

k -R-ISIS, vSIS, BASIS and their Relation

Valerio Cini

Bocconi

Why Hand Out Hints at All?

- ▶ **Goal:** succinct functional commitments from lattices

Why Hand Out Hints at All?

- ▶ **Goal:** succinct functional commitments from lattices
- ▶ Trying to imitate pairing-based construction (and relative assumptions)

Why Hand Out Hints at All?

- ▶ **Goal:** succinct functional commitments from lattices
- ▶ Trying to imitate pairing-based construction (and relative assumptions)

Example: k -Diffie-Hellman Exponent problem

Why Hand Out Hints at All?

- ▶ **Goal:** succinct functional commitments from lattices
- ▶ Trying to imitate pairing-based construction (and relative assumptions)

Example: k -Diffie-Hellman Exponent problem

given $g, g^\alpha, g^{\alpha^2}, \dots, g^{\alpha^{k-1}},$

Why Hand Out Hints at All?

- ▶ **Goal:** succinct functional commitments from lattices
- ▶ Trying to imitate pairing-based construction (and relative assumptions)

Example: k -Diffie-Hellman Exponent problem

given $g, g^\alpha, g^{\alpha^2}, \dots, g^{\alpha^{k-1}}$, compute g^{α^k}

Roadmap

- ▶ k -R-ISIS [ACLMT22]
- ▶ vSIS [CLM23]
- ▶ BASIS [WW23]

Short Integer Solution (SIS) [Ajtai96]

The diagram illustrates the Short Integer Solution (SIS) problem. It features a blue rectangular matrix A with a width of m and a height of n , indicated by curly braces. Below the matrix, the text "over $\mathbb{Z}_q$ " is written. To the right of the matrix is a green vertical vector u . Further right is a white vertical vector containing the number 0 . The equation is represented as $A \cdot u = 0 \pmod q$.

$$\begin{matrix} m \\ \overbrace{\hspace{1.5cm}} \\ \left\{ \begin{array}{c} n \\ \hline \mathbf{A} \end{array} \right. \cdot \begin{array}{c} \text{green box} \\ \mathbf{u} \end{array} = \begin{array}{c} \text{white box} \\ 0 \end{array} \pmod q \\ \text{over } \mathbb{Z}_q \end{matrix}$$

Notation 1/2

Notation 1/2

- ▶ $\mathcal{G} = \{g_1, \dots, g_k\}$: the monomials we *hand out* preimages for,

Notation 1/2

- ▶ $\mathcal{G} = \{g_1, \dots, g_k\}$: the monomials we *hand out* preimages for,
- ▶ g^* : the *challenge* polynomial.

Notation 1/2

- ▶ $\mathcal{G} = \{g_1, \dots, g_k\}$: the monomials we *hand out* preimages for,
- ▶ g^* : the *challenge* polynomial.

Example:

$$\mathcal{G} = \{1, X, X^2, \dots, X^{k-1}\} \quad \text{and} \quad g^* = X^k$$

Public parameters: $\mathbf{A}$, $\mathbf{t}$, $\mathbf{v}$ sampled uniformly at random
monomials $\mathcal{G} = \{g_1, \dots, g_k\}$ challenge monomial g^*

k -R-ISIS [ACLMT22]

$$\boxed{\mathbf{A}} \cdot \underbrace{\boxed{\mathbf{u}_1 \cdots \mathbf{u}_k}}_{\text{short preimages (the hints)}} = \boxed{\mathbf{t}} \cdot \overbrace{\boxed{g_1(\mathbf{v}) \cdots g_k(\mathbf{v})}}^{\text{monomials at public } \mathbf{v}} \bmod q$$

Public parameters: $\mathbf{A}$, $\mathbf{t}$, $\mathbf{v}$ sampled uniformly at random
monomials $\mathcal{G} = \{g_1, \dots, g_k\}$ challenge monomial g^*

k -R-ISIS [ACLMT22]

$$\boxed{\mathbf{A}} \cdot \underbrace{\boxed{\mathbf{u}_1 \cdots \mathbf{u}_k}}_{\text{short preimages (the hints)}} = \boxed{\mathbf{t}} \cdot \overbrace{\boxed{g_1(\mathbf{v}) \cdots g_k(\mathbf{v})}}^{\text{monomials at public } \mathbf{v}} \bmod q$$

Challenge: find short $(\mathbf{u}^*, \mathbf{s}^*) \neq \mathbf{0}$ with $\mathbf{A} \mathbf{u}^* = \mathbf{t} \cdot \mathbf{g}^*(\mathbf{v}) \cdot \mathbf{s}^*$
for a challenge monomial $\mathbf{g}^*$ ($\mathbf{s}^*$ short slack)

challenge monomial g^* + short slack s^*

$$\boxed{A} \cdot \underbrace{\boxed{u^*}}_{\text{the forgery (short)}} = \boxed{t} \cdot \boxed{g^*(v)} \cdot \boxed{s^*} \bmod q$$

Challenge: find short $(u^*, s^*) \neq \mathbf{0}$ with $A u^* = t \cdot g^*(v) \cdot s^*$
for a challenge monomial g^* (s^* short slack)

Public parameters: public random $\mathbf{v}$ (uniform)
monomials $\mathcal{G} = \{g_1, \dots, g_\ell\}$

$g_i(\mathbf{v})$: monomials at public $\mathbf{v}$

$$\begin{bmatrix} g_1(\mathbf{v}) & g_2(\mathbf{v}) & \cdots & g_\ell(\mathbf{v}) \end{bmatrix} \cdot \mathbf{p} = \begin{bmatrix} 0 \end{bmatrix} \bmod q$$

Goal: find short $\mathbf{p} \neq \mathbf{0}$ such that the above holds

$$g_i(\mathbf{v}): \text{ monomials at public } \mathbf{v}$$

$$\begin{bmatrix} g_1(\mathbf{v}) & g_2(\mathbf{v}) & \cdots & g_\ell(\mathbf{v}) \end{bmatrix} \cdot \mathbf{p} = \boxed{0} \bmod q$$

Goal: find short $\mathbf{p} \neq \mathbf{0}$ such that the above holds

vSIS with $\mathbf{v} = v$ and $g_i(\mathbf{v}) = v^{i-1}$: $\mathbf{p}$ is a polynomial vanishing at v

$$\overbrace{g_i(\mathbf{v}): \text{monomials at public } \mathbf{v}} \\ \left[\boxed{g_1(\mathbf{v})} \boxed{g_2(\mathbf{v})} \cdots \boxed{g_\ell(\mathbf{v})} \right] \cdot \boxed{\mathbf{p}} = \boxed{0} \bmod q$$

Goal: find short $\mathbf{p} \neq \mathbf{0}$ such that the above holds
vSIS with $\mathbf{v} \in \mathbb{Z}_q^\ell$ and $g_i(\mathbf{v}) = \mathbf{v}_i$: standard SIS assumption

vSIS $\Rightarrow$ k -R-ISIS

use vSIS on $\{g_1, \dots, g_\ell\}$ to solve k -R-ISIS: $\mathcal{G} = \{g_1, \dots, g_{\ell-1}\}$, $g^* = g_\ell$

vSIS $\Rightarrow$ k -R-ISIS

use vSIS on $\{g_1, \dots, g_\ell\}$ to solve k -R-ISIS: $\mathcal{G} = \{g_1, \dots, g_{\ell-1}\}$, $g^* = g_\ell$

$$\begin{bmatrix} g_1(\mathbf{v}) & \cdots & g_{\ell-1}(\mathbf{v}) & | & g_\ell(\mathbf{v}) \end{bmatrix} \cdot \begin{bmatrix} \mathbf{r}_t \\ \mathbf{r}_b \end{bmatrix} = \mathbf{0} \bmod q$$

vSIS $\Rightarrow$ k -R-ISIS

use vSIS on $\{g_1, \dots, g_\ell\}$ to solve k -R-ISIS: $\mathcal{G} = \{g_1, \dots, g_{\ell-1}\}$, $g^* = g_\ell$

$$\begin{bmatrix} g_1(\mathbf{v}) & \cdots & g_{\ell-1}(\mathbf{v}) & g_\ell(\mathbf{v}) \end{bmatrix} \cdot \begin{bmatrix} \mathbf{r}_t \\ \mathbf{r}_b \end{bmatrix} = \mathbf{0} \bmod q$$

1. vSIS gives short $\mathbf{r} = (\mathbf{r}_t, \mathbf{r}_b)$; isolate the last block:

$$\begin{bmatrix} g_1(\mathbf{v}) & \cdots & g_{\ell-1}(\mathbf{v}) \end{bmatrix} \cdot \mathbf{r}_t = - \begin{bmatrix} g_\ell(\mathbf{v}) \end{bmatrix} \cdot \mathbf{r}_b$$

vSIS $\Rightarrow$ k -R-ISIS

use vSIS on $\{g_1, \dots, g_\ell\}$ to solve k -R-ISIS: $\mathcal{G} = \{g_1, \dots, g_{\ell-1}\}$, $g^* = g_\ell$

$$\mathbf{A} \cdot \mathbf{u}_1 \cdots \mathbf{u}_{\ell-1} = \mathbf{t} \cdot g_1(\mathbf{v}) \cdots g_{\ell-1}(\mathbf{v})$$

1. vSIS gives short $\mathbf{r} = (\mathbf{r}_t, \mathbf{r}_b)$; isolate the last block:

$$g_1(\mathbf{v}) \cdots g_{\ell-1}(\mathbf{v}) \cdot \mathbf{r}_t = -g_\ell(\mathbf{v}) \cdot \mathbf{r}_b$$

vSIS $\Rightarrow$ k -R-ISIS

use vSIS on $\{g_1, \dots, g_\ell\}$ to solve k -R-ISIS: $\mathcal{G} = \{g_1, \dots, g_{\ell-1}\}$, $g^* = g_\ell$

$$\boxed{\mathbf{A}} \cdot \boxed{\mathbf{u}_1 \cdots \mathbf{u}_{\ell-1}} = \boxed{\mathbf{t}} \cdot \boxed{g_1(\mathbf{v}) \cdots g_{\ell-1}(\mathbf{v})}$$

2. right-multiply by $\mathbf{r}_t$, set $\mathbf{u}^* = [\mathbf{u}_1 \cdots \mathbf{u}_{\ell-1}] \mathbf{r}_t$, $\mathbf{s}^* = -\mathbf{r}_b$:

vSIS $\Rightarrow$ k -R-ISIS

use vSIS on $\{g_1, \dots, g_\ell\}$ to solve k -R-ISIS: $\mathcal{G} = \{g_1, \dots, g_{\ell-1}\}$, $g^* = g_\ell$

$$\mathbf{A} \cdot \begin{bmatrix} \mathbf{u}_1 & \cdots & \mathbf{u}_{\ell-1} \end{bmatrix} \mathbf{r}_t = \mathbf{t} \cdot \begin{bmatrix} g_1(\mathbf{v}) & \cdots & g_{\ell-1}(\mathbf{v}) \end{bmatrix} \mathbf{r}_t$$

2. right-multiply by $\mathbf{r}_t$, set $\mathbf{u}^* = [\mathbf{u}_1 \cdots \mathbf{u}_{\ell-1}] \mathbf{r}_t$, $s^* = -\mathbf{r}_b$:

vSIS $\Rightarrow$ k -R-ISIS

use vSIS on $\{g_1, \dots, g_\ell\}$ to solve k -R-ISIS: $\mathcal{G} = \{g_1, \dots, g_{\ell-1}\}$, $g^* = g_\ell$

$$\boxed{\mathbf{A}} \cdot \boxed{\mathbf{u}^*} = \boxed{\mathbf{t}} \cdot \boxed{g_\ell(\mathbf{v})} \cdot (-\boxed{\mathbf{r}_b})$$

2. right-multiply by $\mathbf{r}_t$, set $\mathbf{u}^* = [\mathbf{u}_1 \cdots \mathbf{u}_{\ell-1}] \mathbf{r}_t$, $s^* = -\mathbf{r}_b$:

vSIS $\Rightarrow$ k -R-ISIS

use vSIS on $\{g_1, \dots, g_\ell\}$ to solve k -R-ISIS: $\mathcal{G} = \{g_1, \dots, g_{\ell-1}\}$, $g^* = g_\ell$

$$\boxed{A} \cdot \boxed{u^*} = \boxed{t} \cdot \boxed{g^*(v)} \cdot \boxed{s^*}$$

2. right-multiply by r_t , set $u^* = [u_1 \cdots u_{\ell-1}] r_t$, $s^* = -r_b$:

Notation 2/2

► $\mathbf{G} = \mathbf{I}_n \otimes \mathbf{g}$: *gadget* matrix, $\mathbf{g} = (2^0, 2^1, 2^2, \dots, 2^{\lceil \log q \rceil - 1})$

$$\overbrace{\mathbf{G}}^{n \lceil \log q \rceil \text{ columns}} \cdot \mathbf{u} = \mathbf{t} \bmod q$$

Notation 2/2

► $\mathbf{G} = \mathbf{I}_n \otimes \mathbf{g}$: *gadget* matrix, $\mathbf{g} = (2^0, 2^1, 2^2, \dots, 2^{\lceil \log q \rceil - 1})$

$$\overbrace{\mathbf{G}}^{n \lceil \log q \rceil \text{ columns}} \cdot \mathbf{u} = \mathbf{t} \bmod q$$

every target $\mathbf{t}$ has a *short* preimage $\mathbf{u}$ under $\mathbf{G}$

(bit-decomposition: $\mathbf{u} = \mathbf{G}^{-1}(\mathbf{t})$)

Notation 2/2

► $\mathbf{G} = \mathbf{I}_n \otimes \mathbf{g}$: *gadget* matrix, $\mathbf{g} = (2^0, 2^1, 2^2, \dots, 2^{\lceil \log q \rceil - 1})$

$$\overbrace{\mathbf{G}}^{n \lceil \log q \rceil \text{ columns}} \cdot \mathbf{u} = \mathbf{t} \bmod q$$

1. SIS is easy for $\mathbf{G}$,

Notation 2/2

► $\mathbf{G} = \mathbf{I}_n \otimes \mathbf{g}$: *gadget* matrix, $\mathbf{g} = (2^0, 2^1, 2^2, \dots, 2^{\lceil \log q \rceil - 1})$

$$\overbrace{\mathbf{G}}^{n \lceil \log q \rceil \text{ columns}} \cdot \mathbf{u} = \mathbf{t} \bmod q$$

1. SIS is easy for $\mathbf{G}$, 2. if $\mathbf{A} \cdot \mathbf{R} = \mathbf{G}$, then SIS is easy for $\mathbf{A}$.

A uniform random

$\mathbf{A}_1, \dots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \text{Samp}(1^\lambda, \mathbf{A})$

.

BASIS

[WW23]

$\mathbf{A}$ uniform random

$\mathbf{A}_1, \dots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \text{Samp}(1^\lambda, \mathbf{A})$

$$\underbrace{\begin{bmatrix} \mathbf{A}_1 & & & \\ & \ddots & & \\ & & \mathbf{A}_\ell & \\ & & & \begin{bmatrix} -\mathbf{G} \\ \vdots \\ -\mathbf{G} \end{bmatrix} \end{bmatrix}}_{\mathbf{B}_\ell} \cdot \underbrace{\mathbf{R}}_{\text{trapdoor (short) = hint}} = \mathbf{I}_\ell \otimes \mathbf{G}$$

BASIS

[WW23]

$\mathbf{A}$ uniform random

$\mathbf{A}_1, \dots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \text{Samp}(1^\lambda, \mathbf{A})$

$$\underbrace{\left[\begin{array}{ccc|c} \mathbf{A}_1 & & & -\mathbf{G} \\ & \ddots & & \vdots \\ & & \mathbf{A}_\ell & -\mathbf{G} \end{array} \right]}_{\mathbf{B}_\ell} \cdot \mathbf{R} = \mathbf{I}_\ell \otimes \mathbf{G}$$

Goal: solve SIS w.r.t. $\mathbf{A}$

BASIS_{rand} [WW23]

$\mathbf{A}$ uniform random

$\mathbf{A}_1, \dots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \text{Samp}(1^\lambda, \mathbf{A})$

$$\underbrace{\left[\begin{array}{c|c} \boxed{\mathbf{A}_1} & \boxed{-\mathbf{G}} \\ \vdots & \vdots \\ \boxed{\mathbf{A}_\ell} & \boxed{-\mathbf{G}} \end{array} \right]}_{\mathbf{B}_\ell} \cdot \boxed{\mathbf{R}} = \boxed{\mathbf{I}_\ell \otimes \mathbf{G}}$$

BASIS_{rand} [WW23]

$\mathbf{A}$ uniform random

$\mathbf{A}_1, \dots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \text{Samp}(1^\lambda, \mathbf{A})$

$$\underbrace{\left[\begin{array}{c|c} \boxed{\mathbf{A}_1} & \boxed{-\mathbf{G}} \\ \vdots & \vdots \\ \boxed{\mathbf{A}_\ell} & \boxed{-\mathbf{G}} \end{array} \right]}_{\mathbf{B}_\ell} \cdot \boxed{\mathbf{R}} = \boxed{\mathbf{I}_\ell \otimes \mathbf{G}}$$

$\mathbf{A}_i$ uniform $\forall i \neq i^*, \mathbf{A}_{i^*} = \mathbf{A}$

BASIS_{rand} [WW23]

$\mathbf{A}$ uniform random

$\mathbf{A}_1, \dots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \text{Samp}(1^\lambda, \mathbf{A})$

$$\underbrace{\left[\begin{array}{c|c} \boxed{\mathbf{A}_1} & \boxed{-\mathbf{G}} \\ \vdots & \vdots \\ \boxed{\mathbf{A}_\ell} & \boxed{-\mathbf{G}} \end{array} \right]}_{\mathbf{B}_\ell} \cdot \boxed{\mathbf{R}} = \boxed{\mathbf{I}_\ell \otimes \mathbf{G}}$$

$\mathbf{A}_i$ uniform $\forall i \neq i^*, \mathbf{A}_{i^*} = \mathbf{A} \implies \text{BASIS}_{\text{rand}}$

BASIS_{struct} [WW23]

A uniform random

$\mathbf{A}_1, \dots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \text{Samp}(1^\lambda, \mathbf{A})$

$$\underbrace{\left[\begin{array}{c|c} \boxed{\mathbf{A}_1} & \boxed{-\mathbf{G}} \\ \vdots & \vdots \\ \boxed{\mathbf{A}_\ell} & \boxed{-\mathbf{G}} \end{array} \right]}_{\mathbf{B}_\ell} \cdot \boxed{\mathbf{R}} = \boxed{\mathbf{I}_\ell \otimes \mathbf{G}}$$

BASIS_{struct} [WW23]

$\mathbf{A}$ uniform random

$\mathbf{A}_1, \dots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \text{Samp}(1^\lambda, \mathbf{A})$

The diagram illustrates the construction of a matrix product. On the left, a block matrix is shown, partitioned into two main sections. The first section, labeled $\mathbf{B}_\ell$ with a brace underneath, contains a vertical stack of blocks: $\mathbf{A}_1$ (in a red box), followed by three dots, and then $\mathbf{A}_\ell$ (also in a red box). The second section, separated by a vertical line, contains a vertical stack of blocks: $-\mathbf{G}$ (in a gray box), followed by three dots, and then $-\mathbf{G}$ (in a gray box). This block matrix is multiplied by a large green square block labeled $\mathbf{R}$. The result of this multiplication is shown as a gray square block labeled $\mathbf{I}_\ell \otimes \mathbf{G}$.

$\mathbf{W}_i$ random square invertible, $\mathbf{A}_i = \mathbf{W}_i \cdot \mathbf{A}$

BASIS_{struct} [WW23]

$\mathbf{A}$ uniform random

$\mathbf{A}_1, \dots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \text{Samp}(1^\lambda, \mathbf{A})$

$$\underbrace{\begin{bmatrix} \boxed{\mathbf{A}_1} & & \\ & \ddots & \\ & & \boxed{\mathbf{A}_\ell} \end{bmatrix} \begin{array}{c} \boxed{-\mathbf{G}} \\ \vdots \\ \boxed{-\mathbf{G}} \end{array}}_{\mathbf{B}_\ell} \cdot \begin{array}{c} \boxed{\mathbf{R}} \end{array} = \boxed{\mathbf{I}_\ell \otimes \mathbf{G}}$$

$\mathbf{W}_i$ random square invertible, $\mathbf{A}_i = \mathbf{W}_i \cdot \mathbf{A} \implies \text{BASIS}_{\text{struct}}$

BASIS_{struct} [WW23]

$\mathbf{A}$ uniform random

$\mathbf{A}_1, \dots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \text{Samp}(1^\lambda, \mathbf{A})$

$$\underbrace{\begin{bmatrix} \boxed{\mathbf{W}_1 \mathbf{A}} & \boxed{-\mathbf{G}} \\ \vdots & \vdots \\ \boxed{\mathbf{W}_\ell \mathbf{A}} & \boxed{-\mathbf{G}} \end{bmatrix}}_{\mathbf{B}_\ell} \cdot \begin{bmatrix} \mathbf{R} \end{bmatrix} = \begin{bmatrix} \mathbf{I}_\ell \otimes \mathbf{G} \end{bmatrix}$$

$\mathbf{W}_i$ random square invertible, $\mathbf{A}_i = \mathbf{W}_i \cdot \mathbf{A} \implies \text{BASIS}_{\text{struct}}$

$\text{BASIS}_{\text{rand}} \Rightarrow \text{SIS}$ [WW23]

$\text{BASIS}_{\text{rand}} \Rightarrow \text{SIS}$ [WW23]

- ▶ Plant the SIS challenge $\mathbf{A}$ as $\mathbf{A}_{i^*}$

BASIS_{rand} $\Rightarrow$ SIS [WW23]

- ▶ Plant the SIS challenge $\mathbf{A}$ as $\mathbf{A}_{i^*}$
- ▶ Sample $\mathbf{A}_i$, $i \neq i^*$, *with* gadget trapdoors ($\mathbf{A}_i \mathbf{R}_i = \mathbf{G}$)

BASIS_{rand} $\Rightarrow$ SIS [WW23]

- ▶ Plant the SIS challenge $\mathbf{A}$ as $\mathbf{A}_{i^*}$
- ▶ Sample $\mathbf{A}_i$, $i \neq i^*$, *with* gadget trapdoors ($\mathbf{A}_i \mathbf{R}_i = \mathbf{G}$)
- ▶ Extend these into a trapdoor $\mathbf{R}$ for the augmented $\mathbf{B}_\ell$

BASIS_{rand} $\Rightarrow$ SIS [WW23]

- ▶ Plant the SIS challenge $\mathbf{A}$ as $\mathbf{A}_{i^*}$
- ▶ Sample $\mathbf{A}_i$, $i \neq i^*$, with gadget trapdoors ($\mathbf{A}_i \mathbf{R}_i = \mathbf{G}$)
- ▶ Extend these into a trapdoor $\mathbf{R}$ for the augmented $\mathbf{B}_\ell$

BASIS_{rand} solution yields SIS solution for $\mathbf{A}_{i^*} = \mathbf{A}$

BASIS_{rand} $\Rightarrow$ SIS [WW23]

$$\left[\begin{array}{ccc|c} \boxed{A_1} & & & \boxed{-G} \\ & \boxed{A_2} & & \boxed{-G} \\ & & \boxed{A_3} & \boxed{-G} \end{array} \right] \begin{array}{c} \overbrace{\left[\begin{array}{cc} \boxed{R_1} & \boxed{-R_1} \\ & \boxed{-R_3} & \boxed{R_3} \\ & & \boxed{-I} \end{array} \right]}^{\mathbf{R}} \end{array}$$

$i^* = 2, \quad \mathbf{A}_1 \mathbf{R}_1 = \mathbf{G}, \quad \mathbf{A}_3 \mathbf{R}_3 = \mathbf{G}$

BASIS_{rand} $\Rightarrow$ SIS [WW23]

$$\begin{bmatrix} \boxed{A_1} & & \\ & \boxed{A_2} & \\ & & \boxed{A_3} \end{bmatrix} \begin{bmatrix} \boxed{-G} \\ \boxed{-G} \\ \boxed{-G} \end{bmatrix} \begin{bmatrix} \boxed{R_1} & \boxed{-R_1} \\ & \boxed{-R_3} & \boxed{R_3} \\ & \boxed{-I} & \end{bmatrix} = \begin{bmatrix} \boxed{G} & & \\ & \boxed{G} & \\ & & \boxed{G} \end{bmatrix}$$

$i^* = 2, \quad \boxed{A_1} \boxed{R_1} = \boxed{G}, \quad \boxed{A_3} \boxed{R_3} = \boxed{G}$

BASIS_{rand} $\Rightarrow$ SIS [WW23]

$$\begin{bmatrix} \boxed{A_1} & & \\ & \boxed{A_2} & \\ & & \boxed{A_3} \end{bmatrix} \begin{bmatrix} \boxed{-G} \\ \boxed{-G} \\ \boxed{-G} \end{bmatrix} \begin{bmatrix} \overbrace{\begin{bmatrix} \boxed{R_1} & \boxed{-R_1} \\ & \boxed{-R_3} & \boxed{R_3} \\ & & \boxed{-I} \end{bmatrix}}^{\mathbf{R}} \\ \\ \\ \end{bmatrix} = \boxed{I_3 \otimes G}$$

$i^* = 2, \quad \mathbf{A_1 R_1} = \mathbf{G}, \quad \mathbf{A_3 R_3} = \mathbf{G}$

Relation b/w k -R-ISIS and $\text{BASIS}_{\text{struct}}$

- ▶ Both hand out structured data tied to $\mathbf{A}_i = \mathbf{W}_i \mathbf{A}$

Relation b/w k -R-ISIS and $\text{BASIS}_{\text{struct}}$

- ▶ Both hand out structured data tied to $\mathbf{A}_i = \mathbf{W}_i \mathbf{A}$
- ▶ $\text{BASIS}_{\text{struct}}$ trapdoor can heuristically be built from k -R-ISIS preimages (and viceversa)

Relation b/w k -R-ISIS and $\text{BASIS}_{\text{struct}}$

$$\boxed{\mathbf{A}} \cdot \boxed{\mathbf{u}_{i,j}} = \underbrace{\boxed{\mathbf{W}_i^{-1}} \cdot \boxed{\mathbf{y}_j}}_{g_{i,j}(\mathbf{v})} \bmod q$$

Relation b/w k -R-ISIS and $\text{BASIS}_{\text{struct}}$

$$\boxed{W_i} \cdot \boxed{A} \cdot \boxed{u_{i,j}} = \boxed{y_j} \bmod q$$

Relation b/w k -R-ISIS and $\text{BASIS}_{\text{struct}}$

$$\boxed{\mathbf{A}_i} \cdot \boxed{\mathbf{u}_{i,j}} = \boxed{\mathbf{y}_j} \bmod q$$

Relation b/w k -R-ISIS and $\text{BASIS}_{\text{struct}}$

$$\boxed{A_i} \cdot \boxed{u_{i,j}} = \boxed{G} \boxed{z_j} \bmod q$$

Relation b/w k -R-ISIS and $\text{BASIS}_{\text{struct}}$

$$\left[\begin{array}{ccc|c} \boxed{A_1} & & & \boxed{-G} \\ & \ddots & & \vdots \\ & & \boxed{A_\ell} & \boxed{-G} \end{array} \right] \begin{bmatrix} \boxed{u_{1,j}} \\ \vdots \\ \boxed{u_{\ell,j}} \\ \boxed{z_j} \end{bmatrix} = \boxed{0} \pmod{q}$$

Relation b/w k -R-ISIS and $\text{BASIS}_{\text{struct}}$

$$\left[\begin{array}{ccc|c} \boxed{A_1} & & & \boxed{-G} \\ & \ddots & & \vdots \\ & & \boxed{A_\ell} & \boxed{-G} \end{array} \right] \begin{bmatrix} \boxed{u_{1,j}} \\ \vdots \\ \boxed{u_{\ell,j}} \\ \boxed{z_j} \end{bmatrix} = \boxed{0} \pmod{q}$$

heuristically linearly independent
 $\Downarrow$
 (Ajtai) trapdoor for $\mathbf{B}_\ell$

Open Problems

- ▶ How does security of $\text{BASIS}_{\text{struct}}$ / k -R-ISIS / vSIS degrade with ℓ or k ?

Open Problems

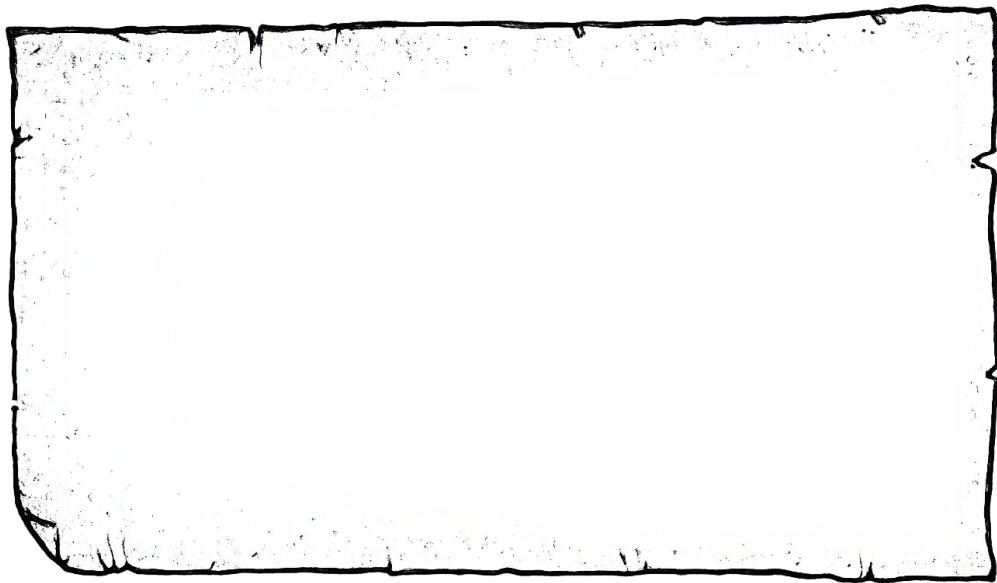
- ▶ How does security of $\text{BASIS}_{\text{struct}}$ / k -R-ISIS / vSIS degrade with ℓ or k ?
- ▶ Reductions for $\text{BASIS}_{\text{struct}}$ / k -R-ISIS / vSIS (or variants) in *useful* regimes

Open Problems

- ▶ How does security of $\text{BASIS}_{\text{struct}}$ / k -R-ISIS / vSIS degrade with ℓ or k ?
- ▶ Reductions for $\text{BASIS}_{\text{struct}}$ / k -R-ISIS / vSIS (or variants) in *useful* regimes (preliminary results for Decomposed-LWE)

Open Problems

- ▶ How does security of $\text{BASIS}_{\text{struct}}$ / $k\text{-R-ISIS}$ / vSIS degrade with ℓ or k ?
- ▶ Reductions for $\text{BASIS}_{\text{struct}}$ / $k\text{-R-ISIS}$ / vSIS (or variants) in *useful* regimes (preliminary results for Decomposed-LWE)
- ▶ “Encryption friendly” vector/functional commitments from weaker assumptions?



k-R-ISIS

[C:ACLMT22]

k -R-ISIS

[C:ACLMT22]



BASIS

[EC:WeeWu23]

k -R-ISIS

[C:ACLMT22]

Succinct SIS

[AC:WeeWu23]

BASIS

[EC:WeeWu23]

k -R-ISIS

[C:ACLMT22]

Decomposed SIS

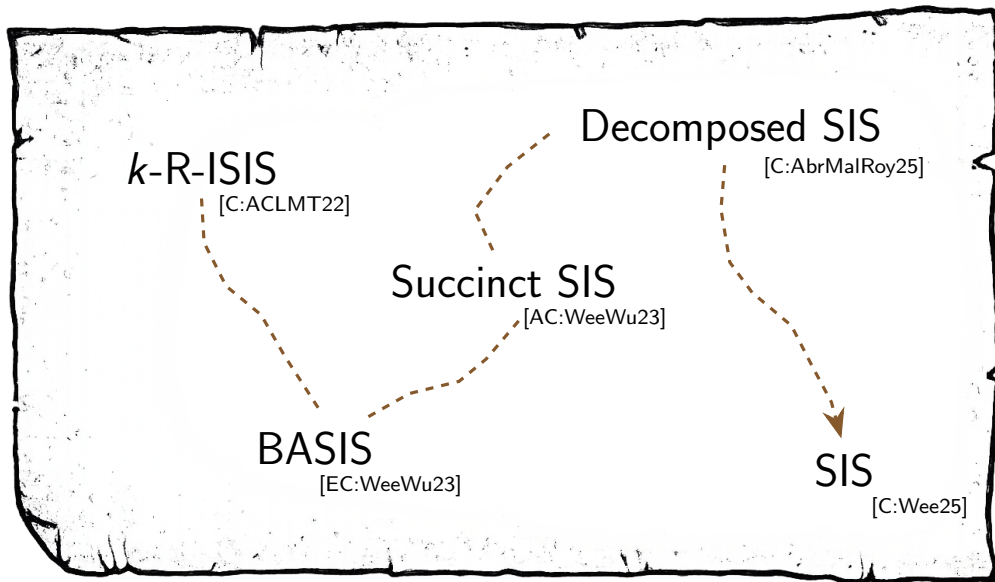
[C:AbrMalRoy25]

Succinct SIS

[AC:WeeWu23]

BASIS

[EC:WeeWu23]



Open Problems

- ▶ How does security of $\text{BASIS}_{\text{struct}}$ / k -R-ISIS / vSIS degrade with ℓ or k ?
- ▶ Reductions for $\text{BASIS}_{\text{struct}}$ / k -R-ISIS / vSIS in *useful* regimes (preliminary results for Decomposed-LWE)
- ▶ “Encryption friendly” vector/functional commitments from weaker assumptions?

Thank you!