K,q} \times \mathcal{O}_{K,q} \\ (a, b) & \longmapsto & (a, \mathbf{t}b \bmod q) \end{array}$$

$\mathcal{A}_{s,\Sigma}^\vee$ to $\mathcal{A}_{s',\Sigma'}$

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

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

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

uniform to uniform

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

$(a, \mathbf{t}b)$ uniform

From RLWE$^\vee$ to RLWE

Assume $\exists\ \mathbf{t} \in (\mathcal{O}_K^\vee)^{-1}$ such that $[\times \mathbf{t}] : \mathcal{O}_{K,q}^\vee \simeq \mathcal{O}_{K,q}$.

$$\theta_{\mathbf{t}} : \begin{array}{ccc} \mathcal{O}_{K,q} \times \mathcal{O}_{K,q}^\vee & \longrightarrow & \mathcal{O}_{K,q} \times \mathcal{O}_{K,q} \\ (a, b) & \longmapsto & (a, \mathbf{t}b \bmod q) \end{array}$$

$\mathcal{A}_{s,\Sigma}^\vee$ to $\mathcal{A}_{s',\Sigma'}$

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

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

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

Does such a $\mathbf{t}$ exist?

uniform to uniform

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

$(a, \mathbf{t}b)$ uniform

From RLWE$^\vee$ to RLWE

Assume $\exists\ \mathbf{t} \in (\mathcal{O}_K^\vee)^{-1}$ such that $[\times \mathbf{t}] : \mathcal{O}_{K,q}^\vee \simeq \mathcal{O}_{K,q}$.

$$\theta_{\mathbf{t}} : \begin{array}{ccc} \mathcal{O}_{K,q} \times \mathcal{O}_{K,q}^\vee & \longrightarrow & \mathcal{O}_{K,q} \times \mathcal{O}_{K,q} \\ (a, b) & \longmapsto & (a, \mathbf{t}b \bmod q) \end{array}$$

$\mathcal{A}_{s,\Sigma}^\vee$ to $\mathcal{A}_{s',\Sigma'}$

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

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

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

uniform to uniform

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

$(a, \mathbf{t}b)$ uniform

Does such a $\mathbf{t}$ exist?

How large is $\mathbf{t}e$?

Control the size of $\mathbf{t}$

[LPR10]

Compute $\mathbf{t}$ in $poly(n)$-time using CRT.

✓ Existence

✗ Size

Control the size of $\mathbf{t}$

[LPR10]

Compute $\mathbf{t}$ in $poly(n)$-time using CRT.

✓ Existence

✗ Size

New result

By Gaussian sampling on $(\mathcal{O}_K^\vee)^{-1}$, we can find $\mathbf{t}$ with small $\|\sigma(\mathbf{t})\|$.[1]

✓ Existence

✓ Size

Idea: show that short vectors are not all trapped in $(\mathcal{O}_K^\vee)^{-1} \cdot J$ for J a divisor of (q).

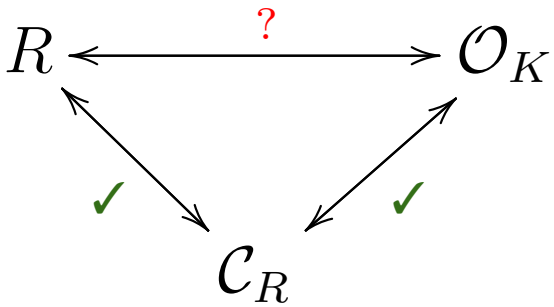
[1] It requires advice on the number field.

From RLWE to PLWE

New result

We can find $\mathbf{t}$ in **the conductor ideal** $\mathcal{C}_R := \{\mathbf{t} \in K : \mathbf{t}\mathcal{O}_K \subset R\}$ s.t.

$$[\times \mathbf{t}] : \mathcal{O}_{K,q} \simeq R_q \text{ and } \|\sigma(\mathbf{t})\| \text{ is small.}$$



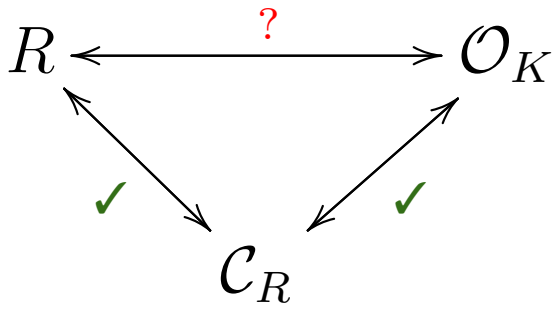
If $\mathcal{C}_R$ coprime to $q\mathcal{O}_K$ then
$\mathcal{O}_{K,q} \simeq \mathcal{C}_R/q\mathcal{C}_R \simeq R_q$.

From RLWE to PLWE

New result

We can find $\mathbf{t}$ in **the conductor ideal** $\mathcal{C}_R := \{\mathbf{t} \in K : \mathbf{t}\mathcal{O}_K \subset R\}$ s.t.

$$[\times\mathbf{t}] : \mathcal{O}_{K,q} \simeq R_q \text{ and } \|\sigma(\mathbf{t})\| \text{ is small.}$$



If $\mathcal{C}_R$ coprime to $q\mathcal{O}_K$ then
$\mathcal{O}_{K,q} \simeq \mathcal{C}_R/q\mathcal{C}_R \simeq R_q$.

$$\theta_{\mathbf{t}} : \begin{array}{ccc} \mathcal{O}_{K,q} \times \mathcal{O}_{K,q} & \longrightarrow & R_q \times R_q \\ (a, b) & \longmapsto & (\mathbf{t}a, \mathbf{t}^2 b \bmod q) \end{array}$$

$\mathcal{A}_{s,\Sigma}$ to $\mathcal{B}_{s',\Sigma'}$

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

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

uniform to uniform

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

$(\mathbf{t}a, \mathbf{t}^2 b)$ uniform

Is this really PLWE? Not yet.

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

The embedding of the error is small in H!

Is this really PLWE? Not yet.

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

The embedding of the error is small in H!

Minkowski vs. Coefficient embeddings:

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

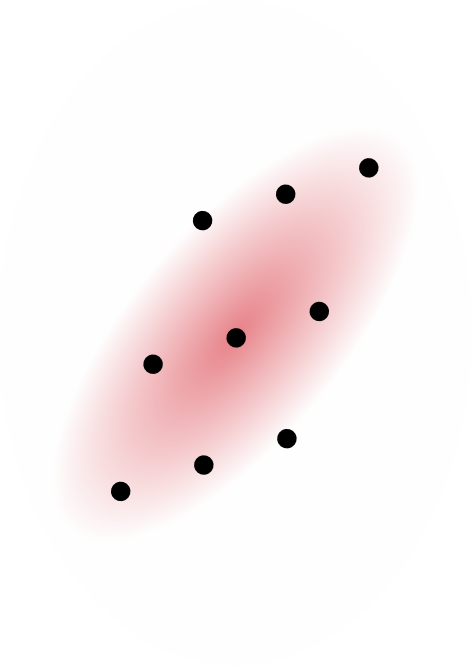
The α_i's are the roots of the polynomial f.

How small is the coefficient embedding?

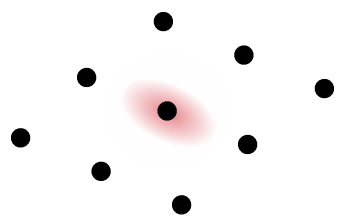
New noise: $\mathbf{V}_f{}^{-1}\sigma(e') \hookleftarrow D_{\Sigma'}$, with $\Sigma' = \mathbf{V}_f{}^{-\top}\Sigma_{\mathbf{t}}\,\mathbf{V}_f^{-1}$

The distorsion introduced by $\mathbf{V}_f^{-1}$ could be:

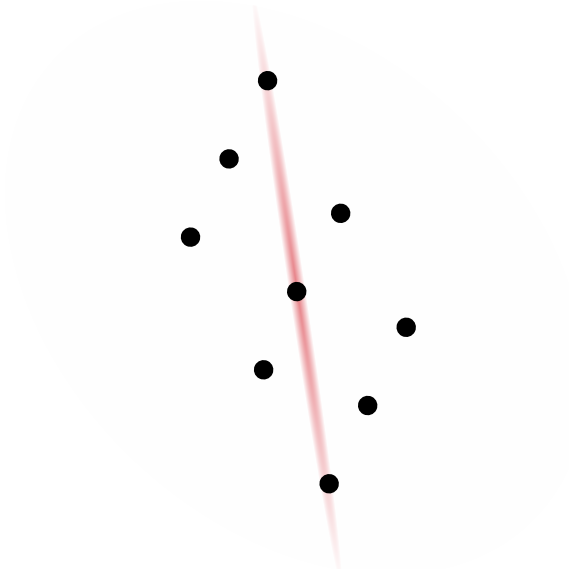
too large



reasonable



too skew



How to get a small distorsion?

$\|\mathbf{V}_f^{-1}\|_\infty$ small for $f := X^n - c \in \mathbb{Z}[X]$.

How to get a small distorsion?

$\|\mathbf{V}_f^{-1}\|_\infty$ small for $f := X^n - c \in \mathbb{Z}[X]$.

Can we find more polynomials?

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

How to get a small distorsion?

$\|\mathbf{V}_f^{-1}\|_\infty$ small for $f := X^n - c \in \mathbb{Z}[X]$.

Can we find more polynomials?

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

Idea: Try to apply a small perturbation on the roots of f and keep the norm small.

Lots of polynomials

$f = X^n - c \in \mathbb{Z}[X]$

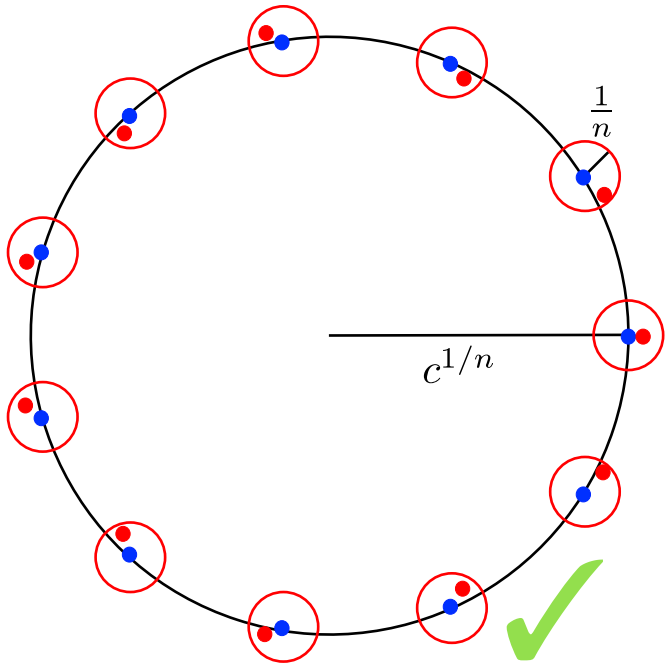
Take $P = \sum_{i=1}^{n/2} p_i X^i \in \mathbb{Z}[X]$

Perturbation: $g := f + P$

Technique: Rouché theorem

New result

For every such $g \in \mathbb{Z}[X]$, we have that $\|\mathbf{V}_g^{-1}\| \leq poly(n)$.



Search to decision

New result

There is a probabilistic poly. time reduction from search RLWE/RLWE$^\vee$ to decision RLWE/RLWE$^\vee$.

Search to decision

New result

There is a probabilistic poly. time reduction from search RLWE/RLWE$^\vee$ to decision RLWE/RLWE$^\vee$.

Technique:

- prove a LHL variant over rings and use it to create new samples

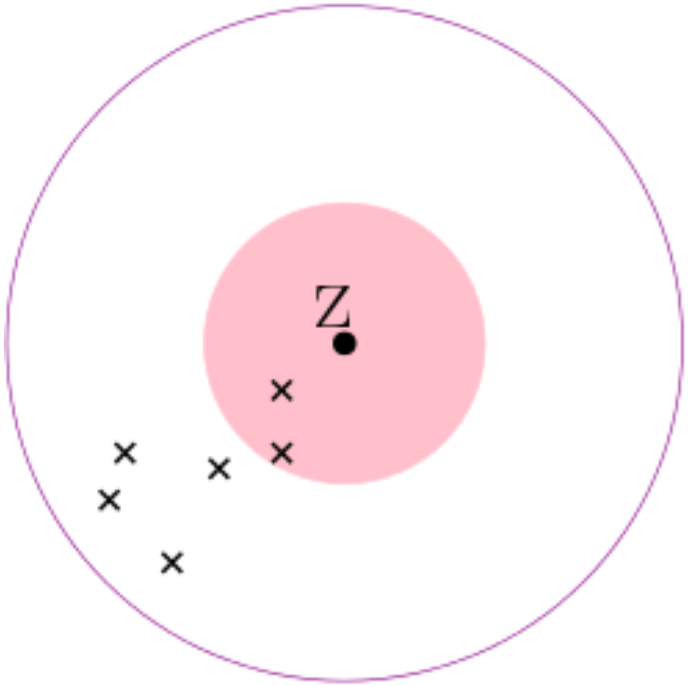
Search to decision

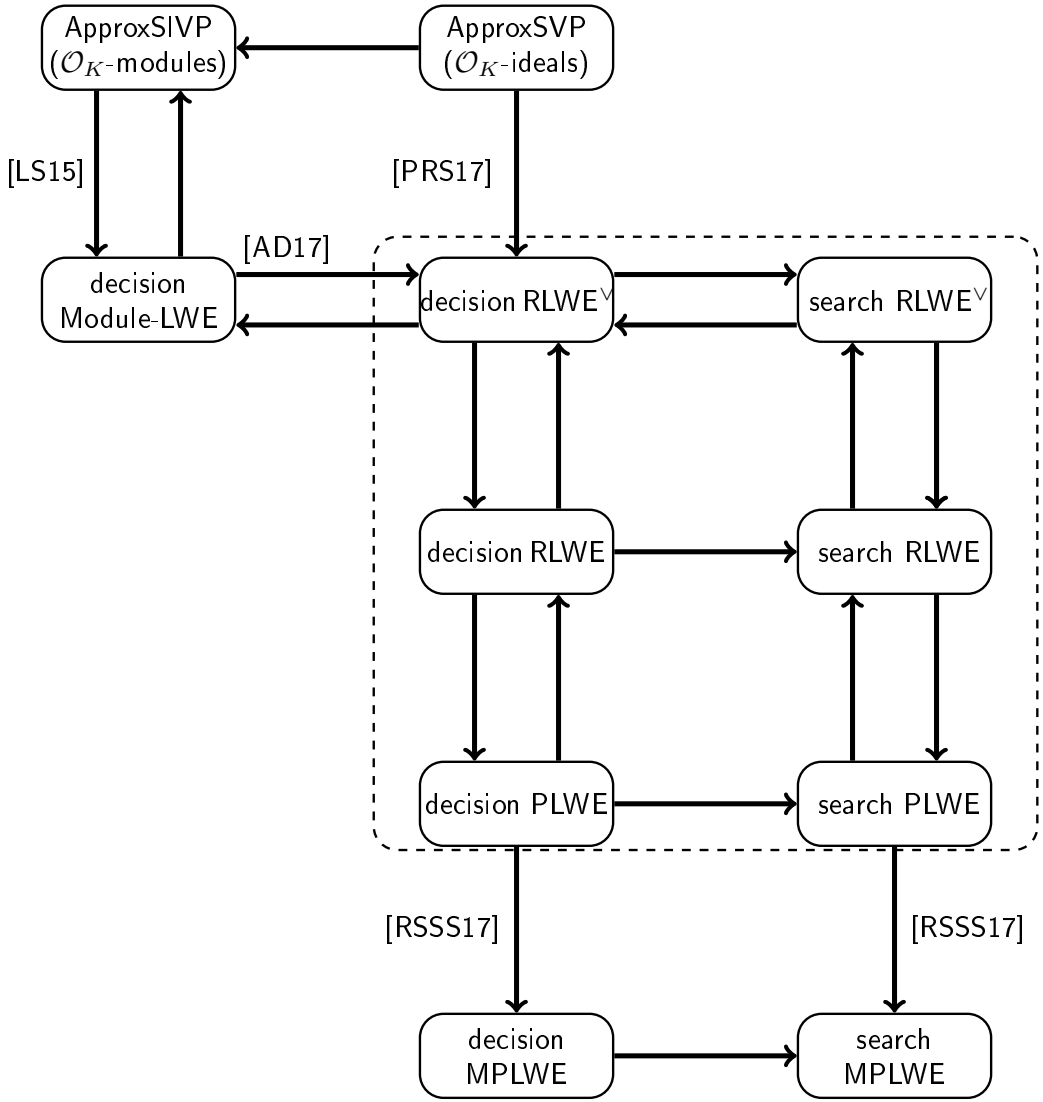
New result

There is a probabilistic poly. time reduction from search RLWE/RLWE$^\vee$ to decision RLWE/RLWE$^\vee$.

Technique:

- prove a LHL variant over rings and use it to create new samples
- find good approx. of the error by using the OHCP technique from [PRS17]
- find the secret




ApproxSIVP
($\mathcal{O}_K$-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

Thank you.