SIS to k-SIS reduction for Modules over Number Fields

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

eprint: 2025/1852

Sasha Lapiha, Silence Laboratories

SIS and k-SIS problems

SIS problem:

Given $\mathbf{A} \leftarrow \mathbb{Z}_q^{r \times m}$ find short $\mathbf{x} \in \mathbb{Z}^m$ such that $\mathbf{A} \cdot \mathbf{x} = 0 \bmod q$

SIS and k-SIS problems

SIS problem:

Given $\mathbf{A} \leftarrow \mathbb{Z}_q^{r \times m}$ find short $\mathbf{x} \in \mathbb{Z}^m$ such that $\mathbf{A} \cdot \mathbf{x} = 0 \bmod q$

k-SIS problem:

Given $\mathbf{A} \leftarrow \mathbb{Z}_q^{r \times m}$ and discrete gaussian $\{\mathbf{x}_1, \ldots, \mathbf{x}_k \mid \mathbf{A} \cdot \mathbf{x}_i = 0 \bmod q\}$

Find another short $\mathbf{x} \in \mathbb{Z}^m$ s.t. $\mathbf{A} \cdot \mathbf{x} = 0 \bmod q$

and $\mathbf{x} \notin \mathbb{Q}\text{-span}(\mathbf{x}_1, \ldots, \mathbf{x}_k)$

k-LWE problem

k-LWE problem:

Given $\mathbf{A} \leftarrow \mathbb{Z}_q^{r\times m}$ and discrete gaussian $\{\mathbf{x}_1, \ldots, \mathbf{x}_k \mid \mathbf{A} \cdot \mathbf{x}_i = 0 \bmod q\}$

Distinguish $\mathbf{A}^T \cdot \mathbf{s} + \mathbf{e} \bmod q$ and $\mathbf{b} \leftarrow \{\mathbf{v} \mid \forall i : \mathbf{x}_i^T \cdot \mathbf{v} = 0 \bmod q\} + \mathbf{e}$

for $\mathbf{s} \leftarrow \chi^r, \mathbf{e} \leftarrow \chi^m$ for some short distribution χ.

The Original Reduction

Boneh-Freeman'11 reduction

$SIS_{r,m,B} \leq k\text{-}SIS_{r,m+k,\sigma,B'}$

Given the SIS challenge $\mathbf{A} \leftarrow \mathbb{Z}_q^{r \times m}$

Sample the hints as

$$\boxed{\mathbf{X}} \leftarrow \left(\mathcal{D}_{\mathbb{Z},\sigma}\right)^{(m+k)\times k}$$

Sasha Lapiha, Silence Laboratories

Boneh-Freeman'11 reduction

$SIS_{r,m,B} \leq k\text{-}SIS_{r,m+k,\sigma,B'}$

Given the SIS challenge $\mathbf{A} \leftarrow \mathbb{Z}_q^{r \times m}$

Sample the hints as

$$\mathbf{X} \leftarrow \left(\mathscr{D}_{\mathbb{Z},\sigma}\right)^{(m+k)\times k}$$

$$\begin{bmatrix} \mathbf{X}_1 \\ \mathbf{X}_2 \end{bmatrix}$$

There exists $\mathbf{X}_2 \in \mathbb{Z}^{k \times k}$ invertible

over $\mathbb{Z}_q$ (and $\mathbb{Q}$) for m, σ large enough.

Boneh-Freeman'11 reduction

$SIS_{r,m,B} \leq k\text{-}SIS_{r,m+k,\sigma,B'}$

Given $(\mathbf{A} \in \mathbb{Z}_q^{r\times m}, \mathbf{X} \in \mathbb{Z}^{(m+k)\times k})$ solve for unique $\mathbf{Y} \in \mathbb{Z}_q^{r\times k}$ such that:

$$[\mathbf{A}\ \mathbf{Y}] \cdot \mathbf{X} = \mathbf{0} \bmod q \implies \mathbf{Y} = (\mathbf{A} \cdot \mathbf{X}_1) \cdot \mathbf{X}_2^{-1} \bmod q$$

Boneh-Freeman'11 reduction

$SIS_{r,m,B} \leq k\text{-}SIS_{r,m+k,\sigma,B'}$

Given $(\mathbf{A} \in \mathbb{Z}_q^{r\times m}, \mathbf{X} \in \mathbb{Z}^{(m+k)\times k})$ solve for unique $\mathbf{Y} \in \mathbb{Z}_q^{r\times k}$ such that:

$$[\mathbf{A}\ \mathbf{Y}] \cdot \mathbf{X} = \mathbf{0} \bmod q \implies \mathbf{Y} = (\mathbf{A} \cdot \mathbf{X}_1) \cdot \mathbf{X}_2^{-1} \bmod q$$

Prove that for $(\mathbf{A}' = [\mathbf{A}\ \mathbf{Y}], \mathbf{X})$ the "order of sampling" does not affect the distribution.

Sasha Lapiha, Silence Laboratories

Boneh-Freeman'11 reduction

$SIS_{r,m,B} \leq k\text{-}SIS_{r,m+k,\sigma,B'}$

Given $\mathbf{x}^* = (\mathbf{x}_1^*, \mathbf{x}_2^*)$ extract the SIS solution

$$\mathbf{x} = \det(\mathbf{X}_2) \cdot (\mathbf{X}_1 \cdot \mathbf{X}_2^{-1} \cdot \mathbf{x}_2^* - \mathbf{x}_1^*)$$

Boneh-Freeman'11 reduction

$SIS_{r,m,B} \leq k\text{-}SIS_{r,m+k,\sigma,B'}$

Given $\mathbf{x}^* = (\mathbf{x}_1^*, \mathbf{x}_2^*)$ extract the SIS solution

$$\mathbf{x} = \det(\mathbf{X}_2) \cdot (\mathbf{X}_1 \cdot \mathbf{X}_2^{-1} \cdot \mathbf{x}_2^* - \mathbf{x}_1^*)$$

Note that $\det(\mathbf{X}_2) \cdot \mathbf{X}_2^{-1} \in \mathbb{Z}^{k \times k}$

Boneh-Freeman'11 reduction

$SIS_{r,m,B} \leq k\text{-}SIS_{r,m+k,\sigma,B'}$

Given $\mathbf{x}^* = (\mathbf{x}_1^*, \mathbf{x}_2^*)$ extract the SIS solution

$$\mathbf{x} = \det(\mathbf{X}_2) \cdot (\mathbf{X}_1 \cdot \mathbf{X}_2^{-1} \cdot \mathbf{x}_2^* - \mathbf{x}_1^*)$$

Note that $\det(\mathbf{X}_2) \cdot \mathbf{X}_2^{-1} \in \mathbb{Z}^{k \times k}$

$\mathbb{Q}$-span condition guarantees that $\mathbf{x} \neq \mathbf{0}$.

Norm grows as $B \geq B' \cdot \det(\mathbf{X}_2) \geq B' \cdot \left(\sigma\sqrt{k}\right)^k$

Boneh-Freeman'11 reduction

$SIS_{r,m,B} \leq k\text{-}SIS_{r,m+k,\sigma,B'}$

Given $\mathbf{x}^* = (\mathbf{x}_1^*, \mathbf{x}_2^*)$ extract the SIS solution

$$\mathbf{x} = \det(\mathbf{X}_2) \cdot (\mathbf{X}_1 \cdot \mathbf{X}_2^{-1} \cdot \mathbf{x}_2^* - \mathbf{x}_1^*)$$

Note that $\det(\mathbf{X}_2) \cdot \mathbf{X}_2^{-1} \in \mathbb{Z}^{k \times k}$

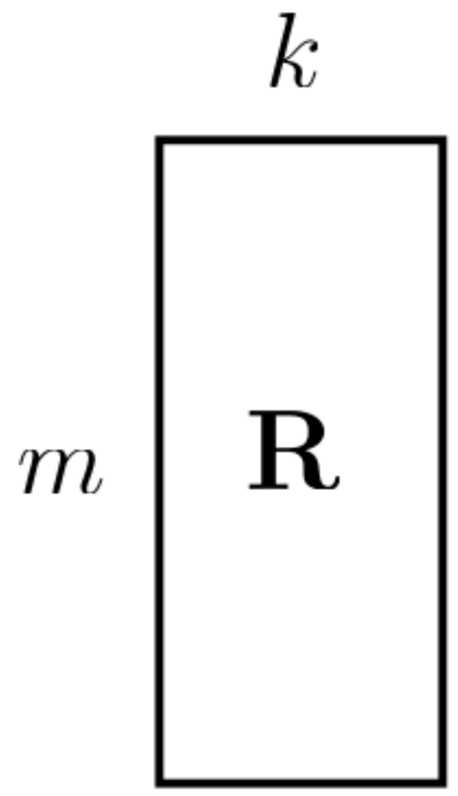
$\mathbb{Q}$-span condition guarantees that $\mathbf{x} \neq \mathbf{0}$.

Norm grows as $B \geq B' \cdot \det(\mathbf{X}_2) \geq B' \cdot \left(\sigma\sqrt{k}\right)^k \implies k = \text{const}(\lambda)$

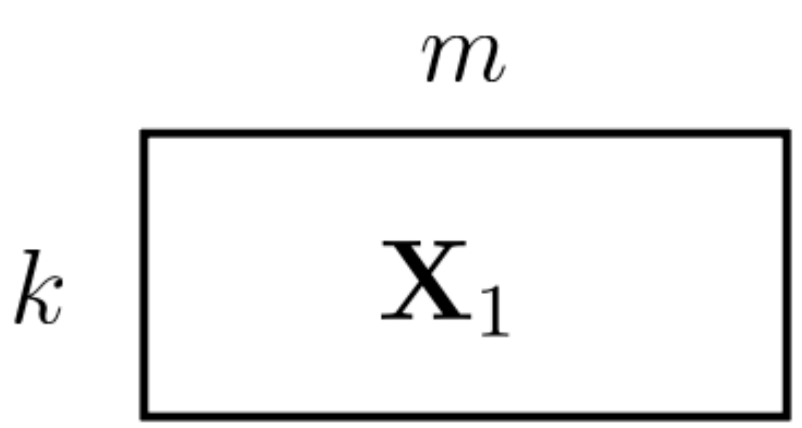
Improving the number of hints

LPSS14 reduction

(borrowing nice pictures from Joël’s slides)



$\leftarrow (\mathcal{D}_{\mathbb{Z},\varsigma_R})^{m \times k}$

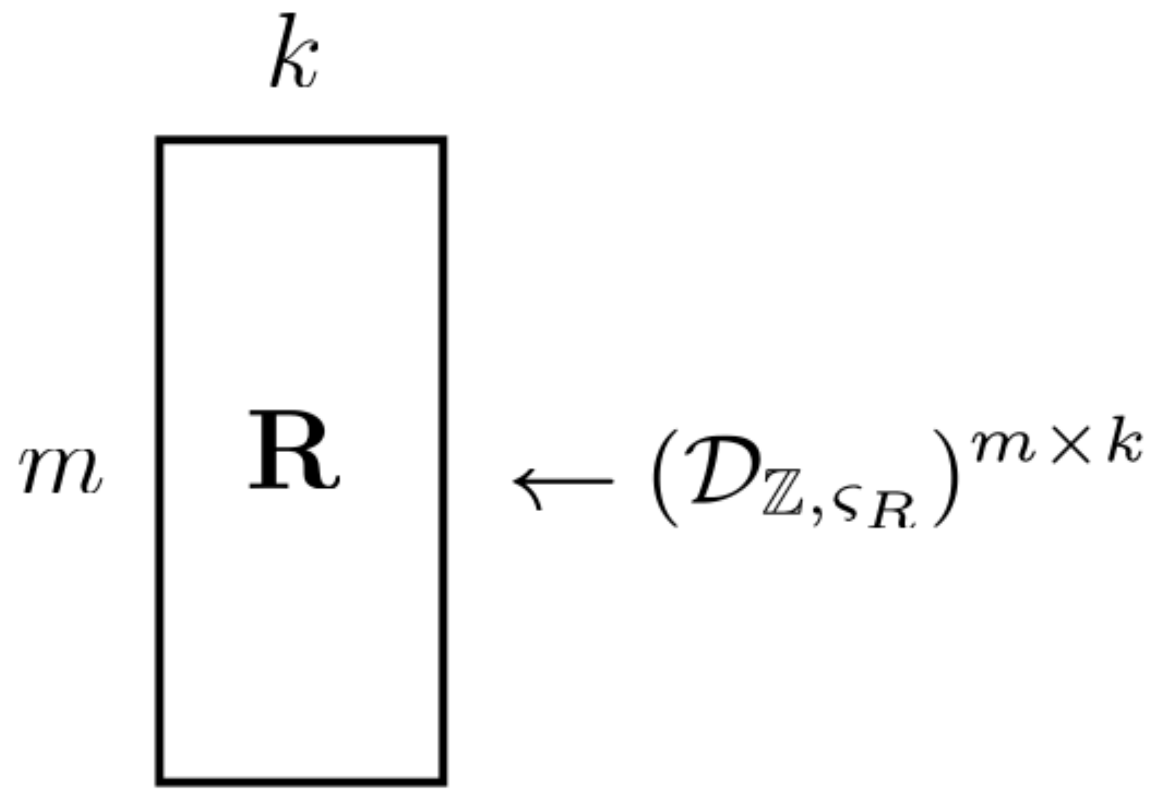


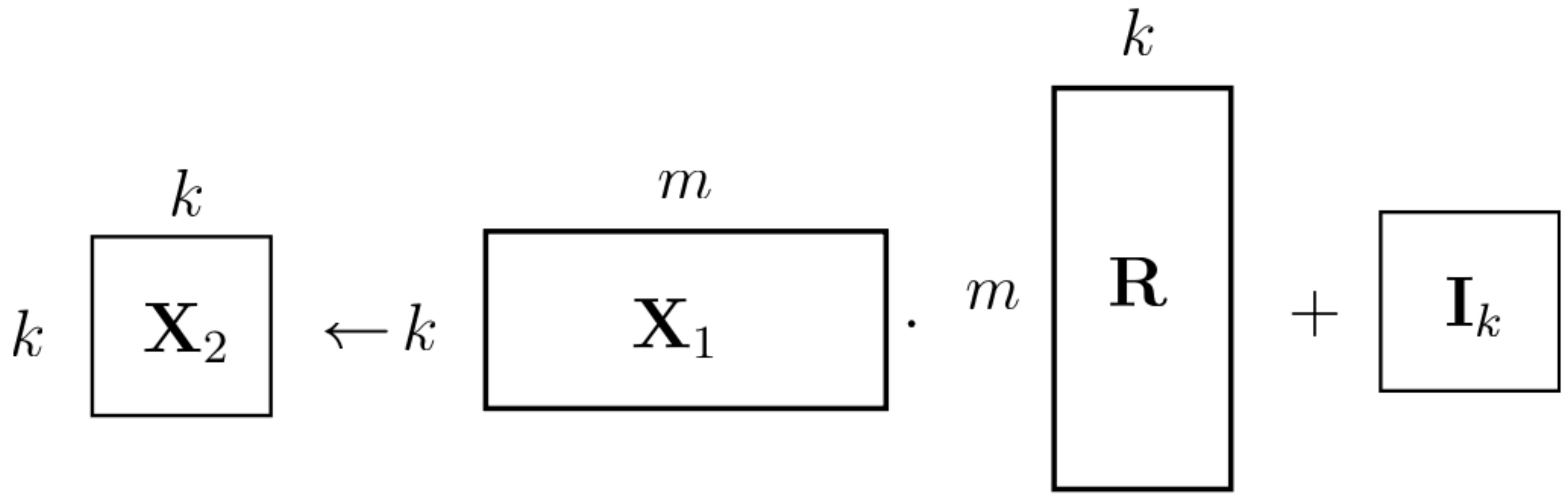
$\leftarrow (\mathcal{D}_{\mathbb{Z},\varsigma_X})^{k \times m}$

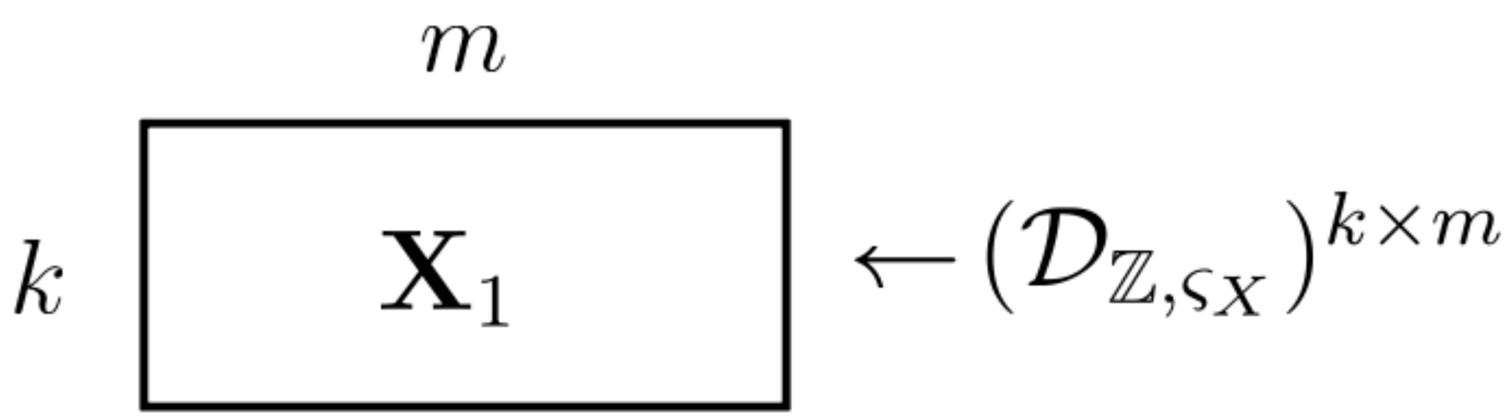
Sasha Lapiha, Silence Laboratories

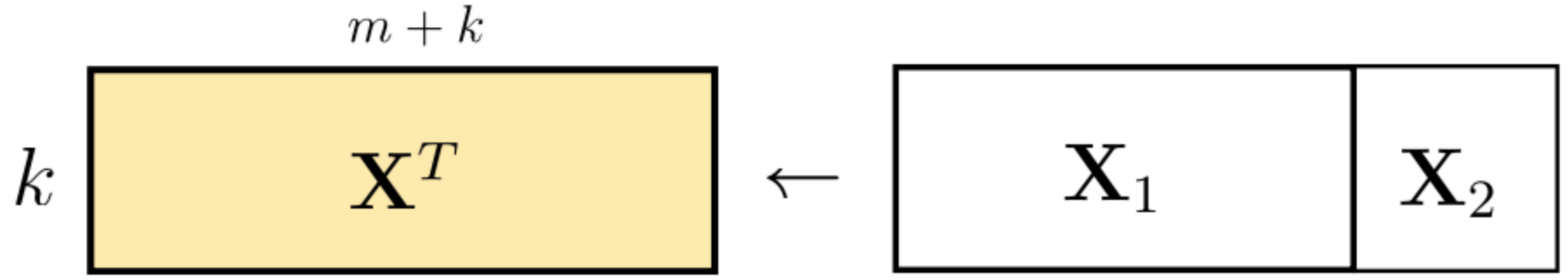
LPSS14 reduction

(borrowing nice pictures from Joël’s slides)









Sasha Lapiha, Silence Laboratories

LPSS14 reduction

(borrowing nice pictures from Joël's slides)

$$\begin{array}{cc} & m+k \\ m+k & \begin{bmatrix} \mathbf{U} \end{bmatrix} \end{array} \leftarrow \begin{bmatrix} \mathbf{I}_m & -\mathbf{R} \\ \mathbf{0} & \mathbf{I}_k \end{bmatrix} \cdot \begin{bmatrix} 0 & \mathbf{I}_m \\ \mathbf{I}_k & -\mathbf{X}_1 \end{bmatrix}$$

Sasha Lapiha, Silence Laboratories

LPSS14 reduction

(borrowing nice pictures from Joël's slides)

$$\underbrace{\mathbf{U}}_{(m+k)\times(m+k)} \leftarrow \begin{bmatrix} \mathbf{I}_m & -\mathbf{R} \\ 0 & \mathbf{I}_k \end{bmatrix} \cdot \begin{bmatrix} 0 & \mathbf{I}_m \\ \mathbf{I}_k & -\mathbf{X}_1 \end{bmatrix}$$

$$\underbrace{\mathbf{X}^T}_{k\times(m+k)} \cdot \begin{array}{c} \begin{array}{cc} k & m \end{array} \\ \begin{bmatrix} \; & \widetilde{\mathbf{U}}^T \end{bmatrix} \end{array}_{m+k} = \underbrace{\begin{bmatrix} \mathbf{I}_k & \mathbf{0} \end{bmatrix}}_{k\times(m+k)}$$

Sasha Lapiha, Silence Laboratories

LPSS14 reduction

(borrowing nice pictures from Joël's slides)

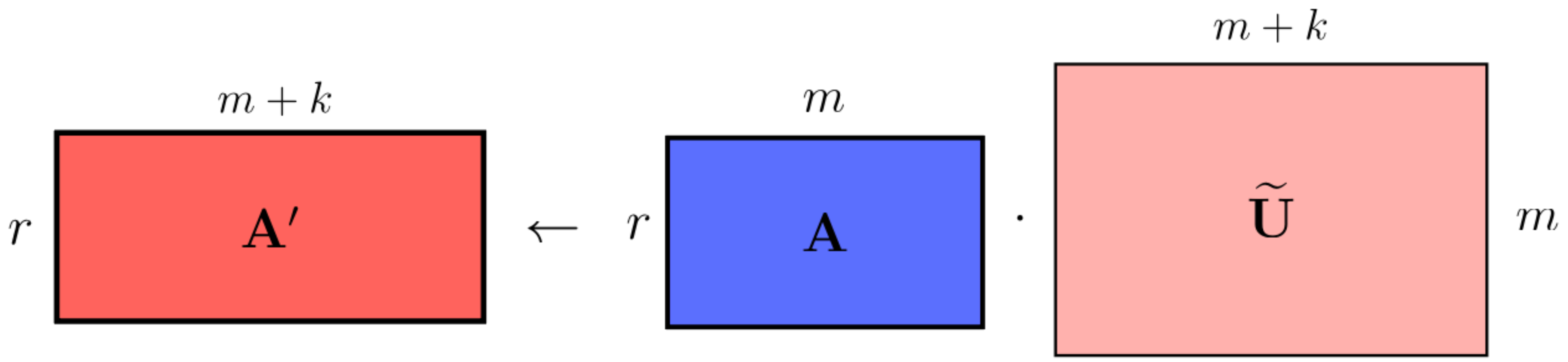
$$\begin{array}{cc} & m+k \\ m+k & \begin{bmatrix} \mathbf{U} \end{bmatrix} \end{array} \leftarrow \begin{bmatrix} \mathbf{I}_m & -\mathbf{R} \\ 0 & \mathbf{I}_k \end{bmatrix} \cdot \begin{bmatrix} 0 & \mathbf{I}_m \\ \mathbf{I}_k & -\mathbf{X}_1 \end{bmatrix}$$

$$\begin{array}{cc} & m+k \\ k & \begin{bmatrix} \mathbf{X}^T \end{bmatrix} \end{array} \cdot \begin{array}{cc} k \quad\quad m & \\ \begin{bmatrix} \, \big| \, \widetilde{\mathbf{U}}^T \end{bmatrix} & m+k \end{array} = \begin{array}{cc} m+k & \\ \begin{bmatrix} \mathbf{I}_k & \mathbf{0} \end{bmatrix} & k \end{array}$$

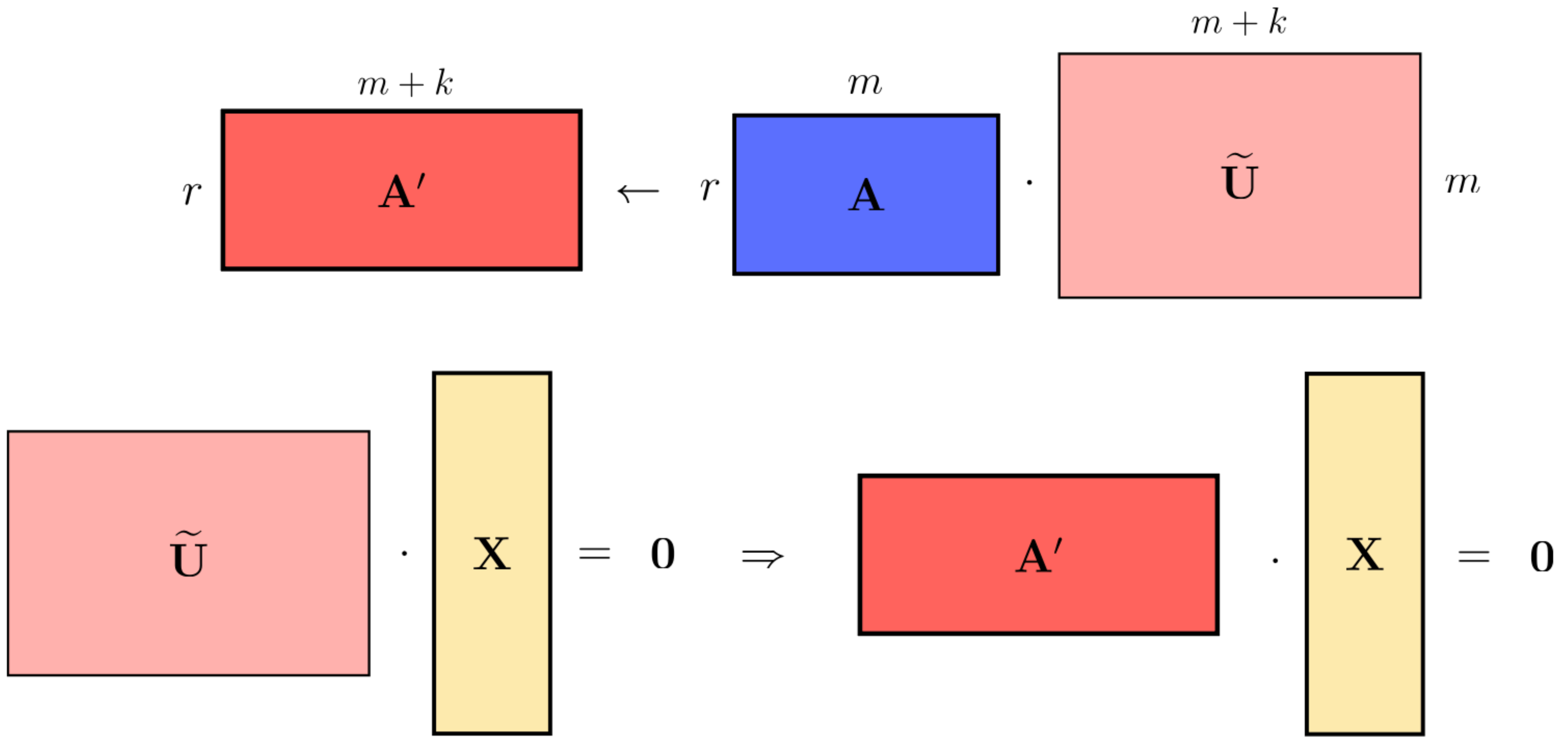
In fact $\widetilde{\mathbf{U}}$ is a basis of $\Lambda^{\perp}(\mathbf{X}^T)$

LPSS14 reduction

(borrowing nice pictures from Joël's slides)



LPSS14 reduction
(borrowing nice pictures from Joël’s slides)



Sasha Lapiha, Silence Laboratories

LPSS14 reduction

$SIS_{r,m,B} \leq k\text{-}SIS_{r,m+k,\mathbf{S},B'}$

1. Prove $\begin{bmatrix}\mathbf{X}_1 & \mathbf{X}_1 \cdot \mathbf{R} + \mathbf{I}\end{bmatrix} \sim \left(\mathscr{D}_{\mathbb{Z}^{m+k},\mathbf{S},\mathbf{c}}\right)^k$

LPSS14 reduction

$SIS_{r,m,B} \leq k\text{-}SIS_{r,m+k,\mathbf{S},B'}$

1. Prove $\begin{bmatrix}\mathbf{X}_1 & \mathbf{X}_1 \cdot \mathbf{R} + \mathbf{I}\end{bmatrix} \sim \left(\mathscr{D}_{\mathbb{Z}^{m+k},\mathbf{S},\mathbf{c}}\right)^k$
2. Prove the "order of sampling" lemma.

LPSS14 reduction

$SIS_{r,m,B} \leq k\text{-}SIS_{r,m+k,\mathbf{S},B'}$

1. Prove $\begin{bmatrix}\mathbf{X}_1 & \mathbf{X}_1 \cdot \mathbf{R} + \mathbf{I}\end{bmatrix} \sim \left(\mathscr{D}_{\mathbb{Z}^{m+k},\mathbf{S},\mathbf{c}}\right)^k$

2. Prove the "order of sampling" lemma.

3. Extract the solution as $\mathbf{x} = \tilde{\mathbf{U}} \cdot \mathbf{x}^*$

LPSS14 reduction

$SIS_{r,m,B} \leq k\text{-}SIS_{r,m+k,\mathbf{S},B'}$

1. Prove $\left[\mathbf{X}_1 \quad \mathbf{X}_1 \cdot \mathbf{R} + \mathbf{I}\right] \sim \left(\mathscr{D}_{\mathbb{Z}^{m+k},\mathbf{S},\mathbf{c}}\right)^k$
2. Prove the “order of sampling” lemma.
3. Extract the solution as $\mathbf{x} = \tilde{\mathbf{U}} \cdot \mathbf{x}^*$

   Span condition guarantees $\mathbf{x} \neq \mathbf{0}$

   Norm grows as $B = B' \cdot ||\tilde{\mathbf{U}}|| = B' \cdot \text{poly}(k, m, \sigma)$ works for $k = \text{poly}(\lambda)$.

LWE version

$LWE_{r,m,B} \leq k\text{-}LWE_{r,m+k,\mathbf{S},B'}$

On input LWE challenge $(\mathbf{A} \in \mathbb{Z}_q^{r \times m}, \mathbf{b} \in \mathbb{Z}^m)$

Simulate $(\mathbf{A}' = \mathbf{A} \cdot \tilde{\mathbf{U}}, \mathbf{X})$ as before.

LWE version

$LWE_{r,m,B} \leq k\text{-}LWE_{r,m+k,\mathbf{S},B'}$

On input LWE challenge $(\mathbf{A} \in \mathbb{Z}_q^{r\times m}, \mathbf{b} \in \mathbb{Z}^m)$

Simulate $(\mathbf{A}' = \mathbf{A} \cdot \tilde{\mathbf{U}}, \mathbf{X})$ as before.

Then $\mathbf{b}' = \tilde{\mathbf{U}}^T \cdot \mathbf{b} + \tilde{\mathbf{e}}$

LWE

$$\tilde{\mathbf{U}}^T \cdot (\mathbf{A}^T \cdot \mathbf{s} + \mathbf{e}) + \tilde{\mathbf{e}} = (\mathbf{A}')^T \cdot \mathbf{s} + (\tilde{\mathbf{U}}^T\mathbf{e} + \tilde{\mathbf{e}})$$

LWE version

$LWE_{r,m,B} \leq k\text{-}LWE_{r,m+k,\mathbf{S},B'}$

On input LWE challenge $(\mathbf{A} \in \mathbb{Z}_q^{r\times m}, \mathbf{b} \in \mathbb{Z}^m)$

Simulate $(\mathbf{A}' = \mathbf{A} \cdot \tilde{\mathbf{U}}, \mathbf{X})$ as before.

Then $\mathbf{b}' = \tilde{\mathbf{U}}^T \cdot \mathbf{b} + \tilde{\mathbf{e}}$

LWE

$$\tilde{\mathbf{U}}^T \cdot (\mathbf{A}^T \cdot \mathbf{s} + \mathbf{e}) + \tilde{\mathbf{e}} = (\mathbf{A}')^T \cdot \mathbf{s} + (\tilde{\mathbf{U}}^T\mathbf{e} + \tilde{\mathbf{e}})$$
$$= (\mathbf{A}')^T \cdot \mathbf{s} + \mathbf{e}'$$

LWE version

$LWE_{r,m,B} \leq k\text{-}LWE_{r,m+k,\mathbf{S},B'}$

On input LWE challenge $(\mathbf{A} \in \mathbb{Z}_q^{r\times m}, \mathbf{b} \in \mathbb{Z}^m)$

Simulate $(\mathbf{A}' = \mathbf{A} \cdot \tilde{\mathrm{U}}, \mathbf{X})$ as before.

Then $\mathbf{b}' = \tilde{\mathbf{U}}^T \cdot \mathbf{b} + \tilde{\mathbf{e}}$

LWE ↙ ↘ Uniform

$$\tilde{\mathbf{U}}^T \cdot (\mathbf{A}^T \cdot \mathbf{s} + \mathbf{e}) + \tilde{\mathbf{e}} = (\mathbf{A}')^T \cdot \mathbf{s} + (\tilde{\mathbf{U}}^T \mathbf{e} + \tilde{\mathbf{e}})$$
$$= (\mathbf{A}')^T \cdot \mathbf{s} + \mathbf{e}'$$

$$\tilde{\mathbf{U}}^T \cdot \mathcal{U}(\mathcal{R}_q^m) + (\tilde{\mathbf{U}}^T \mathbf{e} + \mathbf{e}')$$

Sasha Lapiha, Silence Laboratories

LWE version

$LWE_{r,m,B} \leq k\text{-}LWE_{r,m+k,\mathbf{S},B'}$

On input LWE challenge $(\mathbf{A} \in \mathbb{Z}_q^{r\times m}, \mathbf{b} \in \mathbb{Z}^m)$

Simulate $(\mathbf{A}' = \mathbf{A} \cdot \tilde{\mathbf{U}}, \mathbf{X})$ as before.

Then $\mathbf{b}' = \tilde{\mathbf{U}}^T \cdot \mathbf{b} + \tilde{\mathbf{e}}$

LWE

$$\tilde{\mathbf{U}}^T \cdot (\mathbf{A}^T \cdot \mathbf{s} + \mathbf{e}) + \tilde{\mathbf{e}} = (\mathbf{A}')^T \cdot \mathbf{s} + (\tilde{\mathbf{U}}^T\mathbf{e} + \tilde{\mathbf{e}})$$
$$= (\mathbf{A}')^T \cdot \mathbf{s} + \mathbf{e}'$$

Uniform

$$\tilde{\mathbf{U}}^T \cdot \mathscr{U}(\mathbb{Z}_q^m) + (\tilde{\mathbf{U}}^T\mathbf{e} + \tilde{\mathbf{e}})$$
$$= \mathscr{U}(\{\mathbf{b} \mid \mathbf{X}^T \cdot \mathbf{b} = 0 \bmod q\}) + \mathbf{e}'$$

Sasha Lapiha, Silence Laboratories

Gaussian Leftover Hash Lemma

Central component - Gaussian LHL

$$(X, X \cdot \mathbf{v}) \sim (X, \mathscr{D}_{\mathbb{Z}^r, \sigma})$$

$$X \leftarrow \left(\mathscr{D}_{\mathbb{Z}^r, \mathbf{S}_x}\right)^m, \quad \mathbf{v} \leftarrow \mathscr{D}_{\mathbb{Z}^m, \mathbf{S}_v}$$

Discrete Gaussian over integers

Base statement

$$(\mathbf{X}, \mathbf{X} \cdot \mathbf{v}) \sim (\mathbf{X}, \mathscr{D}_{\mathbf{X}\cdot\mathbb{Z}^m, \sqrt{\mathbf{X} \cdot \mathbf{S}_v \cdot \mathbf{S}_v^T \cdot \mathbf{X}^T}})$$

$$\mathbf{X} \leftarrow \left(\mathscr{D}_{\mathbb{Z}^r, \mathbf{S}_x}\right)^m, \quad \mathbf{v} \leftarrow \mathscr{D}_{\mathbb{Z}^m, \mathbf{S}_v}$$

as long as $\mathbf{S}_v \geq \eta_\varepsilon(\Lambda^\perp(\mathbf{X}))$

Existing results

On the smoothing parameter

	[AGHS13]	[AR16]	[KNSW20]
σ	$\Omega(\eta_\varepsilon(\mathbb{Z}^r))$	$\Omega(\eta_\varepsilon(\mathbb{Z}^r))$	$\Omega\left(\sqrt{r}\right)$
m	$\Omega(r\ln(r\sigma))$	$\Omega(r\ln(r\sigma))$	$\Omega(r\ln(\sigma))$
Smoothing parameter	$O\left(mr\sqrt{\ln(m/\varepsilon)}\right)$	$O\left(r\sigma\sqrt{\ln(r\sigma+m+m/\varepsilon)}\right)$	$O\left(\sqrt{(r+\ln(m))\ln(m/\varepsilon)}\right)$

Existing results

On the smoothing parameter

- [AGHS13] and [KNSW20] lower bound λ_1^∞ of the dual lattice $(\Lambda^\perp(\mathbf{X}))^*$.

Existing results

On the smoothing parameter

- [AGHS13] and [KNSW20] lower bound λ_1^∞ of the dual lattice $(\Lambda^\perp(\mathbf{X}))^*$.
- [AR16] proves existence of short linearly-independent vectors in $\Lambda^\perp(\mathbf{X})$ directly.

LPSS14 reduction over rings

$MSIS_{r,m,B} \leq k\text{-}MSIS_{r,m+k,\mathbf{S},B'}$

✘ 1. Prove $\begin{bmatrix}\mathbf{X}_1 & \mathbf{X}_1 \cdot \mathbf{R} + \mathbf{I}\end{bmatrix} \sim \left(\mathscr{D}_{\mathscr{R}^{m+k},\mathbf{S},\mathbf{c}}\right)^k$

✔ 2. Prove the “order of sampling” lemma.

✔ 3. Extract the solution as $\mathbf{x} = \tilde{\mathbf{U}} \cdot \mathbf{x}^*$

Sasha Lapiha, Silence Laboratories

Notations

- Number field $\mathscr{K}$ of degree d.
- Field discriminant $\Delta_{\mathscr{K}}$.
- The ring of integers $\mathscr{R} = \mathcal{O}_{\mathscr{K}}$.
- We assume the canonical embedding of $\mathscr{R}$ has a basis $||\mathbf{B}_{\mathscr{R}}||_{\infty} \leq \delta_{\mathscr{K}}$.
- We assume $\mathscr{K}$ contains $\mathbb{Q}(\zeta_f)$ for some $f \geq 2$.

Discrete Gaussian over rings

$\tilde{\Phi}(\mathbf{M})$ - canonical embedding of $\mathbf{M}$ for matrix multiplication.

Base statement

$$(\mathbf{X}, \mathbf{X} \cdot \mathbf{v}) \sim (\mathbf{X}, \mathcal{D}_{\mathbf{X}\cdot\mathcal{R}^m, \sqrt{\tilde{\Phi}(\mathbf{X}) \cdot \mathbf{S}_v \cdot \mathbf{S}_v^T \cdot \tilde{\Phi}(\mathbf{X}^T)}})$$

$$\mathbf{X} \leftarrow \left(\mathcal{D}_{\mathcal{R}^r, \mathbf{S}_x}\right)^m, \quad \mathbf{v} \leftarrow \mathcal{D}_{\mathcal{R}^m, \mathbf{S}_v}$$

as long as $$\mathbf{S}_v \geq \eta_\varepsilon(\Lambda^\perp(\mathbf{X}))$$

Discrete Gaussian over rings

$\tilde{\Phi}(\mathbf{M})$ - canonical embedding

of $\mathbf{M}$ for matrix multiplication.

Base statement

$$(\mathbf{X}, \mathbf{X} \cdot \mathbf{v}) \sim \left(\mathbf{X}, \mathscr{D}_{\mathbf{X}\cdot\mathscr{R}^m, \sqrt{\tilde{\Phi}(\mathbf{X}) \cdot \mathbf{S}_v \cdot \mathbf{S}_v^T \cdot \tilde{\Phi}(\mathbf{X}^T)}}\right)$$

$$\mathbf{X} \leftarrow \left(\mathscr{D}_{\mathscr{R}^r, \mathbf{S}_x}\right)^m, \quad \mathbf{v} \leftarrow \mathscr{D}_{\mathscr{R}^m, \mathbf{S}_v}$$

as long as $\mathbf{S}_v \geq \eta_\varepsilon(\Lambda^\perp(\mathbf{X}))$

we also need $\mathbf{X} \cdot \mathscr{R}^m = \mathscr{R}^r$**, and** $\sqrt{\tilde{\Phi}(\mathbf{X}) \cdot \mathbf{S}_v \cdot \mathbf{S}_v^T \cdot \tilde{\Phi}(\mathbf{X}^T)} \approx \sigma \cdot I$

Short Kernel Basis

Lifting [AR16] to the ring setting

Short Kernel Basis

From the the kernel to the unit vector preimages

- Find short $\mathbf{U} \in \mathscr{R}^{m \times r}$ such that $\mathbf{X} \cdot \mathbf{U} = \mathbf{I}_r$
- Then for $\mathbf{I}_m - \mathbf{U} \cdot \mathbf{X}$ we have $\mathbf{X} \cdot (\mathbf{I}_m - \mathbf{U} \cdot \mathbf{X}) = \mathbf{X} - \mathbf{I}_r \cdot \mathbf{X} = \mathbf{0}$

Short Kernel Basis

Integer case

For $\mathbf{X} = [\mathbf{x}_1, \ldots, \mathbf{x}_m]$ with $||\mathbf{x}_i||_\infty \leq B$ consider the set $S_j = \sum_{i=1}^{j} \{0,1\} \cdot \mathbf{x}_i$

Short Kernel Basis

Integer case

For $\mathbf{X} = [\mathbf{x}_1, \ldots, \mathbf{x}_m]$ with $||\mathbf{x}_i||_\infty \leq B$ consider the set $S_j = \sum_{i=1}^{j} \{0,1\} \cdot \mathbf{x}_i$

As j grows the norms in S_j grow slower than cardinality.

For $\mathbf{v} \in S$: $||\mathbf{v}||_\infty \leq j \cdot B$ this is a set of size $(2jB + 1)^r$ but $|S| = 2^j$.

Eventually (when $j \geq 2r\log(Br)$) we have a collision or $\sum_{i=1}^{j} \{0, \pm 1\} \cdot \mathbf{x}_i = 0$

Sasha Lapiha, Silence Laboratories

Short Kernel Basis

Adapting to rings

For $\mathbf{X} = [\mathbf{x}_1, \ldots, \mathbf{x}_m]$ with $||\mathbf{x}_i||_\infty \leq B$ consider the set $S_j = \sum_{i=1}^{j} \{0,1\} \cdot \mathbf{x}_i$

Now $\mathbf{v} \in S$: $||\mathbf{v}||_\infty \leq j \cdot B$ this is a set of size $(2jB + 1)^{d \cdot r}$ but $|S| = 2^j$.

Over rings we have $j \geq 2dr\log(Br)$ for $\sum_{i=1}^{j} \{0, \pm 1\} \cdot \mathbf{x}_i = 0$

Short Kernel Basis

Adapting to rings

For $\mathbf{X} = [\mathbf{x}_1, \ldots, \mathbf{x}_m]$ with $||\mathbf{x}_i||_\infty \leq B$ consider the set $S_j = \sum_{i=1}^{j} \{0,1\} \cdot \mathbf{x}_i$

Now $\mathbf{v} \in S$: $||\mathbf{v}||_\infty \leq j \cdot B$ this is a set of size $(2jB + 1)^{d \cdot r}$ but $|S| = 2^j$.

Over rings we have $j \geq 2dr\log(Br)$ for $\sum_{i=1}^{j} \{0, \pm 1\} \cdot \mathbf{x}_i = 0$

We take the set $A = \mathbf{B}_{\mathscr{R}} \cdot \{0,1\}^d$ and $S_j = \{\sum_{i=1}^{j} a_i \cdot \mathbf{x}_i \mid a_i \in A\}, |S_j| = 2^{dj}$

Sasha Lapiha, Silence Laboratories

Short Kernel Basis

The result and open problems

$$\Pr\left(\eta_\varepsilon(\Lambda^\perp(\mathbf{X})) \le O(m^{3/2} \cdot d^{12} \cdot f^2 \cdot \delta_{\mathcal{K}}^{14} \cdot \Delta_{\mathcal{K}}^{4/d} \cdot s_{\min}(\mathbf{S}_x))\right) \ge 1 - 2^{-\lambda}$$

For $m \ge r \log(d \cdot r \cdot s_{\max}(\mathbf{S}_x))^{1+o(1)} + \dfrac{\lambda}{\log f}$.

- Find a different set A:
  - With short unit elements, with short inverses,
  - OR where all elements have many coprime short values.

Sasha Lapiha, Silence Laboratories

Extending other approaches?

For integers we prove

$$\forall \mathbf{z} \in \mathbb{Z}^r, \|\mathbf{z}\| > B : \Pr(\,|\,\mathbf{x}^T\mathbf{z} \bmod q\,| < B') < \frac{1}{\text{const}(\lambda)}$$

Then $\Pr(\|\mathbf{X}^T \cdot \mathbf{z} \bmod q\|_\infty < B) < \dfrac{1}{\text{const}(\lambda)^{m+k}}$ and usually $m = \text{poly}(\lambda)$

Extending other approaches?

For integers we prove

$$\forall \mathbf{z} \in \mathbb{Z}^r, \|\mathbf{z}\| > B : \Pr(|\mathbf{x}^T\mathbf{z} \bmod q| < B') < \frac{1}{\text{const}(\lambda)}$$

Then $\Pr(\|\mathbf{X}^T \cdot \mathbf{z} \bmod q\|_\infty < B) < \dfrac{1}{\text{const}(\lambda)^{m+k}}$ and usually $m = \text{poly}(\lambda)$

Over rings we need $\forall \mathbf{z} \in \mathcal{R}^r, \|\mathbf{z}\| > B : \Pr(|\mathbf{x}^T\mathbf{z} \bmod q| < B') < \dfrac{1}{2^d}$

Thank you!

References

- [AGHS13] - Shweta Agrawal, Craig Gentry, Shai Halevi, and Amit Sahai. Discrete Gaussian leftover hash lemma over infinite domains.
- [AR16] - Divesh Aggarwal and Oded Regev. A note on discrete gaussian combinations of lattice vectors
- [BF11] - Dan Boneh and David Mandell Freeman. Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures.
- [KNSW20] - Elena Kirshanova, Huyen Nguyen, Damien Stehle, and Alexandre Wallet. On the smoothing parameter and last minimum of random orthogonal lattices.
- [LPSS14] - San Ling, Duong Hieu Phan, Damien Stehle, and Ron Steinfeld. Hardness of k-LWE and applications in traitor tracing.