Gaussian Leftover Hash Lemma for Module Lattices

Joël Felderhoff

Joint work with Martin R. Albrecht, Russell W. F. Lai, Sasha Lapiha and Ivy K. Y. Woo

King's College London

09/10/2025

Outline

In this talk

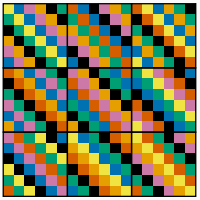
1. Lattices and SIS
2. Structured Matrices and Module Lattices
3. SIS with hints
4. **Module Gaussian LHL** (our contribution)

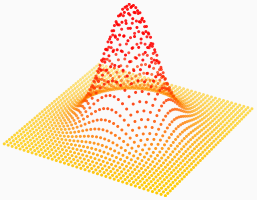
Outline

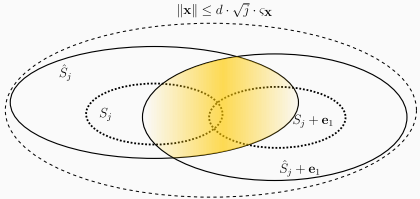
In this talk

1. Lattices and SIS
2. Structured Matrices and Module Lattices
3. SIS with hints
4. **Module Gaussian LHL** (our contribution)

Full of pictures!

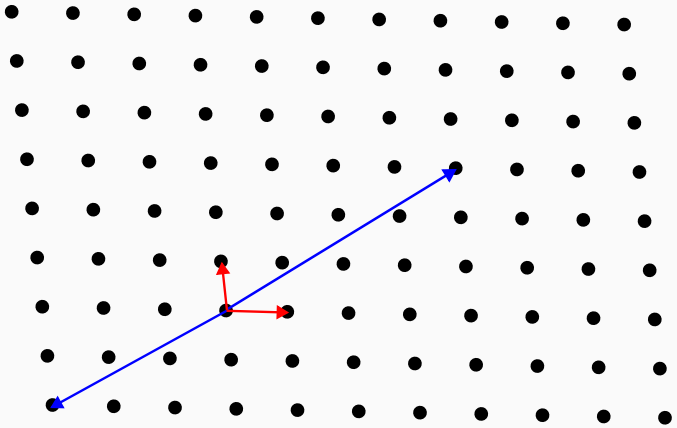






Lattices and SIS

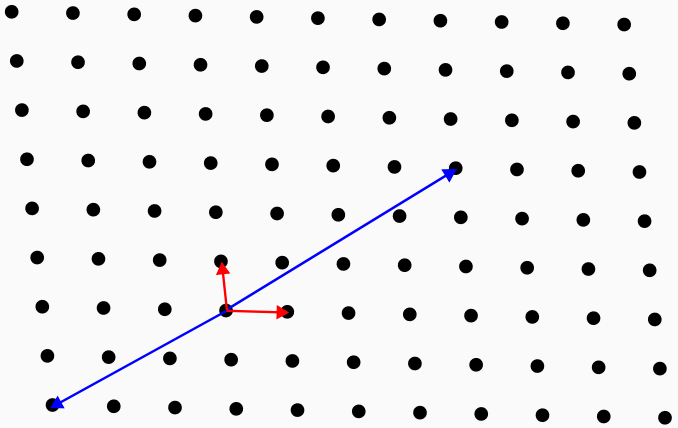
Lattices and SIVP



Lattice spanned by $\mathbf{B} \in \mathbb{Z}^{n \times n}$:

$$\mathcal{L} = \mathcal{L}(\mathbf{B}) = \{\mathbf{B} \cdot \mathbf{x},\ \mathbf{x} \in \mathbb{Z}^n\}.$$

Lattices and SIVP



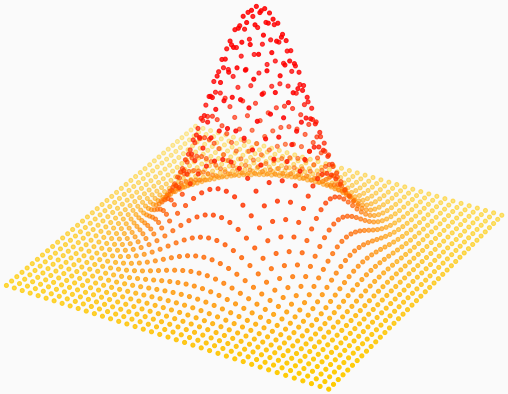
Lattice spanned by $\mathbf{B} \in \mathbb{Z}^{n \times n}$:

$$\mathcal{L} = \mathcal{L}(\mathbf{B}) = \{\mathbf{B} \cdot \mathbf{x},\ \mathbf{x} \in \mathbb{Z}^n\}.$$

($\approx$) SIVP

Given $\mathbf{B}$, find $\mathbf{B}'$ with $\|\mathbf{B}'\|$ small and $\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{B}')$.

Discrete Gaussian Distribution

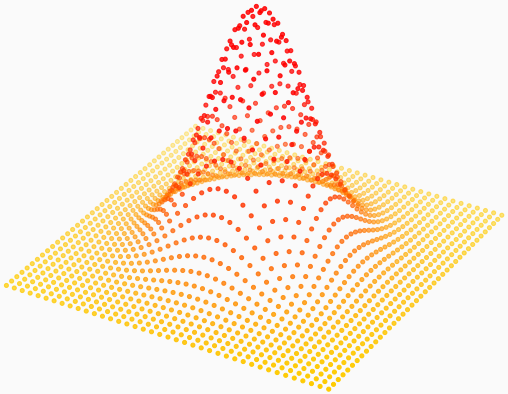


Discrete Gaussian Distribution $\mathcal{D}_{\mathcal{L},\mathbf{S}}$

For any $\mathbf{x} \in \mathcal{L}$,

$$\mathcal{D}_{\mathcal{L},\varsigma}(\mathbf{x}) \propto \exp\left(-\pi \cdot \left\|\mathbf{S}^{-1} \cdot \mathbf{x}\right\|^2\right).$$

Discrete Gaussian Distribution



Discrete Gaussian Distribution $\mathcal{D}_{\mathcal{L},\mathbf{S}}$

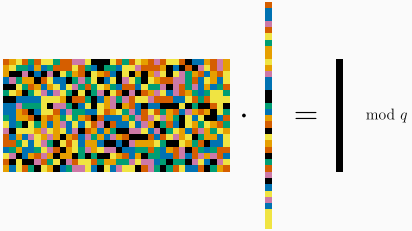
For any $\mathbf{x} \in \mathcal{L}$,

$$\mathcal{D}_{\mathcal{L},\varsigma}(\mathbf{x}) \propto \exp\left(-\pi \cdot \left\|\mathbf{S}^{-1} \cdot \mathbf{x}\right\|^2\right).$$

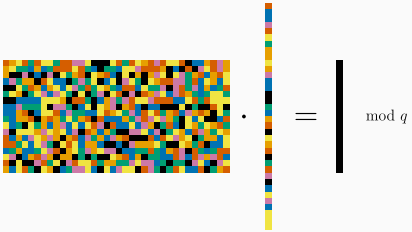
What we use here ($\mathbf{S} = \varsigma \cdot \mathbf{I}$):

- Looks like continuous Gaussian for large ς.
- Give short vectors $\|\mathbf{x}\| \leq \sqrt{n} \cdot \varsigma$.
- Rotation-invariant.

The Short Integer Solution Problem



The Short Integer Solution Problem

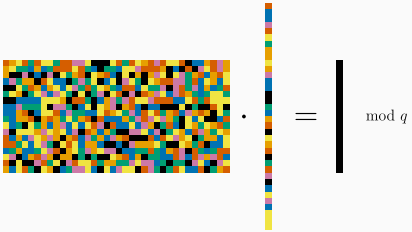


Short Integer Solution ($\mathsf{SIS}_{n,m,q,\beta}$) problem

Given $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$, find $\mathbf{v} \in \mathbb{Z}^m$ such that

$$\mathbf{A} \cdot \mathbf{v} = \mathbf{0} \bmod q \quad \text{and} \quad 0 < \|\mathbf{v}\| \leq \beta.$$

The Short Integer Solution Problem



Short Integer Solution ($\mathsf{SIS}_{n,m,q,\beta}$) problem

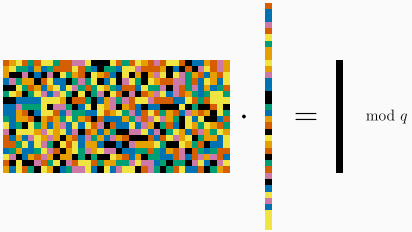
Given $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$, find $\mathbf{v} \in \mathbb{Z}^m$ such that

$$\mathbf{A} \cdot \mathbf{v} = \mathbf{0} \bmod q \quad \text{and} \quad 0 < \|\mathbf{v}\| \leq \beta.$$

Lattice problem with:

$$\mathcal{L} = \Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{v} \in \mathbb{Z}^m, \mathbf{A} \cdot \mathbf{v} = \mathbf{0} \bmod q\}.$$

The Short Integer Solution Problem



Short Integer Solution ($\mathsf{SIS}_{n,m,q,\beta}$) problem

Given $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$, find $\mathbf{v} \in \mathbb{Z}^m$ such that

$$\mathbf{A} \cdot \mathbf{v} = \mathbf{0} \bmod q \quad \text{and} \quad 0 < \|\mathbf{v}\| \leq \beta.$$

Lattice problem with:

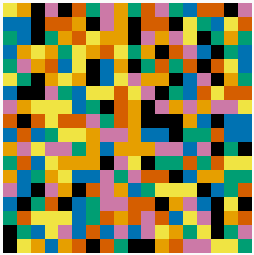
$$\mathcal{L} = \Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{v} \in \mathbb{Z}^m, \mathbf{A} \cdot \mathbf{v} = \mathbf{0} \bmod q\}.$$

Hard Lattice Problem: as hard as SIVP for proper parameters.

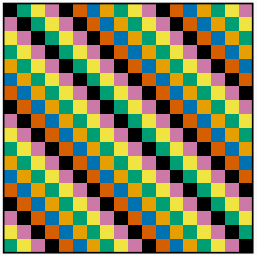
Structured Matrices and Module Lattices

Structured Matrices

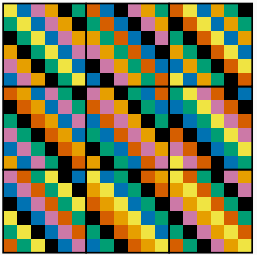
For speed, in reality, we use matrices with structure (e.g. from algebraic number theory).



Unstructured



Rank 1
Ideal Lattices



Rank 3
Module lattice

Rank r, degree d: dimension $n = r \cdot d$ with $r^2 \cdot d$ integers + NTT

In more details: Number fields and Modules

$\mathbb{Z}^n$	$\mathcal{O}_\mathcal{K} = \mathbb{Z}[X]/(X^n+1)$	$\mathbb{Z}[X]/(X^2+1)$
$\mathbf{v} = \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix}$	$P(X) = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1}$	$X + 2$
$\|\mathbf{v}\|$	$\sqrt{\sum_{i=0}^{n-1} a_i^2}$	$\sqrt{5}$

In more details: Number fields and Modules

$\mathbb{Z}^n$	$\mathcal{O}_\mathcal{K} = \mathbb{Z}[X]/(X^n+1)$	$\mathbb{Z}[X]/(X^2+1)$
$\mathbf{v} = \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix}$	$P(X) = a_0 + a_1 X + \ldots + a_{n-1}X^{n-1}$	$X + 2$
$\|\mathbf{v}\|$	$\sqrt{\sum_{i=0}^{n-1} a_i^2}$	$\sqrt{5}$

(free) Module Lattice

$\mathcal{K}$ number field of degree d, $\mathbf{M} \in \mathcal{O}_\mathcal{K}^{r\times r}$

$$\mathcal{M} := \{\mathbf{M}\cdot\mathbf{v},\ \mathbf{v} \in \mathcal{O}_\mathcal{K}^r\} \subseteq \mathcal{O}_\mathcal{K}^r \simeq \mathbb{Z}^{dr}.$$

SIS with hints

Add a twist to SIS: hints

"If I already give you k random short solutions, can you find another one?"

Add a twist to SIS: hints

"If I already give you k random short solutions, can you find another one?"

"SIS with hints": k-SIS$_{n,m,q,\beta}$

Given $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$ and $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}),\varsigma}$ find $\mathbf{v} \in \mathbb{Z}^m$ such that $\mathbf{v} \notin \mathrm{span}_{\mathbb{Q}}(\mathbf{x}_1, \ldots, \mathbf{x}_k)$,

$$\mathbf{A} \cdot \mathbf{v} = \mathbf{0} \bmod q \quad \text{and} \quad 0 < \|\mathbf{v}\| \leq \beta.$$

Add a twist to SIS: hints

"If I already give you k random short solutions, can you find another one?"

"SIS with hints": k-SIS$_{n,m,q,\beta}$

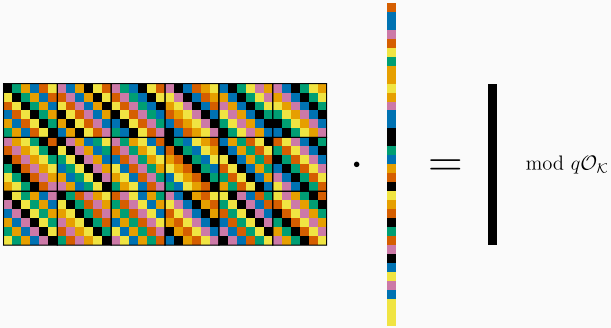
Given $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ and $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}),\varsigma}$ find $\mathbf{v} \in \mathbb{Z}^m$ such that $\mathbf{v} \notin \mathrm{span}_{\mathbb{Q}}(\mathbf{x}_1, \ldots, \mathbf{x}_k)$,

$$\mathbf{A} \cdot \mathbf{v} = \mathbf{0} \bmod q \quad \text{and} \quad 0 < \|\mathbf{v}\| \leq \beta.$$

Applications:

- Linearly homomorphic signatures [BF11];
- New lattice trapdoors [ALLW25];
- k-M-ISIS: SNARKs [ACL+22].

The structured version: M-SIS and k-M-SIS



k-M-SIS

Given $\mathbf{A} \xleftarrow{\$} (\mathcal{O}_\mathcal{K}/q)^{n\times m}$ and $\mathbf{x}_1, \ldots, \mathbf{x}_k \leftarrow \mathcal{D}_{\Lambda_q^\perp(\mathbf{A}),\varsigma}$ find $\mathbf{v} \in \mathcal{O}_\mathcal{K}^m$ such that

$$\mathbf{v} \notin \underset{\mathcal{K}}{\operatorname{span}}(\mathbf{x}_1, \ldots, \mathbf{x}_k) \quad \text{and} \quad \mathbf{A}\cdot\mathbf{v} = \mathbf{0} \bmod q\mathcal{O}_\mathcal{K} \quad \text{and} \quad 0 < \|\mathbf{v}\| \leq \beta.$$

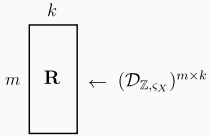
Hints do not break anything: $\mathrm{SIS}_r \to k\text{-}\mathrm{SIS}_{r+k}$ [LPSS14]

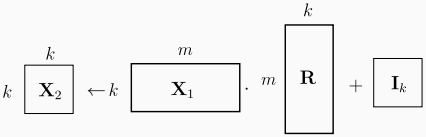
Hints do not break anything: $\mathrm{SIS}_r \to k\text{-}\mathrm{SIS}_{r+k}$ [LPSS14]

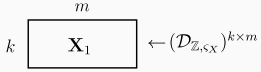
Idea: First build the hints, then build the matrix around them.

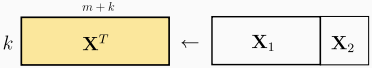
Hints do not break anything: $\mathrm{SIS}_r \to k\text{-}\mathrm{SIS}_{r+k}$ [LPSS14]

Idea: First build the hints, then build the matrix around them.

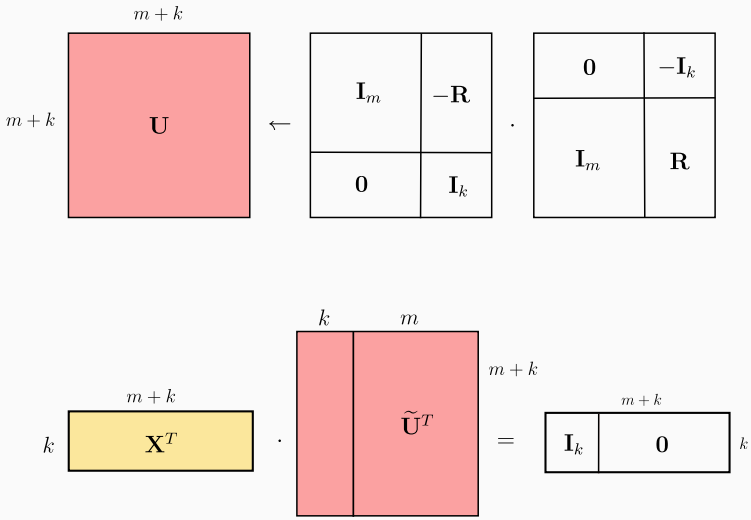






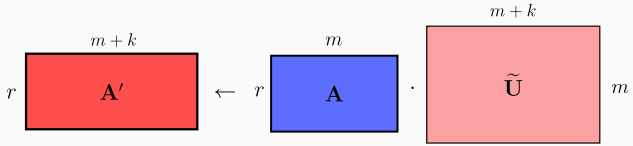


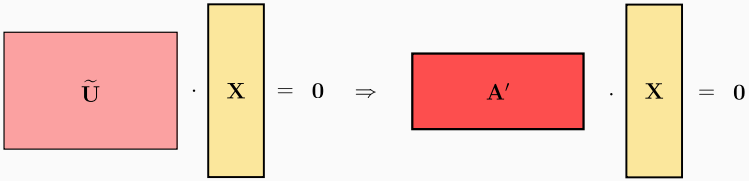
Hints do not break anything: Trapdoor construction [LPSS14]



Hints do not break anything: k-SIS instance [LPSS14]

Reduction: we get $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{r \times m}$ and construct a k-SIS instance $(\mathbf{A}', \mathbf{x}_1, \dots \mathbf{x}_k)$.





The Result of Merit: the Gaussian Leftover Hash Lemma [AGHS13]

This only works if $\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_1 \cdot \mathbf{R} + \mathbf{I}_k)$ looks like a discrete Gaussian.

The Result of Merit: the Gaussian Leftover Hash Lemma [AGHS13]

This only works if $\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_1 \cdot \mathbf{R} + \mathbf{I}_k)$ looks like a discrete Gaussian.

Gaussian Leftover Hash Lemma [AGHS13]

Let $\varepsilon > 0$. Let $1 \leq r \leq m$ and $\varsigma_{\mathbf{X}}, \varsigma_{\mathbf{r}} > 0$. If $\mathbf{X} \xleftarrow{\$} \mathcal{D}^{r \times m}_{\mathcal{O}_\mathcal{K}, \varsigma_{\mathbf{X}}}$ and $\mathbf{r} \xleftarrow{\$} \mathcal{D}^{m}_{\mathcal{O}_\mathcal{K}, \varsigma_{\mathbf{r}}}$, then it holds that

$$(\mathbf{X}, \mathbf{X} \cdot \mathbf{r}) \approx_\varepsilon \left(\mathcal{D}^{r \times m}_{\mathbb{Z}, \varsigma_{\mathbf{X}}}, \mathcal{D}^{r}_{\mathbb{Z}, \sqrt{\mathbf{X}\mathbf{X}^T} \cdot \varsigma_{\mathbf{r}}} \right)$$

The Result of Merit: the Gaussian Leftover Hash Lemma [AGHS13]

This only works if $\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_1 \cdot \mathbf{R} + \mathbf{I}_k)$ looks like a discrete Gaussian.

Gaussian Leftover Hash Lemma [AGHS13]

Let $\varepsilon > 0$. Let $1 \leq r \leq m$ and $\varsigma_{\mathbf{X}}, \varsigma_{\mathbf{r}} > 0$. If $\mathbf{X} \xleftarrow{\$} \mathcal{D}^{r \times m}_{\mathcal{O}_\mathcal{K}, \varsigma_{\mathbf{X}}}$ and $\mathbf{r} \xleftarrow{\$} \mathcal{D}^{m}_{\mathcal{O}_\mathcal{K}, \varsigma_{\mathbf{r}}}$, then it holds that

$$(\mathbf{X}, \mathbf{X} \cdot \mathbf{r}) \approx_\varepsilon \left(\mathcal{D}^{r \times m}_{\mathbb{Z}, \varsigma_{\mathbf{X}}}, \mathcal{D}^{r}_{\mathbb{Z}, \sqrt{\mathbf{X}\mathbf{X}^T} \cdot \varsigma_{\mathbf{r}}} \right)$$

One needs [KNSW20]:

- $m \geq \Omega(r \log(\varsigma_{\mathbf{X}}))$;
- $\varsigma_{\mathbf{X}} \geq \Omega(\sqrt{r})$;
- $\varsigma_{\mathbf{r}} \geq \Omega(\sqrt{r \ln(m/\varepsilon)})$.

Hints do not break anything: $\text{M-SIS}_r^{\mathcal{K}} \to k\text{-M-SIS}_{r+k}^{\mathcal{K}}$

The exact same reduction works.

$\mathbf{X}_1 \leftarrow \mathcal{D}_{\mathcal{O}_\mathcal{K}, s_\mathbf{X}}^{m \times k}$

$\mathbf{R} \leftarrow \mathcal{D}_{\mathcal{O}_\mathcal{K}, s_\mathbf{X}}^{k \times m}$

$\mathbf{X}_2 \leftarrow \mathbf{X}_1 \cdot \mathbf{R} + \mathbf{I}_k$

Hints do not break anything: M-SIS$_r^{\mathcal{K}} \to k$-M-SIS$_{r+k}^{\mathcal{K}}$

The exact same reduction works.

$\mathbf{X}_1 \leftarrow \mathcal{D}_{\mathcal{O}_\mathcal{K},s_\mathbf{X}}^{m \times k}$

$\mathbf{R} \leftarrow \mathcal{D}_{\mathcal{O}_\mathcal{K},s_\mathbf{X}}^{k \times m}$

$\mathbf{X}_2 \leftarrow \mathbf{X}_1 \cdot \mathbf{R} + \mathbf{I}_k$

$\mathbf{X}^T \leftarrow [\mathbf{X}_1 | \mathbf{X}_2]$

Same $\mathbf{U}^T = [\mathbf{U}' | \widetilde{\mathbf{U}}^T]$

$\mathbf{X} \cdot \widetilde{\mathbf{U}} = \mathbf{0}$

On input $\mathbf{A} \xleftarrow{\$} (\mathcal{O}_\mathcal{K}/q)^{r \times m}$,
Output $\mathbf{A} \cdot \mathbf{U}'$ with hints $\mathbf{X}$.

Hints do not break anything: $\text{M-SIS}_r^{\mathcal{K}} \to k\text{-M-SIS}_{r+k}^{\mathcal{K}}$

The exact same reduction works.

$\mathbf{X}_1 \leftarrow \mathcal{D}_{\mathcal{O}_\mathcal{K},\varsigma_\mathbf{X}}^{m\times k}$

$\mathbf{R} \leftarrow \mathcal{D}_{\mathcal{O}_\mathcal{K},\varsigma_\mathbf{X}}^{k\times m}$

$\mathbf{X}_2 \leftarrow \mathbf{X}_1 \cdot \mathbf{R} + \mathbf{I}_k$

$\mathbf{X}^T \leftarrow [\mathbf{X}_1|\mathbf{X}_2]$

Same $\mathbf{U}^T = [\mathbf{U}'|\widetilde{\mathbf{U}}^T]$

$\mathbf{X} \cdot \widetilde{\mathbf{U}} = \mathbf{0}$

On input $\mathbf{A} \xleftarrow{\$} (\mathcal{O}_\mathcal{K}/q)^{r\times m}$,
Output $\mathbf{A} \cdot \mathbf{U}'$ with hints $\mathbf{X}$.

Conditions on m, r and ς

- $\underbrace{m \geq \Omega(rd\log(\varsigma_\mathbf{X}))}_{\text{Way too large}}$;
- $\varsigma_\mathbf{X} \geq \Omega\sqrt{rd}$;
- $\varsigma_\mathbf{r} \geq \Omega(\sqrt{rd\ln(m/\varepsilon)})$.

Module Gaussian LHL

The statement we want

Module Gaussian LHL (conditions omited)

Let $\varepsilon > 0$. Let $\mathcal{K}$ of degree $d \geq 2$, $1 \leq r \leq m$ and $\varsigma_{\mathbf{X}}, \varsigma_{\mathbf{r}} > 0$. If $\mathbf{X} \xleftarrow{\$} \mathcal{D}^{r \times m}_{\mathcal{O}_{\mathcal{K}}, \varsigma_{\mathbf{X}}}$ and $\mathbf{r} \xleftarrow{\$} \mathcal{D}^{m}_{\mathcal{O}_{\mathcal{K}}, \varsigma_{\mathbf{r}}}$, then it holds that

$$(\mathbf{X}, \mathbf{X} \cdot \mathbf{r}) \approx_{\varepsilon} \left(\mathcal{D}^{r \times m}_{\mathcal{O}_{\mathcal{K}}, \varsigma_{\mathbf{X}}}, \mathcal{D}^{r}_{\mathcal{O}_{\mathcal{K}}, \sqrt{\mathbf{X}\mathbf{X}^{T}} \cdot \varsigma_{\mathbf{r}}} \right)$$

The statement we want

Module Gaussian LHL (conditions omited)

Let $\varepsilon > 0$. Let $\mathcal{K}$ of degree $d \geq 2$, $1 \leq r \leq m$ and $\varsigma_{\mathbf{X}}, \varsigma_{\mathbf{r}} > 0$. If $\mathbf{X} \xleftarrow{\$} \mathcal{D}^{r \times m}_{\mathcal{O}_{\mathcal{K}}, \varsigma_{\mathbf{X}}}$ and $\mathbf{r} \xleftarrow{\$} \mathcal{D}^{m}_{\mathcal{O}_{\mathcal{K}}, \varsigma_{\mathbf{r}}}$, then it holds that

$$(\mathbf{X}, \mathbf{X} \cdot \mathbf{r}) \approx_{\varepsilon} \left(\mathcal{D}^{r \times m}_{\mathcal{O}_{\mathcal{K}}, \varsigma_{\mathbf{X}}}, \mathcal{D}^{r}_{\mathcal{O}_{\mathcal{K}}, \sqrt{\mathbf{X}\mathbf{X}^{T}} \cdot \varsigma_{\mathbf{r}}} \right)$$

Our goal:

- $m \geq \widetilde{\Omega}(r \cdot \log(rd \cdot \varsigma_{\mathbf{X}}))$
- $\varsigma_{\mathbf{X}} \geq \mathrm{poly}(d, m, \log(1/\varepsilon))$
- $\varsigma_{\mathbf{r}} \geq \mathrm{poly}(d, m, \log(1/\varepsilon))$

The statement we want

Module Gaussian LHL (conditions omited)

Let $\varepsilon > 0$. Let $\mathcal{K}$ of degree $d \geq 2$, $1 \leq r \leq m$ and $\varsigma_{\mathbf{X}}, \varsigma_{\mathbf{r}} > 0$. If $\mathbf{X} \xleftarrow{\$} \mathcal{D}^{r \times m}_{\mathcal{O}_{\mathcal{K}}, \varsigma_{\mathbf{X}}}$ and $\mathbf{r} \xleftarrow{\$} \mathcal{D}^{m}_{\mathcal{O}_{\mathcal{K}}, \varsigma_{\mathbf{r}}}$, then it holds that

$$(\mathbf{X}, \mathbf{X} \cdot \mathbf{r}) \approx_{\varepsilon} \left(\mathcal{D}^{r \times m}_{\mathcal{O}_{\mathcal{K}}, \varsigma_{\mathbf{X}}}, \mathcal{D}^{r}_{\mathcal{O}_{\mathcal{K}}, \sqrt{\mathbf{X}\mathbf{X}^{T}} \cdot \varsigma_{\mathbf{r}}} \right)$$

Our goal:

- $m \geq \widetilde{\Omega}(r \cdot \log(rd \cdot \varsigma_{\mathbf{X}}))$
- $\varsigma_{\mathbf{X}} \geq \mathrm{poly}(d, m, \log(1/\varepsilon))$
- $\varsigma_{\mathbf{r}} \geq \mathrm{poly}(d, m, \log(1/\varepsilon))$

Conditions on $\mathbf{X}$ to prove this [AGHS13]:

- $\mathbf{X}$ surjective in $\mathcal{O}^{r}_{\mathcal{K}}$: $\mathbf{X} \cdot \mathcal{O}^{m}_{\mathcal{K}} = \mathcal{O}^{r}_{\mathcal{K}}$.

The statement we want

Module Gaussian LHL (conditions omited)

Let $\varepsilon > 0$. Let $\mathcal{K}$ of degree $d \geq 2$, $1 \leq r \leq m$ and $\varsigma_{\mathbf{X}}, \varsigma_{\mathbf{r}} > 0$. If $\mathbf{X} \xleftarrow{\$} \mathcal{D}^{r \times m}_{\mathcal{O}_{\mathcal{K}}, \varsigma_{\mathbf{X}}}$ and $\mathbf{r} \xleftarrow{\$} \mathcal{D}^{m}_{\mathcal{O}_{\mathcal{K}}, \varsigma_{\mathbf{r}}}$, then it holds that

$$(\mathbf{X}, \mathbf{X} \cdot \mathbf{r}) \approx_{\varepsilon} \left(\mathcal{D}^{r \times m}_{\mathcal{O}_{\mathcal{K}}, \varsigma_{\mathbf{X}}}, \mathcal{D}^{r}_{\mathcal{O}_{\mathcal{K}}, \sqrt{\mathbf{X}\mathbf{X}^{T}} \cdot \varsigma_{\mathbf{r}}} \right)$$

Our goal:

- $m \geq \widetilde{\Omega}(r \cdot \log(rd \cdot \varsigma_{\mathbf{X}}))$
- $\varsigma_{\mathbf{X}} \geq \mathrm{poly}(d, m, \log(1/\varepsilon))$
- $\varsigma_{\mathbf{r}} \geq \mathrm{poly}(d, m, \log(1/\varepsilon))$

Conditions on $\mathbf{X}$ to prove this [AGHS13]:

- $\mathbf{X}$ surjective in $\mathcal{O}^{r}_{\mathcal{K}}$: $\mathbf{X} \cdot \mathcal{O}^{m}_{\mathcal{K}} = \mathcal{O}^{r}_{\mathcal{K}}$.
- $\Lambda^{\perp}(\mathbf{X}) = \{\mathbf{x} \in \mathcal{O}^{m}_{\mathcal{K}}, \mathbf{X} \cdot \mathbf{x} = \mathbf{0}\}$ has a small basis.

Surjectivity of a Matrix in $\mathcal{O}_K^r$: Finite Fields

Surjectivity of integral matrices

A matrix $\mathbf{X} \in \mathbb{Z}^{r \times m}$ is surjective in $\mathbb{Z}^r$ iff it is surjective modulo p for any prime p.

Surjectivity of a Matrix in $\mathcal{O}_{\mathcal{K}}^r$: Finite Fields

Surjectivity of integral matrices

A matrix $\mathbf{X} \in \mathcal{O}_{\mathcal{K}}^{r \times m}$ is surjective in $\mathcal{O}_{\mathcal{K}}^r$ iff it is surjective modulo $\mathfrak{p}$ for any prime ideal $\mathfrak{p}$.

Surjectivity of a Matrix in $\mathcal{O}_{\mathcal{K}}^r$: Finite Fields

Surjectivity of integral matrices

A matrix $\mathbf{X} \in \mathcal{O}_{\mathcal{K}}^{r \times m}$ is surjective in $\mathcal{O}_{\mathcal{K}}^r$ iff it is surjective modulo $\mathfrak{p}$ for any prime ideal $\mathfrak{p}$.

Surjectivity on finite fields is easy:

Theorem (Surjectivity of Random Matrices over Finite Fields[NP20])

If $\mathbf{X} = (x_{i,j}) \in \mathbb{F}_q^{r \times m}$ *has independent entries with min-entropy* $\geq \ln(1/\alpha)$, *then*

$$\Pr\left(\mathbf{X} \cdot \mathbb{F}_q^m = \mathbb{F}_q^r\right) \geq 1 - r \cdot \alpha^{m-r+1}.$$

Surjectivity of a Matrix in $\mathcal{O}_{\mathcal{K}}^r$: Finite Fields

Surjectivity of integral matrices

A matrix $\mathbf{X} \in \mathcal{O}_{\mathcal{K}}^{r \times m}$ is surjective in $\mathcal{O}_{\mathcal{K}}^r$ iff it is surjective modulo $\mathfrak{p}$ for any prime ideal $\mathfrak{p}$.

Surjectivity on finite fields is easy:

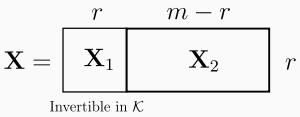
Theorem (Surjectivity of Random Matrices over Finite Fields[NP20])

If $\mathbf{X} = (x_{i,j}) \in \mathbb{F}_q^{r \times m}$ *has independent entries with min-entropy* $\geq \ln(1/\alpha)$, *then*

$$\Pr\left(\mathbf{X} \cdot \mathbb{F}_q^m = \mathbb{F}_q^r\right) \geq 1 - r \cdot \alpha^{m-r+1}.$$

But there are infinitely many primes...

Surjectivity of a Matrix in $\mathcal{O}_{\mathcal{K}}^{r}$



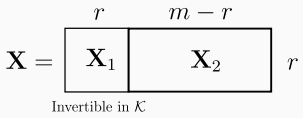
Surjectivity of a Matrix in $\mathcal{O}_{\mathcal{K}}^{r}$

$$\mathbf{X} = \begin{array}{c} \overset{r}{\mathbf{X}_1} \quad \overset{m-r}{\mathbf{X}_2} \\ \boxed{\phantom{\mathbf{X}_1}\,\boxed{\phantom{\mathbf{X}_2}}} \end{array} \; r$$

Invertible in $\mathcal{K}$

We just have to test $\mathfrak{p} \mid \det_K(\mathbf{X}_1)$!

Surjectivity of a Matrix in $\mathcal{O}_{\mathcal{K}}^r$



We just have to test $\mathfrak{p} | \det_K(\mathbf{X}_1)$!

Prime $\mathfrak{p}$: probability $1 - r \cdot \mathcal{N}(\mathfrak{p})^{-m+r-1}$.

Surjectivity of a Matrix in $\mathcal{O}_{\mathcal{K}}^{r}$

$$\mathbf{X} = \begin{array}{c} \overset{r}{\mathbf{X}_1} \quad \overset{m-r}{\mathbf{X}_2} \\ \text{Invertible in } \mathcal{K} \end{array} \; r$$

We just have to test $\mathfrak{p} | \det_K(\mathbf{X}_1)$!

Prime $\mathfrak{p}$: probability $1 - r \cdot \mathcal{N}(\mathfrak{p})^{-m+r-1}$.

Summing for small primes: $\Pr(\mathbf{X} \text{ is surjective}) \geq 1 - r \cdot \underbrace{P_K(m-r+1)}_{\text{Dedekind Prime } \zeta \text{ function}}$.

Surjectivity of a Matrix in $\mathcal{O}_{\mathcal{K}}^r$

$$\mathbf{X} = \overset{\overset{r}{\downarrow}}{\boxed{\mathbf{X}_1}} \; \overset{\overset{m-r}{\downarrow}}{\boxed{\mathbf{X}_2}} \; \leftarrow r$$

Invertible in $\mathcal{K}$

We just have to test $\mathfrak{p} | \det_K(\mathbf{X}_1)$!

Prime $\mathfrak{p}$: probability $1 - r \cdot \mathcal{N}(\mathfrak{p})^{-m+r-1}$.

Summing for small primes: $\Pr(\mathbf{X} \text{ is surjective}) \geq 1 - r \cdot \underbrace{P_K(m-r+1)}_{\text{Dedekind Prime } \zeta \text{ function}}$.

Theorem (Surjectivity of Gaussian Matrices (under GRH))

If $\mathcal{K}$ is a number field of degree d and $N_{\mathcal{K}}$ is the norm of its smallest ideal then for any $r \geq 1$, $\varepsilon > 0$, ς large enough and $m \geq 2r + \log(1/\varepsilon)/\log(N_{\mathcal{K}})$, it holds that

$$\Pr_{\mathbf{X} \leftarrow \mathcal{D}^{r \times m}_{\mathcal{O}_{\mathcal{K}}, \varsigma}} \left(\mathbf{X} \textit{ is surjective} \right) \gtrsim 1 - \varepsilon.$$

Short Kernel Basis and Finding short vectors in the kernel of X [AR16]

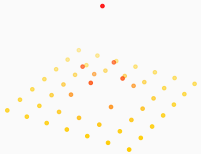
The parameter $\varsigma_{\mathbf{r}}$ needs to be greater than $\eta_{\varepsilon}(\Lambda^{\perp}(\mathbf{X}))$.

Short Kernel Basis and Finding short vectors in the kernel of X [AR16]

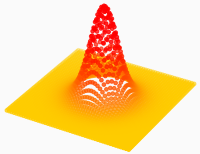
The parameter $\varsigma_{\mathbf{r}}$ needs to be greater than $\eta_{\varepsilon}(\Lambda^{\perp}(\mathbf{X}))$.

$\mathcal{D}_{\mathcal{L},\varsigma}$ for two different $\mathcal{L}$

No short vectors in $\mathcal{L}$



$\mathcal{L}$ has a short basis

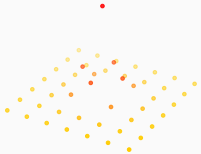


Short Kernel Basis and Finding short vectors in the kernel of X [AR16]

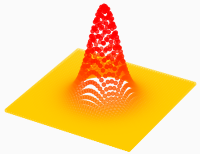
The parameter $\varsigma_{\mathbf{r}}$ needs to be greater than $\eta_{\varepsilon}(\Lambda^{\perp}(\mathbf{X}))$.

$\mathcal{D}_{\mathcal{L},\varsigma}$ for two different $\mathcal{L}$

No short vectors in $\mathcal{L}$



$\mathcal{L}$ has a short basis



Only large vectors in $\Lambda^{\perp}(\mathbf{X}) \Rightarrow \varsigma_{\mathbf{r}}$ large $\Rightarrow$ ☹.

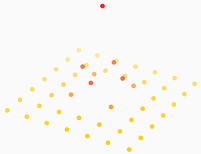
Main trick: find short $\mathbf{U} \in \mathbb{Z}^{m \times r}$ such that $\mathbf{X} \cdot \mathbf{U} = \mathbf{I}_r$.

Short Kernel Basis and Finding short vectors in the kernel of X [AR16]

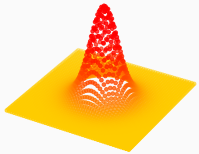
The parameter $\varsigma_{\mathbf{r}}$ needs to be greater than $\eta_\varepsilon(\Lambda^\perp(\mathbf{X}))$.

$\mathcal{D}_{\mathcal{L},\varsigma}$ for two different $\mathcal{L}$

No short vectors in $\mathcal{L}$



$\mathcal{L}$ has a short basis

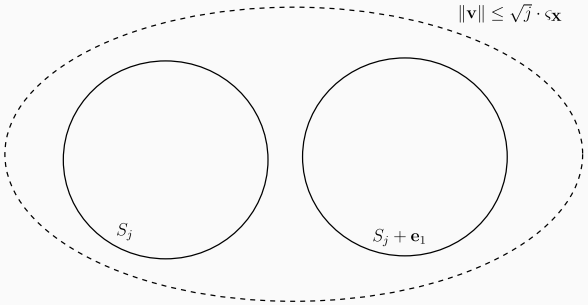


Only large vectors in $\Lambda^\perp(\mathbf{X}) \Rightarrow \varsigma_{\mathbf{r}}$ large $\Rightarrow$ ☹.

Main trick: find short $\mathbf{U} \in \mathbb{Z}^{m \times r}$ such that $\mathbf{X} \cdot \mathbf{U} = \mathbf{I}_r$.
Then, for $\mathbf{Y} = \mathbf{I}_m - \mathbf{U} \cdot \mathbf{X}$ we have $\mathbf{X} \cdot \mathbf{Y} = \mathbf{0} \Rightarrow$ short basis of $\Lambda^\perp(\mathbf{X})$.

Finding a preimage of $\mathbf{I}_r$, the $\mathbb{Z}$ case [AR16]

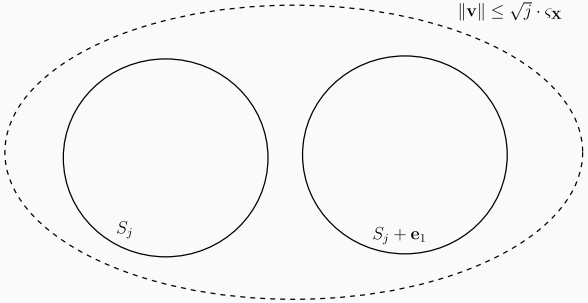
We build $\mathbf{X}$ column by column. Let $\mathbf{X}_j = [\mathbf{x}_1, \ldots, \mathbf{x}_j]$ and $S_j = \left\{ \sum_{i=1}^{j} \{\pm 1, 0\} \cdot \mathbf{x}_i \right\}$.



With constant probability, $|S_{j+1}| = 3 \cdot |S_j|$.

Finding a preimage of $\mathbf{I}_r$, the $\mathbb{Z}$ case [AR16]

We build $\mathbf{X}$ column by column. Let $\mathbf{X}_j = [\mathbf{x}_1, \ldots, \mathbf{x}_j]$ and $S_j = \left\{ \sum_{i=1}^{j} \{\pm 1, 0\} \cdot \mathbf{x}_i \right\}$.

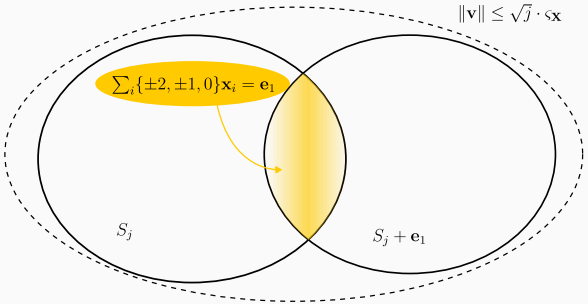


With constant probability, $|S_{j+1}| = 3 \cdot |S_j|$.

$$\left| \left\{ \|v\| \leq \sqrt{j} \cdot \varsigma_{\mathbf{X}} \right\} \right| \approx (\sqrt{j} \cdot \varsigma_{\mathbf{X}})^r.$$

Finding a preimage of $\mathbf{I}_r$, the $\mathbb{Z}$ case [AR16]

We build $\mathbf{X}$ column by column. Let $\mathbf{X}_j = [\mathbf{x}_1, \ldots, \mathbf{x}_j]$ and $S_j = \left\{ \sum_{i=1}^{j} \{\pm 1, 0\} \cdot \mathbf{x}_i \right\}$.



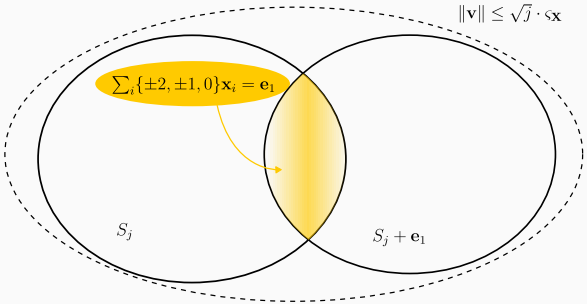
With constant probability, $|S_{j+1}| = 3 \cdot |S_j|$.

$$\left|\left\{\|v\| \leq \sqrt{j} \cdot \varsigma\mathbf{x}\right\}\right| \approx (\sqrt{j} \cdot \varsigma\mathbf{x})^r.$$

For $j \gtrsim r \log(r \cdot \varsigma\mathbf{x})$, $S_j \cap S_j + \mathbf{e}_1 \neq \emptyset$.

Finding a preimage of $\mathbf{I}_r$, the $\mathbb{Z}$ case [AR16]

We build $\mathbf{X}$ column by column. Let $\mathbf{X}_j = [\mathbf{x}_1, \ldots, \mathbf{x}_j]$ and $S_j = \left\{ \sum_{i=1}^{j} \{\pm 1, 0\} \cdot \mathbf{x}_i \right\}$.



With constant probability, $|S_{j+1}| = 3 \cdot |S_j|$.

$$\left|\left\{\|v\| \leq \sqrt{j} \cdot \varsigma_{\mathbf{X}}\right\}\right| \approx (\sqrt{j} \cdot \varsigma_{\mathbf{X}})^r.$$

For $j \gtrsim r \log(r \cdot \varsigma_{\mathbf{X}})$, $S_j \cap S_j + \mathbf{e}_1 \neq \emptyset$.

Preimage of $\mathbf{I}_r$ in $\mathbb{Z}$ [AR16]

If $m \gtrsim r \log(r \cdot \varsigma_{\mathbf{X}}) + \log(1/\varepsilon)$, with probability $1 - \varepsilon$ there exists short $\mathbf{U}$ with $\mathbf{X} \cdot \mathbf{U} = \mathbf{I}_r$.

Finding a preimage of $\mathbf{I}_r$, the $\mathcal{O}_\mathcal{K}$ case

Preimage of $\mathbf{I}_r$ in $\mathcal{O}_\mathcal{K}$ with [AR16]

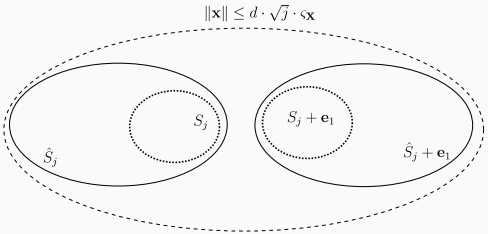
If $m \gtrsim \underbrace{rd}_{\text{Too big!}} \log(rd \cdot \varsigma_{\mathbf{X}}) + \log(1/\varepsilon)$, with probability $1-\varepsilon$ there exists short $\mathbf{U}$ with $\mathbf{X} \cdot \mathbf{U} = \mathbf{I}_r$.

Finding a preimage of $\mathbf{I}_r$, the $\mathcal{O}_\mathcal{K}$ case

Preimage of $\mathbf{I}_r$ in $\mathcal{O}_\mathcal{K}$ with [AR16]

If $m \gtrsim \underbrace{rd}_{\text{Too big!}} \log(rd \cdot \varsigma_\mathbf{X}) + \log(1/\varepsilon)$, with probability $1-\varepsilon$ there exists short $\mathbf{U}$ with $\mathbf{X} \cdot \mathbf{U} = \mathbf{I}_r$.

Let $\mathbf{X}_j = [\mathbf{x}_i]_i$, $A = \left\{ a \in \mathcal{O}_\mathcal{K}, \|a\| \leq \sqrt{d} \right\}$, $S_j = \left\{ \sum_{i=1}^{j} a_i \cdot \mathbf{x}_i \right\}$ and $\hat{S}_j = \{\mathbf{s}/a, \quad \mathbf{s} \in S_j, a \in A\}$.



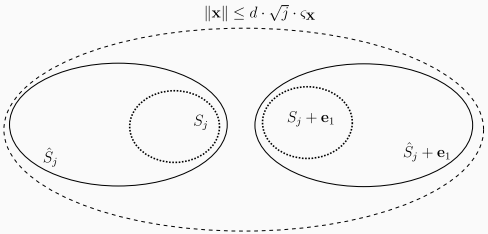
With constant probability, $|S_{j+1}| \geq 2^d \cdot |S_j|$.

Finding a preimage of $\mathbf{I}_r$, the $\mathcal{O}_\mathcal{K}$ case

Preimage of $\mathbf{I}_r$ in $\mathcal{O}_\mathcal{K}$ with [AR16]

If $m \gtrsim \underbrace{rd}_{\text{Too big!}} \log(rd \cdot \varsigma_\mathbf{X}) + \log(1/\varepsilon)$, with probability $1-\varepsilon$ there exists short $\mathbf{U}$ with $\mathbf{X} \cdot \mathbf{U} = \mathbf{I}_r$.

Let $\mathbf{X}_j = [\mathbf{x}_i]_i$, $A = \left\{ a \in \mathcal{O}_\mathcal{K}, \|a\| \leq \sqrt{d} \right\}$, $S_j = \left\{ \sum_{i=1}^{j} a_i \cdot \mathbf{x}_i \right\}$ and $\hat{S}_j = \{\mathbf{s}/a, \quad \mathbf{s} \in S_j, a \in A\}$.



With constant probability, $|S_{j+1}| \geq 2^d \cdot |S_j|$.

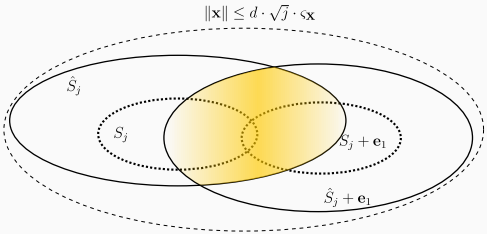
$$\left| \left\{ \|v\| \leq d \cdot \sqrt{j} \cdot \varsigma_\mathbf{X} \right\} \right| \approx (d \cdot \sqrt{j} \cdot \varsigma_\mathbf{X})^{rd}.$$

Finding a preimage of $\mathbf{I}_r$, the $\mathcal{O}_\mathcal{K}$ case

Preimage of $\mathbf{I}_r$ in $\mathcal{O}_\mathcal{K}$ with [AR16]

If $m \gtrsim \underbrace{rd}_{\text{Too big!}} \log(rd \cdot \varsigma_\mathbf{X}) + \log(1/\varepsilon)$, with probability $1-\varepsilon$ there exists short $\mathbf{U}$ with $\mathbf{X} \cdot \mathbf{U} = \mathbf{I}_r$.

Let $\mathbf{X}_j = [\mathbf{x}_i]_i$, $A = \left\{ a \in \mathcal{O}_\mathcal{K}, \|a\| \leq \sqrt{d} \right\}$, $S_j = \left\{ \sum_{i=1}^{j} a_i \cdot \mathbf{x}_i \right\}$ and $\hat{S}_j = \{\mathbf{s}/a, \quad \mathbf{s} \in S_j, a \in A\}$.

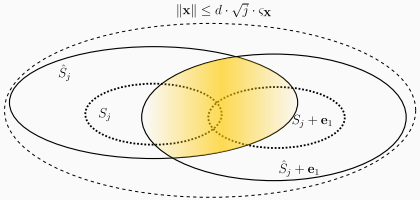


With constant probability, $|S_{j+1}| \geq 2^d \cdot |S_j|$.

$$\left| \left\{ \|v\| \leq d \cdot \sqrt{j} \cdot \varsigma_\mathbf{X} \right\} \right| \approx (d \cdot \sqrt{j} \cdot \varsigma_\mathbf{X})^{rd}.$$

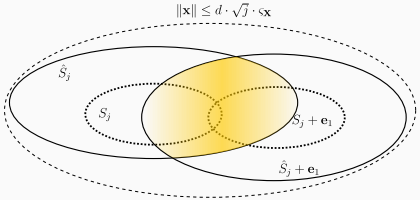
For $j \gtrsim r \log(rd \cdot \varsigma_\mathbf{X})$, $S_j \cap S_j + \mathbf{e}_1 \neq \emptyset$.

We detect a collision



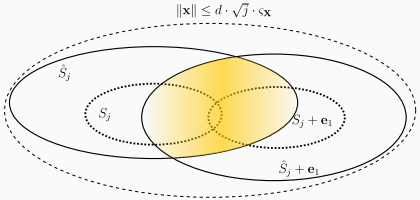
$$\hat{S}_j \cap \hat{S}_j + \mathbf{e}_1 \neq \emptyset$$

We detect a collision



$$\hat{S}_j \cap \hat{S}_j + \mathbf{e}_1 \neq \emptyset \;\Rightarrow\; \frac{1}{a_0}\sum_i a_i \mathbf{x}_i = \frac{1}{b_0}\sum_i b_i \mathbf{x}_i + \mathbf{e}_1$$

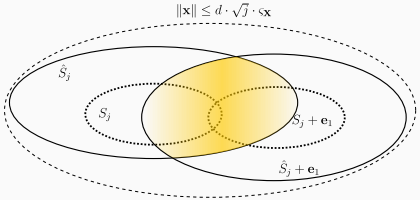
We detect a collision



$$\hat{S}_j \cap \hat{S}_j + \mathbf{e}_1 \neq \emptyset \;\Rightarrow\; \frac{1}{a_0}\sum_i a_i \mathbf{x}_i = \frac{1}{b_0}\sum_i b_i \mathbf{x}_i + \mathbf{e}_1$$

$$\Rightarrow \quad \sum_i (b_0 \cdot a_i - a_0 \cdot b_i)\mathbf{x}_i = a_0 \cdot b_0 \cdot \mathbf{e}_1$$

We detect a collision

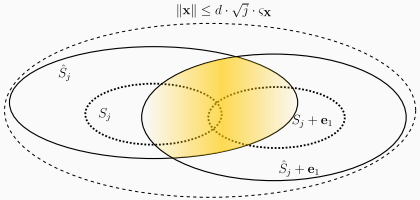


$$\hat{S}_j \cap \hat{S}_j + \mathbf{e}_1 \neq \emptyset \;\Rightarrow\; \frac{1}{a_0}\sum_i a_i \mathbf{x}_i = \frac{1}{b_0}\sum_i b_i \mathbf{x}_i + \mathbf{e}_1$$

$$\Rightarrow \quad \sum_i (b_0 \cdot a_i - a_0 \cdot b_i)\mathbf{x}_i = a_0 \cdot b_0 \cdot \mathbf{e}_1$$

$$\Rightarrow \quad \mathbf{X} \cdot \mathbf{c} = a_0 \cdot b_0 \cdot \mathbf{e}_1.$$

We detect a collision



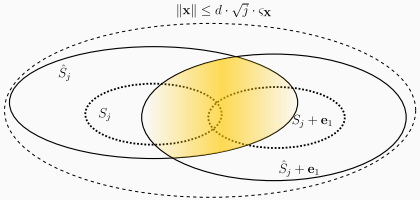
$$\hat{S}_j \cap \hat{S}_j + \mathbf{e}_1 \neq \emptyset \;\Rightarrow\; \frac{1}{a_0}\sum_i a_i \mathbf{x}_i = \frac{1}{b_0}\sum_i b_i \mathbf{x}_i + \mathbf{e}_1$$

$$\Rightarrow \quad \sum_i (b_0 \cdot a_i - a_0 \cdot b_i)\mathbf{x}_i = a_0 \cdot b_0 \cdot \mathbf{e}_1$$

$$\Rightarrow \quad \mathbf{X} \cdot \mathbf{c} = a_0 \cdot b_0 \cdot \mathbf{e}_1.$$

Short preimage of **a short multiple of $\mathbf{e}_1$**. ☹

We detect a collision



$$\hat{S}_j \cap \hat{S}_j + \mathbf{e}_1 \neq \emptyset \;\Rightarrow\; \frac{1}{a_0}\sum_i a_i \mathbf{x}_i = \frac{1}{b_0}\sum_i b_i \mathbf{x}_i + \mathbf{e}_1$$

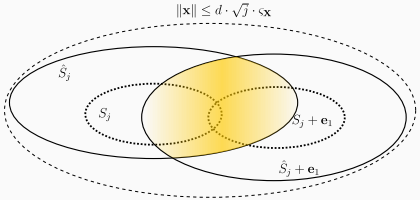
$$\Rightarrow \quad \sum_i (b_0 \cdot a_i - a_0 \cdot b_i)\mathbf{x}_i = a_0 \cdot b_0 \cdot \mathbf{e}_1$$

$$\Rightarrow \quad \mathbf{X} \cdot \mathbf{c} = a_0 \cdot b_0 \cdot \mathbf{e}_1.$$

Short preimage of **a short multiple of $\mathbf{e}_1$**. ☹

Same argument with $A' = \{a' \in \mathcal{O}_\mathcal{K}, a' \text{ coprime with } a_0 \cdot b_0, \|a'\| \le R\}$.

We detect a collision



$$\hat{S}_j \cap \hat{S}_j + \mathbf{e}_1 \neq \emptyset \;\Rightarrow\; \frac{1}{a_0}\sum_i a_i \mathbf{x}_i = \frac{1}{b_0}\sum_i b_i \mathbf{x}_i + \mathbf{e}_1$$

$$\Rightarrow \quad \sum_i (b_0 \cdot a_i - a_0 \cdot b_i)\mathbf{x}_i = a_0 \cdot b_0 \cdot \mathbf{e}_1$$

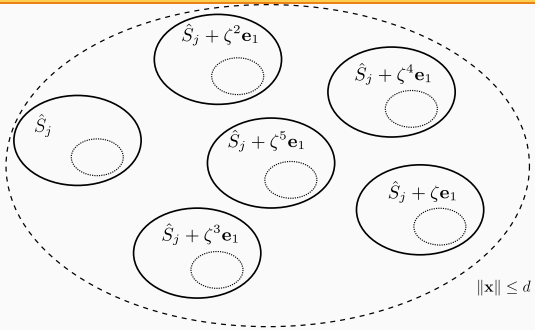
$$\Rightarrow \quad \mathbf{X} \cdot \mathbf{c} = a_0 \cdot b_0 \cdot \mathbf{e}_1.$$

Short preimage of **a short multiple of** $\mathbf{e}_1$. ☹

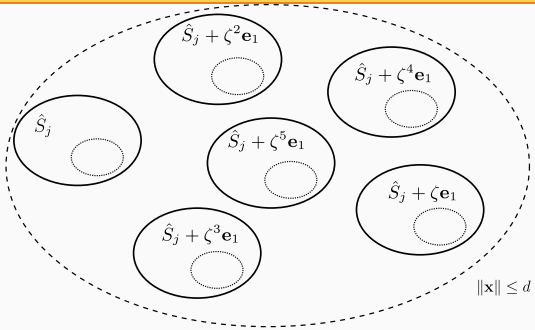
Same argument with $A' = \{a' \in \mathcal{O}_\mathcal{K}, a' \text{ coprime with } a_0 \cdot b_0, \|a'\| \le R\}$.

$$\mathbf{X} \cdot (u \cdot \mathbf{c}) + \mathbf{X} \cdot (v \cdot \mathbf{c}') = (u \cdot a_0 \cdot b_0 + v \cdot a_0' \cdot b_0') \cdot \mathbf{e}_1 = \mathbf{e}_1. \quad ☺$$

Improving further: when $\mathbb{Q}(\zeta_f)$ is a subfield

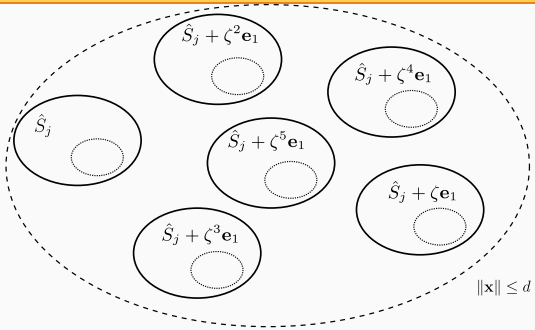


Improving further: when $\mathbb{Q}(\zeta_f)$ is a subfield



Pro: $|S_j| \geq 2^d |S_{j-1}|$ w.p. $\geq 1 - 1/f$.

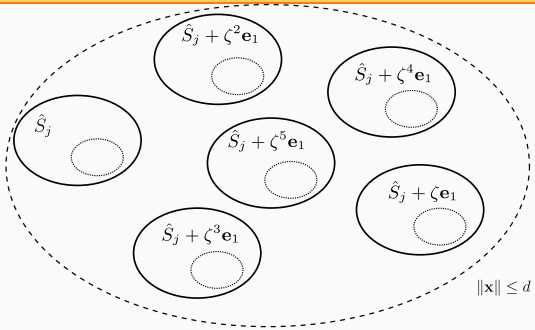
Improving further: when $\mathbb{Q}(\zeta_f)$ is a subfield



Pro: $|S_j| \geq 2^d |S_{j-1}|$ w.p. $\geq 1 - 1/f$.

Con: We get a preimage of $(1 - \zeta_f^x) \cdot \mathbf{e}_1$.

Improving further: when $\mathbb{Q}(\zeta_f)$ is a subfield

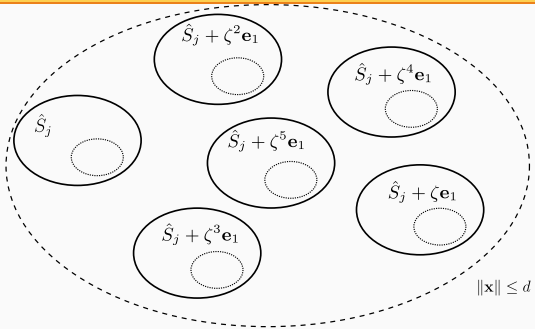


Pro: $|S_j| \geq 2^d |S_{j-1}|$ w.p. $\geq 1 - 1/f$.

Con: We get a preimage of $(1 - \zeta_f^x) \cdot \mathbf{e}_1$.

Number theory trick: $\prod_{x=1}^{f} (1 - \zeta_f^x) = f$

Improving further: when $\mathbb{Q}(\zeta_f)$ is a subfield



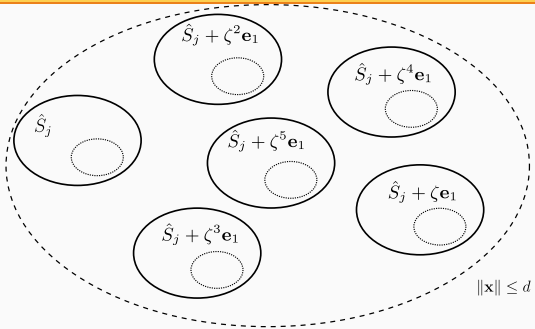
Pro: $|S_j| \geq 2^d |S_{j-1}|$ w.p. $\geq 1 - 1/f$.

Con: We get a preimage of $(1 - \zeta_f^x) \cdot \mathbf{e}_1$.

Number theory trick: $\prod_{x=1}^{f} (1 - \zeta_f^x) = f$

At the end, we have $\mathbf{X} \cdot \mathbf{U} = f \cdot \mathbf{I}_r$. We can use $\mathbf{Y} = \underbrace{f \cdot \mathbf{I}_m - \mathbf{U} \cdot \mathbf{X}}_{\text{Short!}}$.

Improving further: when $\mathbb{Q}(\zeta_f)$ is a subfield



Pro: $|S_j| \geq 2^d |S_{j-1}|$ w.p. $\geq 1 - 1/f$.

Con: We get a preimage of $(1 - \zeta_f^x) \cdot \mathbf{e}_1$.

Number theory trick: $\prod_{x=1}^{f} (1 - \zeta_f^x) = f$

At the end, we have $\mathbf{X} \cdot \mathbf{U} = f \cdot \mathbf{I}_r$. We can use $\mathbf{Y} = \underbrace{f \cdot \mathbf{I}_m - \mathbf{U} \cdot \mathbf{X}}_{\text{Short!}}$.

$\Lambda^{\perp}(\mathbf{X})$ has a short basis!

The result

Theorem ("Small" smoothing parameter of $\Lambda^{\perp}(\mathbf{X})$)

If $\mathcal{K}$ is a number field of degree d such that $\mathbb{Q}(\zeta_f) \subseteq \mathcal{K}$ then for any $r \geq 1$, $\varepsilon > 0$, ς large enough and $m \geq r \cdot (\log(dr\varsigma))^{1+o(1)} + \log(1/\varepsilon)/\log(f)$, there exists an absolute polynomial P such that

$$\Pr_{\mathbf{X} \leftarrow \mathcal{D}^{r \times m}_{\mathcal{O}_{\mathcal{K}}, \varsigma}} \left(\eta_{\varepsilon} \left(\Lambda^{\perp}(\mathbf{X}) \right) \leq P(d, \Delta_K^{1/d}, m) \right) \geq 1 - \varepsilon.$$

The result

Theorem ("Small" smoothing parameter of $\Lambda^{\perp}(\mathbf{X})$)

If $\mathcal{K}$ is a number field of degree d such that $\mathbb{Q}(\zeta_f) \subseteq \mathcal{K}$ then for any $r \geq 1$, $\varepsilon > 0$, ς large enough and $m \geq r \cdot (\log(dr\varsigma))^{1+o(1)} + \log(1/\varepsilon)/\log(f)$, there exists an absolute polynomial P such that

$$\Pr_{\mathbf{X} \leftarrow \mathcal{D}^{r \times m}_{\mathcal{O}_{\mathcal{K}}, \varsigma}} \left(\eta_{\varepsilon}\left(\Lambda^{\perp}(\mathbf{X})\right) \leq P(d, \Delta_K^{1/d}, m) \right) \;\geq\; 1 - \varepsilon.$$

Under the rug

- Computation of R so that $A' = \{a' \in \mathcal{O}_{\mathcal{K}}, a' \text{ coprime with } a_0 \cdot b_0, \|a'\| \leq R\}$ has size 2^d.
- This polynomial P is very large (degree 12). But we think it is very loose.

The statement of Module Gaussian LHL

Theorem (Module Gaussian LHL)

If $\mathcal{K}$ is a number field of degree d such that $\mathbb{Q}(\zeta_f) \subseteq \mathcal{K}$ then there exists an absolute polynomial P such that for any $r \geq 1$, $\varepsilon > 0$, $\varsigma_{\mathbf{X}}$ large enough, $\varsigma_{\mathbf{r}} \geq P(d, \Delta_K^{1/d}, m)$, $N = \min(f, N_{\mathcal{K}})$ and

$$m \gtrsim r \cdot (\log(dr\varsigma_{\mathbf{X}}))^{1+o(1)} + \log(1/\varepsilon)/\log(N),$$

it holds that

$$(\mathbf{X}, \mathbf{X} \cdot \mathbf{r}) \approx_\varepsilon \left(\mathcal{D}^{r \times m}_{\mathcal{O}_{\mathcal{K}}, \varsigma_{\mathbf{X}}}, \mathcal{D}^{r}_{\mathcal{O}_{\mathcal{K}}, \sqrt{\mathbf{X}\mathbf{X}^T} \cdot \varsigma_{\mathbf{r}}}\right)$$

The statement of Module Gaussian LHL

Theorem (Module Gaussian LHL)

If $\mathcal{K}$ is a number field of degree d such that $\mathbb{Q}(\zeta_f) \subseteq \mathcal{K}$ then there exists an absolute polynomial P such that for any $r \geq 1$, $\varepsilon > 0$, $\varsigma_{\mathbf{X}}$ large enough, $\varsigma_{\mathbf{r}} \geq P(d, \Delta_K^{1/d}, m)$, $N = \min(f, N_{\mathcal{K}})$ and

$$m \gtrsim r \cdot (\log(dr\varsigma_{\mathbf{X}}))^{1+o(1)} + \log(1/\varepsilon)/\log(N),$$

it holds that

$$(\mathbf{X}, \mathbf{X} \cdot \mathbf{r}) \approx_\varepsilon \left(\mathcal{D}^{r \times m}_{\mathcal{O}_{\mathcal{K}}, \varsigma_{\mathbf{X}}}, \mathcal{D}^{r}_{\mathcal{O}_{\mathcal{K}}, \sqrt{\mathbf{X}\mathbf{X}^T} \cdot \varsigma_{\mathbf{r}}}\right)$$

Improvements from previous results

- Works on rings.
- Works for all ε.
- Optimised for m.

Perspectives

- Making the polynomial P smaller (non-pigeonhole techniques?).
- More precise tradeoff m vs $\varsigma_{\mathbf{r}}$.

Perspectives

- Making the polynomial P smaller (non-pigeonhole techniques?).
- More precise tradeoff m vs $\varsigma_{\mathbf{r}}$.

Now on eprint: `https://eprint.iacr.org/2025/1852`

Perspectives

- Making the polynomial P smaller (non-pigeonhole techniques?).
- More precise tradeoff m vs $\varsigma_{\mathbf{r}}$.

Now on eprint: `https://eprint.iacr.org/2025/1852`

Thank you for your attention! Do you have any question?

References

References i

Martin R. Albrecht, Valerio Cini, Russell W. F. Lai, Giulio Malavolta, and Sri Aravinda Krishnan Thyagarajan.
Lattice-based SNARKs: Publicly verifiable, preprocessing, and recursively composable - (extended abstract).
In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part II*, volume 13508 of *LNCS*, pages 102–132. Springer, Cham, August 2022.

Shweta Agrawal, Craig Gentry, Shai Halevi, and Amit Sahai.
Discrete Gaussian leftover hash lemma over infinite domains.
In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 97–116. Springer, Berlin, Heidelberg, December 2013.

Martin R. Albrecht, Russell W. F. Lai, Oleksandra Lapiha, and Ivy K. Y. Woo.
Partial lattice trapdoors: How to split lattice trapdoors, literally.
Cryptology ePrint Archive, Report 2025/367, 2025.

References ii

Divesh Aggarwal and Oded Regev.
A note on discrete gaussian combinations of lattice vectors.
Chicago Journal of Theoretical Computer Science, 2016.

Dan Boneh and David Mandell Freeman.
Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures.
In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *PKC 2011*, volume 6571 of *LNCS*, pages 1–16. Springer, Berlin, Heidelberg, March 2011.

Elena Kirshanova, Huyen Nguyen, Damien Stehlé, and Alexandre Wallet.
On the smoothing parameter and last minimum of random orthogonal lattices.
DCC, 88(5):931–950, 2020.

References iii


San Ling, Duong Hieu Phan, Damien Stehlé, and Ron Steinfeld.
Hardness of k-LWE and applications in traitor tracing.
In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 315–334. Springer, Berlin, Heidelberg, August 2014.


Hoi H. Nguyen and Elliot Paquette.
Surjectivity of near-square random matrices.
Combinatorics, Probability and Computing, 29(2):267292, March 2020.