Hawk: Module LIP makes lattice signatures fast, compact and simple

Léo Ducas
Eamonn W. Postlethwaite
Ludo N. Pulles
Wessel van Woerden

CWI

Genealogy:

[DvW22]: signatures from "LIP"

worst case → average case

suggestion of $\mathbb{Z}^n$

Genealogy:

[DvW22]: signatures from "LIP"

worst case → average case

suggestion of $\mathbb{Z}^n$

+ module structure →

NTRU lattices with determinant 1

redefine and prove

worst case → average case

Genealogy:

[DvW22]: signatures from "LIP"

worst case → average case

suggestion of $\mathbb{Z}$"

+ module structure

NTRU lattices with determinant 1

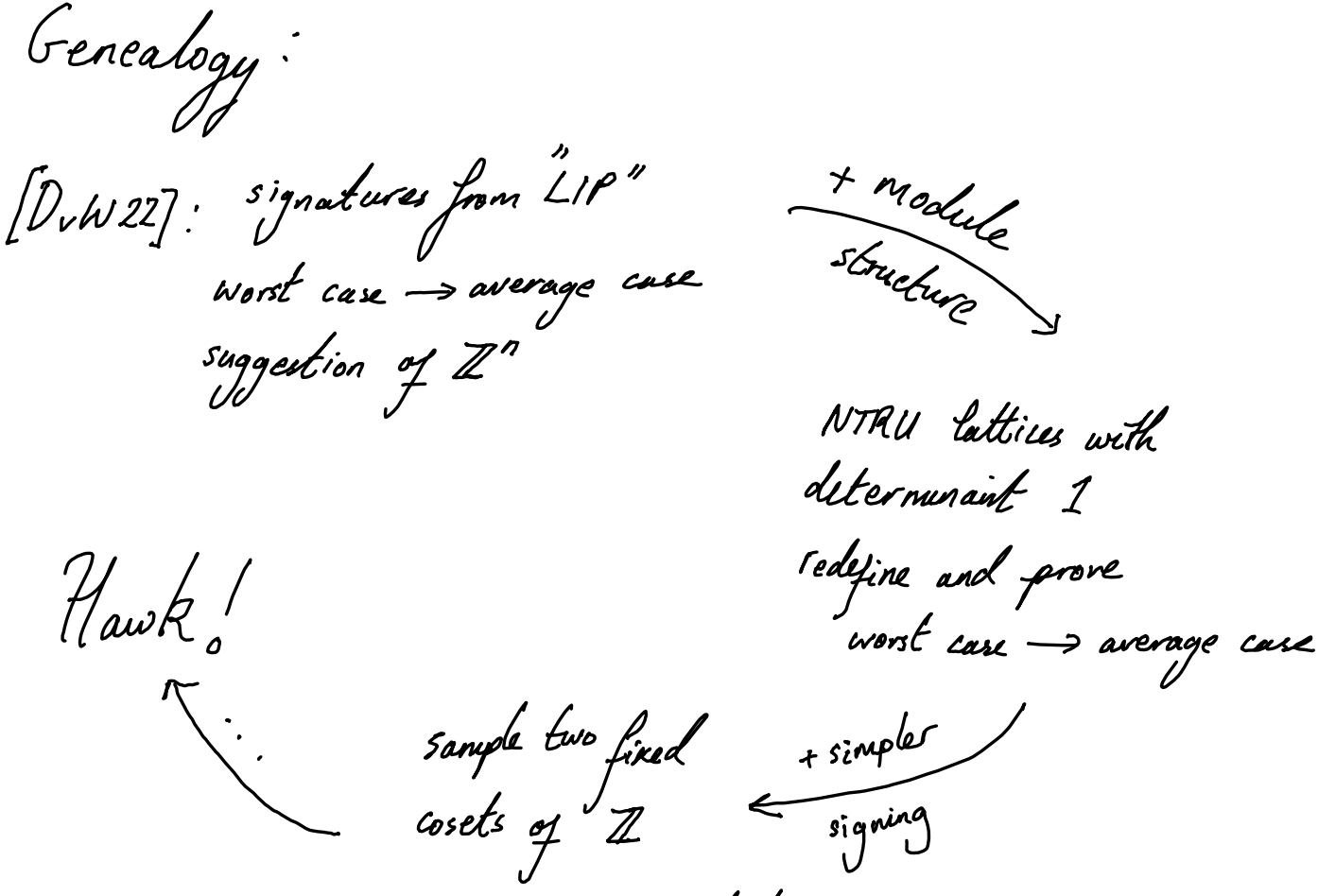
redefine and prove

worst case → average case

+ simpler signing

sample two fixed cosets of $\mathbb{Z}$

ROM-SUF-CMA reduction to "omSVP"


Genealogy:
[DvW22]: signatures from "LIP"
worst case → average case
suggestion of ℤ"
+ module structure
NTRU lattices with determinant 1
redefine and prove
worst case → average case
+ simpler signing
sample two fixed cosets of ℤ
...
Hawk!
ROM-SUF-CMA reduction to "omSVP"

Primer on LIP:

Lattice $B \in \mathbb{R}^{n \times n}$ linearly independent columns.

$$\mathcal{L} = \mathcal{L}(B) = B \cdot \mathbb{Z}^n = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\}.$$

Primer on LIP:

Lattice $B \in \mathbb{R}^{n \times n}$ linearly independent columns.

$$\mathcal{L} = \mathcal{L}(B) = B \cdot \mathbb{Z}^n = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\}.$$

Change of Basis: Ring R then $U \in R^{n \times n}$ has

$$U \in GL_n(R) \iff \det(U) \in R^{\times}.$$

Primer on LIP:

Lattice $B \in \mathbb{R}^{n \times n}$ linearly independent columns.

$$\mathcal{L} = \mathcal{L}(B) = B \cdot \mathbb{Z}^n = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\}.$$

Change of Basis: Ring R then $U \in R^{n \times n}$ has

$$U \in GL_n(R) \iff \det(U) \in R^\times.$$

E.g. $R = \mathbb{Z} \longrightarrow \det(U) \in \{1, -1\}$,

$R = \mathcal{O}_K \longrightarrow \det(U) \in \mathcal{O}_K^\times \iff$ all elements of norm 1

Primer on LIP:

Lattice $B \in \mathbb{R}^{n \times n}$ linearly independent columns.

$$\mathcal{L} = \mathcal{L}(B) = B \cdot \mathbb{Z}^n = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\}.$$

Change of Basis: Ring R then $U \in R^{n \times n}$ has

$$U \in GL_n(R) \iff \det(U) \in R^\times.$$

$\varphi_U : R^n \to R^n$, $x \mapsto Ux$ a bijection and $B \cdot \mathbb{Z}^n = B \cdot (U\mathbb{Z}^n)$

$= (BU) \cdot \mathbb{Z}^n$

Primer on LIP:

Lattice $B \in \mathbb{R}^{n \times n}$ linearly independent columns.

$$\mathcal{L} = \mathcal{L}(B) = B \cdot \mathbb{Z}^n = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z} \right\}.$$

Change of Basis: Ring R then $U \in R^{n \times n}$ has

$$U \in GL_n(R) \iff \det(U) \in R^\times.$$

$\ell_U : R^n \to R^n$, $x \mapsto Ux$ a bijection and $B \cdot \mathbb{Z}^n = B \cdot (U\mathbb{Z}^n) = \underbrace{(BU)}_{\text{different basis, same } \mathcal{L}} \cdot \mathbb{Z}^n$

(full rank n) lattice are the space $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$

(full rank n) lattice are the space $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$

Any "hardness"?

Given $(B, B' = BU)$ → "search" do $B^{-1}B' = U$

→ "decision" as above

(full rank n) lattice are the space $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$

Any "hardness"?

Given $(B, B' = BU)$ → "search" do $B^{-1}B' = U$

→ "decision" as above

Need a coarser notion...

(full rank n) lattice are the space $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$

Any "hardness"?

Given $(B, B' = BU)$ → "search" do $B^{-1}B' = U$

→ "decision" as above

Recall $O_n(\mathbb{R}) \leq GL_n(\mathbb{R})$ the "orthogonal group".

- endomorphisms $O : \mathbb{R}^n \to \mathbb{R}^n$, $\forall x \in \mathbb{R}^n$ $\|Ox\| = \|x\|$
- $O^t O = I_n(\mathbb{R})$.

Def Lattice Isomorphism (lattice rotations version)

Λ, Λ' lattices are isomorphic when $O \in O_n(\mathbb{R})$

$O \cdot \Lambda = \Lambda'$, written $\Lambda \sim \Lambda'$.

Def Lattice Isomorphism (lattice rotations version)

Λ, Λ' lattices are isomorphic when $O \in O_n(\mathbb{R})$

$O \cdot \Lambda = \Lambda'$, written $\Lambda \sim \Lambda'$.

If rank n lattices are the space $GL_n(\mathbb{R}) / GL_n(\mathbb{Z})$ then

isomorphic rank n lattices are $O_n(\mathbb{R}) \backslash \left(GL_n(\mathbb{R}) / GL_n(\mathbb{Z}) \right)$

Def Lattice Isomorphism (lattice rotations version)

Λ, Λ' lattices are isomorphic when $O \in O_n(\mathbb{R})$

$O \cdot \Lambda = \Lambda'$, written $\Lambda \sim \Lambda'$.

If rank n lattices are the space $GL_n(\mathbb{R}) / GL_n(\mathbb{Z})$ then

isomorphic rank n lattices are $O_n(\mathbb{R}) \backslash \left(GL_n(\mathbb{R}) / GL_n(\mathbb{Z}) \right)$

Concretely, if $\Lambda = \Lambda(B)$, $\Lambda' = \Lambda(B')$ then $\Lambda \sim \Lambda' \longleftrightarrow B' = OBU$.

Def Lattice Isomorphism (lattice rotations version)

Λ, Λ' lattices are isomorphic when $O \in O_n(\mathbb{R})$

$O \cdot \Lambda = \Lambda'$, written $\Lambda \sim \Lambda'$.

If rank n lattices are the space $GL_n(\mathbb{R}) / GL_n(\mathbb{Z})$ then

isomorphic rank n lattices are $O_n(\mathbb{R}) \backslash \left(GL_n(\mathbb{R}) / GL_n(\mathbb{Z}) \right)$

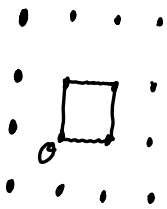
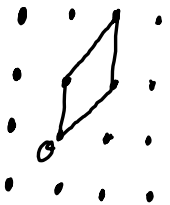
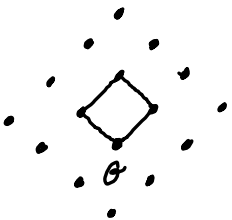
Concretely, if $\Lambda = \Lambda(B)$, $\Lambda' = \Lambda(B')$ then $\Lambda \sim \Lambda' \longleftrightarrow B' = OBU$.

$U = I_n(\mathbb{Z})$ also easy

Example $\Lambda = \mathbb{Z}^2$, $\Lambda' = O_{\frac{\pi}{4}} \cdot \mathbb{Z}^2$, $\Lambda \sim \Lambda'$

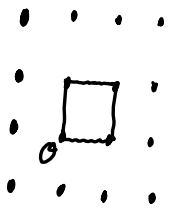
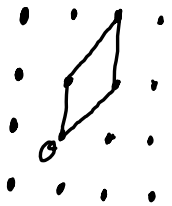
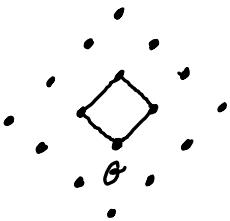
Example $\Lambda = \mathbb{Z}^2$, $\Lambda' = O_{\frac{\pi}{4}} \cdot \mathbb{Z}^2$, $\Lambda \sim \Lambda'$

Easy $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $B = I_2(\mathbb{Z})$

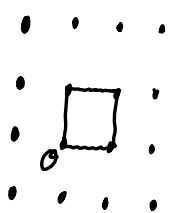
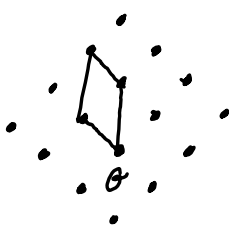
B  BU  OB 

Example $\Lambda = \mathbb{Z}^2$, $\Lambda' = O_{\frac{\pi}{4}} \cdot \mathbb{Z}^2$, $\Lambda \sim \Lambda'$

Easy $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $B = I_2(\mathbb{Z})$

B  BU  OB 

Hard?

B  OBU 

Practical Concerns

$O_n(\mathbb{R})$
$GL_n(\mathbb{R})$

difficult for implementations and "robust" cryptography

Practical Concerns

$O_n(\mathbb{R})$, $GL_n(\mathbb{R})$ } difficult for implementations and "robust" cryptography

To remove $O_n(\mathbb{R})$ ⟶ use quadratic forms

To remove $GL_n(\mathbb{R})$ ⟶ choose e.g. integer lattices

Practical Concerns

$O_n(\mathbb{R})$, $GL_n(\mathbb{R})$ } difficult for implementations and "robust" cryptography

Quadratic forms:

If $\Lambda = \Lambda(B)$, $B \longrightarrow B^t B = Q \in S_n^{>0}(\mathbb{R})$

Practical Concerns

$O_n(\mathbb{R})$, $GL_n(\mathbb{R})$ } difficult for implementations and "robust" cryptography

Quadratic forms:

If $\Lambda = \Lambda(B)$, $B \longrightarrow B^t B = Q \in S_n^{>0}(\mathbb{R})$

If $\Lambda' \sim \Lambda \Rightarrow B' = OBU \Rightarrow (B')^t B' = U^t Q U$.

We now first consider $O_n(\mathbb{R}) \backslash GL_n(\mathbb{R}) \simeq S_n^{>0}(\mathbb{R})$

then can define isomorphic $Q, Q' \in S_n^{>0}(\mathbb{R})$ when $U \in GL_n(\mathbb{Z})$

$Q' = U^t Q U$, i.e. $\left(O_n(\mathbb{R}) \backslash GL_n(\mathbb{R})\right) / GL_n(\mathbb{Z})$.

We now first consider $O_n(\mathbb{R}) \backslash GL_n(\mathbb{R}) \simeq S_n^{>0}(\mathbb{R})$

then can define isomorphic $Q, Q' \in S_n^{>0}(\mathbb{R})$ when $U \in GL_n(\mathbb{Z})$

$Q' = U^t Q U$, i.e. $\left(O_n(\mathbb{R}) \backslash GL_n(\mathbb{R})\right) / GL_n(\mathbb{Z})$.

If $\Lambda = \Lambda(B)$ and $Q = B^t B$ then:

- Q contains geometric information of Λ
- no embedding into $\mathbb{R}^n$

We now first consider $O_n(\mathbb{R}) \backslash GL_n(\mathbb{R}) \simeq S_n^{>0}(\mathbb{R})$

then can define isomorphic $Q, Q' \in S_n^{>0}(\mathbb{R})$ when $U \in GL_n(\mathbb{Z})$

$Q' = U^t Q U$, i.e. $\left(O_n(\mathbb{R}) \backslash GL_n(\mathbb{R})\right) / GL_n(\mathbb{Z})$.

If $\Lambda = \Lambda(B)$ and $Q = B^t B$ then:

- Q contains geometric information of Λ
- no embedding into $\mathbb{R}^n$

e.g. $x, y \in \mathbb{Z}^n \Rightarrow Bx, By \in \Lambda$, and $\langle Bx, By \rangle = x^t B^t B y$

$= x^t Q y$

Summary

Def Lattice Isomorphism (Quadratic forms)

$Q, Q' \in S_n^{>0}(\mathbb{R})$ are isomorphic, written $Q' \sim Q$ when $U \in GL_n(\mathbb{Z})$, $Q' = U^t Q U$.

Def $Q \in S_n^{>0}(\mathbb{R})$

$$\langle \cdot, \cdot \rangle_Q : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$$
$$(x, y) \longmapsto x^t Q y$$

$$\| \cdot \|_Q : \mathbb{R}^n \longrightarrow \mathbb{R}$$
$$x \longmapsto \sqrt{\langle x, x \rangle_Q}$$

Summary

Def Lattice Isomorphism (Quadratic forms)

$Q, Q' \in S_n^{>0}(\mathbb{R})$ are isomorphic, written $Q' \sim Q$ when $U \in GL_n(\mathbb{Z})$, $Q' = U\,{}^tQ\,U$.

Def $Q \in S_n^{>0}(\mathbb{R})$

$$\langle \cdot, \cdot \rangle_Q : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R}$$
$$(x, y) \longmapsto x^t Q y$$

$$\| \cdot \|_Q : \mathbb{R}^n \longrightarrow \mathbb{R}$$
$$x \longmapsto \sqrt{\langle x, x \rangle_Q}$$

- $Q = I_n(\mathbb{R}) \longrightarrow$ Euclidean norm
- $x, y \in \mathbb{R}^n$, $\langle x, y \rangle_Q = \langle Bx, By \rangle$, $\|x\|_Q = \|Bx\|$

Algorithms on $\mathbb{Q}$

Often A is described by B. We perform computations $A(B)$.

Algorithms on Q

Often $\mathcal{A}$ is described by B. We perform computations $\mathcal{A}(B)$.

If $\mathcal{A}$ only requires:
- geometric information
- $B \longrightarrow BX$

then we have an equivalent $\mathcal{A}(Q)$, $Q \longrightarrow X^t Q X$

Algorithms on Q

Often $\mathcal{A}$ is described by B. We perform computations $\mathcal{A}(B)$.

If $\mathcal{A}$ only requires: - geometric information
- $B \longrightarrow BX$

then we have an equivalent $\mathcal{A}(Q)$, $Q \longrightarrow X^t Q X$

e.g.
- eros
- size reduction
- LLL
- BKZ

Cryptography how ?

Given $Q' \sim Q$ we define $[Q] = \{Q' : Q' \sim Q\}$

Cryptography how ?

Given $Q' \sim Q$ we define $[Q] = \{Q' : Q' \sim Q\}$

We can define problems on $[Q]$ and build cryptography.

Cryptography how?

Given $Q' \sim Q$ we define $[Q] = \{Q' : Q' \sim Q\}$

We can define problems on $[Q]$ and build cryptography.

(!!) Problems on $[Q]$, <u>not</u> all of $\Sigma_n^{>0}(\mathbb{R})$

Cryptography how?

Given $Q' \sim Q$ we define $[Q] = \{Q' : Q' \sim Q\}$

We can define problems on $[Q]$ and build cryptography.

(!!) Problems on $[Q]$, not all of $\mathcal{S}_n^{>0}(\mathbb{R})$

$[Q]$ is "all rotations of $\mathcal{L}$"
may be easy/hard depending on $\mathcal{L}$

Cryptography how?

Given $Q' \sim Q$ we define $[Q] = \{Q' : Q' \sim Q\}$

We can define problems on $[Q]$ and build cryptography.

(!!) Problems on $[Q]$, <u>not</u> all of $S_n^{>0}(\mathbb{R})$

$[Q]$ is "all rotations of Λ"
may be easy/hard depending on Λ

following problems conjectured hard over $\Lambda = \mathbb{Z}^n$.

Cryptography now!

$\underline{\text{wc-sLIP}^{Q}}$

Given $Q, Q' \in [Q]$ find $U \in GL_n(\mathbb{Z})$, $Q' = U^t Q U$

$\underline{\text{wc-}\Delta\text{LIP}^{Q_0, Q_1}}$

Given Q_0, Q_1 and $Q' \in [Q_b]$ for some $b \in \{0,1\}$, return b

Cryptography now!

wc-sLIP^{Q}

Given $Q, Q' \in [Q]$ find $U \in GL_n(\mathbb{Z})$, $Q' = U^t Q U$

wc-ΔLIP$^{Q_0, Q_1}$

Given Q_0, Q_1 and $Q' \in [Q_b]$ for some $b \in \{0,1\}$, return b

Note again: hardness may vary with Q, (Q_0, Q_1)

Coding theory equivalent

Two linear $[n,k]_q$ codes C, C' are equivalent when

$\sigma \in S_n$, $a \in (\mathbb{F}_q^\times)^n$

$$C' = \{(a_1 x_{\sigma^{-1}(1)}, \dots, a_n x_{\sigma^{-1}(n)}) : (x_1, \dots, x_n) \in C\}$$

Coding theory equivalent

Two linear $[n,k]_q$ codes C, C' are equivalent when

$\sigma \in S_n$, $a \in (\mathbb{F}_q^\times)^n$

$$C' = \{(a_1 x_{\sigma^{-1}(1)}, \dots, a_n x_{\sigma^{-1}(n)}) : (x_1, \dots, x_n) \in C\}$$

Def Code equivalence

$C' \sim C$ when $D \in \mathrm{Diag}_n(\mathbb{F}_q^\times)$, $P_\sigma \in \mathrm{Perm}_n$

$$C' = D P_\sigma C$$

Coding theory equivalent

Two linear $[n,k]_q$ codes C, C' are equivalent when

$\sigma \in S_n$, $a \in (\mathbb{F}_q^\times)^n$

$$C' = \{(a_1 x_{\sigma^{-1}(1)}, \dots, a_n x_{\sigma^{-1}(n)}) : (x_1, \dots, x_n) \in C\}$$

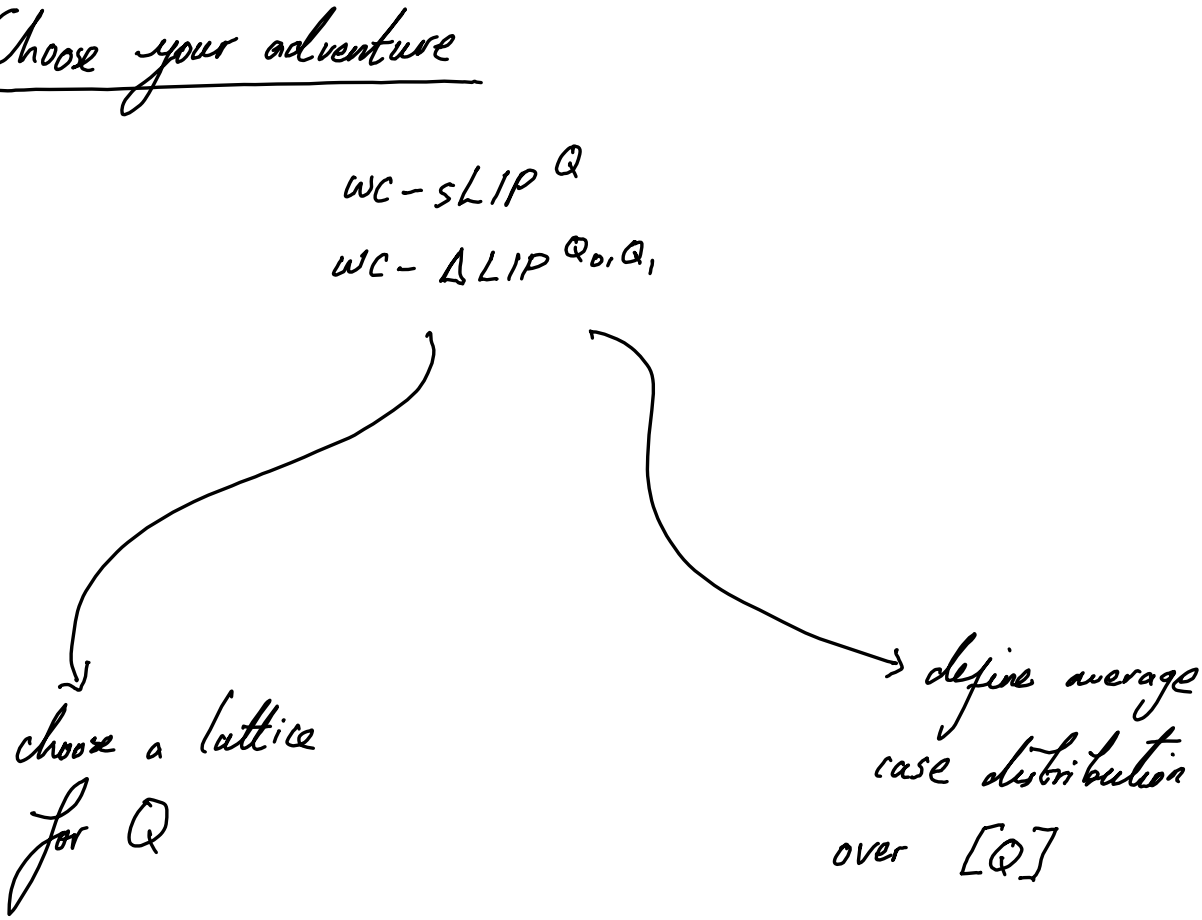
Def Code equivalence

$C' \sim C$ when $D \in \mathrm{Diag}_n(\mathbb{F}_q^\times)$, $P_\sigma \in \mathrm{Perm}_n$

$$C' = D P_\sigma C$$

↳ recall $\lambda' = 0 \cdot \lambda$

Choose your adventure



Discrete Gaussians $\quad Q \in S_n^{>0}(\mathbb{R})$

$$\rho_{Q,\sigma} : \mathbb{R}^n \longrightarrow \mathbb{R} \quad x \longmapsto \exp\left(\frac{-\|x\|_Q^2}{2\sigma^2}\right)$$

$$\|x\|_Q^2 = x^t Q x$$

Then for $c \in \mathbb{R}^n$

$$D_{Q,\mathbb{Z}^n+c,\sigma} : \mathbb{Z}^n + c \longrightarrow [0,1]$$

$$x \longmapsto \frac{\rho_{Q,\sigma}(x)}{\rho_{Q,\sigma}(\mathbb{Z}^n + c)}$$

Note

- For "large enough" σ we can sample efficiently

Note

- For "large enough" σ we can sample efficiently

- If $\Lambda = \Lambda(B)$ and $Q = B^t B$ then

$$D_{Q, \mathbb{Z}^n, \sigma}(x) = D_{\Lambda, \sigma}(Bx), \text{ and}$$

$$D_{Q, \mathbb{Z}^n + c, \sigma}(x) = D_{\Lambda + Bc, \sigma}(Bx)$$

Note

- For "large enough" σ we can sample efficiently
- If $\Lambda = \Lambda(B)$ and $Q = B^t B$ then

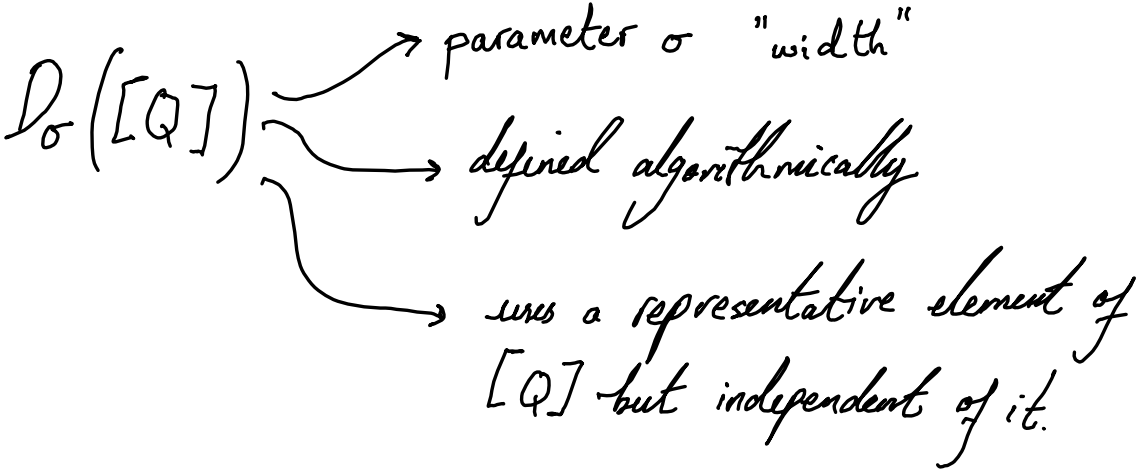
$$D_{Q, \mathbb{Z}^n, \sigma}(x) = D_{\Lambda, \sigma}(Bx), \text{ and}$$

$$D_{Q, \mathbb{Z}^n + c, \sigma}(x) = D_{\Lambda + Bc, \sigma}(Bx)$$

- Usual tail bound

$$\Pr_{x \leftarrow D_{Q, \mathbb{Z}^n + c, \sigma}} \left[\|x\| > t \sigma \sqrt{n} \right] \leq C t^n e^{-\frac{n}{2}(t^2 - 1)}$$

A distribution over $[Q]$.



A distribution over $[Q]$.

$D_\sigma([Q])$:

Input: $Q \in [Q]$, $\sigma > 0$

Output: (R, U) with $R = U^t Q U$, $U \in GL_n(\mathbb{Z})$

A distribution over $[Q]$.

$D_\sigma([Q])$:

Input: $Q \in [Q]$, $\sigma > 0$

Output: (R, U) with $R = U^t Q U$, $U \in GL_n(\mathbb{Z})$

1. $\{y_i\}_{i=1}^n \xleftarrow{\text{i.i.d.}} D_{Q,\sigma}$
2. $(R, U) = \text{Extract}(\{y_i\}_{i=1}^n, Q)$

A distribution over $[Q]$.

$D_\sigma([Q])$:

Input: $Q \in [Q]$, $\sigma > 0$

Output: (R, U) with $R = U^t Q U$, $U \in GL_n(\mathbb{Z})$

1. $\{y_i\}_{i=1}^n \xleftarrow{\text{i.i.d.}} D_{\mathbb{Q},\sigma}$
2. $(R, U) = \mathrm{Extract}(\{y_i\}_{i=1}^n, Q)$ → uses HNF to find a canonical form

[DvW22]: - constant success probability for large σ

- $R \in [Q]$ and independent of Q.

average case problems

$ac\text{-}sLIP_\sigma^Q$

Given Q and $Q' \leftarrow D_\sigma([Q])$ find $U \in GL_n(\mathbb{Z})$

$$Q' = U^t Q U.$$

$ac\text{-}\Delta LIP_\sigma^{Q_0,Q_1}$

Let $b \leftarrow \mathcal{U}(\{0,1\})$, given (Q_0, Q_1) and $Q' \leftarrow D_\sigma([Q_b])$

find b.

average case problems

$ac\text{-}sLIP_\sigma^Q$

Given Q and $Q' \leftarrow D_\sigma([Q])$ find $U \in GL_n(\mathbb{Z})$

$$Q' = U^t Q U.$$

$ac\text{-}\Delta LIP_\sigma^{Q_0,Q_1}$

Let $b \leftarrow \mathcal{U}(\{0,1\})$, given (Q_0,Q_1) and $Q' \leftarrow D_\sigma([Q_b])$

find b.

For large enough σ $\begin{cases} wc\text{-}sLIP^Q \longrightarrow ac\text{-}sLIP_\sigma^Q \\ wc\text{-}\Delta LIP^{Q_0,Q_1} \longrightarrow ac\text{-}\Delta LIP_\sigma^{Q_0,Q_1} \end{cases}$

Left with a selection of $[Q]$

- $[Q] \subseteq S_n^{>0}(\mathbb{Z})$,

Left with a selection of $[Q]$

- $[Q] \subseteq \mathcal{S}_n^{>0}(\mathbb{Z})$,

- $\varepsilon([Q])$ "small" for e.g. $\varepsilon(n) = 2^{-n}$

Left with a selection of $[Q]$

$\Lambda = \mathbb{Z}^n$ is "best" so for

- $[Q] \subseteq S_n^{>0}(\mathbb{Z})$,
- $\eta_\varepsilon([Q])$ "small" for e.g. $\varepsilon(n) = 2^{-n}$

Left with a selection of $[Q]$

$\Lambda = \mathbb{Z}^n$ is "best" so far

- $[Q] \subseteq S_n^{>0}(\mathbb{Z})$,
- $\gamma_\varepsilon([Q])$ "small" for e.g. $\varepsilon(n) = 2^{-n}$

$\mathbb{Z}^n$ BAD then GOOD

- Λ and $\tilde{\Lambda}$ have minima close to Minkowski's bound. Easy to decode in Λ.

Left with a selection of $[Q]$

$\Lambda = \mathbb{Z}^n$ is "best" so for

- $[Q] \subseteq S_n^{>0}(\mathbb{Z})$,
- $\eta_\varepsilon([Q])$ "small" for e.g. $\varepsilon(n) = 2^{-n}$

We reduce forgery to a different problem in Hawk.

[DvW22] signature ⚡ made to "look like" Hawk

Public parameters:

- $H : \{0,1\}^* \longrightarrow \mathcal{T}_q^n$
- A form Q determining $[Q]$, e.g. $Q = I_n(\mathbb{Z})$
- $\sigma_{keygen}, \sigma_{sign}$ "large enough"

[DvW22] signature ⚡ made to "look like" Hawk

Public parameters:

- $H : \{0,1\}^* \longrightarrow \mathbb{T}_q^n$

$\mathbb{T}_q$ is discretised $\mathbb{R}/\mathbb{Z}$, $\{0, \frac{1}{q}, \dots, \frac{q-1}{q}\}$.

- A form Q determining $[Q]$, e.g. $Q = I_n(\mathbb{Z})$

- $\sigma_{keygen}, \sigma_{sign}$ "large enough"

Moving between forms

Let $R = U^{E} Q U$ then

Moving between forms

Let $R = U^T Q U$ then

$$-\|x\|_R = x^T R x = x^T U^T Q U x = (Ux)^T Q (Ux)$$
$$= \|Ux\|_Q$$

Moving between forms

Let $R = U^t Q U$ then

$$-\|x\|_R = x^t R x = x^t U^t Q U x = (Ux)^t Q (Ux)$$
$$= \|Ux\|_Q$$

$$- D_{Q, \mathbb{Z}^n + Uc, \sigma}(x) = D_{R, \mathbb{Z}^n + c, \sigma}(U^{-1} x)$$

[DvW22] signatures:

$H: \{0,1\}^* \to \Pi_q^n$, $Q = I_n(\mathbb{Z})$, $(\sigma_{keygen}, \sigma_{sign})$

$KGen(1^n)$:

$(R, u) \leftarrow D_{\sigma_{keygen}}([Q])$, return $(pk = R, sk = u)$

[DvW22] signatures:

$H: \{0,1\}^* \longrightarrow \Pi_Q^n$, $Q = I_n(\mathbb{Z})$, $(\sigma_{keygen}, \sigma_{sign})$

$KGen(1^n)$:

$(R, U) \leftarrow D_{\sigma_{keygen}}([Q])$, return $(pk = R, sk = U)$

key recovery is $ac\text{-}sLIP_\sigma^Q$

[DvW22] signatures:

$H: \{0,1\}^* \longrightarrow \mathbb{T}_q^n$, $Q = I_n(\mathbb{Z})$, $(\sigma_{keygen}, \sigma_{sign})$

$KGen(1^n)$:

$(R, U) \leftarrow D_{\sigma_{keygen}}([Q])$, return $(pk = R, sk = U)$

$Sign(sk, m)$:

$r \xleftarrow{\$} \{0,1\}^{\text{salt}}$

$h = H(m, r)$

$x \longleftarrow D_{Q, \mathbb{Z}^n + Uh, \sigma_{sign}}$

return $sig = (r, h - U^{-1}x)$

[DvW22] signatures:

$H: \{0,1\}^* \to \Pi_Q^n$, $Q = I_n(\mathbb{Z})$, $(\sigma_{keygen}, \sigma_{sign})$

$KGen(1^n)$:

$(R, U) \leftarrow D_{\sigma_{keygen}}([Q])$, return $(pk = R, sk = U)$

$Sign(sk, m)$:

$r \xleftarrow{\$} \{0,1\}^{salt}$

$h = H(m, r)$

$x \leftarrow D_{Q, \mathbb{Z}^n + Uh, \sigma_{sign}}$

return $sig = (r, h - U^{-1}x)$

- $x \in \mathbb{Z}^n + Uh$ so $h - U^{-1}x \in \mathbb{Z}^n$
- $\|x\|_Q = \|U^{-1}x\|_R$

[DvW22] signatures:

$H: \{0,1\}^* \longrightarrow \mathbb{T}_Q^n$, $Q = I_n(\mathbb{Z})$, $(\sigma_{keygen}, \sigma_{sign})$

$KGen(1^n)$:

$(R, U) \leftarrow D_{\sigma_{keygen}}([Q])$, return $(pk = R, sk = U)$

$Vf(pk, m, sig = (r, h - U^{-1}x))$

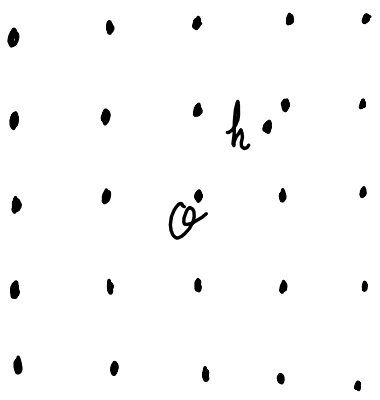
$h = H(m, r)$

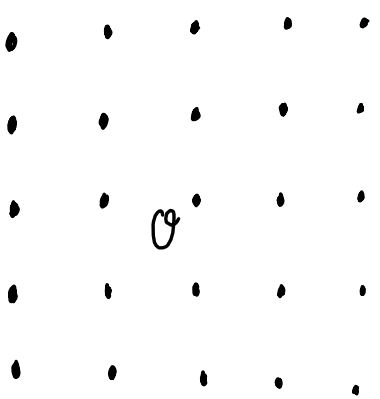
return $[\![h - U^{-1}x \in \mathbb{Z}^n]\!]$

$\wedge [\![\|U^{-1}x\|_R \leq (1+\varepsilon)\sigma_{sign}\sqrt{n}]\!]$

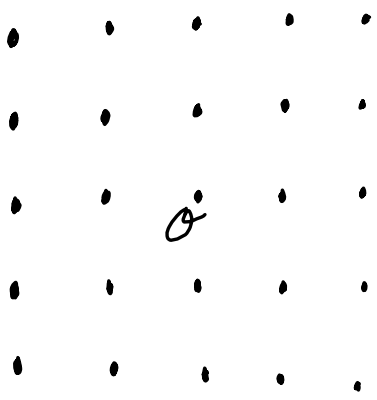
- $x \in \mathbb{Z}^n + Uh$ so $h - U^{-1}x \in \mathbb{Z}^n$
- $\|x\|_Q = \|U^{-1}x\|_R$

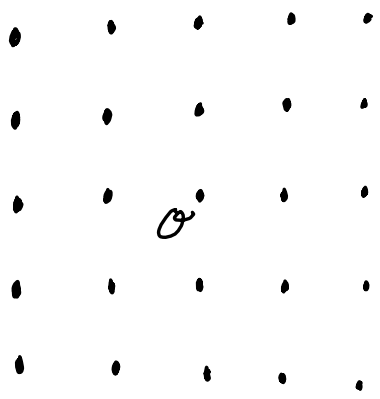
$R = U^t Q U$





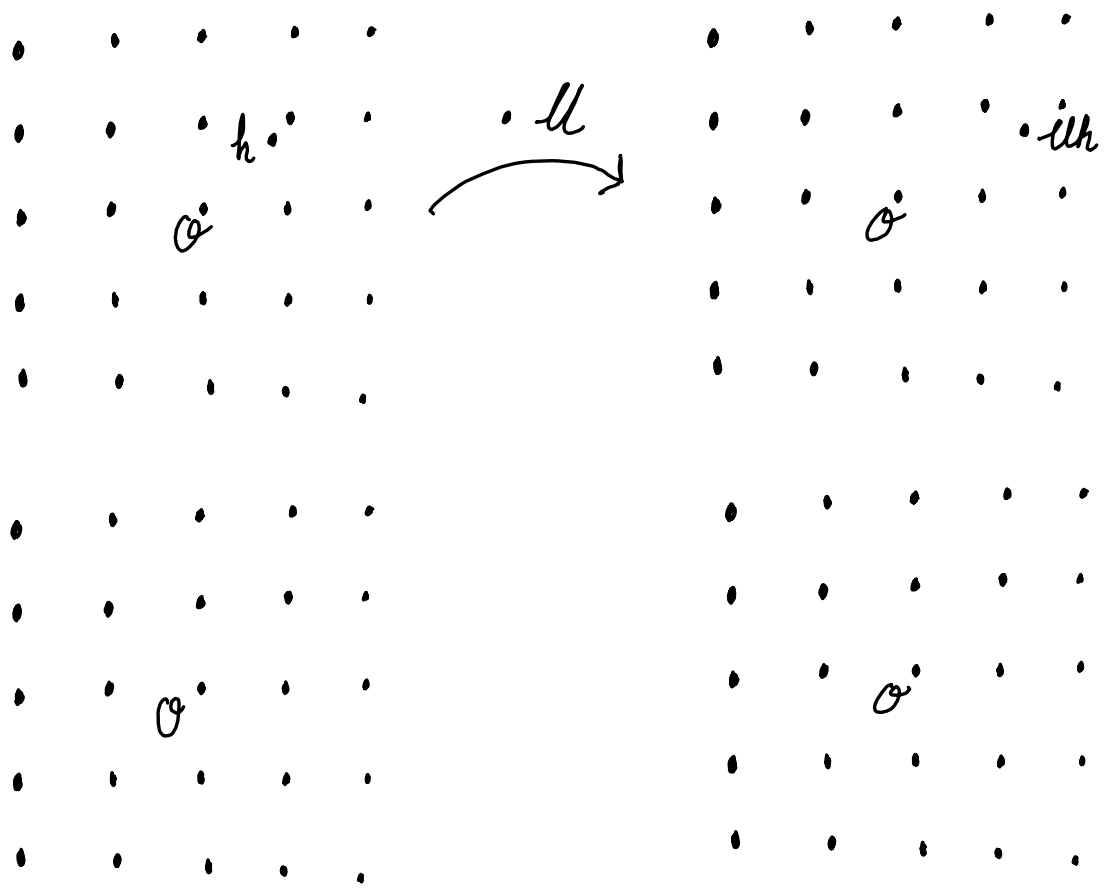
Q





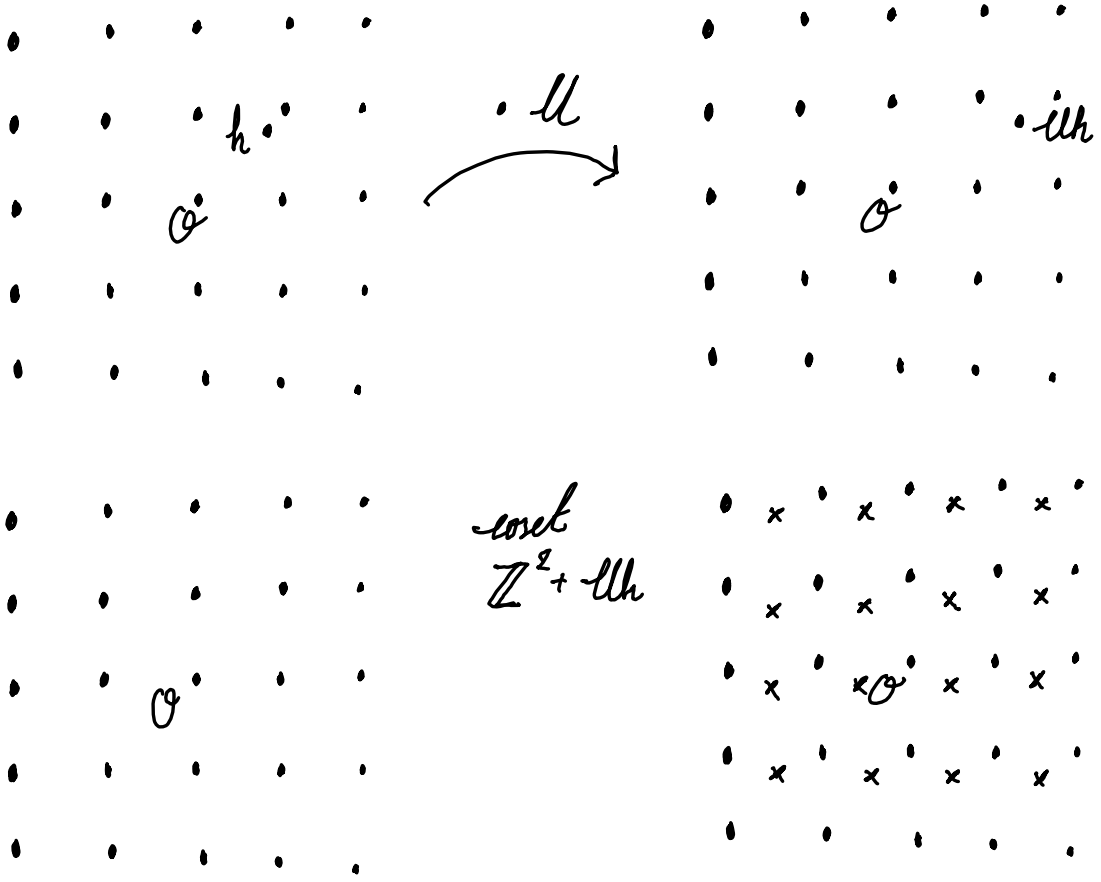
$R = U^t Q U$

Q

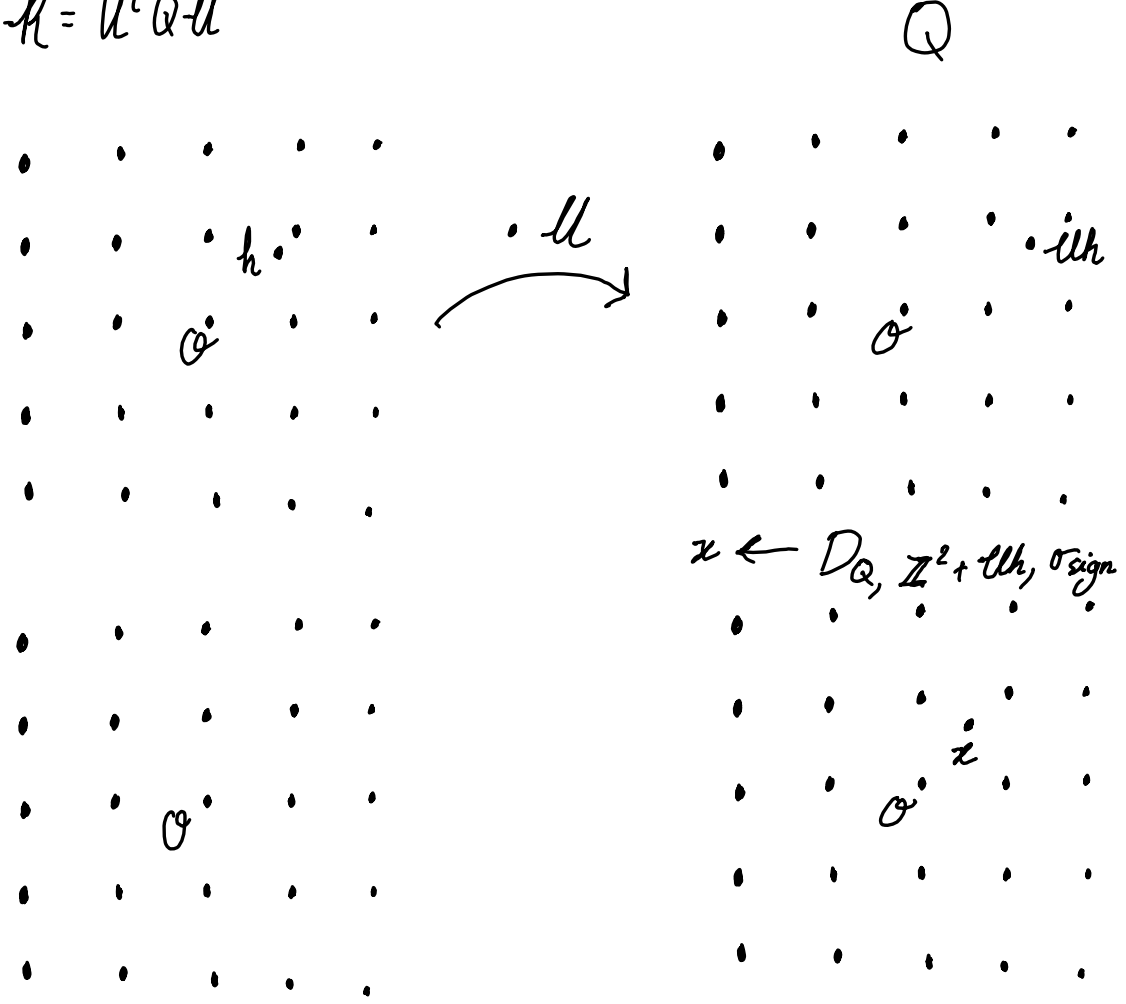


$R = U^t Q U$

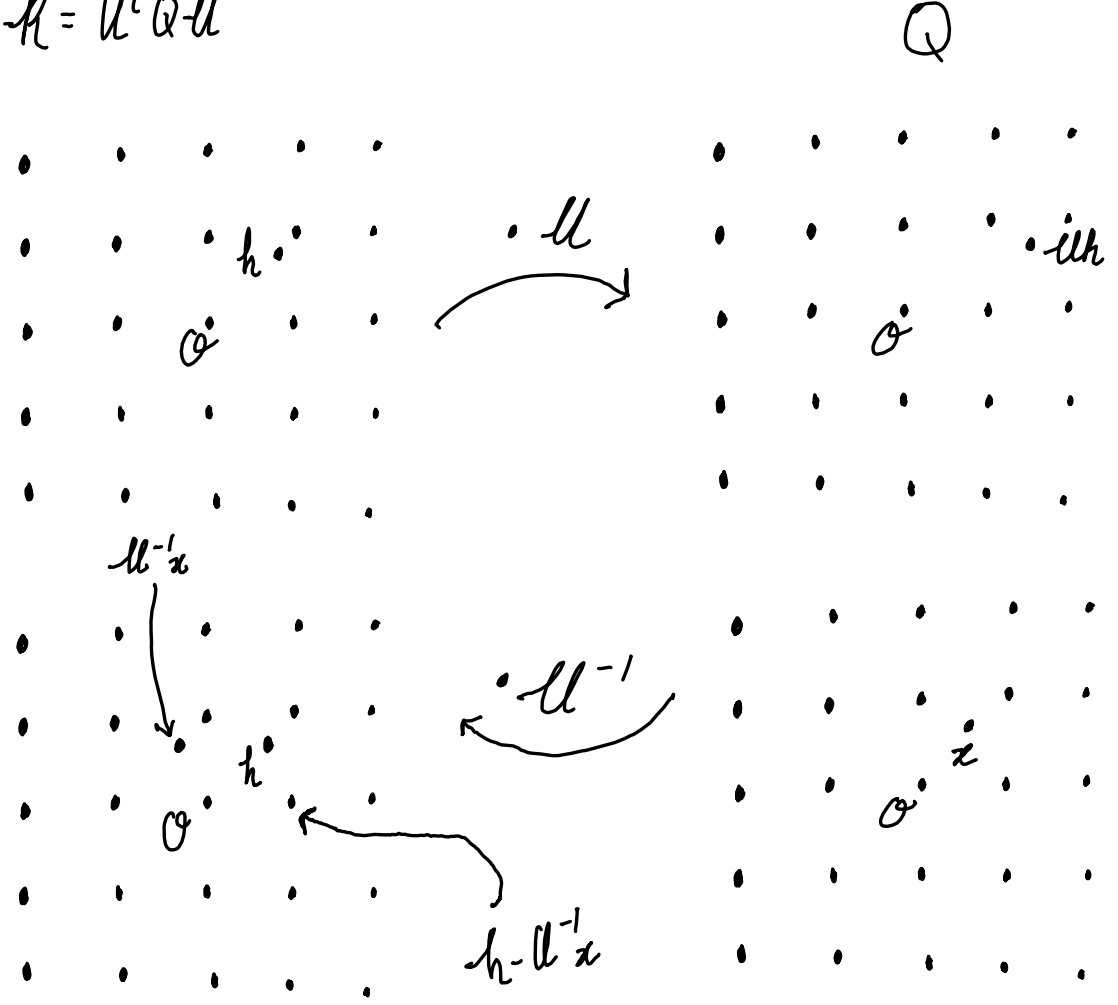
Q



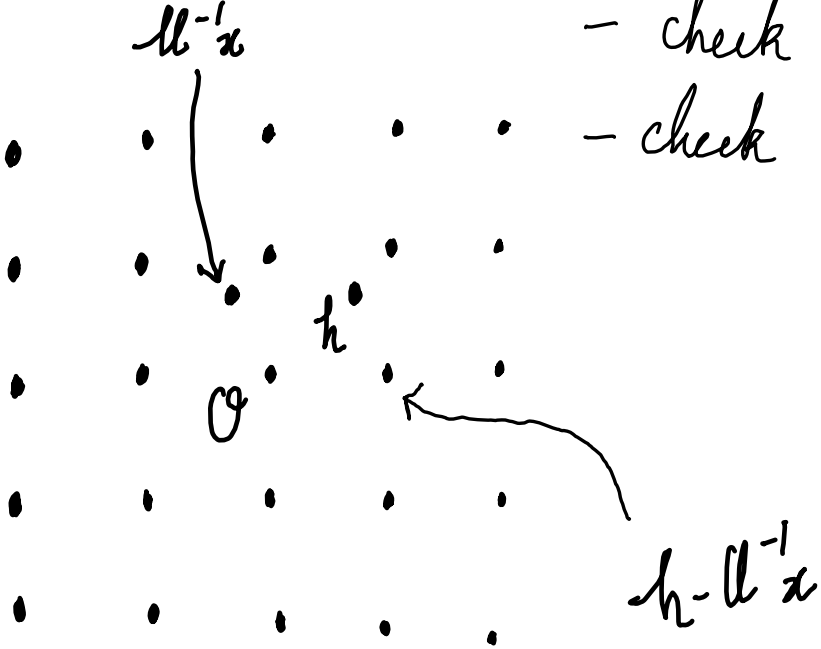
$R = U^t Q U$

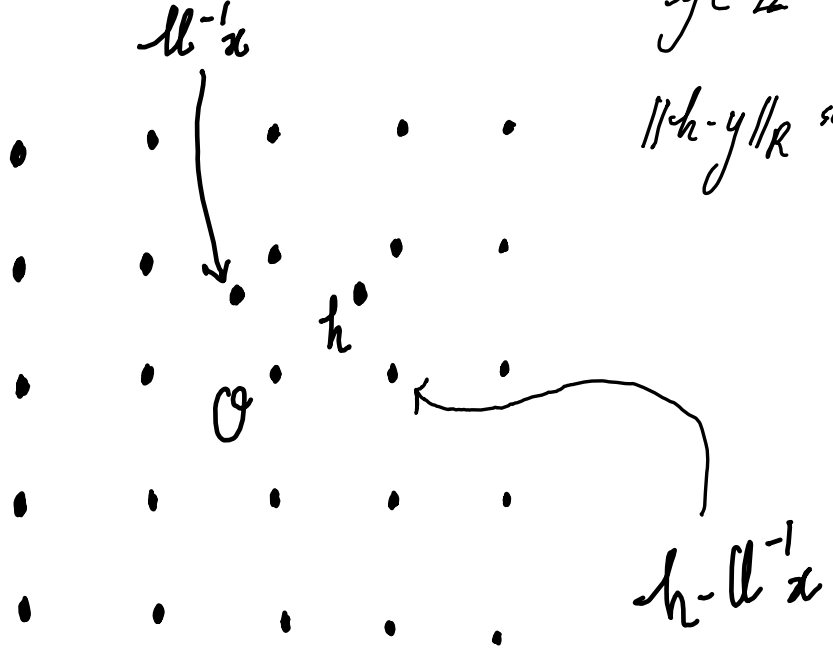


$R = U^t Q U$



- Can publicly compute h
- check $h - U^{-1}x \in \mathbb{Z}^n$
- check $\|U^{-1}x\|_R$





Forgery

$y \in \mathbb{Z}^n$

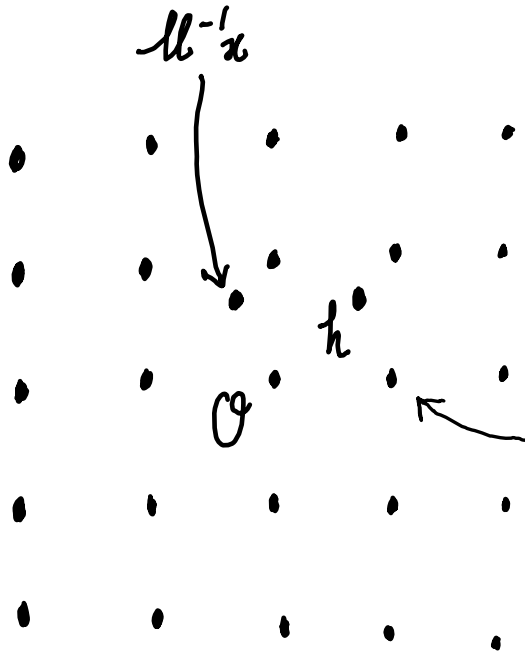
$\|h - y\|_R$ small

Honest

$h - U^{-1}x \in \mathbb{Z}^n$

$\|U^{-1}x\|_R$ small

$= \|x\|_Q$



Forgery

$y \in \mathbb{Z}^n$

$\|h - y\|_R$ small

Honest

$h - U^{-1}x \in \mathbb{Z}^n$

$\|U^{-1}x\|_R$ small $= \|x\|_Q$

If $Q = B^t B$

$R = U^t Q U$

then BUy is an approx CVP solution for $B \cdot Uh$ over $\Lambda = \Lambda(BU)$


lattice reduction cost estimates

↳ lattice reduction cost estimates

Reduction based security:

Theorem [DvW22]

For well chosen $Q, S \in \mathcal{S}_n^{>0}(\mathbb{R})$ and large enough $(\sigma_{keygen}, \sigma_{sign}), q$

↳ lattice reduction cost estimates

Reduction based security:

Theorem [DvW22]

For well chosen $Q, S \in \mathcal{S}_n^{>0}(\mathbb{R})$ and large enough $(\sigma_{keygen}, \sigma_{sign}), q$

$\Pi = (KGen, Sign, Vf)$ is ROM-EUF-CMA secure

if $ac\text{-}\Delta LIP^{Q,S^{-1}}_{\sigma_{keygen}}$ is hard

$KGen(1^n)$:

$pk = R$, $sk = u$ // $n \times n$ matrices

$Sign(m, sk)$

...

$x \leftarrow D_{Q, \mathbb{Z}^n + uh, \sigma_{sign}}$ // sample q cosets of $\mathbb{Z}$

$\mathbb{Z} + \frac{i}{q}$, $i \in \{0, \ldots, q-1\}$.

$KGen(1^n)$:

$pk = R$, $sk = u$ // $n \times n$ matrices

$Sign(m, sk)$

...

$x \leftarrow D_{Q, \mathbb{Z}^n + uh, \sigma_{sign}}$ // sample q cosets of $\mathbb{Z}$

$\mathbb{Z} + \frac{i}{q}$, $i \in \{0, \dots, q-1\}$.

① Use module structure $\rightsquigarrow$ NTRU lattices

- Define average case
- Worst case $\longrightarrow$ average case

KGen(1^n):

$pk = R$, $sk = \mathcal{U}$ // $n \times n$ matrices

Sign(m, sk)

...

$x \leftarrow D_{Q,\mathbb{Z}^n + \mathcal{U}h, \sigma_{sign}}$ // sample q cosets of $\mathbb{Z}$

$\mathbb{Z} + \frac{i}{q}$, $i \in \{0, \dots, q-1\}$.

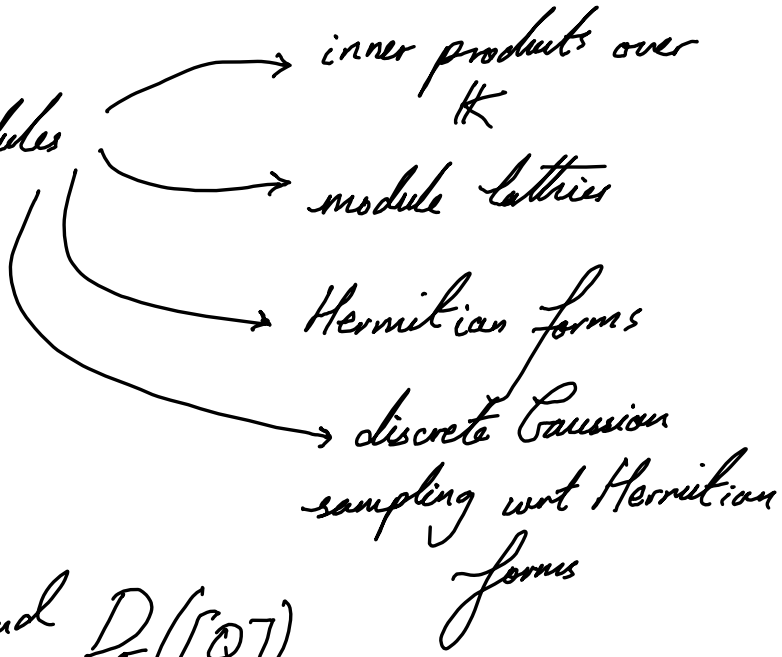
① Use module structure $\rightsquigarrow$ NTRU lattices

- Define average case
- Worst case $\longrightarrow$ average case

② Set $q = 2$, $H: \{0,1\}^* \longrightarrow \{0, \frac{1}{2}\}^2$, new reduction

Adding module structure

1) Define SIP over modules



2) Choice of $[Q]$ and $D_\sigma([Q])$.

Number field $\mathbb{K}$ of degree n $\xrightarrow{\sigma}$ $\mathbb{R}^n$

$\mathcal{O}_{\mathbb{K}}^{\ell}$, $M \in GL_\ell(\mathcal{O}_{\mathbb{K}}) \longrightarrow \mathbb{Z}^{\ell n}$, $M \in GL_{\ell n}(\mathbb{Z})$

$B \in \mathbb{K}^{\ell \times \ell} \longrightarrow B \in \mathbb{R}^{\ell n \times \ell n}$

$M = B \cdot \mathcal{O}_{\mathbb{K}}^{\ell} \longrightarrow \Lambda = B \cdot \mathbb{Z}^{\ell n}$

$B^* \longrightarrow B^t$

$B^*B \in \mathcal{H}_\ell^{>0}(\mathbb{K}) \longrightarrow B^tB \in \mathcal{S}_{\ell n}^{>0}(\mathbb{R})$

Number field $\mathbb{K}$ of degree n $\xrightarrow{\sigma}$ $\mathbb{R}^n$

$\mathcal{O}_{\mathbb{K}}^{\ell}$, $U \in GL_\ell(\mathcal{O}_{\mathbb{K}}) \longrightarrow \mathbb{Z}^{\ell n}$, $U \in GL_{\ell n}(\mathbb{Z})$

$B \in \mathbb{K}^{\ell \times \ell} \longrightarrow B \in \mathbb{R}^{\ell n \times \ell n}$

$M = B \cdot \mathcal{O}_{\mathbb{K}}^{\ell} \longrightarrow \Lambda = B \cdot \mathbb{Z}^{\ell n}$

$B^* \longrightarrow B^t$

$B^*B \in \mathcal{H}_\ell^{>0}(\mathbb{K}) \longrightarrow B^tB \in \mathcal{S}_{\ell n}^{>0}(\mathbb{R})$

rank ℓ Hermitian form

let's fix : $K = \frac{\mathbb{Q}[X]}{\langle X^{2^k}+1 \rangle}$, $\mathcal{O}_K = \frac{\mathbb{Z}[X]}{\langle X^{2^k}+1 \rangle}$, $n = 2^l$ $l > 1$

$\sigma_i : K \longrightarrow \mathbb{C}$ $\quad i \in \{1, \dots, n\}$ and $\sigma_i = \overline{\sigma_{i+\frac{n}{2}}}$

$\sigma : K \longrightarrow \mathbb{C}^n \quad x \longmapsto (\sigma_1(x), \dots, \sigma_n(x))$

let's fix : $K = \frac{\mathbb{Q}[X]}{\langle X^{2^k}+1 \rangle}$, $\mathcal{O}_K = \frac{\mathbb{Z}[X]}{\langle X^{2^k}+1 \rangle}$, $n = 2^k$ $k > 1$

$\sigma_i : K \longrightarrow \mathbb{C}$ $\quad i \in \{1, \dots, n\}$ and $\sigma_i = \overline{\sigma_{i+\frac{n}{2}}}$

$\sigma : K \longrightarrow \mathbb{C}^n \quad x \longmapsto (\sigma_1(x), \dots, \sigma_n(x))$

let's fix : $K = \frac{\mathbb{Q}[X]}{\langle X^{2^k}+1 \rangle}$, $\mathcal{O}_K = \frac{\mathbb{Z}[X]}{\langle X^{2^k}+1 \rangle}$, $n = 2^k$ $k > 1$

$\sigma_i : K \longrightarrow \mathbb{C}$ $\quad i \in \{1, \dots, n\}$ and $\sigma_i = \overline{\sigma_{i+\frac{n}{2}}}$

$\sigma : K \longrightarrow \mathbb{C}^n \quad x \longmapsto (\sigma_1(x), \dots, \sigma_n(x))$

$\sigma(K) \subseteq \{(z_1, \dots, z_n) : z_i = \overline{z_{i+\frac{n}{2}}}\} \cong \mathbb{R}^n$

let's fix: $K = \frac{\mathbb{Q}[X]}{\langle X^{2^k}+1 \rangle}$, $\mathcal{O}_K = \frac{\mathbb{Z}[X]}{\langle X^{2^k}+1 \rangle}$, $n = 2^k$ $k > 1$

$\sigma_i : K \longrightarrow \mathbb{C}$ $\quad i \in \{1, \dots, n\}$ and $\sigma_i = \overline{\sigma_{i+\frac{n}{2}}}$

$\sigma : K \longrightarrow \mathbb{C}^n \quad x \longmapsto (\sigma_1(x), \dots, \sigma_n(x))$

$\sigma(K) \subseteq \{(z_1, \dots, z_n) : z_i = \overline{z_{i+\frac{n}{2}}}\} \underset{w}{\simeq} \mathbb{R}^n$

↳ as an inner-product space, will consider $Im(\sigma)$ in $\mathbb{R}^n$ or $\mathbb{C}^n$

let's fix: $K = \frac{\mathbb{Q}[X]}{\langle X^{2^k}+1 \rangle}$, $\mathcal{O}_K = \frac{\mathbb{Z}[X]}{\langle X^{2^k}+1 \rangle}$, $n = 2^k$ $k > 1$

$\sigma_i : K \longrightarrow \mathbb{C}$ $\quad i \in \{1, \dots, n\}$ and $\sigma_i = \overline{\sigma_{i+\frac{n}{2}}}$

$\sigma : K \longrightarrow \mathbb{C}^n \quad x \longmapsto (\sigma_1(x), \dots, \sigma_n(x))$

$\sigma(K) \subseteq \{(z_1, \dots, z_n) : z_i = \overline{z_{i+\frac{n}{2}}}\} \underset{w}{\simeq} \mathbb{R}^n$

All of this to say $I \trianglelefteq \mathcal{O}_K \longrightarrow$ consider $\sigma(I)$ a lattice in $\mathbb{R}^n$.

σ also gives an inner product

$$\langle \cdot, \cdot \rangle_\sigma : \mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{R}$$

$$(a,b) \longmapsto \langle \sigma(a), \sigma(b) \rangle_{\mathbb{C}} = \sum_{i=1}^{n} \overline{\sigma_i(a)}\, \sigma_i(b)$$

σ also gives an inner product

$$\langle \cdot, \cdot \rangle_\sigma : K \times K \longrightarrow \mathbb{R}$$

$$(a, b) \longmapsto \langle \sigma(a), \sigma(b) \rangle_{\mathbb{C}} = \sum_{i=1}^{n} \overline{\sigma_i(a)}\, \sigma_i(b)$$

When $K = \dfrac{\mathbb{Q}[X]}{\langle X^k + 1 \rangle}$ (!)

vec is a scaled isometry of σ

$$\text{vec} : K \longrightarrow \mathbb{Q}^n$$

$$a = \sum_{i=0}^{n-1} a_i X^i \longmapsto (a_0, \ldots, a_{n-1})$$

σ also gives an inner product

$$\langle \cdot, \cdot \rangle_\sigma : K \times K \longrightarrow \mathbb{R}$$

$$(a,b) \longmapsto \frac{1}{n} \langle \sigma(a), \sigma(b) \rangle_{\mathbb{C}} = \frac{1}{n} \sum_{i=1}^{n} \overline{\sigma_i(a)}\, \sigma_i(b)$$

$$\mathrm{vec} : K \longrightarrow \mathbb{Q}^n$$

$$a = \sum_{i=0}^{n-1} a_i X^i \longmapsto (a_0, \dots, a_{n-1})$$

$$\langle \mathrm{vec}(a), \mathrm{vec}(b) \rangle_{\mathbb{R}} = \langle a, b \rangle_\sigma$$

(!) We often use coefficient embedding as simpler.

For $\langle a \rangle \triangleleft \mathcal{O}_K$ we give a basis of $\sigma(\langle a \rangle)$

$$rot(a) = \begin{pmatrix} | & | & & | \\ vec(a) & vec(\chi_a) & \cdots & vec(\chi_a^{n-1}) \\ | & | & & | \end{pmatrix} \in \mathbb{Q}^{n \times n}$$

For $\langle a \rangle \triangleleft \mathcal{O}_K$ we give a basis of $\sigma(\langle a \rangle)$

$$rot(a) = \begin{pmatrix} | & | & & | \\ vec(a) & vec(\chi_a) & \cdots & vec(\chi_a^{n-1}) \\ | & | & & | \end{pmatrix} \in \mathbb{Q}^{n \times n}$$

- Describe $\sigma(\langle a \rangle)$ as $a \in K$
- consider $Q = rot(a)^t rot(a) \in S_n^{>0}(\mathbb{Q})$ $\quad \| \ell = 1$

For $\langle a \rangle \triangleleft \mathcal{O}_K$ we give a basis of $\sigma(\langle a \rangle)$

$$rot(a) = \begin{pmatrix} | & | & & | \\ vec(a) & vec(\chi_a) & \cdots & vec(\chi_a^{n-1}) \\ | & | & & | \end{pmatrix} \in \mathbb{Q}^{n \times n}$$

- Describe $\sigma(\langle a \rangle)$ as $a \in K$
- consider $Q = rot(a)^t rot(a) \in S_n^{>0}(\mathbb{Q})$ $\quad //\ell = 1$

Enter "adjoint"

$* : \mathbb{K} \longrightarrow \mathbb{K}$ is an involutary automorphism

$a \longmapsto a^*$ (that exists for "CM fields")

$* : \mathbb{K} \longrightarrow \mathbb{K}$ is an involutary automorphism

$a \longmapsto a^*$ (that exists for "CM fields")

$\sigma_i(a^*) = \overline{\sigma_i(a)} \Rightarrow \dots \Rightarrow rot(a)^t = rot(a^*)$

and $rot(a)^t rot(a) = rot(a^* a)$

$* : K \longrightarrow K$ is an involutary automorphism

$a \longmapsto a^*$ (that exists for "CM fields")

$\sigma_i(a^*) = \overline{\sigma_i(a)} \Rightarrow \ldots \Rightarrow rot(a)^t = rot(a^*)$

and $rot(a)^t rot(a) = rot(a^* a)$

$\longrightarrow$ describe $Q \in \mathcal{S}_n^{>0}(\mathbb{Q})$ by $a^* a$.

$* : K \longrightarrow K$ is an involutary automorphism
$a \longmapsto a^*$ (that exists for "CM fields")

$\sigma_i(a^*) = \overline{\sigma_i(a)} \Rightarrow \dots \Rightarrow rot(a)^t = rot(a^*)$

and $rot(a)^t rot(a) = rot(a^* a)$

$\longrightarrow$ describe $Q \in S_n^{>0}(\mathbb{Q})$ by $a^* a$.

(!) Problem: Coeby–Szydlo can recover
a from $a^* a$. "Ideal-sLIP" not hard.

We need rank $\mathcal{L} > 1$.

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in K^{2\times 2} \quad \text{and} \quad M = B \cdot \mathcal{O}_K^2$$

and generalise rot, vec, adjoint...

We need rank $\ell > 1$.

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in K^{2\times 2} \quad \text{and} \quad M = B \cdot \mathcal{O}_K^2$$

and generalise rot, vec, adjoint...

$$\mathrm{rot}(B) = \begin{pmatrix} \mathrm{rot}(b_{11}) & \mathrm{rot}(b_{12}) \\ \mathrm{rot}(b_{21}) & \mathrm{rot}(b_{22}) \end{pmatrix} \in \mathbb{Q}^{2n\times 2n}$$

$$\mathrm{vec}(x=(x_1,x_2)) = \begin{pmatrix} \mathrm{vec}(x_1) \\ \hline \mathrm{vec}(x_2) \end{pmatrix} \in \mathbb{Q}^{2n}$$

$$B^* = \begin{pmatrix} b_{11}^* & b_{21}^* \\ b_{12}^* & b_{22}^* \end{pmatrix}$$

} as "expected"

We need rank $\ell > 1$.

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in K^{2\times 2} \quad \text{and} \quad M = B \cdot \mathcal{O}_K^2$$

$$B^* B \in \mathcal{H}_2^{>0}(K) \longleftrightarrow \mathrm{rot}(B)^t \mathrm{rot}(B) \in \mathcal{S}_{2n}^{>0}(\mathbb{Q})$$

We need rank $\ell > 1$.

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in K^{2\times 2} \quad \text{and} \quad M = B \cdot \mathcal{O}_K^2$$

$$B^*B \in \mathcal{H}_2^{>0}(K) \longleftrightarrow \mathrm{rot}(B)^t \mathrm{rot}(B) \in \mathcal{S}_{2n}^{>0}(\mathbb{Q})$$

$$U_2(K_{\mathbb{R}}) \backslash GL_2(K) \qquad \mathcal{O}_{2n}(\mathbb{R}) \backslash GL_{2n}(\mathbb{R})$$

We need rank $\ell > 1$.

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in K^{2\times 2} \quad \text{and} \quad M = B \cdot \mathcal{O}_K^2$$

$$B^* B \in \mathcal{H}_2^{>0}(K) \longleftrightarrow \mathrm{rot}(B)^t \mathrm{rot}(B) \in \mathcal{S}_{2n}^{>0}(\mathbb{Q})$$

Def module lattice isomorphism (Hermitian form version)

$Q, Q' \in \mathcal{H}_\ell^{>0}(K)$ are $Q' \sim Q$ when

$U \in GL_\ell(\mathcal{O}_K)$ $\quad Q' = U^* Q U$

Write $[Q] = \{Q' : Q \sim Q'\}$.

We need rank $\ell > 1$.

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in K^{2\times 2} \quad \text{and} \quad M = B \cdot \mathcal{O}_K^2$$

$$B^* B \in \mathcal{H}_2^{>0}(K) \longleftrightarrow \mathrm{rot}(B)^t \mathrm{rot}(B) \in S_{2n}^{>0}(\mathbb{Q})$$

Def module lattice isomorphism (Hermitian form version)

$Q, Q' \in \mathcal{H}_\ell^{>0}(K)$ are $Q' \sim Q$ when

$U \in SL_\ell(\mathcal{O}_K)$ $\quad Q' = U^* Q U$

Write $[Q] = \{Q' : Q \sim Q'\}$.

Upside of $\ell > 2$

- Gentry-Szydlo not known
- move between $Q = B^* B \in \mathcal{H}_2^{>0}(K)$

$$\mathrm{rot}(Q) = \mathrm{rot}(B)^t \mathrm{rot}(B) \in \mathcal{S}_{2n}^{>0}(\mathbb{Q})$$

as desired

Upside of $\ell > 2$

- Centry-Szegedo not known
- move between $Q = B^* B \in \mathcal{H}_\ell^{>0}(K)$

$$\mathrm{rot}(Q) = \mathrm{rot}(B)^t \mathrm{rot}(B) \in \mathcal{S}_{2n}^{>0}(Q)$$

as desired

$\longrightarrow$ efficient manipulation and storage using K

$\longrightarrow$ simple Gaussian sampling using $\mathcal{S}_{2n}^{>0}(Q)$.

Gaussian sampling wrt $Q \in \mathcal{H}_\ell^{>0}(K)$

Our setup

$$D_{Q, \mathcal{O}_K^\ell + c, \sigma}(x) = D_{\mathrm{rot}(Q), \mathbb{Z}^{n\ell} + \mathrm{vec}(c), \sigma}(\mathrm{vec}(x))$$

Gaussian sampling wrt $Q \in \mathcal{H}_\ell^{>0}(K)$

Our setup

$$D_{Q, \mathcal{O}_K^\ell + c, \sigma}(x) = \underbrace{D_{\mathrm{rot}(Q), \mathbb{Z}^{n\ell} + \mathrm{vec}(c), \sigma}(\mathrm{vec}(x))}$$

$Q = I_\ell(K)$ then

coordinatwise $\mathbb{Z} + \mathrm{vec}(c)_i$

i.e. $D_{\mathbb{Z}^{n\ell} + \mathrm{vec}(c), \sigma}$

Def wc-msLIP^Q

Given $Q, Q' \in [Q]$ find $U \in SL_\ell(\mathcal{O}_K)$

$Q' = U^* Q U$.

Def wc-msLIP^Q

Given $Q, Q' \in [Q]$ find $U \in SL_2(\mathcal{O}_K)$

$Q' = U^* Q U$.

Our case: $Q = I_2(K)$ then

$$[Q] = \{U^* U : U \in SL_2(\mathcal{O}_K)\}$$

$$\mathrm{rot}(Q) = \left(\begin{array}{c|c} 1 & \\ \ddots & \\ 1 & \\ \hline & 1 \\ & \ddots \\ & 1 \end{array}\right) \in \mathbb{Z}^{2n \times 2n} \longrightarrow \Lambda = \mathbb{Z}^{2n \times 2n}$$

Need to sample [Q] for an average case.

Need to sample $[Q]$ for an average case.

In NTRU one samples $\begin{pmatrix} f \\ g \end{pmatrix} \in \mathcal{O}_K^2$ from "D" and "completes" to

$$\begin{pmatrix} f & F \\ g & G \end{pmatrix} \in \mathcal{O}_K^{2\times 2} \text{ such that } fG - gF = d.$$

Need to sample $[Q]$ for an average case.

In NTRU one samples $\begin{pmatrix} f \\ g \end{pmatrix} \in \mathcal{O}_K^2$ from "D" and "completes" to

$$\begin{pmatrix} f & F \\ g & G \end{pmatrix} \in \mathcal{O}_K^{2\times 2} \text{ such that } fG - gF = d.$$

$\hookrightarrow \begin{pmatrix} f & F \\ g & G \end{pmatrix} \in SL_2(\mathcal{O}_K)$, when $d = 1$

$\hookrightarrow$ D gives distribution on $\mathcal{O}_K^2$

$\hookrightarrow$ $(D \mid \text{Complete}(D))$ gives distribution on $\mathcal{O}_K^{2\times 2}$

$D_\sigma^{NTRU}([Q]), \quad Q \in \mathcal{H}_Z^{20}(K)$

1.) $\begin{pmatrix} f \\ g \end{pmatrix} \leftarrow D_{Q,\sigma}$

2.) $\begin{pmatrix} F \\ G \end{pmatrix} \leftarrow \text{Complete}(d=1, f, g)$

3.) $\begin{pmatrix} F \\ G \end{pmatrix} \leftarrow \text{SizeRed}(Q, f, g, F, G)$

4.) $\mathcal{U} = \begin{pmatrix} f & F \\ g & G \end{pmatrix}, \quad R = \mathcal{U}^* Q \mathcal{U}$

5. return $(R, \mathcal{U})$

$D_\sigma^{NTRU}([Q]), \quad Q \in \mathcal{H}_Z^{+0}(K)$

1.) $\begin{pmatrix} f \\ g \end{pmatrix} \leftarrow D_{Q,\sigma}$

2.) $\begin{pmatrix} F \\ G \end{pmatrix} \leftarrow \text{Complete}(d=1, f, g)$

3.) $\begin{pmatrix} F \\ G \end{pmatrix} \leftarrow \text{SizeRed}(Q, f, g, F, G)$

4.) $\mathcal{U} = \begin{pmatrix} f & F \\ g & G \end{pmatrix}, \quad R = \mathcal{U}^* Q \mathcal{U}$

5. return $(R, \mathcal{U})$

- efficient for large enough σ
- $R \in [Q]$ and independent of Q.

Def $ac\text{-}mskIP_\sigma^Q$

Given $Q, Q' \leftarrow D_\sigma^{NTRU}([Q])$ find $U \in SL_2(\mathcal{O}_K)$

$Q' = U^* Q U$

Def $ac\text{-}mslIP_\sigma^Q$

Given $Q, Q' \leftarrow D_\sigma^{NTRU}([Q])$ find $U \in SL_2(\mathcal{O}_K)$

$Q' = U^* Q U$

Thm (Similar to [DvW22])

$$wc\text{-}mslIP_\sigma^Q \longrightarrow ac\text{-}mslIP_\sigma^Q$$

Hawk: $H : \{0,1\}^* \longrightarrow \{0,\tfrac{1}{2}\}^{2n}$, $Q = I_2(K)$, $(\sigma_{keygen}, \sigma_{sign})$

$KGen(1^n)$:

$(R, U) \leftarrow D_{\sigma}^{NTRU}([Q])$, $pk = R$, $sk = U$

$Sign(sk, m)$:

$r \leftarrow \mathcal{U}(\{0,1\}^{saltlen})$

$h = H(m, r)$

$x \leftarrow D_{Q, \mathbb{Z}^{2n} + Uh, \sigma_{sign}}$

return $sig = (r,\ h - U^{-1}x)$

$Vf(pk, m, sig)$: $h = H(m, r)$

return $[\![h - U^{-1}x \in \mathcal{O}_K^2]\!] \wedge [\![\|Ux\|_K \leq (1+\varepsilon)\sqrt{n}\,\sigma_{sign}]\!]$

Hawk: $H : \{0,1\}^* \longrightarrow \{0,\tfrac{1}{2}\}^{2n}$, $Q = I_2(K)$, $(\sigma_{keygen}, \sigma_{sign})$

$KGen(1^n)$:

$(R, \mathcal{U}) \leftarrow D^{NTRU}_{\sigma}([Q])$, $pk = R$, $sk = \mathcal{U}$

↳ $ac - msLIP^{Q}_{\sigma_{keygen}}$

$Sign(sk, m)$:

$r \leftarrow \mathcal{U}(\{0,1\}^{saltlen})$

$h = H(m, r)$

$x \leftarrow D_{Q, \mathbb{Z}^{2n} + \mathcal{U}h, \sigma_{sign}}$ } purposefully "casual"

return $sig = (r,\ h - \mathcal{U}^{-1}x)$ }

$Vf(pk, m, sig)$: $h = H(m, r)$

return $[\![h - \mathcal{U}^{-1}x \in \mathcal{O}_K^2]\!] \wedge [\![\|\mathcal{U}^{-1}x\|_K \le (1+\varepsilon)\sqrt{n}\,\sigma_{sign}]\!]$

Practical security — an approx module CVP over NTRU like lattices

Practical security — an approx module CVP over NTRU like lattices

Reductionist security:

To "omSVP"

Intuition: Given $Q' \leftarrow D_\sigma^{NTRU}([Q])$

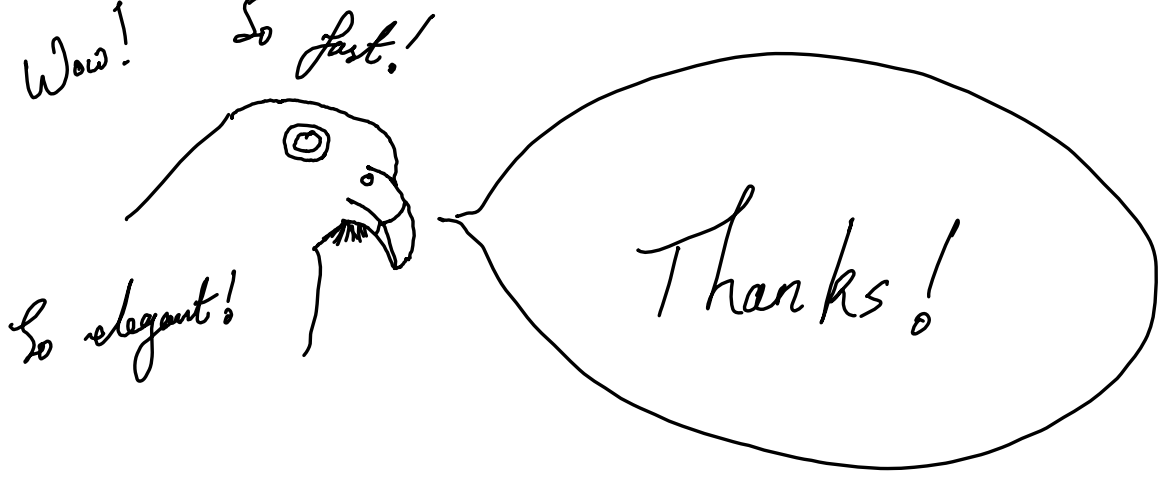
and $\mathcal{O}^{samp(\cdot)}$ giving $x \leftarrow D_{Q',\sigma}$

find "new" $x^* \in \mathcal{O}_K^2$, $\|x^*\|_Q \approx \sqrt{2n}\sigma$.

Implementation:

- No floating points
- Drop and (publicly) recover half of sig
- small table based sampling of $D_{\mathbb{Z}, \sigma_{sign}}$, $D_{\mathbb{Z}+\frac{1}{2}, \sigma_{sign}}$
- fully isochronous

	[46] Falcon 512	This work Hawk 512	Gain ($\frac{\text{Falcon}}{\text{Hawk}}$)	[46] Falcon 1024	This work Hawk 1024	Gain ($\frac{\text{Falcon}}{\text{Hawk}}$)
AVX2 KGen	7.95 ms	4.25 ms	×1.87	23.60 ms	17.88 ms	×1.32
Reference KGen	19.32 ms	13.14 ms	×1.47	54.65 ms	41.39 ms	×1.32
AVX2 Sign	193 µs	50 µs	× 3.9	382 µs	99 µs	× 3.9
Reference Sign	2449 µs	168 µs	×14.6	5273 µs	343 µs	×15.4
AVX2 Vf	50 µs	19 µs	×2.63	99 µs	46 µs	×2.15
Reference Vf	53 µs	178 µs	×0.30	105 µs	392 µs	×0.27
Secret key (bytes)	1281	1153	×1.11	2305	2561	×0.90
Public key (bytes)	897	1006 ± 6	×0.89	1793	2329 ± 11	×0.77
Signature (bytes)	652 ± 3	542 ± 4	×1.21	1261 ± 4	1195 ± 6	×1.05



eprint: 2022/1155

code: ludopulles/hawk-aux