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

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

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

$$\text{given } g, g^{\alpha}, g^{\alpha^2}, \ldots, g^{\alpha^{k-1}}, \quad \text{compute } g^{\alpha^k}$$

Roadmap

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

Short Integer Solution (SIS) [Ajtai96]

$$n\left\{ \overbrace{\mathbf{A}}^{m} \right. \cdot \mathbf{u} = \mathbf{0} \mod q$$

over $\mathbb{Z}_q$

Notation 1/2

Notation 1/2

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

Notation 1/2

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

Notation 1/2

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

Example:

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

k-R-ISIS [ACLMT22]

Public parameters: $\mathbf{A}$, $\mathbf{t}$, $\mathbf{v}$ sampled uniformly at random

monomials $\mathcal{G} = \{g_1, \ldots, g_k\}$ challenge monomial g^*

k-R-ISIS [ACLMT22]

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

Public parameters: $\mathbf{A}$, $\mathbf{t}$, $\mathbf{v}$ sampled uniformly at random

monomials $\mathcal{G} = \{g_1, \ldots, g_k\}$ challenge monomial g^*

k-R-ISIS [ACLMT22]

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

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

k-R-ISIS [ACLMT22]

challenge monomial g^* + short slack s^*

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

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

vSIS [CLM23]

Public parameters: public random $\mathbf{v}$ (uniform)

monomials $\mathcal{G} = \{g_1, \ldots, g_\ell\}$

vSIS [CLM23]

$$\underbrace{\begin{bmatrix} \boxed{g_1(\mathbf{v})} & \boxed{g_2(\mathbf{v})} & \cdots & \boxed{g_\ell(\mathbf{v})} \end{bmatrix}}_{}^{g_i(\mathbf{v}):\ \text{monomials at public } \mathbf{v}} \cdot \boxed{\mathbf{p}} = \boxed{\mathbf{0}} \bmod q$$

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

vSIS [CLM23]

$$\overbrace{\begin{bmatrix} \boxed{g_1(\mathbf{v})} & \boxed{g_2(\mathbf{v})} & \cdots & \boxed{g_\ell(\mathbf{v})} \end{bmatrix}}^{g_i(\mathbf{v})\text{: monomials at public } \mathbf{v}} \cdot \boxed{\mathbf{p}} = \boxed{\mathbf{0}} \bmod q$$

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

vSIS [CLM23]

$$\overbrace{\begin{bmatrix} \boxed{g_1(\mathbf{v})} & \boxed{g_2(\mathbf{v})} & \cdots & \boxed{g_\ell(\mathbf{v})} \end{bmatrix}}^{g_i(\mathbf{v})\text{: monomials at public } \mathbf{v}} \cdot \boxed{\mathbf{p}} = \boxed{\mathbf{0}} \bmod q$$

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

vSIS $\Rightarrow$ k-R-ISIS

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

$$\left[\boxed{g_1(\mathbf{v})} \cdots \boxed{g_{\ell-1}(\mathbf{v})} \,\middle|\, \boxed{g_\ell(\mathbf{v})}\right] \cdot \begin{bmatrix} \boxed{\mathbf{r}_{\mathrm{t}}} \\ \boxed{\mathbf{r}_{\mathrm{b}}} \end{bmatrix} = \boxed{\mathbf{0}} \bmod q$$

vSIS $\Rightarrow$ k-R-ISIS

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

$$\left[\, \boxed{g_1(\mathbf{v})} \cdots \boxed{g_{\ell-1}(\mathbf{v})} \;\middle|\; \boxed{g_\ell(\mathbf{v})} \,\right] \cdot \begin{bmatrix} \boxed{\mathbf{r}_{\mathrm{t}}} \\ \boxed{\mathbf{r}_{\mathrm{b}}} \end{bmatrix} = \boxed{\mathbf{0}} \bmod q$$

1. vSIS gives short $\mathbf{r} = (\mathbf{r}_{\mathrm{t}}, \mathbf{r}_{\mathrm{b}})$; isolate the last block:

$$\boxed{g_1(\mathbf{v}) \cdots g_{\ell-1}(\mathbf{v})} \cdot \boxed{\mathbf{r}_{\mathrm{t}}} = -\boxed{g_\ell(\mathbf{v})} \cdot \boxed{\mathbf{r}_{\mathrm{b}}}$$

vSIS $\Rightarrow$ k-R-ISIS

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

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

1. vSIS gives short $\mathbf{r} = (\mathbf{r}_\mathrm{t}, \mathbf{r}_\mathrm{b})$; isolate the last block:

$$\boxed{g_1(\mathbf{v}) \cdots g_{\ell-1}(\mathbf{v})} \cdot \boxed{\mathbf{r}_\mathrm{t}} = -\boxed{g_\ell(\mathbf{v})} \cdot \boxed{\mathbf{r}_\mathrm{b}}$$

vSIS $\Rightarrow$ k-R-ISIS

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

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

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

vSIS $\Rightarrow$ k-R-ISIS

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

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

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

vSIS $\Rightarrow$ k-R-ISIS

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

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

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

vSIS $\Rightarrow$ k-R-ISIS

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

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

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

Notation 2/2

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

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

Notation 2/2

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

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

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, $\mathbf{g} = (2^0, 2^1, 2^2, \ldots, 2^{\lceil \log q \rceil - 1})$

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

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

Notation 2/2

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

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

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

BASIS [WW23]

$\mathbf{A}$ uniform random $\qquad \mathbf{A}_1, \cdots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \mathsf{Samp}(1^\lambda, \mathbf{A})$

$\ddots$

BASIS [WW23]

$\mathbf{A}$ uniform random

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

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

BASIS [WW23]

$\mathbf{A}$ uniform random $\qquad$ $\mathbf{A}_1, \cdots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \mathsf{Samp}(1^\lambda, \mathbf{A})$

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

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

$\mathsf{BASIS}_{\mathsf{rand}}$ [WW23]

$\mathbf{A}$ uniform random

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

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

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

$\mathbf{A}$ uniform random

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

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

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

$\mathsf{BASIS}_{\mathsf{rand}}$ [WW23]

$\mathbf{A}$ uniform random $\qquad\qquad$ $\mathbf{A}_1, \cdots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \mathsf{Samp}(1^\lambda, \mathbf{A})$

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

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

BASIS$_{\mathsf{struct}}$ [WW23]

$\mathbf{A}$ uniform random $\qquad\qquad$ $\mathbf{A}_1, \cdots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \mathsf{Samp}(1^\lambda, \mathbf{A})$

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

BASIS$_{\text{struct}}$ [WW23]

$\mathbf{A}$ uniform random

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

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

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

$\mathsf{BASIS}_{\mathsf{struct}}$ [WW23]

$\mathbf{A}$ uniform random $\qquad\qquad$ $\mathbf{A}_1, \cdots, \mathbf{A}_\ell, \mathbf{R} \leftarrow \mathsf{Samp}(1^\lambda, \mathbf{A})$

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

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

$\mathsf{BASIS}_{\mathsf{struct}}$ [WW23]

$\mathbf{A}$ uniform random

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

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

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

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

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

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

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

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

$\mathsf{BASIS}_{\mathsf{rand}} \Rightarrow \mathsf{SIS}$ [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 $\mathbf{B}_\ell$

$\mathsf{BASIS}_{\mathsf{rand}} \Rightarrow \mathsf{SIS}$ [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 $\mathbf{B}_\ell$

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

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

$$\left[\begin{array}{ccc|c} \mathbf{A}_1 & & & -\mathbf{G} \\ & \mathbf{A}_2 & & -\mathbf{G} \\ & & \mathbf{A}_3 & -\mathbf{G} \end{array}\right] \overbrace{\begin{bmatrix} \mathbf{R}_1 & -\mathbf{R}_1 & \\ & & \\ & -\mathbf{R}_3 & \mathbf{R}_3 \\ & -\mathbf{I} & \end{bmatrix}}^{\mathbf{R}}$$

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

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

$$\left[\begin{array}{ccc|c} \mathbf{A}_1 & & & -\mathbf{G} \\ & \mathbf{A}_2 & & -\mathbf{G} \\ & & \mathbf{A}_3 & -\mathbf{G} \end{array}\right] \overbrace{\begin{bmatrix} \mathbf{R}_1 & -\mathbf{R}_1 & \\ & & \\ & -\mathbf{R}_3 & \mathbf{R}_3 \\ & -\mathbf{I} & \end{bmatrix}}^{\mathbf{R}} = \begin{bmatrix} \mathbf{G} & & \\ & \mathbf{G} & \\ & & \mathbf{G} \end{bmatrix}$$

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

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

$$\left[\begin{array}{ccc|c} \mathbf{A}_1 & & & -\mathbf{G} \\ & \mathbf{A}_2 & & -\mathbf{G} \\ & & \mathbf{A}_3 & -\mathbf{G} \end{array}\right] \overbrace{\begin{bmatrix} \mathbf{R}_1 & -\mathbf{R}_1 & \\ & & \\ & -\mathbf{R}_3 & \mathbf{R}_3 \\ & -\mathbf{I} & \end{bmatrix}}^{\mathbf{R}} = \mathbf{I}_3 \otimes \mathbf{G}$$

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

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

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

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

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

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

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

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

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

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

$$\boxed{\mathbf{A}_i} \cdot \boxed{\mathbf{u}_{i,j}} = \boxed{\mathbf{G}} \, \boxed{\mathbf{z}_j} \mod q$$

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

$$\left[\begin{array}{ccc|c} \mathbf{A}_1 & & & -\mathbf{G} \\ & \ddots & & \vdots \\ & & \mathbf{A}_\ell & -\mathbf{G} \end{array}\right] \begin{bmatrix} \mathbf{u}_{1,j} \\ \vdots \\ \mathbf{u}_{\ell,j} \\ \mathbf{z}_j \end{bmatrix} = \mathbf{0} \mod q$$

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

$$\left[\begin{array}{ccc|c} \mathbf{A}_1 & & & -\mathbf{G} \\ & \ddots & & \vdots \\ & & \mathbf{A}_\ell & -\mathbf{G} \end{array}\right] \begin{bmatrix} \mathbf{u}_{1,j} \\ \vdots \\ \mathbf{u}_{\ell,j} \\ \mathbf{z}_j \end{bmatrix} = \begin{bmatrix} \mathbf{0} \end{bmatrix} \mod q$$

heuristically linearly independent

$\Downarrow$

(Ajtai) trapdoor for $\mathbf{B}_\ell$

Open Problems

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

Open Problems

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

Open Problems

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

Open Problems

- How does security of $\mathsf{BASIS}_{\mathsf{struct}}$ / k-R-ISIS / vSIS degrade with ℓ or k?
- Reductions for $\mathsf{BASIS}_{\mathsf{struct}}$ / k-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]

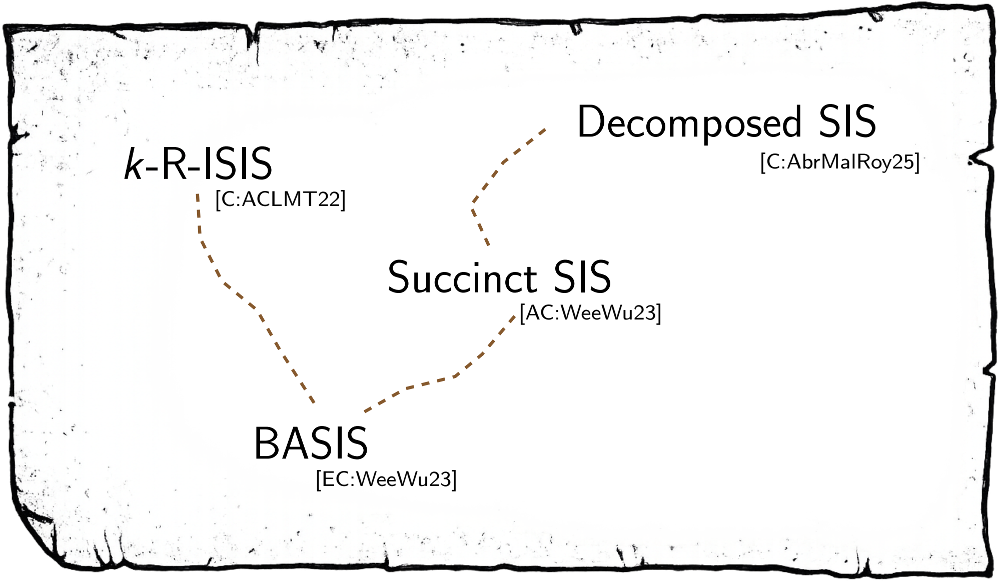
BASIS

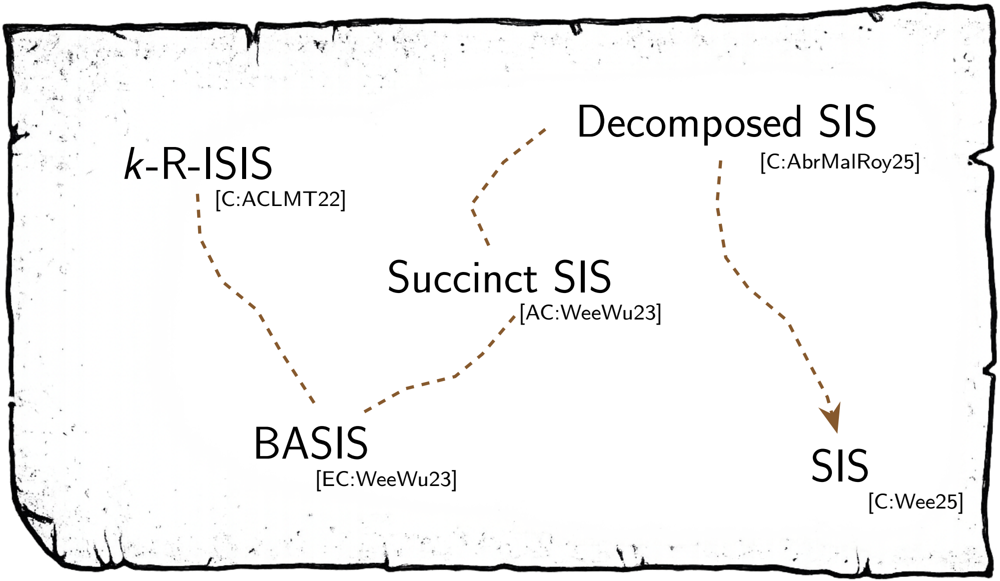
[EC:WeeWu23]

k-R-ISIS
[C:ACLMT22]

Succinct SIS
[AC:WeeWu23]

BASIS
[EC:WeeWu23]


Decomposed SIS
[C:AbrMalRoy25]
k-R-ISIS
[C:ACLMT22]
Succinct SIS
[AC:WeeWu23]
BASIS
[EC:WeeWu23]


Decomposed SIS
[C:AbrMalRoy25]
k-R-ISIS
[C:ACLMT22]
Succinct SIS
[AC:WeeWu23]
BASIS
[EC:WeeWu23]
SIS
[C:Wee25]

Open Problems

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

Thank you!