On Algebraic Embedding for Unstructured Lattices

Madalina Bolboceanu[1], Zvika Brakerski[2], Devika Sharma[2]

[1]Bitdefender, Romania, [2]Weizmann Institute of Science, Israel

PKC, April 2024

Outline of this talk

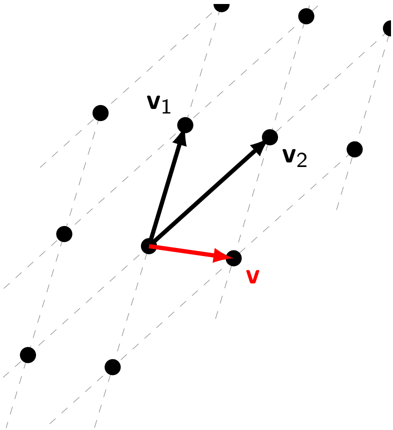
- Learning with Errors and (some of) its algebraic friends
- State of the art

Our contributions

- Improving Order-LWE (OLWE) hardness
- Gradient of hardness from Ring-LWE to LWE

Intro

Lattices



Lattice

Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ be linearly independent vectors from $\mathbb{R}^m$. Then

$$L = L(\mathbf{v}_1, \ldots, \mathbf{v}_n) = \{\sum_{i=1}^{n} a_i \mathbf{v}_i | a_i \in \mathbb{Z}\}$$

is the lattice generated by them.

ApproxSVP$_\gamma$

Find a nonzero vector $\mathbf{v} \in L$ s.t. $\|\mathbf{v}\| \leq \gamma \min_{\mathbf{x} \in L \setminus \{0\}} \|\mathbf{x}\|$.

$\gamma = \text{poly}(n) \Rightarrow$ ✓ quantum resistant

Learning with Errors (LWE) [Reg05]

- $q = \text{poly}(n)$
- ψ distribution which produces "short" elements in $\mathbb{Z}_q$ w.h.p. (e.g. D_α)

LWE

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

$A_{\mathbf{s},\psi}$ distribution

$$\begin{cases} \mathbf{a} \hookleftarrow U(\mathbb{Z}_q^n) \\ e \hookleftarrow \psi \end{cases}$$

$$(\mathbf{a}, \tfrac{1}{q}\langle \mathbf{a}, \mathbf{s}\rangle + e \bmod \mathbb{Z}).$$

Search: Given m samples from $A_{\mathbf{s},\psi}$, find $\mathbf{s}$.
Decision: Distinguish between m samples from $A_{\mathbf{s},\psi}$ and $U(\mathbb{Z}_q^n \times \mathbb{R}/\mathbb{Z})$.

Learning with Errors (LWE) [Reg05]

- $q = \text{poly}(n)$
- ψ distribution which produces "short" elements in $\mathbb{Z}_q$ w.h.p. (e.g. D_α)

LWE

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

$A_{\mathbf{s},\psi}$ distribution

$$\begin{cases} \mathbf{a} \hookleftarrow U(\mathbb{Z}_q^n) \\ e \hookleftarrow \psi \end{cases}$$

$$(\mathbf{a}, \tfrac{1}{q}\langle \mathbf{a}, \mathbf{s}\rangle + e \bmod \mathbb{Z}).$$

Search: Given m samples from $A_{\mathbf{s},\psi}$, find $\mathbf{s}$.
Decision: Distinguish between m samples from $A_{\mathbf{s},\psi}$ and $U(\mathbb{Z}_q^n \times \mathbb{R}/\mathbb{Z})$.

hard lattice problems in $\mathbb{R}^n$ $\xrightarrow{\text{[Reg05, Pei09, BLP}^{+}\text{13]}}$ search LWE $\xrightarrow{\text{[Reg05]}}$ decision LWE $\longrightarrow$ much crypto HE, IBE, etc...

Learning with Errors (LWE) [Reg05]

LWE

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

- $q = \mathrm{poly}(n)$
- ψ distribution which produces "short" elements in $\mathbb{Z}_q$ w.h.p. (e.g. D_α)

$A_{\mathbf{s},\psi}$ distribution

$$\begin{cases} \mathbf{a} \hookleftarrow U(\mathbb{Z}_q^n) \\ e \hookleftarrow \psi \end{cases}$$

$$\left(\mathbf{a}, \frac{1}{q}\langle \mathbf{a}, \mathbf{s}\rangle + e \bmod \mathbb{Z}\right).$$

Search: Given m samples from $A_{\mathbf{s},\psi}$, find $\mathbf{s}$.
Decision: Distinguish between m samples from $A_{\mathbf{s},\psi}$ and $U(\mathbb{Z}_q^n \times \mathbb{R}/\mathbb{Z})$.

hard lattice problems in $\mathbb{R}^n$ $\xrightarrow{\text{[Reg05, Pei09, BLP}^+\text{13]}}$ search LWE $\xrightarrow{\text{[Reg05]}}$ decision LWE $\longrightarrow$ much crypto HE, IBE, etc...

✗ not so efficient

Add structure: Ring-LWE [LPR10], Order-LWE [BBPS19]

q integer[1]
$f \in \mathbb{Z}[x]$ monic, irreducible, degree n.
$K = \mathbb{Q}[x]/(f)$ number field.

ψ distribution which produces "short" elements in K w.h.p.

can be any ideal modulus of $\mathcal{O}$.

Add structure: Ring-LWE [LPR10], Order-LWE [BBPS19]

q integer[1]
$f \in \mathbb{Z}[x]$ monic, irreducible, degree n.
$K = \mathbb{Q}[x]/(f)$ number field.

ψ distribution which produces "short" elements in K w.h.p.

$\mathcal{O}_K$ ring of integers
e.g. $\mathcal{O}_K = \mathbb{Z}[x]/(f)$, if f = cyclotomic

can be any ideal modulus of $\mathcal{O}$.

Add structure: Ring-LWE [LPR10], Order-LWE [BBPS19]

q integer[1]
$f \in \mathbb{Z}[x]$ monic, irreducible, degree n.
$K = \mathbb{Q}[x]/(f)$ number field.

ψ distribution which produces "short" elements in K w.h.p.

$\mathcal{O}_K$ ring of integers
$\mathcal{O}_K^\vee$ its *dual*

RLWE

$$s \in \mathcal{O}_{K,q}^\vee := \mathcal{O}_K^\vee / q\mathcal{O}_K^\vee$$

$\mathcal{A}_{s,\psi}$ distribution

$$\begin{cases} a \hookleftarrow U(\mathcal{O}_{K,q}) \\ e \hookleftarrow \psi \end{cases}$$

$$\left(a, \frac{1}{q} a \cdot s + e \bmod \mathcal{O}_K^\vee\right).$$

---

[1] can be any ideal modulus of $\mathcal{O}$.

Add structure: Ring-LWE [LPR10], Order-LWE [BBPS19]

q integer[1]
$f \in \mathbb{Z}[x]$ monic, irreducible, degree n.
$K = \mathbb{Q}[x]/(f)$ number field.

ψ distribution which produces "short" elements in K w.h.p.

$\mathcal{O}_K$ ring of integers
$\mathcal{O}_K^\vee$ its *dual*

RLWE

$$s \in \mathcal{O}_{K,q}^\vee := \mathcal{O}_K^\vee / q\mathcal{O}_K^\vee$$

$\mathcal{A}_{s,\psi}$ distribution

$$\begin{cases} a \hookleftarrow U(\mathcal{O}_{K,q}) \\ e \hookleftarrow \psi \end{cases}$$

$$(a, \frac{1}{q} a \cdot s + e \bmod \mathcal{O}_K^\vee).$$

$\mathcal{O}$ order (subring of $\mathcal{O}_K$ of finite index)

e.g. $\mathcal{O} = \mathbb{Z}[x]/(f), \mathcal{O}_K$

can be any ideal modulus of $\mathcal{O}$.

Add structure: Ring-LWE [LPR10], Order-LWE [BBPS19]

q integer[1]
$f \in \mathbb{Z}[x]$ monic, irreducible, degree n.
$K = \mathbb{Q}[x]/(f)$ number field.

ψ distribution which produces "short" elements in K w.h.p.

$\mathcal{O}_K$ ring of integers
$\mathcal{O}_K^\vee$ its *dual*

RLWE

$$s \in \mathcal{O}_{K,q}^\vee := \mathcal{O}_K^\vee / q\mathcal{O}_K^\vee$$

$\mathcal{A}_{s,\psi}$ distribution

$$\begin{cases} a \hookleftarrow U(\mathcal{O}_{K,q}) \\ e \hookleftarrow \psi \end{cases}$$
$$(a, \frac{1}{q} a \cdot s + e \bmod \mathcal{O}_K^\vee).$$

$\mathcal{O}$ order (subring of $\mathcal{O}_K$ of finite index)
$\mathcal{O}^\vee$ its *dual*

OLWE

$$s \in \mathcal{O}_q^\vee := \mathcal{O}^\vee / q\mathcal{O}^\vee$$

$\mathcal{O}_{s,\psi}$ distribution

$$\begin{cases} a \hookleftarrow U(\mathcal{O}_q) \\ e \hookleftarrow \psi \end{cases}$$
$$(a, \frac{1}{q} a \cdot s + e \bmod \mathcal{O}^\vee).$$

Search and **Decision** problems are defined as before.

[1] can be any ideal modulus of $\mathcal{O}$.

Add structure: Ring-LWE [LPR10], Order-LWE [BBPS19]

q integer[1]
$f \in \mathbb{Z}[x]$ monic, irreducible, degree n.
$K = \mathbb{Q}[x]/(f)$ number field.

ψ distribution which produces "short" elements in K w.h.p.

$\mathcal{O}_K$ ring of integers
$\mathcal{O}_K^\vee$ its *dual*

RLWE=$\mathcal{O}_K$-LWE

$$s \in \mathcal{O}_{K,q}^\vee := \mathcal{O}_K^\vee / q\mathcal{O}_K^\vee$$

$\mathcal{A}_{s,\psi}$ distribution

$$\begin{cases} a \hookleftarrow U(\mathcal{O}_{K,q}) \\ e \hookleftarrow \psi \end{cases}$$
$$\left(a, \frac{1}{q} a \cdot s + e \bmod \mathcal{O}_K^\vee\right).$$

$\mathcal{O}$ order (subring of $\mathcal{O}_K$ of finite index)
$\mathcal{O}^\vee$ its *dual*

OLWE=$\mathcal{O}$-LWE

$$s \in \mathcal{O}_q^\vee := \mathcal{O}^\vee / q\mathcal{O}^\vee$$

$\mathcal{O}_{s,\psi}$ distribution

$$\begin{cases} a \hookleftarrow U(\mathcal{O}_q) \\ e \hookleftarrow \psi \end{cases}$$
$$\left(a, \frac{1}{q} a \cdot s + e \bmod \mathcal{O}^\vee\right).$$

Search and **Decision** problems are defined as before.

---

can be any ideal modulus of $\mathcal{O}$.

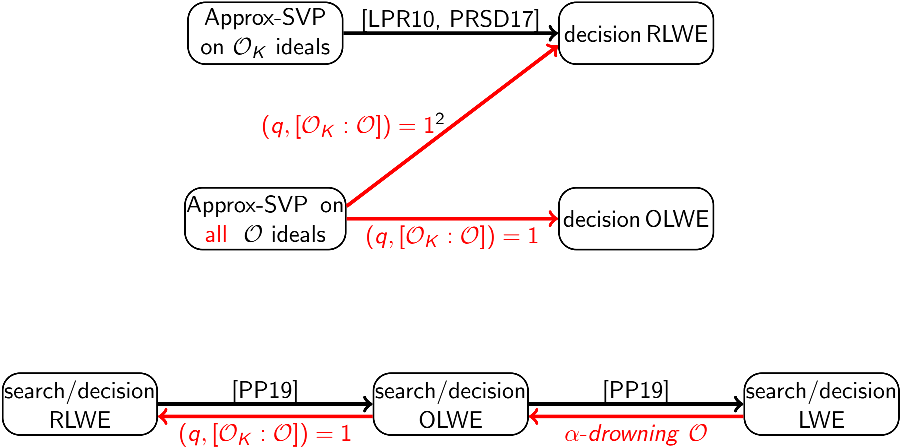
State of the art and contributions

Approx-SVP on $\mathcal{O}_K$ ideals $\xrightarrow{\text{[LPR10, PRSD17]}}$ decision RLWE

Approx-SVP on special $\mathcal{O}$ ideals $\xrightarrow{\text{[BBPS19]}}$ decision OLWE

search/decision RLWE $\xrightarrow{\text{[PP19]}}$ search/decision OLWE $\xrightarrow{\text{[PP19]}}$ search/decision LWE

State of the art and contributions



results hold for an ideal modulus $\mathcal{Q}$ with coprimality properties.

Improving OrderLWE hardness

How to get OLWE hardness?

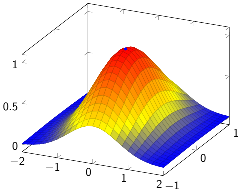
Approx-SVP on all $\mathcal{O}$ ideals $\xrightarrow{(q, [\mathcal{O}_K : \mathcal{O}]) = 1}$ decision OLWE

How to get OLWE hardness?

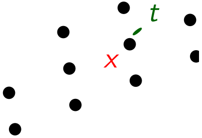
$$\begin{tikzcd}[column sep=huge] \boxed{\begin{array}{c}\text{Approx-SVP}\\ \text{on all } \mathcal{O} \text{ ideals}\end{array}} \arrow[r, "{(q,[\mathcal{O}_K:\mathcal{O}])=1}"'] & \boxed{\text{decision OLWE}} \end{tikzcd}$$

Follow [PRSD17, BBPS19] hardness blueprint:

- focus only on the BDD-to-OLWE conversion.



$+$



$=$ OLWE samples
$\left(a, \frac{1}{q} a \cdot s + e \bmod \mathcal{O}^\vee\right)$

Discrete Gaussian over
$\mathcal{I} \subseteq \mathcal{O}$: $z \in \mathcal{I}$

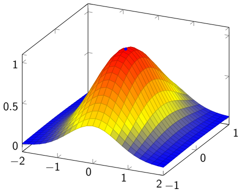
BDD instance:
$t = x + e', \ x \in \mathcal{I}^\vee$

Idea: 'Cancel' $\mathcal{I}$: find *compatible* maps:

$$z \in \frac{\mathcal{I}}{q\mathcal{I}} \xrightarrow[f]{\sim} a \in \frac{\mathcal{O}}{q\mathcal{O}}$$

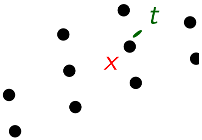
$$x \in \frac{\mathcal{I}^\vee}{q\mathcal{I}^\vee} \xrightarrow[g^{-1}]{\sim} s \in \frac{\mathcal{O}^\vee}{q\mathcal{O}^\vee}$$

BDD-to-OLWE conversion



Discrete Gaussian over $\mathcal{I} \subseteq \mathcal{O}$: $z \in \mathcal{I}$

$+$



BDD instance: $t = x + e'$, $x \in \mathcal{I}^\vee$

$=$ OLWE samples $(a, \frac{1}{q} a \cdot s + e \bmod \mathcal{O}^\vee)$

Idea: 'Cancel' $\mathcal{I}$: find *compatible* maps:

$$z \in \frac{\mathcal{I}}{q\mathcal{I}} \xrightarrow[f]{\sim} a \in \frac{\mathcal{O}}{q\mathcal{O}}$$

$$x \in \frac{\mathcal{I}^\vee}{q\mathcal{I}^\vee} \xrightarrow[g^{-1}]{\sim} s \in \frac{\mathcal{O}^\vee}{q\mathcal{O}^\vee}$$

Cancellation Lemma [BBPS19]

f and g exist for a subset of $\mathcal{O}$ ideals $\mathcal{I}$.

Can we get f and g for all $\mathcal{I}$'s?

New Cancellation Lemma

f and g exist[3], for all $\mathcal{O}$ ideals, if $(q, [\mathcal{O}_K : \mathcal{O}]) = 1$.

[3] efficiently computable and invertible, if given advice on K and factorization of $q\mathcal{O}$.

Can we get f and g for all $\mathcal{I}$'s?

New Cancellation Lemma

f and g exist[3], for all $\mathcal{O}$ ideals, if $(q, [\mathcal{O}_K : \mathcal{O}]) = 1$.

Idea:

[3] efficiently computable and invertible, if given advice on K and factorization of $q\mathcal{O}$.

Can we get f and g for all $\mathcal{I}$'s?

New Cancellation Lemma

f and g exist[3], for all $\mathcal{O}$ ideals, if $(q, [\mathcal{O}_K : \mathcal{O}]) = 1$.

Idea:

- Embed $\mathcal{I}$ in a *good* $\mathcal{P}$ such that:
  - can apply [BBPS19]: $\frac{\mathcal{P}}{q\mathcal{P}} \xrightarrow{\sim} \frac{\mathcal{O}}{q\mathcal{O}}$.
  - can apply [PP19]: $\frac{\mathcal{I}}{q\mathcal{I}} \overset{\sim}{\hookrightarrow} \frac{\mathcal{P}}{q\mathcal{P}}$.

How to find a good $\mathcal{P}$:

- Jordan-Hölder filtration

[3] efficiently computable and invertible, if given advice on K and factorization of $q\mathcal{O}$.

Can we get f and g for all $\mathcal{I}$'s?

New Cancellation Lemma

f and g exist[3], for all $\mathcal{O}$ ideals, if $(q, [\mathcal{O}_K : \mathcal{O}]) = 1$.

Idea:

- Embed $\mathcal{I}$ in a *good* $\mathcal{P}$ such that:
  - can apply [BBPS19]: $\frac{\mathcal{P}}{q\mathcal{P}} \xrightarrow{\sim} \frac{\mathcal{O}}{q\mathcal{O}}$.
  - can apply [PP19]: $\frac{\mathcal{I}}{q\mathcal{I}} \overset{\sim}{\hookrightarrow} \frac{\mathcal{P}}{q\mathcal{P}}$.
- Compose maps to get f (and g).

How to find a good $\mathcal{P}$:

- Jordan-Hölder filtration

[3] efficiently computable and invertible, if given advice on K and factorization of $q\mathcal{O}$.

How to get RLWE hardness?

$$\boxed{\text{Approx-SVP on all } \mathcal{O} \text{ ideals}} \xrightarrow[(q,[\mathcal{O}_K:\mathcal{O}])=1]{} \boxed{\text{decision OLWE}} \xrightarrow[(q,[\mathcal{O}_K:\mathcal{O}])=1]{} \boxed{\text{decision RLWE}}$$

Idea: Use $t \in \mathcal{C}_{\mathcal{O}} = \{x \in K | x\mathcal{O}_K \subseteq \mathcal{O}\}$ (*the conductor ideal of* $\mathcal{O}$):

$$(a, b) \longmapsto (a, tb).$$

- similar proof as in [RSW18, BBPS19].
- existence of short t: [RSW18, BBPS19].

Gradient of hardness

from Ring-LWE to LWE

Gradient of hardness

K number field
q LWE modulus, p coprime with q.
$p\mathcal{O}_K = \mathcal{P}_1 \cdot \ldots \cdot \mathcal{P}_t$, for prime ideals $\mathcal{P}_i$. Then,

$$\mathcal{O}_K \supseteq \mathbb{Z} + \mathcal{P}_1 \supseteq \mathbb{Z} + \mathcal{P}_1 \cdot \mathcal{P}_2 \supseteq \ldots \supseteq \mathbb{Z} + p\mathcal{O}_K.$$

preserves error

$$\begin{tikzcd}
\boxed{\begin{array}{c}\text{search/decision}\\ \mathcal{O}_K\text{-LWE}\end{array}} \arrow[r] & \boxed{\begin{array}{c}\text{search/decision}\\ \mathbb{Z}+\mathcal{P}_1\text{-LWE}\end{array}} \arrow[r] & \boxed{\begin{array}{c}\text{search/decision}\\ \mathbb{Z}+\mathcal{P}_1\mathcal{P}_2\text{-LWE}\end{array}} \arrow[r] & \cdots \arrow[r] & \boxed{\begin{array}{c}\text{search/decision}\\ \mathbb{Z}+p\mathcal{O}_K\text{-LWE}\end{array}} \\
 & & & & \boxed{\begin{array}{c}\text{search/decision}\\ \text{LWE}\end{array}}
\end{tikzcd}$$

all black arrows are special cases of [PP19].

Gradient of hardness

K number field
q LWE modulus, p coprime with q.
$p\mathcal{O}_K = \mathcal{P}_1 \cdot \ldots \cdot \mathcal{P}_t$, for prime ideals $\mathcal{P}_i$. Then,

$$\mathcal{O}_K \supseteq \mathbb{Z} + \mathcal{P}_1 \supseteq \mathbb{Z} + \mathcal{P}_1 \cdot \mathcal{P}_2 \supseteq \ldots \supseteq \mathbb{Z} + p\mathcal{O}_K .$$

preserves error

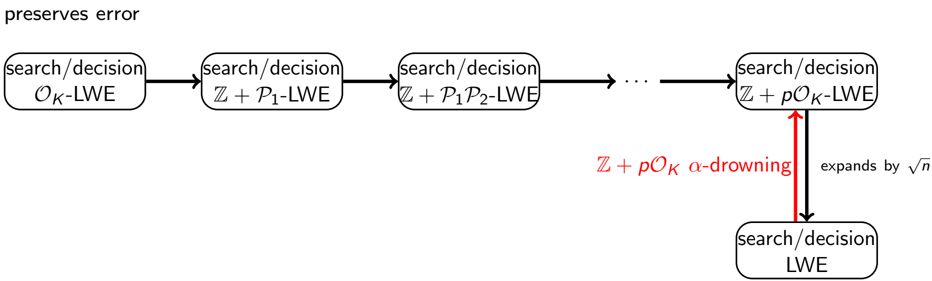
$$\begin{tikzcd}
\begin{array}{c}\text{search/decision}\\ \mathcal{O}_K\text{-LWE}\end{array} \arrow[r] & \begin{array}{c}\text{search/decision}\\ \mathbb{Z}+\mathcal{P}_1\text{-LWE}\end{array} \arrow[r] & \begin{array}{c}\text{search/decision}\\ \mathbb{Z}+\mathcal{P}_1\mathcal{P}_2\text{-LWE}\end{array} \arrow[r] & \cdots \arrow[r] & \begin{array}{c}\text{search/decision}\\ \mathbb{Z}+p\mathcal{O}_K\text{-LWE}\end{array} \arrow[d, "\text{expands by } \sqrt{n}"] \\
 & & & & \begin{array}{c}\text{search/decision}\\ \text{LWE}\end{array}
\end{tikzcd}$$

all black arrows are special cases of [PP19].

Gradient of hardness

K number field
q LWE modulus, p coprime with q.
$p\mathcal{O}_K = \mathcal{P}_1 \cdot \ldots \cdot \mathcal{P}_t$, for prime ideals $\mathcal{P}_i$. Then,

$$\mathcal{O}_K \supseteq \mathbb{Z} + \mathcal{P}_1 \supseteq \mathbb{Z} + \mathcal{P}_1 \cdot \mathcal{P}_2 \supseteq \ldots \supseteq \mathbb{Z} + p\mathcal{O}_K.$$



all black arrows are special cases of [PP19].

α-drowning orders

Let $e \hookleftarrow D_\alpha$.

How does $e \bmod \mathcal{O}^\vee$ look like?

α-drowning orders

Let $e \hookleftarrow D_\alpha$.

How does e mod $\mathcal{O}^\vee$ look like?

Take $(\mathbf{e}_0, \ldots, \mathbf{e}_{n-1})$ its coefficients w.r.t $\mathbb{Z}$-basis of $\mathcal{O}^\vee$ and mod $\mathbb{Z}$.

α-drowning orders

Let $e \hookleftarrow D_\alpha$.

How does e mod $\mathcal{O}^\vee$ look like?

Take $(\mathbf{e}_0, \ldots, \mathbf{e}_{n-1})$ its coefficients w.r.t $\mathbb{Z}$-basis of $\mathcal{O}^\vee$ and mod $\mathbb{Z}$.

$\mathcal{O}$ is α-drowning if for $e \hookleftarrow D_\alpha$
$$\begin{cases} \mathbf{e}_0 \bmod \mathbb{Z} \leftarrow D_{\alpha\sqrt{n}} \bmod \mathbb{Z} \\ (\mathbf{e}_1, \ldots, \mathbf{e}_{n-1}) | \mathbf{e}_0 = x \bmod \mathbb{Z}^{n-1} \overset{\text{s.i.}}{\approx} U((\mathbb{R}/\mathbb{Z})^{n-1}). \end{cases}$$

α-drowning orders

Let $e \hookleftarrow D_\alpha$.

How does e mod $\mathcal{O}^\vee$ look like?

Take $(\mathbf{e}_0, \ldots, \mathbf{e}_{n-1})$ its coefficients w.r.t $\mathbb{Z}$-basis of $\mathcal{O}^\vee$ and mod $\mathbb{Z}$.

$\mathcal{O}$ is α-drowning if for $e \hookleftarrow D_\alpha$
$$\begin{cases} \mathbf{e}_0 \bmod \mathbb{Z} \leftarrow D_{\alpha\sqrt{n}} \bmod \mathbb{Z} \\ (\mathbf{e}_1, \ldots, \mathbf{e}_{n-1}) | \mathbf{e}_0 = x \bmod \mathbb{Z}^{n-1} \overset{\text{s.i.}}{\approx} U((\mathbb{R}/\mathbb{Z})^{n-1}). \end{cases}$$

K =power-of-two cyclotomic, $\mathcal{O} = \mathbb{Z} + p\mathcal{O}_K$ is α-drowning for $p >> \frac{1}{\alpha}$.

LWE-OLWE equivalence

$$\boxed{\begin{array}{c}\text{search/decision}\\ \text{OLWE}\end{array}} \underset{\alpha\text{-drowning } \mathcal{O}}{\overset{\text{[PP19]}}{\rightleftarrows}} \boxed{\begin{array}{c}\text{search/decision}\\ \text{LWE}\end{array}}$$

Idea:

- $\{p_i\}_i$ $\mathbb{Z}$-basis of $\mathcal{O}$, $p_0 = 1$, $\{p_i^\vee\}_i$ *dual* $\mathbb{Z}$*-basis of* $\mathcal{O}^\vee$
- $u_1, \ldots, u_{n-1} \hookleftarrow U(\mathbb{R}/\mathbb{Z})$:

$$(\mathbf{a}, b_0) \longmapsto (a = \sum \mathbf{a}_i p_i, b = b_0 p_0^\vee + \sum u_i p_i^\vee).$$

$A_{\mathbf{s},D_{\alpha\sqrt{n}}}$ to $\mathcal{O}_{s,D_\alpha}$

If $(\mathbf{a}, b_0 = \frac{1}{q}\langle \mathbf{a}, \mathbf{s}\rangle + e_0)$:

$b \overset{s.i.}{\approx} \frac{1}{q} a \cdot s + e$, as

$e_0 p_0^\vee + \sum u_i p_i^\vee \overset{s.i.}{\approx} e \hookleftarrow D_\alpha$ ($\mathcal{O}$ α-drowning)

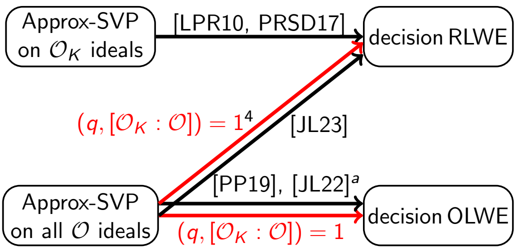
$s = \sum \mathbf{s}_i p_i^\vee$

uniform to uniform

If $(\mathbf{a}, b_0) \hookleftarrow$ uniform:

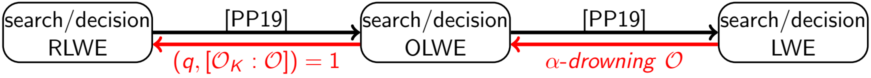
(a, b_0) uniform

Summary and follow-up works



[JL23] has fixed penalty error, perhaps larger.

same approximation factor



---

our results hold for an ideal modulus $\mathcal{Q}$ with coprimality properties.

[PP19] holds for same coprimality property on $\mathcal{Q}$.

[JL22], [JL23] hold only for integer modulus q.

Thank you.