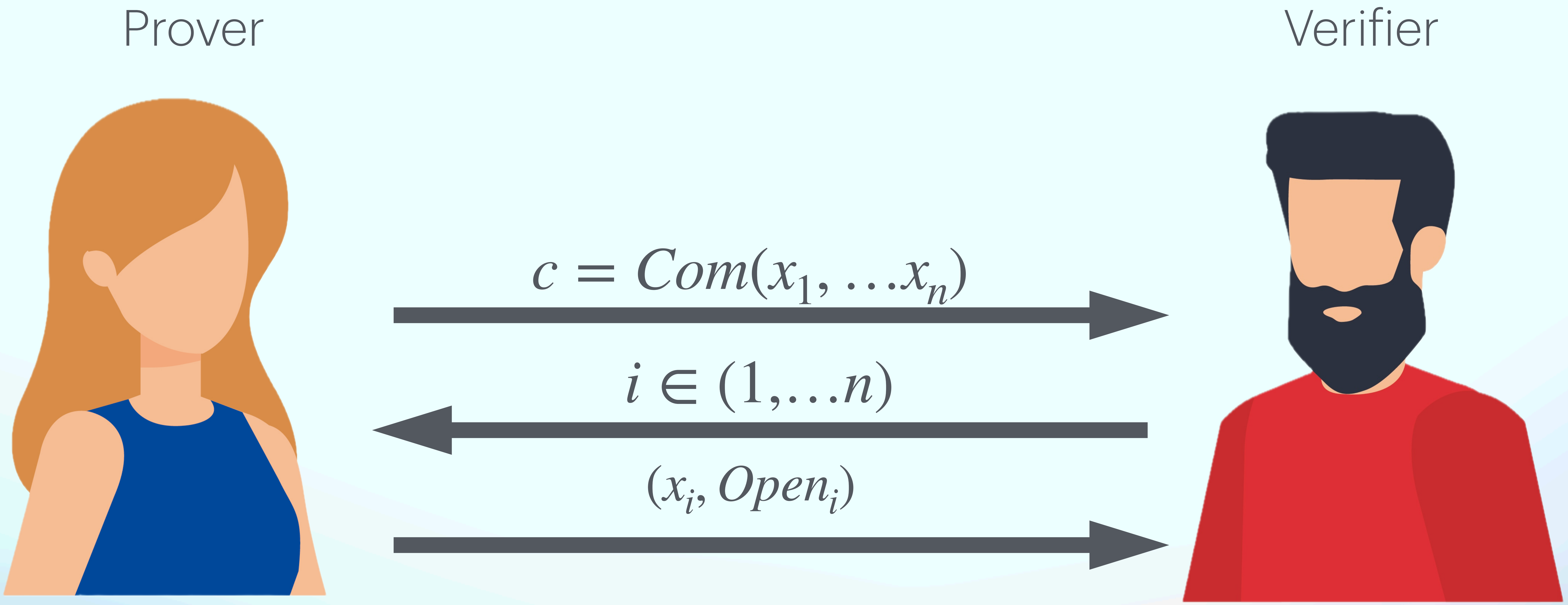
SLAP: Succinct Lattice-Based Polynomial Commitments from Standard Assumptions.

Joint work with *Martin Albrecht, Giacomo Fenzi and Khanh Nguyen [EC24]*

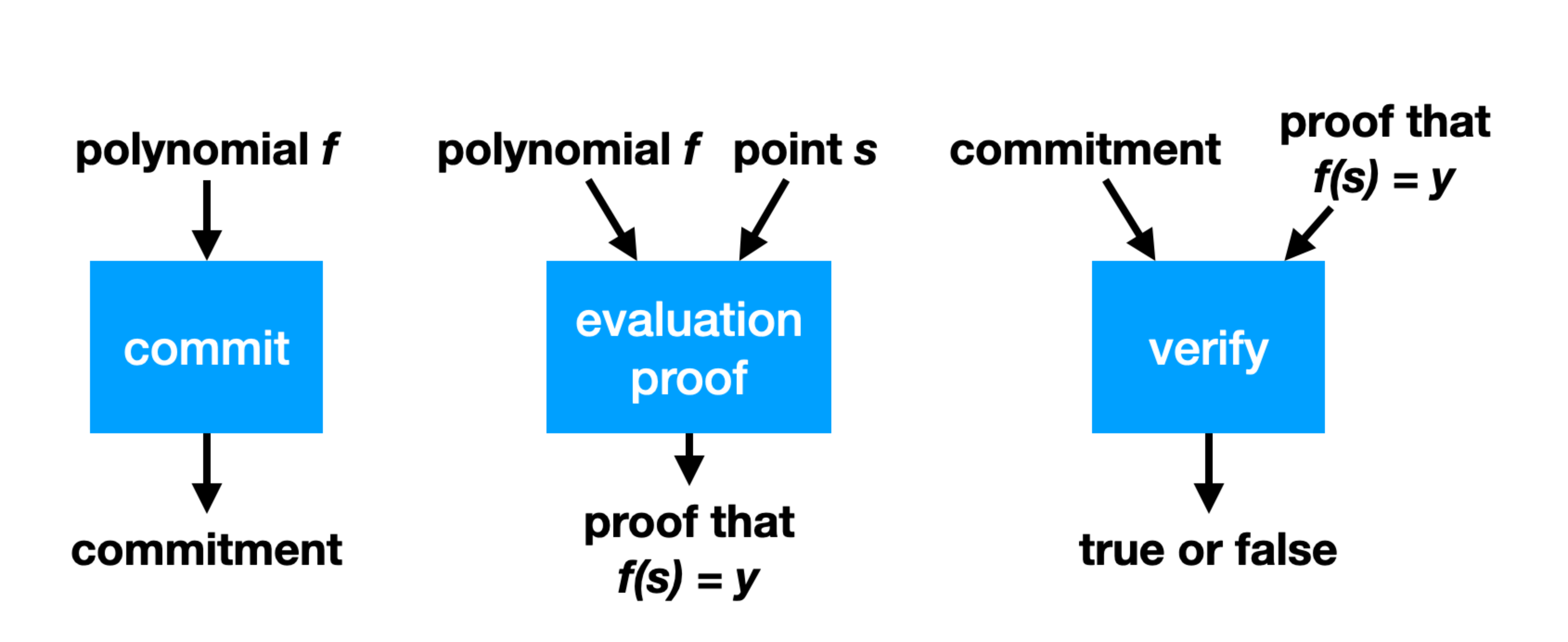
Sasha Lapiha. Royal Holloway, University of London

Vector commitments.



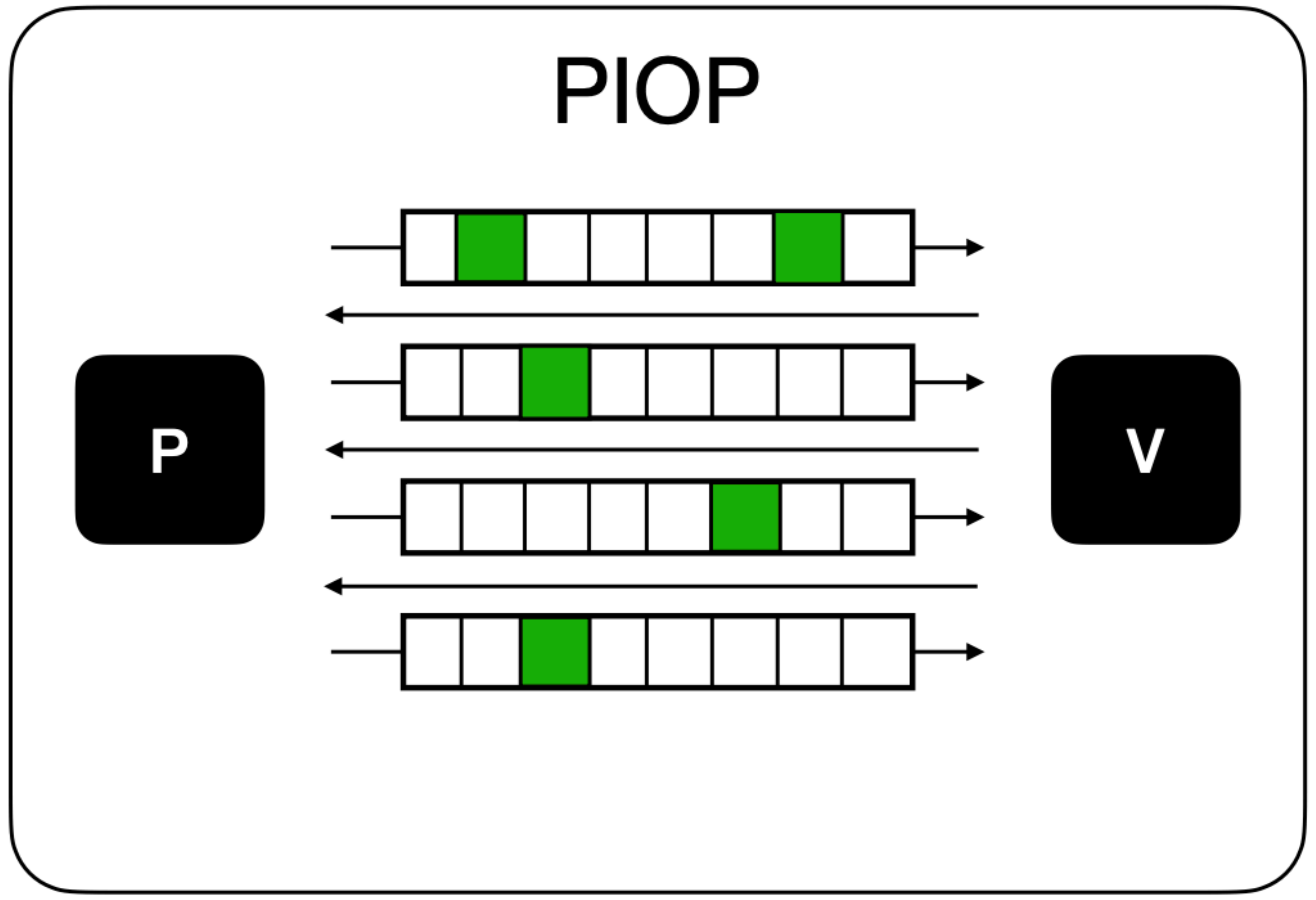
$$Verify(c,\ x_i, Open_i\ ) = 1$$

Polynomial commitments.

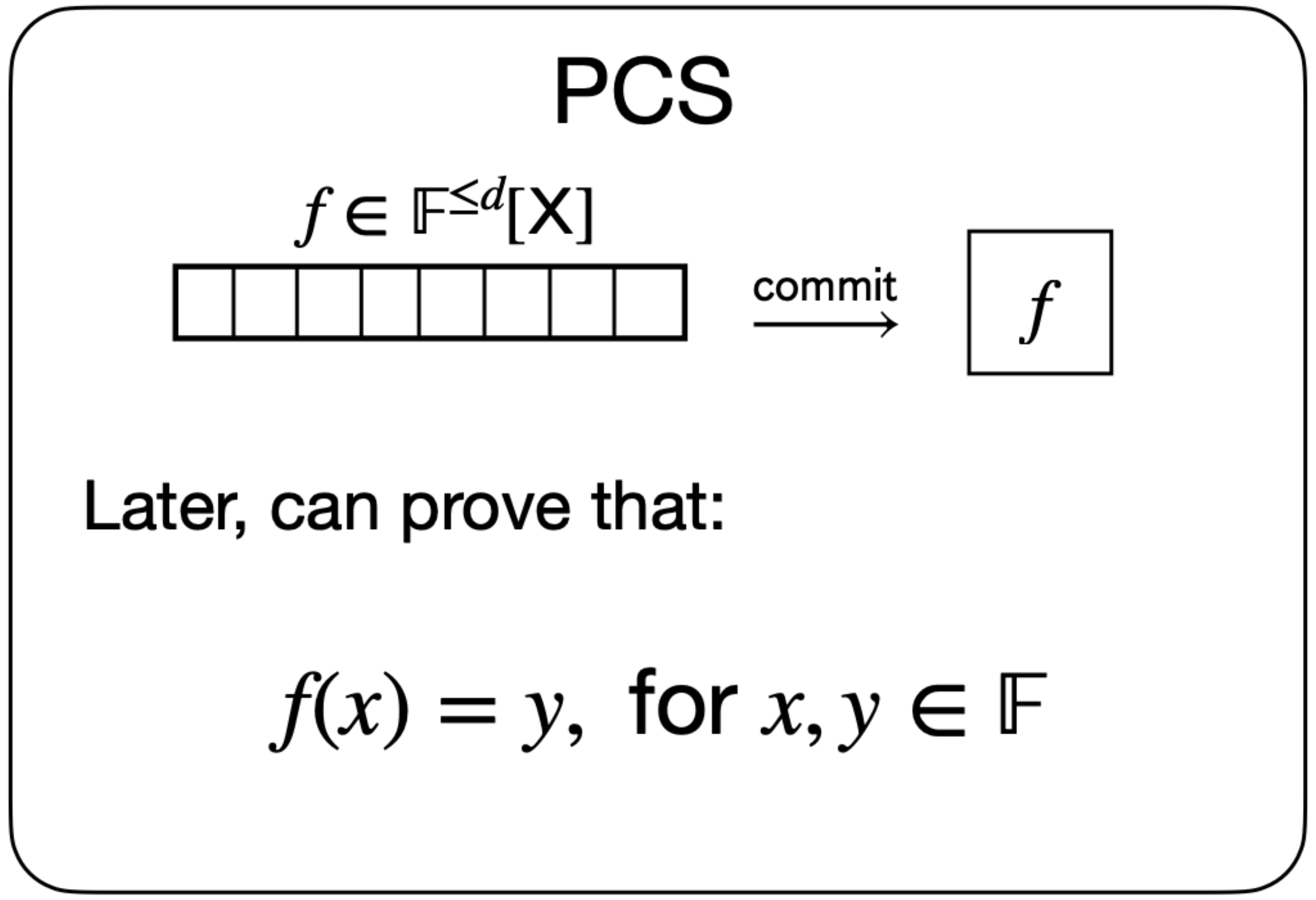


Source: Cryptography Documentation of the Mina blockchain.

Building SNARKS



+
FS



- Oracles are polynomials
- Security is information-theoretical
- Proof length is $\Omega(n)$ (not succinct)
- Verifiers are very efficient

- Cryptography goes here!
- Computational security
- We can achieve succinctness

*The slide courtesy to Giacomo.

Hard Problems.

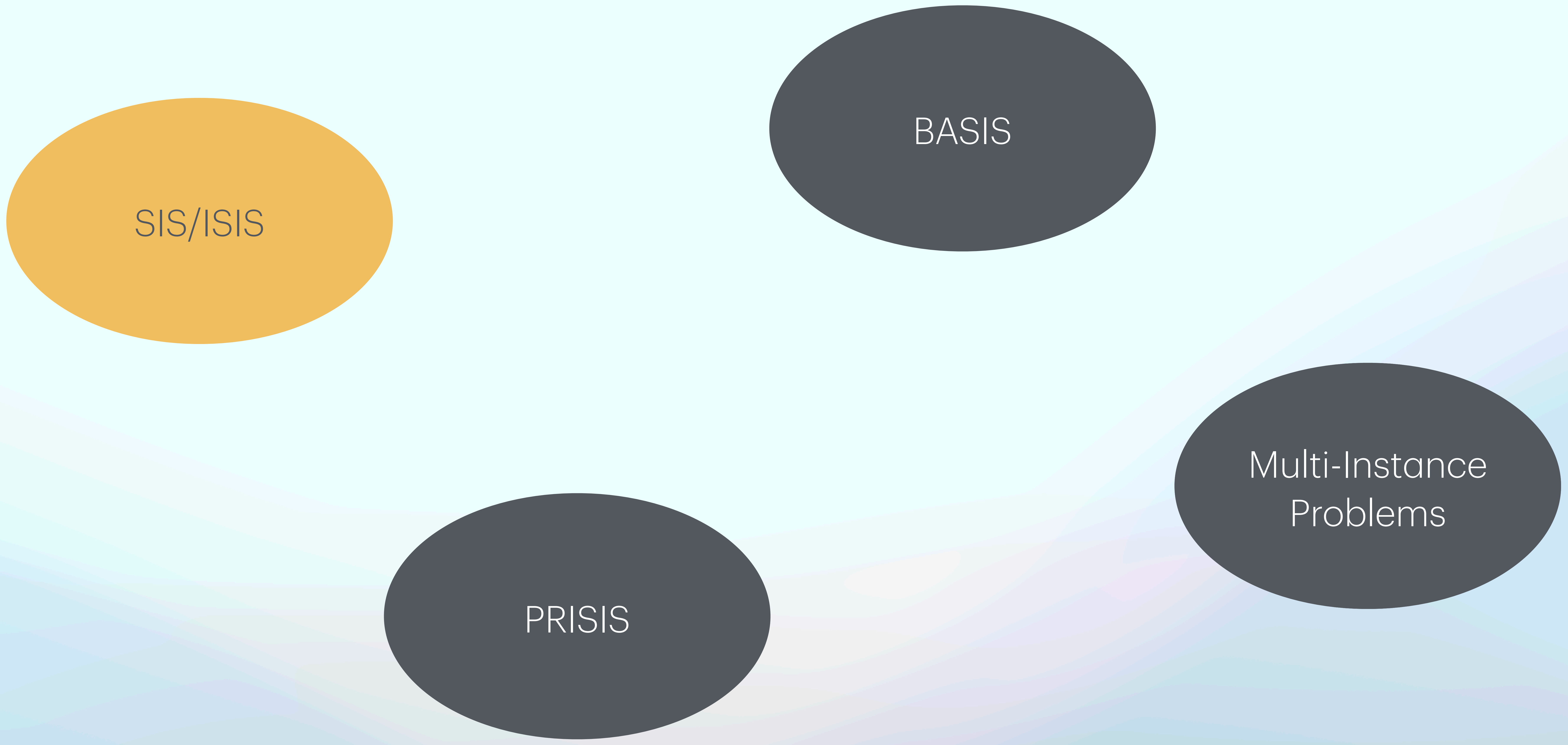
BASIS

SIS/ISIS

Multi-Instance Problems

PRISIS

Hard Problems.



Short Integer Solution (SIS).

- **Given** a matrix $A \leftarrow \mathcal{U}(\mathbb{Z}_q^{n \times m})$, m >> n.
- **Find** $x \in \mathbb{Z}^m$ s.t. $A \cdot x = 0 \bmod q$ and $|x|_2 < \beta$

Inhomogeneous SIS (ISIS): for a given $t \in \mathbb{Z}_q^n$ find $x \in \mathbb{Z}^m$ s.t. $A \cdot x = t \bmod q$ and $|x|_2 < \beta$

SIS Trapdoors.

Solving SIS is equivalent to finding a short vector in

$$\Lambda_q^{\perp}(A) = \{x \in \mathbb{Z}^m : A \cdot x = 0 \bmod q\}$$

A trapdoor for a matrix $A \in \mathbb{Z}_q^{n \times m}$ is a full rank “short” matrix $T_A \in \mathbb{Z}^{m \times m}$ s.t.

$$A \cdot T_A = 0 \bmod q$$

For ISIS: Find any $A \cdot y = t \bmod q$. Using T_A find z in the kernel close to y. Output : $x = y - z$.

SIS Trapdoors.

Gadget matrix: $G_n = \begin{bmatrix} 1 & 2 & \dots & 2^k & & & & \\ & & & & \ddots & & & \\ & & & & & 1 & 2 & \dots & 2^k \end{bmatrix}$ where

$k = \lfloor \log_2 q \rfloor + 1$

Gadget Trapdoor: a "short" matrix $T_A \in \mathbb{Z}^{m \times nk}$ such that $A \cdot T_A = G_n \bmod q$

SIS Trapdoors.

Gadget matrix: $G_n = \begin{bmatrix} 1 & 2 & \dots & 2^k & & & & \\ & & & & \ddots & & & \\ & & & & & 1 & 2 & \dots & 2^k \end{bmatrix}$ where

$k = \lfloor \log_2 q \rfloor + 1$

Gadget Trapdoor: a "short" matrix $T_A \in \mathbb{Z}^{m \times nk}$ such that $A \cdot T_A = G_n \bmod q$

To solve ISIS: Let t_{bin} be *binary decomposition* of t. Output $x = T_A \cdot t_{bin}$.

Preimage Sampling: $SamplePre(\cdot)$ generates "well distributed" preimages for A

$$\{x \leftarrow SamplePre(A, T_A, t, \sigma)\} \approx \{x \leftarrow \mathcal{D}_{\Lambda_q^t(A),\sigma}\}$$

Notations.

- $(u \,|\, v)$ or $(A \,|\, B)$ means stacking horisontally.
- $(u \,||\, v) = (u^T \,|\, v^T)^T$ or $(A \,||\, B)$ means stacking vertically.

Hard Problems.

SIS/ISIS

BASIS

PRISIS

Multi-Instance Problems

BASIS assumption [WW23].

Given: $A \in \mathbb{Z}_q^{n \times m}, W \in \mathbb{Z}_q^{n \times n}, T_B \in \mathbb{Z}^{3m \times 2m}, m = nk$ such that

$$\begin{bmatrix} A & & -G_n \\ & WA & -G_n \end{bmatrix} \cdot T_B = G_{2n} \bmod q$$

Compute: $x \in \mathbb{Z}^m : A \cdot x = 0 \bmod q$ such that $|x|_2 \leq \beta$

BASIS assumption [WW23].

Given: $A \in \mathbb{Z}_q^{n \times m}, W \in \mathbb{Z}_q^{n \times n}, T_B \in \mathbb{Z}^{3m \times 2m}, m = nk$ such that

$$\begin{bmatrix} A & & -G_n \\ & WA & -G_n \end{bmatrix} \cdot T_B = G_{2n} \bmod q$$

Compute: $x \in \mathbb{Z}^m : A \cdot x = 0 \bmod q$ such that $|x|_2 \leq \beta$

As hard as SIS when $B = \begin{bmatrix} A_1 & & -G_n \\ & A_2 & -G_n \end{bmatrix}$

BASIS assumption [WW23].

Given: $A \in \mathbb{Z}_q^{n \times m}, W \in \mathbb{Z}_q^{n \times n}, T_B \in \mathbb{Z}^{3m \times 2m}$ such that $\begin{bmatrix} A & & -G_n \\ & WA & -G_n \end{bmatrix} \cdot T_B = G_{2n} \bmod q$

Compute: $x \in \mathbb{Z}^m : A \cdot x = 0 \bmod q$ such that $|x|_2 \leq \beta$

Version with higher arity:

$$B = \begin{bmatrix} A & & & & -G_n \\ & W_1 A & & & -G_n \\ & & \ddots & & \\ & & & W_{\ell-1} A & -G_n \end{bmatrix}$$

and $B \cdot T_B = G_{\ell n} \bmod q$

BASIS vector commitment.

Trusted Setup: $(A, \{W_i\}_{i=1}^{\ell-1}, T_B)$ such that $B \cdot T_B = G_{\ell n} \bmod q$

Message: $(f_0, \ldots, f_{\ell-1}) \in \mathbb{Z}_q^{\ell}$ and vector $e_1^T = (1,0,\ldots,0) \in \mathbb{Z}^n$

BASIS vector commitment.

Trusted Setup: $(A, \{W_i\}_{i=1}^{\ell-1}, T_B)$ such that $B \cdot T_B = G_{\ell n} \bmod q$

Message: $(f_0, \ldots, f_{\ell-1}) \in \mathbb{Z}_q^{\ell}$ and vector $e_1^T = (1,0,\ldots,0) \in \mathbb{Z}^n$

Stack: $f_v = (-f_0 \cdot e_1 || \ldots || -f_{\ell-1} \cdot e_1)$ vertically

Run: $(s_0 || \ldots || s_{\ell-1} || \hat{t}) \leftarrow SamplePre(B, T_B, f_v, \sigma)$

The commitment is: $t = G \cdot \hat{t}$

BASIS verification.

$$\begin{bmatrix} A & & & & -G_n \\ & W_1 A & & & -G_n \\ & & \ddots & & \\ & & & W_{\ell-1} A & -G_n \end{bmatrix} \cdot \begin{bmatrix} s_0 \\ \vdots \\ s_{\ell-1} \\ \hat{t} \end{bmatrix} = \begin{bmatrix} -f_0 \cdot e_1 \\ \vdots \\ \vdots \\ -f_{\ell-1} \cdot e_1 \end{bmatrix} \bmod q$$

For the coordinate $i = 0, \ldots, \ell - 1$ we have:

$$W_i \cdot A \cdot s_i - G \cdot \hat{t} = -f_i \cdot e_1 \bmod q$$

Or: $W_i \cdot A \cdot s_i + f_i \cdot e_1 = t \bmod q$

Also check: $|s_i|_2 < \beta$

BASIS verification.

$$\begin{bmatrix} A & & & & -G_n \\ & W_1 A & & & -G_n \\ & & \ddots & & \\ & & & W_{\ell-1}A & -G_n \end{bmatrix} \cdot \begin{bmatrix} s_0 \\ \vdots \\ s_{\ell-1} \\ \hat{t} \end{bmatrix} = \begin{bmatrix} -f_0 \cdot e_1 \\ \vdots \\ \vdots \\ -f_{\ell-1} \cdot e_1 \end{bmatrix} \bmod q$$

For the coordinate $i = 0,\ldots,\ell - 1$ we have:

$$W_i \cdot A \cdot s_i - G \cdot \hat{t} = -f_i \cdot e_1 \bmod q$$

Or: $W_i \cdot A \cdot s_i + f_i \cdot e_1 = t \bmod q$

Also check: $|s_i|_2 < \beta$

Can be transformed into a polynomial commitment by opening to $f_v^T \cdot \bar{u}$ for $\bar{u} = (1, u, \ldots u^{l-1})$

Hard Problems.

SIS/ISIS

BASIS

PRISIS

Multi-Instance Problems

Power-Ring-BASIS (PRISIS) [FMN 23].

Given: $(A, w \in \mathcal{R}, T_B)$ such that

$$B = \begin{bmatrix} A & & & & -G_n \\ & w \cdot A & & & -G_n \\ & & \ddots & & \\ & & & w^{\ell-1} \cdot A & -G_n \end{bmatrix} \text{ and } \; B \cdot T_B = G_{\ell n} \bmod q$$

Compute: $x \in \mathcal{R}^m : A \cdot x = 0 \bmod q$ such that $|x|_2 \leq \beta$

Power-Ring-BASIS (PRISIS) [FMN 23].

Given: $(A, w \in \mathcal{R}, T_B)$ such that

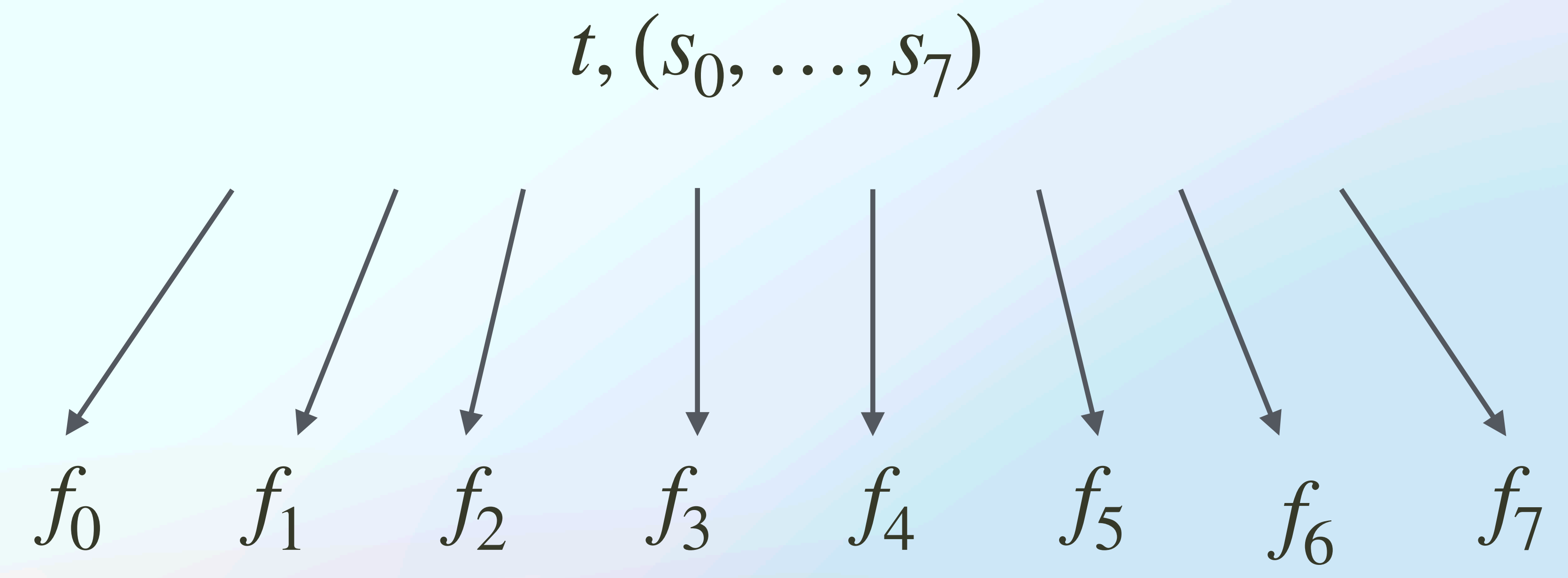
$$B = \begin{bmatrix} A & & & & -G_n \\ & w \cdot A & & & -G_n \\ & & \ddots & & \\ & & & w^{\ell-1} \cdot A & -G_n \end{bmatrix}$$ and $B \cdot T_B = G_{\ell n} \bmod q$

Compute: $x \in \mathcal{R}^m : A \cdot x = 0 \bmod q$ such that $|x|_2 \leq \beta$

As hard as SIS + NTRU for $l = 2$

PRISIS polynomial commitment.

- Same as BASIS commitment scheme.
- Allows evaluating polynomials due to the additional power structure.
- Split and fold: $f(X) = f_L(X^2) + X \cdot f_R(X^2)$



Split and Fold.

$f(X) = f_L(X^2) + X \cdot f_R(X^2)$, $f(u) = v$

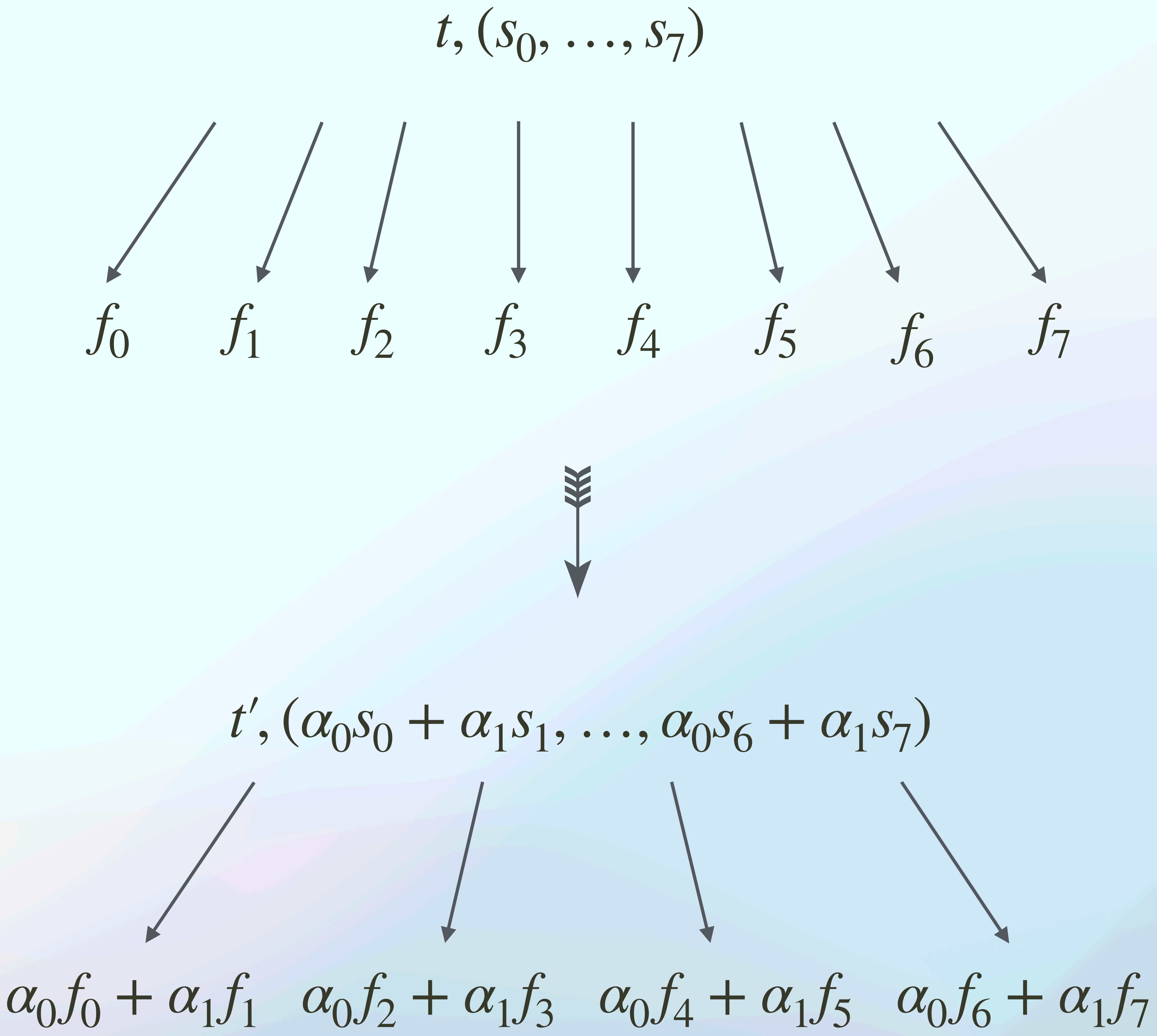
Verifier sends random short $\alpha_0, \alpha_1 \in \mathbb{Z}_q$

Prover sets $g(X) = \alpha_0 \cdot f_L(X) + \alpha_1 \cdot f_R(X)$

Sends $z_0 = f_L(u^2)$, $z_1 = f_R(u^2)$

Verifier checks $v = z_0 + uz_1$

Remains to prove $g(u) = \alpha_0 z_0 + \alpha_1 z_1$



*the technique developed in FRI [BBHR18]

Parameters.

as function of polynomial degree - l

- Verifier - Logarithmic
- Prover - Quadratic
- Communication - Polylog
- Public Params - $(A, w \in \mathscr{R}, T_B)$ - Quadratic
- Trusted Setup - YES

Merkle-PRISIS [this work].

$$f(x) = \sum_{i=0}^{7} f_i x^i, crs = \{(A_1, w_1, T_1), \ldots, (A_3, w_3, T_3)\}$$

Constructing the tree:

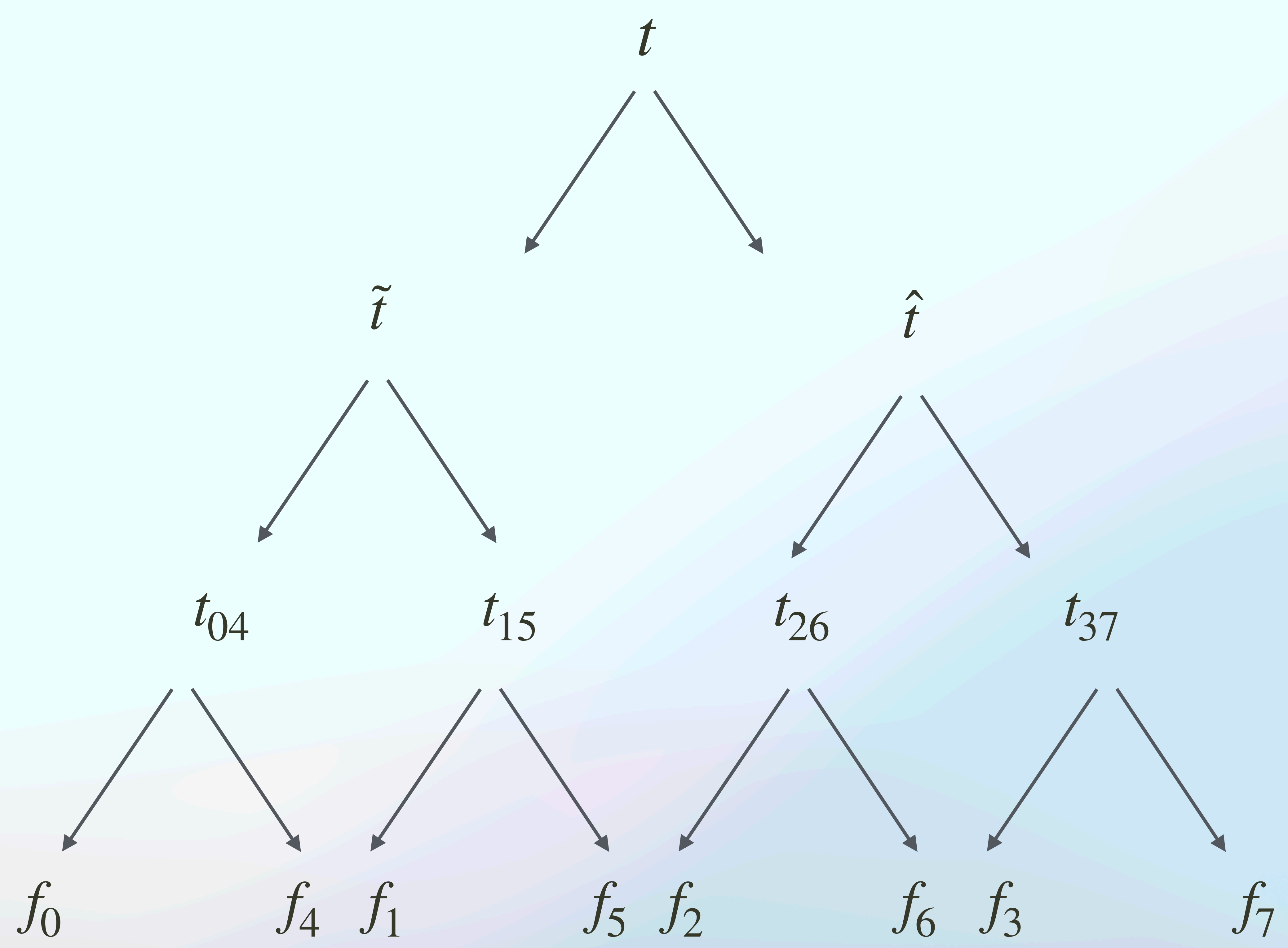
$$(s_0, s_4), t_{04} = Com(f_0 \cdot e_1, f_4 \cdot e_1)$$

$$\downarrow$$

$$(s_{04}, s_{15}), \tilde{t} = Com(t_{04}, t_{15})$$

$$\downarrow$$

$$(\tilde{s}, \hat{s}), t = Com(\tilde{t}, \hat{t})$$



To open and verify

To open f_0 send $(\tilde{s}, s_{04}, s_0)$

Verification:

Compute $A_3 \cdot s_0 + f_0 \cdot e_1 = t_{04} \bmod q$

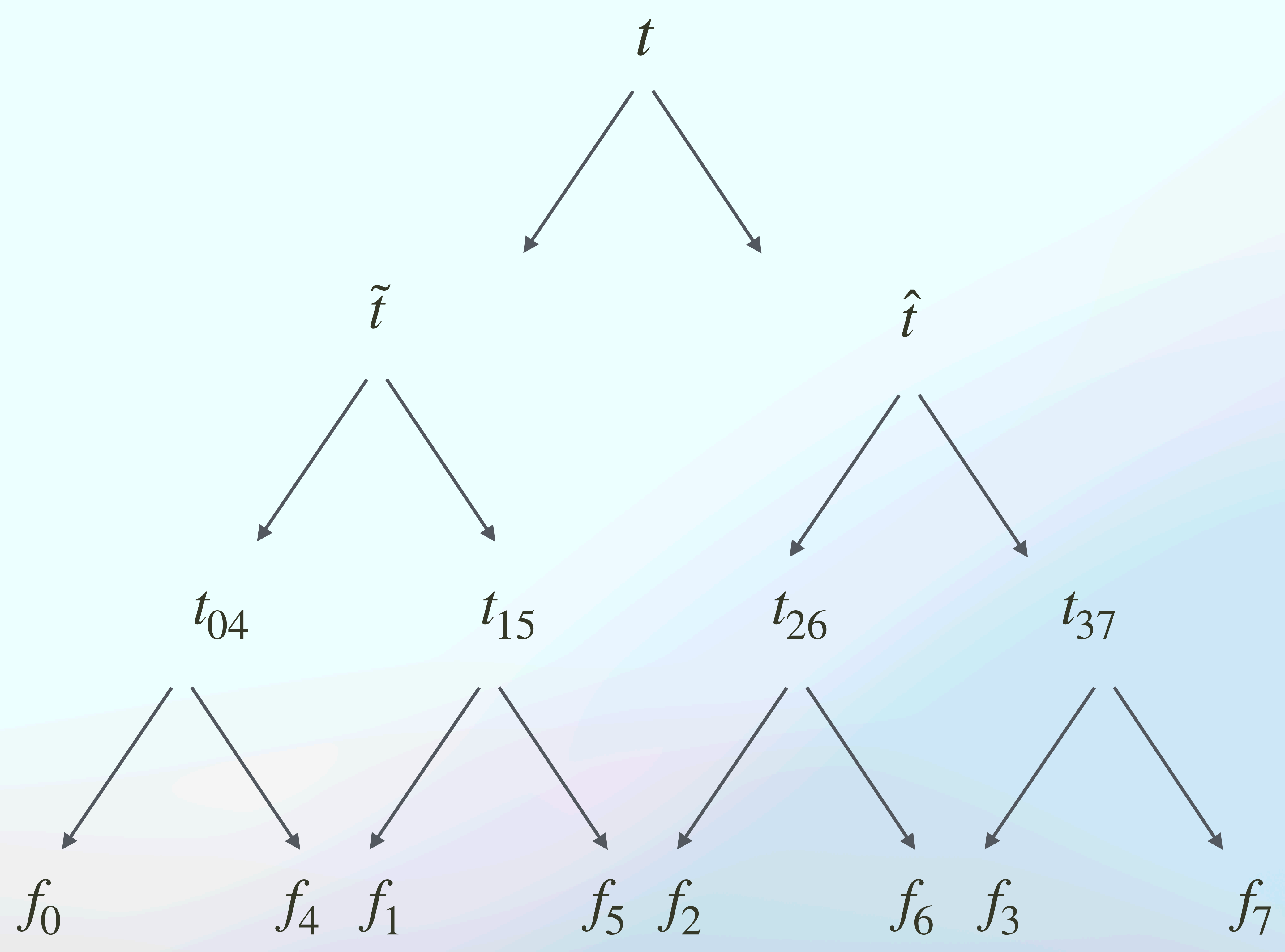
Compute $A_2 \cdot s_{04} + t_{04} = \tilde{t} \bmod q$

Verify $A_1 \cdot \tilde{s} + \tilde{t} = t \bmod q$

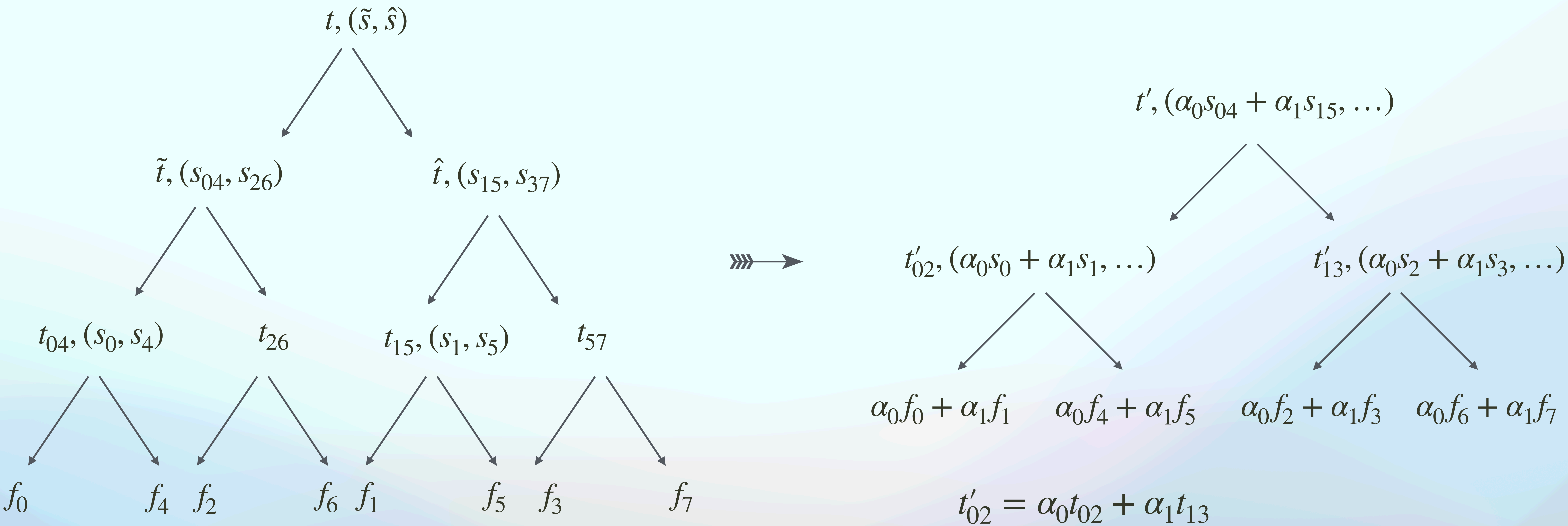
Or equivalently:

For $f_0 : A_1\tilde{s} + A_2 s_{04} + A_3 s_0 + f_0 \cdot e_1 = t \bmod q$

For $f_5 : A_1\tilde{s} + w_2 A_2 s_{15} + w_3 A_3 s_5 + f_5 \cdot e_1 = t \bmod q$



Folding Trees.



$$t'_{02} = \alpha_0 t_{02} + \alpha_1 t_{13}$$

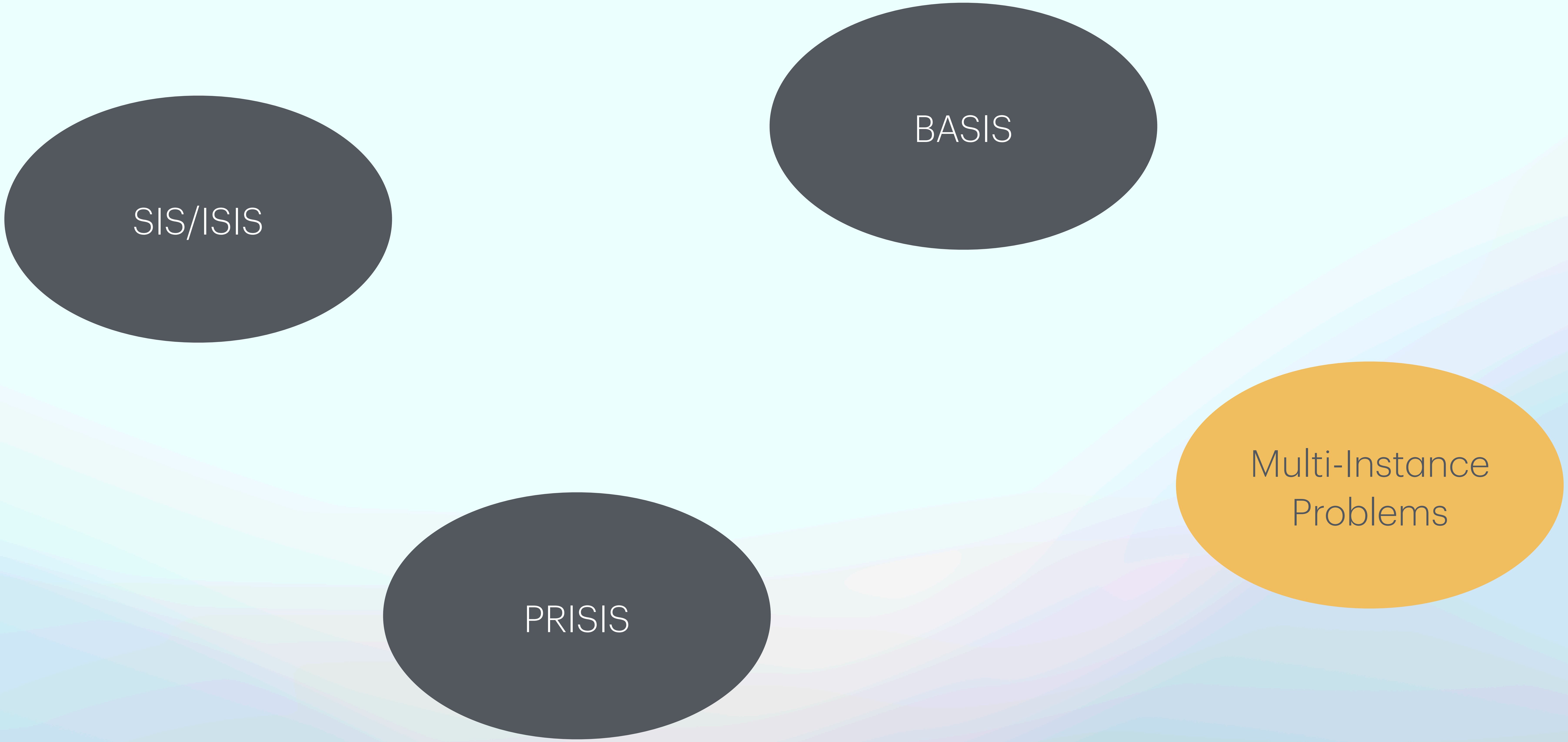
$$t' = \alpha_0 (t - A_3 \cdot \tilde{s}) + \alpha_1 (t - w_3 A_3 \cdot \hat{s})$$

Parameters.

as function of polynomial degree - l

- Verifier - Polylog (folding and verifying the one opening)
- Prover - Quasi - linear (building the tree with $2l - 1$ nodes)
- Communication - Polylog (folding communication)
- Public Params - $(A_1, w_1, T_1), \ldots, (A_h, w_h, T_h), h = \log l$ - Polylog
- Trusted Setup - YES

Hard Problems.



Multi-instance PRISIS (h-PRISIS)

Given: $(A_1, w_1, T_1), \ldots, (A_h, w_h, T_h)$ PRISIS instances of arity ℓ

Compute: $x \in \mathbb{Z}^{mh} : [A_1 | \ldots | A_h] \cdot x = 0 \bmod q$ such that $|x|_2 \leq \beta$

As hard as SIS + NTRU for
$\ell = 2, h = poly(\lambda)$

Reduction h-PRISIS to PRISIS.

- Consider $\ell = O(1),\ h = poly(\lambda)$.
- Plan:
    - Randomise A.
    - Randomise w.
    - Adapt the trapdoor accordingly.

$$(A, w \in \mathcal{R}, T_B)$$

$$\downarrow$$

$$(A_1, w_1, T_1), \ldots, (A_h, w_h, T_h)$$

The same technique applies to other "Multi-instance" assumptions.

Progress Since

More SIS and LWE with Hints.

- SIS with hints zoo (https://malb.io/sis-with-hints.html)
- Some are proved standard
- Many are still open problems

Workshop on funky assumptions is coming to Edinburgh in Spring 2026

Progress Since

More Efficient Commitments

- Concrete opening sizes are quite large (for $l = 2^{20}$)
    - [FMN23] - 3.4MB
    - [this work] - 36.5 MB
    - [C: HSS24] - 8.93 MB, [C: MNW24] - 500KB, [C: NS24] - < 46KB
- All new schemes also feature Transparent Setup.

Other things we can chat about

- Leftover Hash Lemmas over rings.
- Threshold SIS Trapdoors / Signatures.
- Threshold CCA Secure Encryption.

Keep in touch!

sasha.lapiha.2021@live.rhul.ac.uk
sasha.lapiha@kcl.ac.uk

References

- [BBHR18] - Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev "Fast Reed-Solomon Interactive Oracle Proofs of Proximity"
- [WW23] - Hoeteck Wee, and David J. Wu "Succinct Vector, Polynomial, and Functional Commitments from Lattices"
- [FMN23] - Giacomo Fenzi, Hossein Moghaddas, and Ngoc Khanh Nguyen "Lattice-Based Polynomial Commitments: Towards Asymptotic and Concrete Efficiency"
- [C: CMNW24] - Valerio Cini, Giulio Malavolta, Ngoc Khanh Nguyen, and Hoeteck Wee "Polynomial Commitments from Lattices: Post-quantum Security, Fast Verification and Transparent Setup"
- [C: HSS24] - Intak Hwang , Jinyeong Seo , and Yongsoo Song "Concretely Efficient Lattice-based Polynomial Commitment from Standard Assumptions"
- [C: NS24] - Ngoc Khanh Nguyen and Gregor Seiler "Greyhound: Fast Polynomial Commitments from Lattices"

Folding Trees.

Basic Σ-Protocol

Prover		**Verifier**
$f(\mathsf{X}) = f_0(\mathsf{X}^2) + \mathsf{X} f_1(\mathsf{X}^2)$		
$z_i := f_i(u^2)$ for $i \in \mathbb{Z}_2$	$\xrightarrow{z_0, z_1, \mathbf{s}_0, \mathbf{s}_1}$	Check: $z_0 + u z_1 =_? z$; Check: $\mathbf{s}_0, \mathbf{s}_1$ short
$g(\mathsf{X}) := \alpha_0 f_0(\mathsf{X}) + \alpha_1 f_1(\mathsf{X})$	$\xleftarrow{\alpha_0, \alpha_1}$	$\alpha_0, \alpha_1 \leftarrow \{ X^i : i \in \mathbb{Z} \}$
$\mathbf{z_b} := \alpha_0 \mathbf{s}_{\mathbf{b},0} + \alpha_1 \mathbf{s}_{\mathbf{b},1}$ for $\mathbf{b} \in \mathbb{Z}_2^{\leq h-1}$	$\xrightarrow{g, (\mathbf{z_b})_\mathbf{b}}$	$\mathsf{crs}' := (\mathbf{A}_{1+t}, w_{1+t}, \mathbf{T}_{1+t})_{t \in [h-1]}$
		$\mathbf{t}' := \alpha_0 \cdot (\mathbf{t} - w_1^0 \mathbf{A}_1 \mathbf{s}_0) + \alpha_1 \cdot (\mathbf{t} - w_1^1 \mathbf{A}_1 \mathbf{s}_1)$
		$u' := u^2; z' := \alpha_0 \cdot z_0 + \alpha_1 \cdot z_1$
		Check: $g(u') = z'$
		Check: $\mathsf{Open}(\mathsf{crs}', \mathbf{t}', g, (\mathbf{z_b})_\mathbf{b}) = 1$