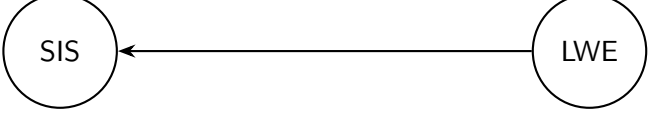
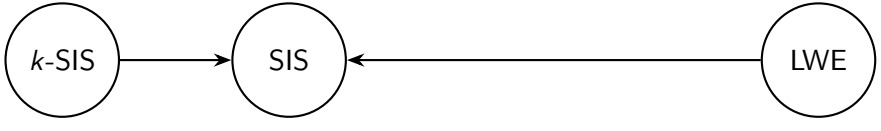
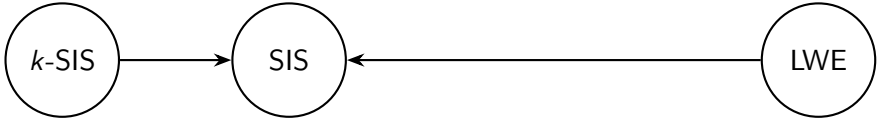
Tight Reductions for SIS-with-Hints Assumptions with Applications to Anonymous Credentials

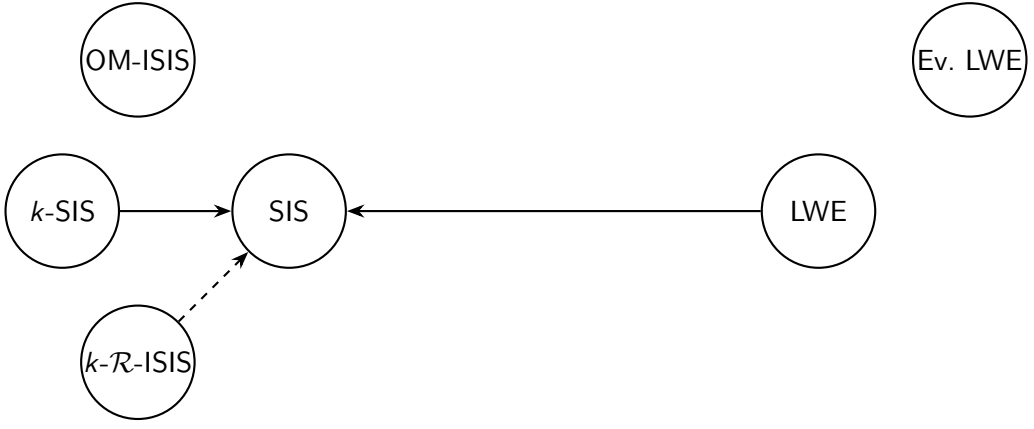
Ngoc Khanh Nguyen and Jan Niklas Siemer
King's College London
May 26, 2026

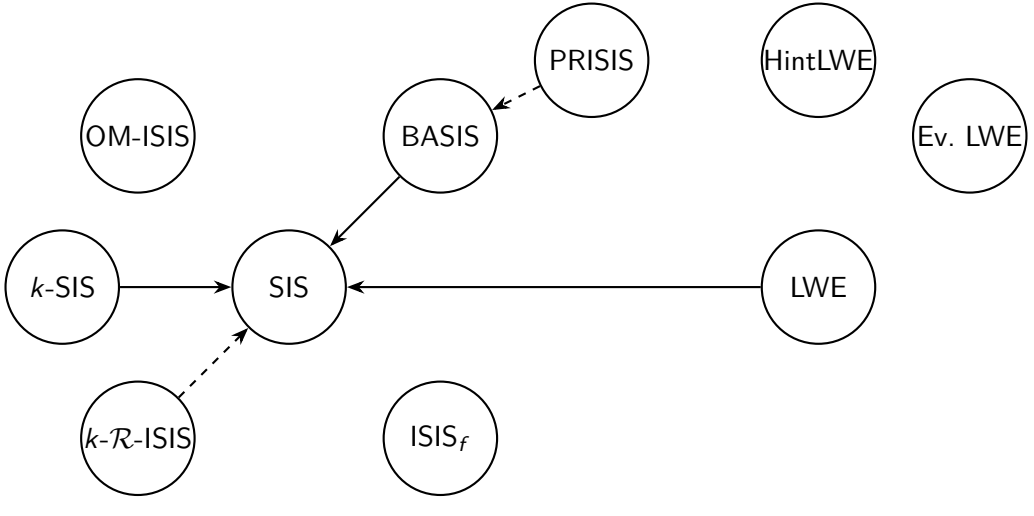

SIS

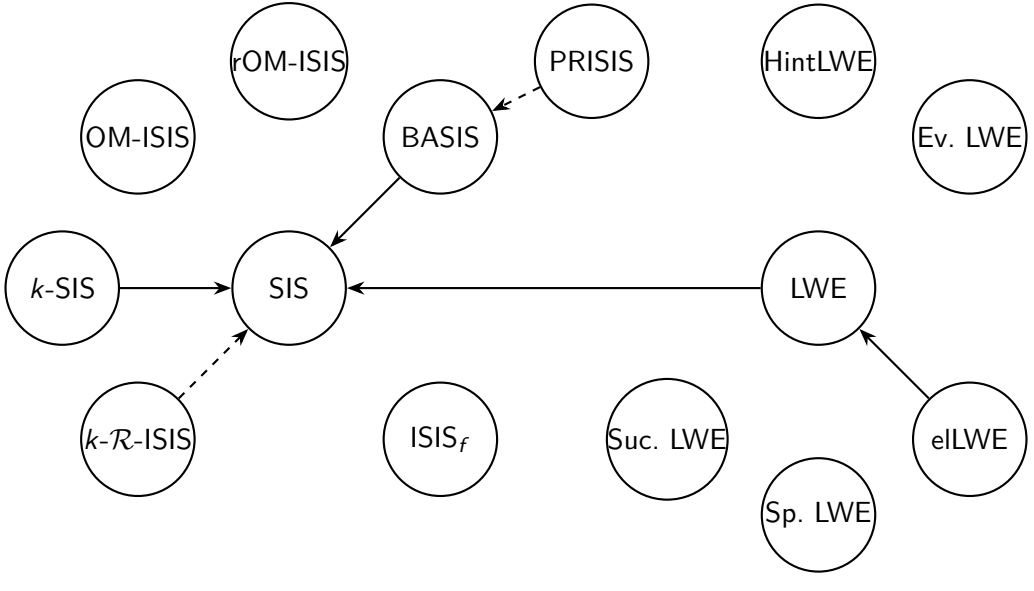

SIS
LWE


k-SIS
SIS
LWE

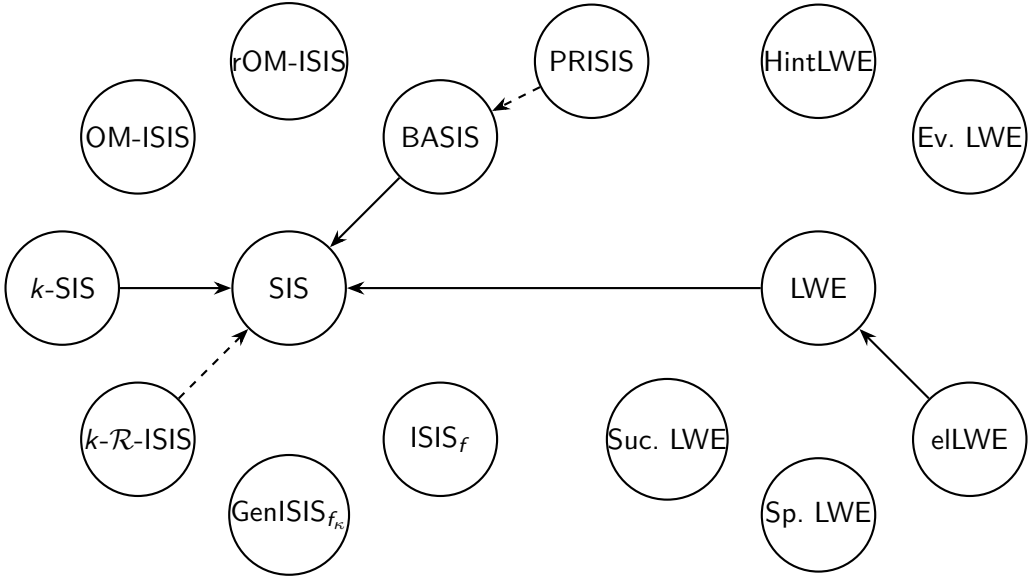

k-SIS
SIS
LWE


OM-ISIS
Ev. LWE
k-SIS
SIS
LWE
k-$\mathcal{R}$-ISIS


PRISIS
HintLWE
OM-ISIS
BASIS
Ev. LWE
k-SIS
SIS
LWE
k-$\mathcal{R}$-ISIS
ISIS$_f$


rOM-ISIS
PRISIS
HintLWE
OM-ISIS
BASIS
Ev. LWE
k-SIS
SIS
LWE
k-$\mathcal{R}$-ISIS
ISIS_f
Suc. LWE
elLWE
Sp. LWE

Lattice-Based Cryptographic Assumptions - 2025

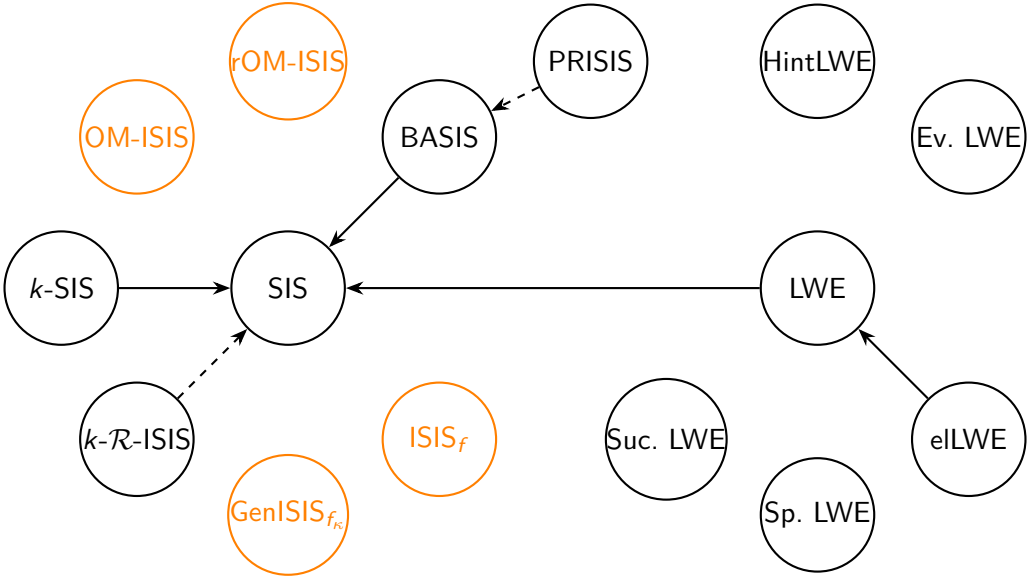


Takeaway

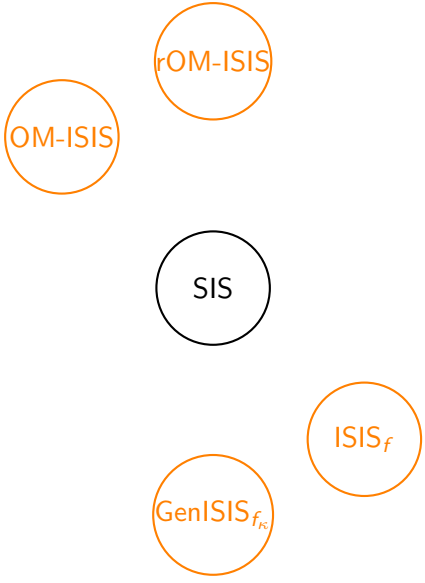
- It's time for a structured, community-driven wiki for lattice-based assumptions and their relations
  - Wiki for assumptions: `https://LatticeAssumptionZoo.org`

Takeaway

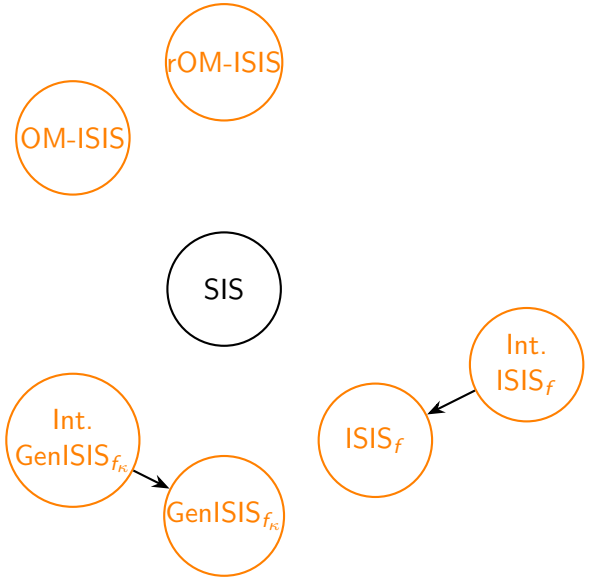
- It's time for a structured, community-driven wiki for lattice-based assumptions and their relations
  - Wiki for assumptions: `https://LatticeAssumptionZoo.org`
- Deepen insights on relations between novel assumptions
  - Reliable security analysis by reducing standard assumptions to new assumptions where possible

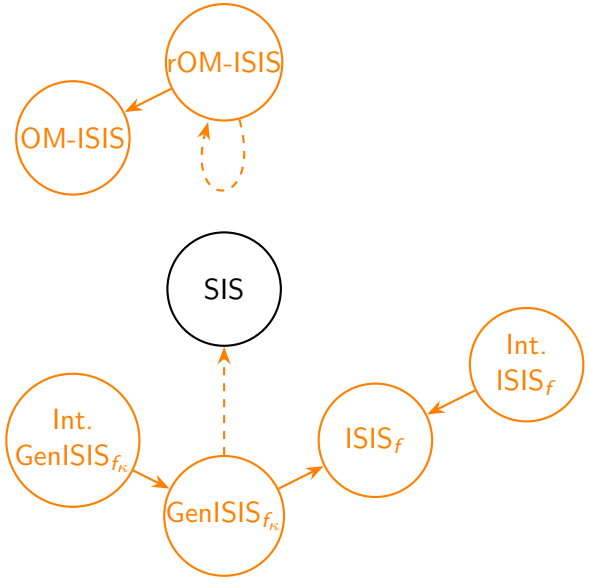

rOM-ISIS
PRISIS
HintLWE
OM-ISIS
BASIS
Ev. LWE
k-SIS
SIS
LWE
k-$\mathcal{R}$-ISIS
ISIS_f
Suc. LWE
elLWE
$\mathrm{GenISIS}_{f_\kappa}$
Sp. LWE

Idea of this Paper



Idea of this Paper




rOM-ISIS
OM-ISIS
SIS
Int.
ISIS$_f$
Int.
GenISIS$_{f_\kappa}$
ISIS$_f$
GenISIS$_{f_\kappa}$

ISIS$_f$ Assumptions

- Construction-friendly assumption
  - Problem definition resembles signature
  - Any instance generically provides strongly unforgeable signature, group signature, blind signature, and anonymous credentials system
- Synergy of interactive and non-interactive version
  - Security of constructions relies on interactive version
  - Hardness of non-interactive version easier to analyze
  - Interactive version provably at least as hard as non-interactive version

Experiment($\mathcal{A}$):

- $\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n \times m}$
- Sample k hints $(x_i, \mathbf{s}_i)$ with $x_i \leftarrow\$ [N], \mathbf{s}_i \leftarrow\$ D_{\mathbb{Z}^m, s}$ conditioned on

$$\mathbf{A} \cdot \mathbf{s}_i = f(x_i).$$

- $(x^*, \mathbf{s}^*) \leftarrow \mathcal{A}\left(\mathbf{A}, \{(x_i, \mathbf{s}_i)\}_{i \in [k]}\right)$
- $\mathcal{A}$ wins if $(x^*, \mathbf{s}^*) \notin \{(x_i, \mathbf{s}_i)\}_{i \in [k]}$ and

$$\mathbf{A} \cdot \mathbf{s}^* = f(x^*) \wedge \|\mathbf{s}^*\| \leq \beta$$

Experiment($\mathcal{A}$):

- $\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n\times m}$
- $\mathbf{C} \leftarrow\!\$\ \mathbb{Z}_q^{n\times \ell}$
- $\mathcal{H} = \emptyset$
- $(x^*, \mathbf{s}^*, \mathbf{m}^*) \leftarrow \mathcal{A}^{O_{\mathsf{pre}}}(\mathbf{A}, \mathbf{C})$
- $\mathcal{A}$ wins if $(x^*, \mathbf{s}^*, \mathbf{m}^*) \notin \mathcal{H}$ and

$$\mathbf{A}\cdot\mathbf{s}^* = f(x^*) + \mathbf{C}\cdot\mathbf{m}^*$$

and $\|\mathbf{s}^*\| \le \beta_s \wedge \|\mathbf{m}^*\| \le \beta_m$

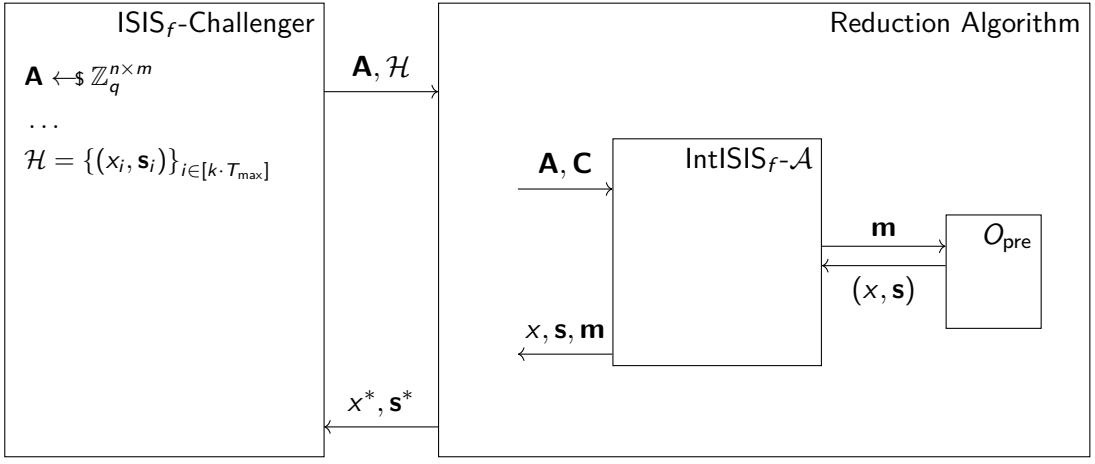
$O_{\mathsf{pre}}(\mathbf{m} \in \mathbb{Z}^\ell)$:

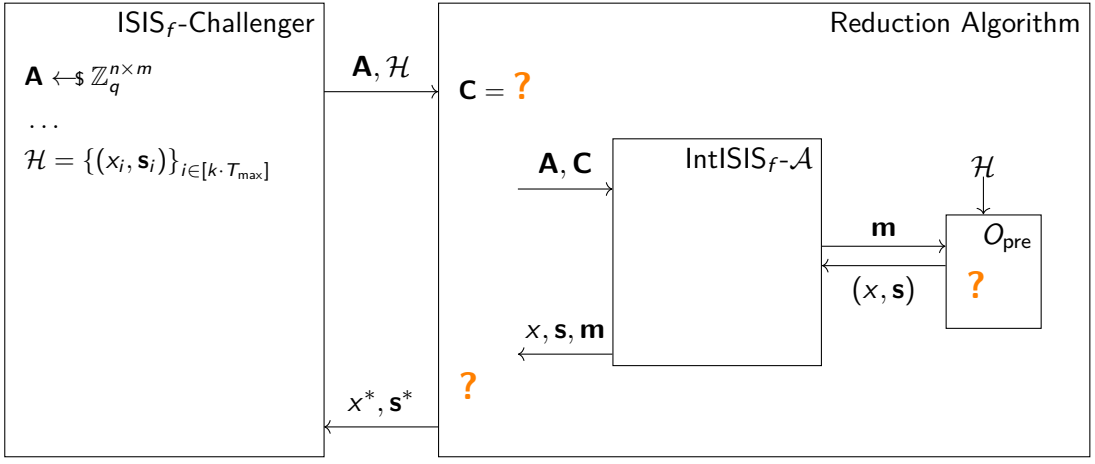
- assert $\|\mathbf{m}\| \le \beta_m$
- Sample $(x_i, \mathbf{s}_i)$ with $x_i \leftarrow\!\$\ [N]$, $\mathbf{s}_i \leftarrow\!\$\ D_{\mathbb{Z}^m, s}$ conditioned on $\mathbf{A}\cdot\mathbf{s}_i = f(x_i) + \mathbf{C}\cdot\mathbf{m}$.
- $\mathcal{H} \leftarrow \mathcal{H} \cup \{(x, \mathbf{s}, \mathbf{m})\}$
- **return** $(x, \mathbf{s})$

Optimised Reduction between ISIS$_f$ Assumptions

Theorem

Any interactive $ISIS_f$ assumption allowing at most k queries is at least as hard as $ISIS_f$ handing out at least $k \cdot T_{\max}$ hints.


ISIS$_f$-Challenger
$\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n \times m}$
$\ldots$
$\mathcal{H} = \{(x_i, \mathbf{s}_i)\}_{i \in [k \cdot T_{\max}]}$
$\mathbf{A}, \mathcal{H}$
$x^*, \mathbf{s}^*$
Reduction Algorithm
$\mathbf{A}, \mathbf{C}$
IntISIS$_f$-$\mathcal{A}$
$x, \mathbf{s}, \mathbf{m}$
$\mathbf{m}$
$(x, \mathbf{s})$
O_{pre}


ISIS$_f$-Challenger
$\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n \times m}$
...
$\mathcal{H} = \{(x_i, \mathbf{s}_i)\}_{i \in [k \cdot T_{\max}]}$
$\mathbf{A}, \mathcal{H}$
$x^*, \mathbf{s}^*$
Reduction Algorithm
$\mathbf{C} = ?$
$\mathbf{A}, \mathbf{C}$
IntISIS$_f$-$\mathcal{A}$
$x, \mathbf{s}, \mathbf{m}$
?
$\mathbf{m}$
$(x, \mathbf{s})$
$\mathcal{H}$
O_{pre}
?

Given ISIS_f hints

- $(x_i, \mathbf{s}_i)$ s.t.
  - $x_i \leftarrow\$ [N]$
  - $\mathbf{s}_i \leftarrow\$ D_{\mathbb{Z}^m, s}$
  - conditioned on $\mathbf{A} \cdot \mathbf{s}_i = f(x_i)$.

Required return values by $\mathsf{O}_{\mathsf{pre}}(\mathbf{m} \in \mathbb{Z}^\ell)$

- $(x_i, \mathbf{s}_i)$ s.t.
  - $x_i \leftarrow\$ [N]$
  - $\mathbf{s}_i \leftarrow\$ D_{\mathbb{Z}^m, s}$
  - conditioned on $\mathbf{A} \cdot \mathbf{s}_i = f(x_i) + \mathbf{C} \cdot \mathbf{m}$.

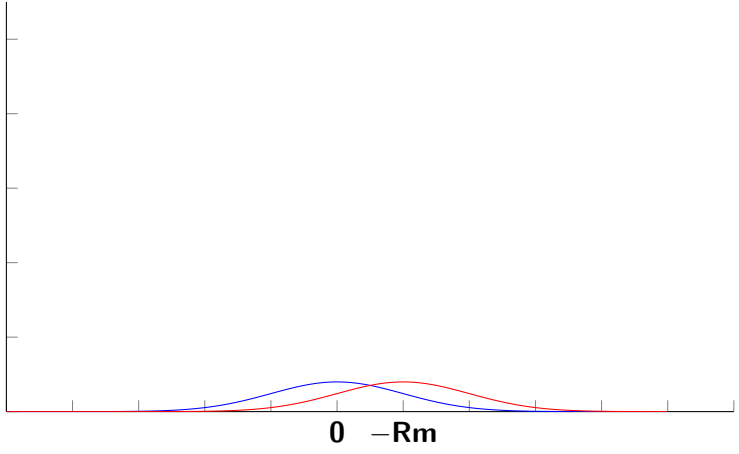
Given ISIS_f hints

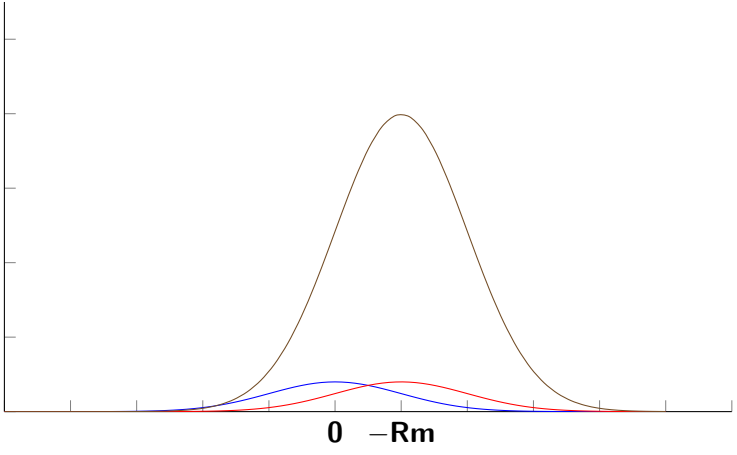
- $(x_i, \mathbf{s}_i)$ s.t.
  - $x_i \leftarrow\!\!\$\ [N]$
  - $\mathbf{s}_i \leftarrow\!\!\$\ D_{\mathbb{Z}^m, s}$
  - conditioned on $\mathbf{A} \cdot \mathbf{s}_i = f(x_i)$.

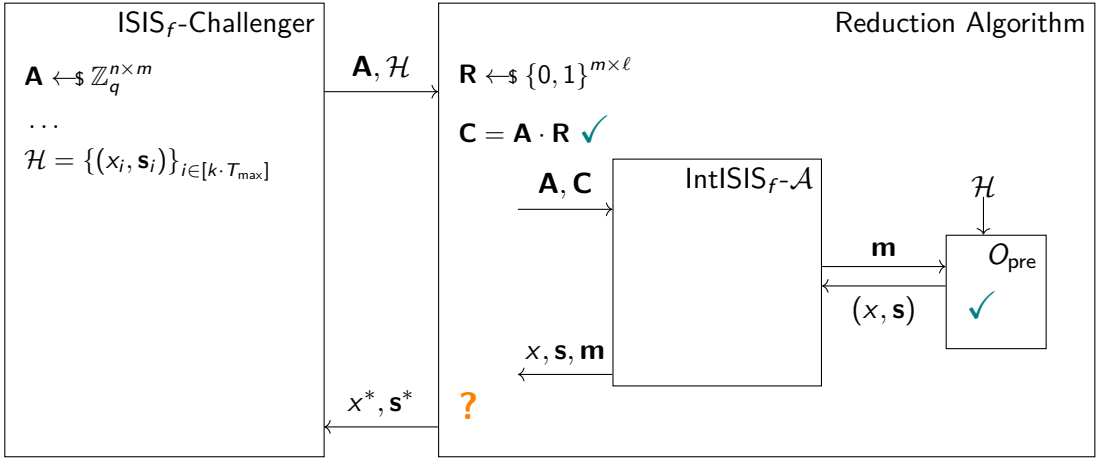
- Sample $\mathbf{R} \leftarrow\!\!\$\ \{0,1\}^{m \times \ell}$
- Set $\mathbf{C} = \mathbf{A} \cdot \mathbf{R}$
- Return $(x_i, \mathbf{s}_i - \mathbf{R} \cdot \mathbf{m})$

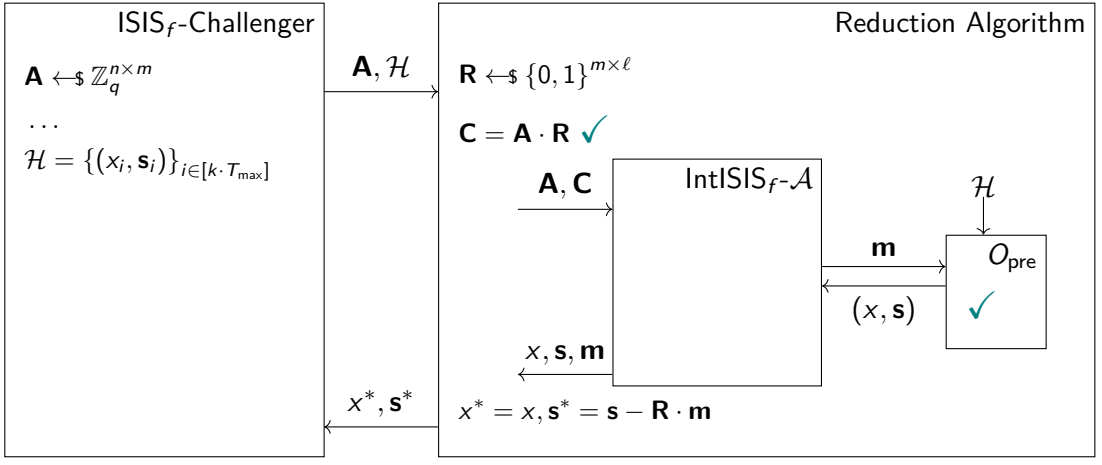
Required return values by $\mathsf{O}_{\mathsf{pre}}(\mathbf{m} \in \mathbb{Z}^\ell)$

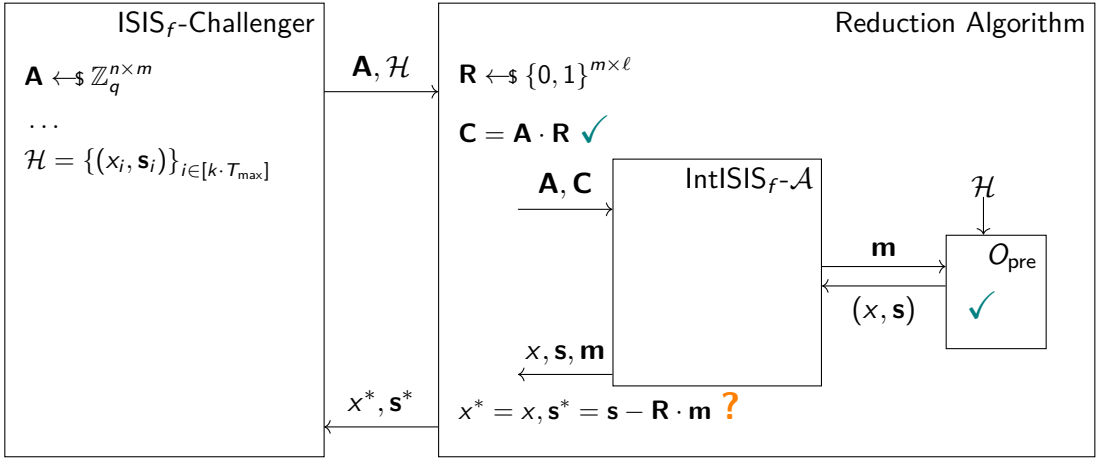
- $(x_i, \mathbf{s}_i)$ s.t.
  - $x_i \leftarrow\!\!\$\ [N]$
  - $\mathbf{s}_i \leftarrow\!\!\$\ D_{\mathbb{Z}^m, s}$
  - conditioned on $\mathbf{A} \cdot \mathbf{s}_i = f(x_i) + \mathbf{C} \cdot \mathbf{m}$.


0
−Rm


0
−Rm


ISIS$_f$-Challenger
$\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$
$\dots$
$\mathcal{H} = \{(x_i, \mathbf{s}_i)\}_{i\in[k\cdot T_{\max}]}$
$\mathbf{A}, \mathcal{H}$
$x^*, \mathbf{s}^*$
Reduction Algorithm
$\mathbf{R} \leftarrow\$ \{0,1\}^{m\times \ell}$
$\mathbf{C} = \mathbf{A}\cdot\mathbf{R}$ ✓
?
$\mathbf{A}, \mathbf{C}$
IntISIS$_f$-$\mathcal{A}$
$x, \mathbf{s}, \mathbf{m}$
$\mathbf{m}$
$(x, \mathbf{s})$
$\mathcal{H}$
O_{pre}
✓


ISIS$_f$-Challenger
$\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$
$\dots$
$\mathcal{H} = \{(x_i, \mathbf{s}_i)\}_{i\in[k\cdot T_{\max}]}$
$\mathbf{A}, \mathcal{H}$
$x^*, \mathbf{s}^*$
Reduction Algorithm
$\mathbf{R} \leftarrow\$ \{0,1\}^{m\times \ell}$
$\mathbf{C} = \mathbf{A}\cdot\mathbf{R}$ ✓
$\mathbf{A}, \mathbf{C}$
IntISIS$_f$-$\mathcal{A}$
$x, \mathbf{s}, \mathbf{m}$
$\mathbf{m}$
$(x, \mathbf{s})$
$\mathcal{H}$
O_{pre}
✓
$x^* = x, \mathbf{s}^* = \mathbf{s} - \mathbf{R}\cdot\mathbf{m}$


ISIS$_f$-Challenger
$\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$
$\cdots$
$\mathcal{H} = \{(x_i, \mathbf{s}_i)\}_{i\in[k\cdot T_{\max}]}$
$\mathbf{A}, \mathcal{H}$
$x^*, \mathbf{s}^*$
Reduction Algorithm
$\mathbf{R} \leftarrow\$ \{0,1\}^{m\times \ell}$
$\mathbf{C} = \mathbf{A}\cdot\mathbf{R}$ ✓
$\mathbf{A}, \mathbf{C}$
IntISIS$_f$-$\mathcal{A}$
$\mathcal{H}$
$\mathbf{m}$
O_{pre}
$(x, \mathbf{s})$
✓
$x, \mathbf{s}, \mathbf{m}$
$x^* = x, \mathbf{s}^* = \mathbf{s} - \mathbf{R}\cdot\mathbf{m}$?

Assume there is a collision with some hint, i.e. $(x, \mathbf{s} - \mathbf{R} \cdot \mathbf{m}) = (x_i, \mathbf{s}_i)$.

- For this talk, assume $\mathbf{m} \neq \mathbf{0} \Rightarrow \exists j \in [\ell] : m_j \neq 0$.

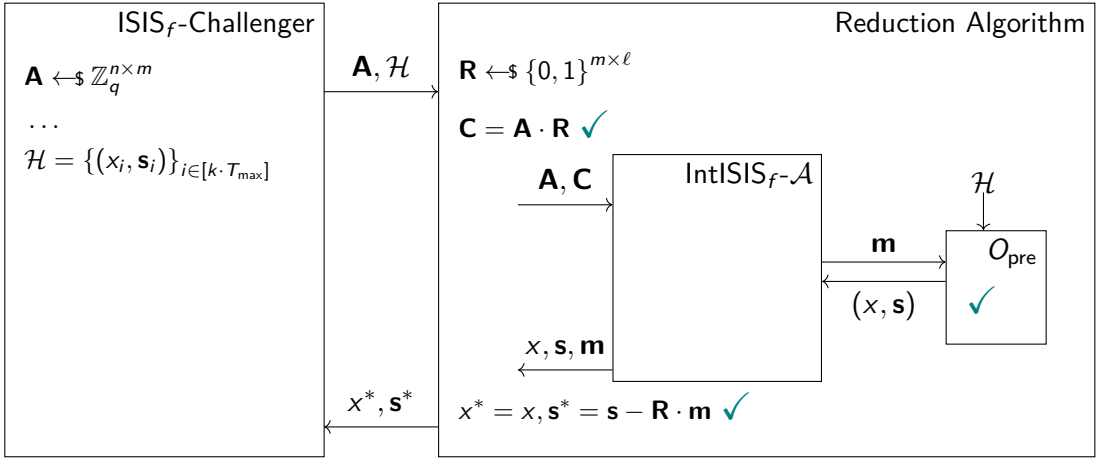
Assume there is a collision with some hint, i.e. $(x, \mathbf{s} - \mathbf{R} \cdot \mathbf{m}) = (x_i, \mathbf{s}_i)$.

- For this talk, assume $\mathbf{m} \neq \mathbf{0} \Rightarrow \exists j \in [\ell] : m_j \neq 0$.
- Assume $\exists \mathbf{r}_j \neq \mathbf{r}'_j : \mathbf{A} \cdot \mathbf{r}_j = \mathbf{A} \cdot \mathbf{r}'_j = \mathbf{c}_j \Rightarrow \mathbf{r}_j \cdot m_j \neq \mathbf{r}'_j \cdot m_j$
- Let $\mathbf{R}' = \mathbf{R}$ except column $\mathbf{r}_j \neq \mathbf{r}'_j \Rightarrow \mathbf{R} \cdot \mathbf{m} \neq \mathbf{R}' \cdot \mathbf{m} \Rightarrow \mathbf{s} - \mathbf{R}' \cdot \mathbf{m} \neq \mathbf{s}_i$

Assume there is a collision with some hint, i.e. $(x, \mathbf{s} - \mathbf{R} \cdot \mathbf{m}) = (x_i, \mathbf{s}_i)$.

- For this talk, assume $\mathbf{m} \neq \mathbf{0} \Rightarrow \exists j \in [\ell] : m_j \neq 0$.
- Assume $\exists \mathbf{r}_j \neq \mathbf{r}'_j : \mathbf{A} \cdot \mathbf{r}_j = \mathbf{A} \cdot \mathbf{r}'_j = \mathbf{c}_j \Rightarrow \mathbf{r}_j \cdot m_j \neq \mathbf{r}'_j \cdot m_j$
- Let $\mathbf{R}' = \mathbf{R}$ except column $\mathbf{r}_j \neq \mathbf{r}'_j \Rightarrow \mathbf{R} \cdot \mathbf{m} \neq \mathbf{R}' \cdot \mathbf{m} \Rightarrow \mathbf{s} - \mathbf{R}' \cdot \mathbf{m} \neq \mathbf{s}_i$
- W.h.p., there are at least two choices for each column of $\mathbf{R}$ s.t. $\mathbf{C} = \mathbf{A} \cdot \mathbf{R}$.
- $\mathbf{R}$ chosen uniformly and $\mathbf{R}$ hidden from $\mathcal{A}$ (by statistical arguments)
  $\Rightarrow$ probability to output a colliding element at most $\frac{1}{2}$

□


ISIS$_f$-Challenger
$\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m}$
$\dots$
$\mathcal{H} = \{(x_i, \mathbf{s}_i)\}_{i\in[k\cdot T_{\max}]}$
$\mathbf{A}, \mathcal{H}$
$x^*, \mathbf{s}^*$
Reduction Algorithm
$\mathbf{R} \leftarrow\$ \{0,1\}^{m\times \ell}$
$\mathbf{C} = \mathbf{A}\cdot\mathbf{R}$ ✓
$\mathbf{A}, \mathbf{C}$
IntISIS$_f$-$\mathcal{A}$
$x, \mathbf{s}, \mathbf{m}$
$\mathbf{m}$
$(x, \mathbf{s})$
$\mathcal{H}$
O_{pre}
✓
$x^* = x, \mathbf{s}^* = \mathbf{s} - \mathbf{R}\cdot\mathbf{m}$ ✓

Theorem

Any interactive ISIS$_f$ assumption allowing at most k queries is at least as hard as ISIS$_f$ handing out at least $k \cdot T_{\max}$ hints.

- Restructuring of original reduction and change of few game hops leads to optimised result
- Reduction naturally extends to Generalised ISIS$_{f_\kappa}$
- Tight reduction removes loss-factor of $\frac{1}{k}$
  - Security can directly rely on non-interactive assumption
  - Removes 4X efficiency loss of anonymous credential system implemented in LaZeR [LSS24] based on ISIS$_f$

Attributes	**ISIS$_f$**	**IntISIS$_f$**
8	122 KB	26 KB
16	133 KB	29 KB

Table: Output sizes for the anonymous credential schemes with 8 and 16 attributes. [BLNS23]

Theorem

Any interactive ISIS$_f$ assumption allowing at most k queries is at least as hard as ISIS$_f$ handing out at least $k \cdot T_{\max}$ hints.

- Restructuring of original reduction and change of few game hops leads to optimised result
- Reduction naturally extends to Generalised ISIS$_{f_\kappa}$
- Tight reduction removes loss-factor of $\frac{1}{k}$
  - Security can directly rely on non-interactive assumption
  - Removes 4X efficiency loss of anonymous credential system implemented in LaZeR [LSS24] based on ISIS$_f$

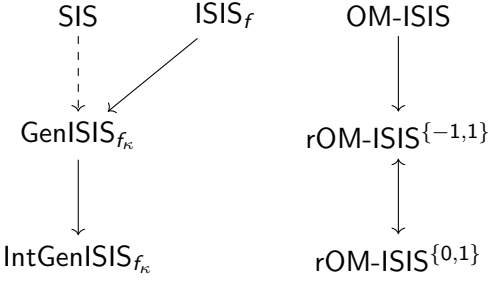
Attributes	**ISIS$_f$**	**IntISIS$_f$**
8	26 ~~122~~ KB	26 KB
16	29 ~~133~~ KB	29 KB

Table: Output sizes for the anonymous credential schemes with 8 and 16 attributes. [BLNS23]

Further Results

- First reduction from SIS to GenISIS$_{f_\kappa}$ for specific choice of f_κ in the standard model
  - ABB-style signature(s) can be embedded into the GenISIS$_{f_\kappa}$ framework
  - Suggests any lattice-based sEUF-SCMA signature can be reduced to GenISIS$_{f_\kappa}$
- Reduction from One-More-ISIS to Randomised One-More-ISIS

- First reduction from SIS to GenISIS$_{f_\kappa}$ for specific choice of f_κ in the standard model
  - ABB-style signature(s) can be embedded into the GenISIS$_{f_\kappa}$ framework
  - Suggests any lattice-based sEUF-SCMA signature can be reduced to GenISIS$_{f_\kappa}$
- Reduction from One-More-ISIS to Randomised One-More-ISIS



The Mission!

Contribute to the understanding of new lattice-based assumptions, their relations and provable connections.

Contribute to the understanding of new lattice-based assumptions, their relations and provable connections.

Keep Track of Lattice Assumptions

- Please check the Lattice Assumption Zoo before establishing a new, ad-hoc assumption.
  - Help reduce the number of assumptions to analyse
  - Increase awareness of your assumptions and work

Questions?

https://ia.cr/2026/291

https://LatticeAssumptionZoo.org

Main References


Shweta Agrawal, Elena Kirshanova, Damien Stehlé, and Anshu Yadav.
Practical, round-optimal lattice-based blind signatures.
In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 39–53, 2022.


Foteini Baldimtsi, Jiaqi Cheng, Rishab Goyal, and Aayush Yadav.
Non-interactive blind signatures: Post-quantum and stronger security.
In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 70–104. Springer, 2025.


Jonathan Bootle, Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Alessandro Sorniotti.
A framework for practical anonymous credentials from lattices.
In *Annual International Cryptology Conference*, pages 384–417. Springer, 2023.

Main References


Adrien Dubois, Michael Klooß, Russell WF Lai, and Ivy KY Woo.
Lattice-based proof-friendly signatures from vanishing short integer solutions.
In *IACR International Conference on Public-Key Cryptography*, pages 452–486. Springer, 2025.


Vadim Lyubashevsky, Gregor Seiler, and Patrick Steuer.
The lazer library: Lattice-based zero knowledge and succinct proofs for quantum-safe privacy.
In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, pages 3125–3137, 2024.


Daniele Micciancio and Chris Peikert.
Trapdoors for lattices: Simpler, tighter, faster, smaller.
In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 700–718. Springer, 2012.