CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

MPC in the head using the subfield bilinear collision problem

Janik Huth and Antoine Joux

CISPA Helmholtz Center for Information Security

The Subfield Bilinear Collision (SBC) Problem

The Subfield Bilinear Collision (SBC) Problem

Parameters: q and $k, n > 0$

The Subfield Bilinear Collision (SBC) Problem

Parameters: q and $k, n > 0$

$$\mathbb{F}_{q^k}$$

$$|$$

$$\mathbb{F}_q$$

The Subfield Bilinear Collision (SBC) Problem

Parameters: q and $k, n > 0$

$$\mathbb{F}_{q^k} \qquad \vec{u}, \vec{v} \in \left(\mathbb{F}_{q^k}\right)^n$$

$$|$$

$$\mathbb{F}_q$$

The Subfield Bilinear Collision (SBC) Problem

Parameters: q and $k, n > 0$

$$\begin{array}{ll} \mathbb{F}_{q^k} & \vec{u}, \vec{v} \in \left(\mathbb{F}_{q^k}\right)^n \\ \Big| & \\ \mathbb{F}_q & \vec{x}, \vec{y} \in \left(\mathbb{F}_q\right)^n \end{array}$$

The Subfield Bilinear Collision (SBC) Problem

$$(\vec{u} \cdot \vec{x}) = \sum_{i=1}^{n} u_i x_i$$

Parameters: q and $k, n > 0$

$$\mathbb{F}_{q^k} \qquad \vec{u}, \vec{v} \in \left(\mathbb{F}_{q^k}\right)^n$$

$$\mathbb{F}_{q} \qquad \vec{x}, \vec{y} \in \left(\mathbb{F}_{q}\right)^n$$

$$\boxed{\left(\vec{u} \cdot \vec{x}\right)\left(\vec{v} \cdot \vec{y}\right) = \left(\vec{u} \cdot \vec{y}\right)\left(\vec{v} \cdot \vec{x}\right)}$$

The Subfield Bilinear Collision (SBC) Problem

$$(\vec{u} \cdot \vec{x}) = \sum_{i=1}^{n} u_i x_i$$

Parameters: q and $k, n > 0$

$$\mathbb{F}_{q^k} \quad \vec{u}, \vec{v} \in \left(\mathbb{F}_{q^k}\right)^n$$

$$\mathbb{F}_{q} \quad \vec{x}, \vec{y} \in \left(\mathbb{F}_{q}\right)^n$$

$$\boxed{(\vec{u} \cdot \vec{x})\,(\vec{v} \cdot \vec{y}) = (\vec{u} \cdot \vec{y})\,(\vec{v} \cdot \vec{x})}$$

Conditions:

The <u>S</u>ubfield <u>B</u>ilinear <u>C</u>ollision (SBC) Problem

$$(\vec{u} \cdot \vec{x}) = \sum_{i=1}^{n} u_i x_i$$

Parameters: q and $k, n > 0$

$$\begin{array}{ll} \mathbb{F}_{q^k} & \vec{u}, \vec{v} \in \left(\mathbb{F}_{q^k}\right)^n \\ \Big| & \\ \mathbb{F}_q & \vec{x}, \vec{y} \in \left(\mathbb{F}_q\right)^n \end{array}$$

$$\boxed{(\vec{u} \cdot \vec{x})\,(\vec{v} \cdot \vec{y}) = (\vec{u} \cdot \vec{y})\,(\vec{v} \cdot \vec{x})}$$

<u>Conditions:</u>

$\vec{x}, \vec{y}$ non-colinear

The Subfield Bilinear Collision (SBC) Problem

$$(\vec{u} \cdot \vec{x}) = \sum_{i=1}^{n} u_i x_i$$

Parameters: q and $k, n > 0$

$$\begin{array}{ll} \mathbb{F}_{q^k} & \vec{u}, \vec{v} \in \left(\mathbb{F}_{q^k}\right)^n \\ | & \\ \mathbb{F}_q & \vec{x}, \vec{y} \in \left(\mathbb{F}_q\right)^n \end{array}$$

$$\boxed{(\vec{u} \cdot \vec{x})\,(\vec{v} \cdot \vec{y}) = (\vec{u} \cdot \vec{y})\,(\vec{v} \cdot \vec{x})}$$

Conditions:

$\vec{x}, \vec{y}$ non-colinear

$\vec{u}, \vec{v}$ linearly independent over $\mathbb{F}_q$

The Subfield Bilinear Collision (SBC) Problem

$$(\vec{u} \cdot \vec{x}) = \sum_{i=1}^{n} u_i x_i$$

Parameters: q and $k, n > 0$

$$\mathbb{F}_{q^k} \qquad \vec{u}, \vec{v} \in \left(\mathbb{F}_{q^k}\right)^n$$

$$\mathbb{F}_{q} \qquad \vec{x}, \vec{y} \in \left(\mathbb{F}_{q}\right)^n$$

$$\boxed{\left(\vec{u} \cdot \vec{x}\right)\left(\vec{v} \cdot \vec{y}\right) = \left(\vec{u} \cdot \vec{y}\right)\left(\vec{v} \cdot \vec{x}\right)}$$

Conditions:

$\vec{x}, \vec{y}$ non-colinear

$\vec{u}, \vec{v}$ linearly independent over $\mathbb{F}_q$

$$\left(\vec{x}, \vec{y}\right) \in \mathrm{SBC}[\vec{u}, \vec{v}]$$

The Subfield Bilinear Collision (SBC) Problem

$$(\vec{u} \cdot \vec{x}) = \sum_{i=1}^{n} u_i x_i$$

Parameters: q and $k, n > 0$

$\mathbb{F}_{q^k}$ $\quad \vec{u}, \vec{v} \in \left(\mathbb{F}_{q^k}\right)^n$

$\mathbb{F}_q$ $\quad \vec{x}, \vec{y} \in \left(\mathbb{F}_q\right)^n$

$$\boxed{(\vec{u} \cdot \vec{x})\,(\vec{v} \cdot \vec{y}) = (\vec{u} \cdot \vec{y})\,(\vec{v} \cdot \vec{x})}$$

Conditions:

$\vec{x}, \vec{y}$ non-colinear

$\vec{u}, \vec{v}$ linearly independent over $\mathbb{F}_q$

$$(\vec{x}, \vec{y}) \in \mathrm{SBC}[\vec{u}, \vec{v}]$$

$$n \approx \frac{k}{2}$$

Testing with polynomials

Testing with polynomials

$$(\vec{x}, \vec{y}) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

$$\left(\vec{u} \cdot \vec{x}\right)\left(\vec{v} \cdot \vec{y}\right) = \left(\vec{u} \cdot \vec{y}\right)\left(\vec{v} \cdot \vec{x}\right)$$

Testing with polynomials

$$(\vec{x}, \vec{y}) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$
$$\left(\vec{u} \cdot \vec{x}\right)\left(\vec{v} \cdot \vec{y}\right) = \left(\vec{u} \cdot \vec{y}\right)\left(\vec{v} \cdot \vec{x}\right)$$

$$X_1, X_2, Y_1, Y_2 \stackrel{\$}{\leftarrow} \mathbb{F}_{q^k}$$

Testing with polynomials

$$(\vec{x}, \vec{y}) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

$$\left(\vec{u} \cdot \vec{x}\right)\left(\vec{v} \cdot \vec{y}\right) = \left(\vec{u} \cdot \vec{y}\right)\left(\vec{v} \cdot \vec{x}\right)$$

$$X_1, X_2, Y_1, Y_2 \xleftarrow{\$} \mathbb{F}_{q^k}$$

$$F(t) = \left(X_1 + t\left(\vec{u} \cdot \vec{x}\right)\right)\left(Y_1 + t\left(\vec{v} \cdot \vec{y}\right)\right) - \left(X_2 + t\left(\vec{v} \cdot \vec{x}\right)\right)\left(Y_2 + t\left(\vec{u} \cdot \vec{y}\right)\right)$$

Testing with polynomials

$$(\vec{x}, \vec{y}) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

$$\left(\vec{u} \cdot \vec{x}\right)\left(\vec{v} \cdot \vec{y}\right) = \left(\vec{u} \cdot \vec{y}\right)\left(\vec{v} \cdot \vec{x}\right)$$

$$X_1, X_2, Y_1, Y_2 \overset{\$}{\leftarrow} \mathbb{F}_{q^k}$$

$$F(t) = \left(X_1 + t\left(\vec{u} \cdot \vec{x}\right)\right)\left(Y_1 + t\left(\vec{v} \cdot \vec{y}\right)\right) - \left(X_2 + t\left(\vec{v} \cdot \vec{x}\right)\right)\left(Y_2 + t\left(\vec{u} \cdot \vec{y}\right)\right)$$

$$F(t) = A + Bt + \left[\left(\vec{u} \cdot \vec{x}\right)\left(\vec{v} \cdot \vec{y}\right) - \left(\vec{u} \cdot \vec{y}\right)\left(\vec{v} \cdot \vec{x}\right)\right] t^2$$

Testing with polynomials

$$(\vec{x}, \vec{y}) \in \text{SBC}\left[\vec{u}, \vec{v}\right]$$

$$(\vec{u} \cdot \vec{x})\,(\vec{v} \cdot \vec{y}) = (\vec{u} \cdot \vec{y})\,(\vec{v} \cdot \vec{x})$$

$$X_1, X_2, Y_1, Y_2 \xleftarrow{\$} \mathbb{F}_{q^k}$$

$$F(t) = \Big(X_1 + t\,(\vec{u} \cdot \vec{x})\Big)\Big(Y_1 + t\,(\vec{v} \cdot \vec{y})\Big) - \Big(X_2 + t\,(\vec{v} \cdot \vec{x})\Big)\Big(Y_2 + t\,(\vec{u} \cdot \vec{y})\Big)$$

$$F(t) = A + Bt + \Big[(\vec{u} \cdot \vec{x})\,(\vec{v} \cdot \vec{y}) - (\vec{u} \cdot \vec{y})\,(\vec{v} \cdot \vec{x})\Big]\,t^2$$

$$\boxed{\deg(F) < 2 \Leftrightarrow (\vec{x}, \vec{y}) \in \text{SBC}\left[\vec{u}, \vec{v}\right]}$$

MPC protocol for the polynomial testing

MPC protocol for the polynomial testing

$$\left(\vec{x}, \vec{y}\right) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

MPC protocol for the polynomial testing

$$[\![\vec{x}]\!] = \left(\vec{x}^{[\![1]\!]}, \ldots, \vec{x}^{[\![N]\!]}\right)$$

$$\vec{x} = \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

$$\left(\vec{x}, \vec{y}\right) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

$$[\![s]\!] = \left([\![\vec{x}]\!], [\![\vec{y}]\!], [\![X_1]\!], [\![X_2]\!], [\![Y_1]\!], [\![Y_2]\!], [\![A]\!], [\![B]\!]\right)$$

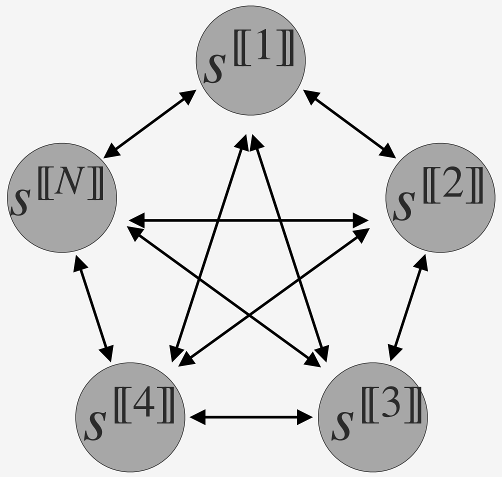
MPC protocol for the polynomial testing

$$[\![\vec{x}]\!] = \left(\vec{x}^{[\![1]\!]}, \ldots, \vec{x}^{[\![N]\!]}\right)$$

$$\vec{x} = \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

$$\left(\vec{x}, \vec{y}\right) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

$$[\![s]\!] = \left([\![\vec{x}]\!], [\![\vec{y}]\!], [\![X_1]\!], [\![X_2]\!], [\![Y_1]\!], [\![Y_2]\!], [\![A]\!], [\![B]\!]\right)$$



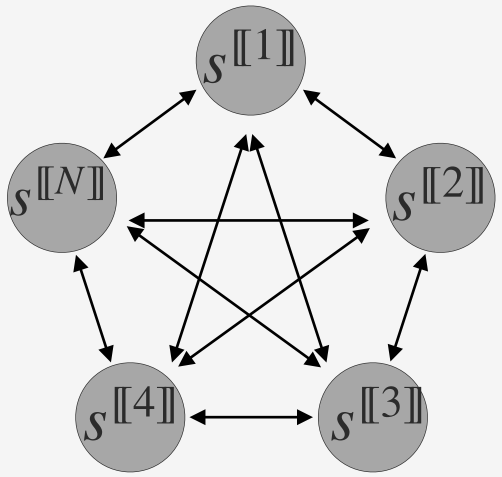
MPC protocol for the polynomial testing

$$[\![\vec{x}]\!] = \left(\vec{x}^{[\![1]\!]}, \ldots, \vec{x}^{[\![N]\!]}\right)$$

$$\vec{x} = \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

$$\left(\vec{x}, \vec{y}\right) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

$$[\![s]\!] = \left([\![\vec{x}]\!], [\![\vec{y}]\!], [\![X_1]\!], [\![X_2]\!], [\![Y_1]\!], [\![Y_2]\!], [\![A]\!], [\![B]\!]\right)$$



MPC protocol:

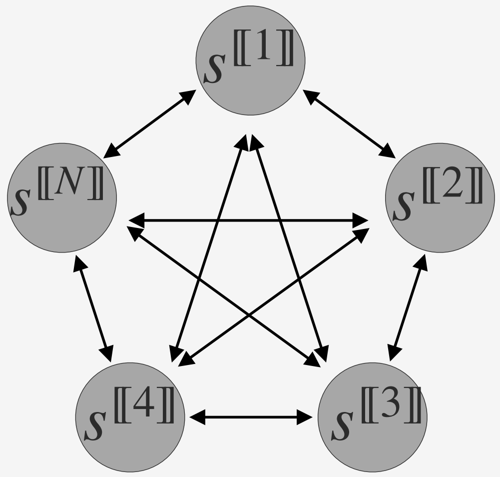
MPC protocol for the polynomial testing

$$[\![\vec{x}]\!] = \left(\vec{x}^{[\![1]\!]}, \ldots, \vec{x}^{[\![N]\!]}\right)$$

$$\vec{x} = \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

$$\left(\vec{x}, \vec{y}\right) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

$$[\![s]\!] = \left([\![\vec{x}]\!], [\![\vec{y}]\!], [\![X_1]\!], [\![X_2]\!], [\![Y_1]\!], [\![Y_2]\!], [\![A]\!], [\![B]\!]\right)$$



MPC protocol:

Create a random $t_0 = \sum_{i=1}^{N} t_0^{[\![i]\!]}$

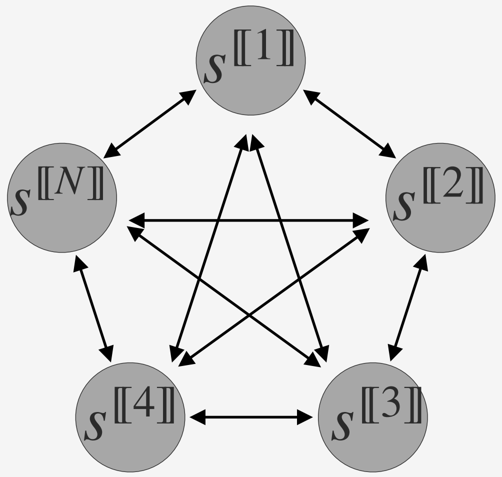
MPC protocol for the polynomial testing

$$[\![\vec{x}]\!] = \left(\vec{x}^{[\![1]\!]}, \ldots, \vec{x}^{[\![N]\!]}\right)$$

$$\vec{x} = \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

$$\left(\vec{x}, \vec{y}\right) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

$$[\![s]\!] = \left([\![\vec{x}]\!], [\![\vec{y}]\!], [\![X_1]\!], [\![X_2]\!], [\![Y_1]\!], [\![Y_2]\!], [\![A]\!], [\![B]\!]\right)$$



MPC protocol:

Create a random $t_0 = \sum_{i=1}^{N} t_0^{[\![i]\!]}$

Evaluate $F(t_0)$

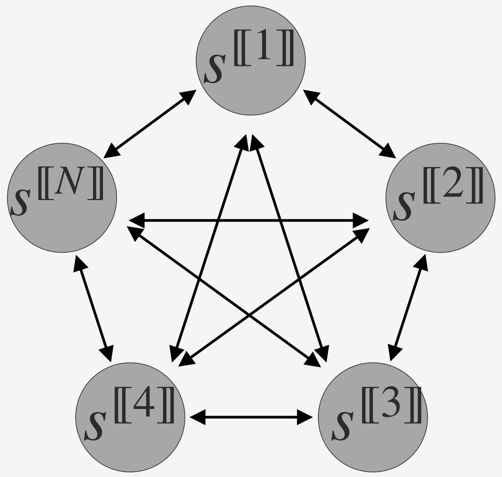
MPC protocol for the polynomial testing

$$[\![\vec{x}]\!] = \left(\vec{x}^{[\![1]\!]}, \ldots, \vec{x}^{[\![N]\!]}\right)$$

$$\vec{x} = \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

$$\left(\vec{x}, \vec{y}\right) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

$$[\![s]\!] = \left([\![\vec{x}]\!], [\![\vec{y}]\!], [\![X_1]\!], [\![X_2]\!], [\![Y_1]\!], [\![Y_2]\!], [\![A]\!], [\![B]\!]\right)$$



MPC protocol:

Create a random $t_0 = \sum_{i=1}^{N} t_0^{[\![i]\!]}$

Evaluate $F(t_0)$

Evaluate $A + Bt_0$

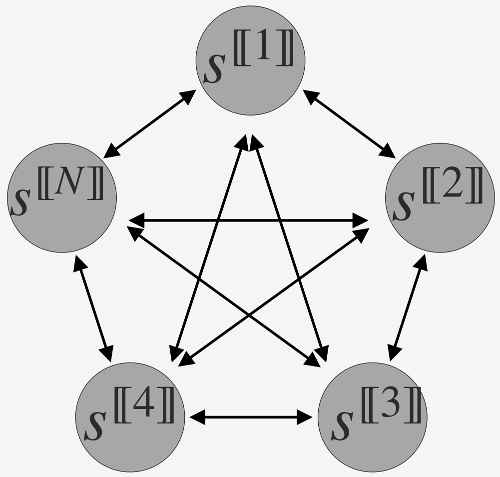
MPC protocol for the polynomial testing

$$[\![\vec{x}]\!] = \left(\vec{x}^{[\![1]\!]}, \ldots, \vec{x}^{[\![N]\!]}\right)$$

$$\vec{x} = \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

$$\left(\vec{x}, \vec{y}\right) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

$$[\![s]\!] = \left([\![\vec{x}]\!], [\![\vec{y}]\!], [\![X_1]\!], [\![X_2]\!], [\![Y_1]\!], [\![Y_2]\!], [\![A]\!], [\![B]\!]\right)$$



MPC protocol:

Create a random $t_0 = \sum_{i=1}^{N} t_0^{[\![i]\!]}$

Evaluate $F(t_0)$

Evaluate $A + Bt_0$

Check if $F(t_0) = A + Bt_0$

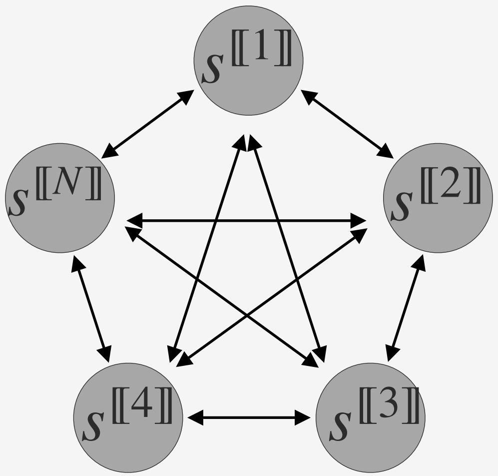
MPC protocol for the polynomial testing

$$[\![\vec{x}]\!] = \left(\vec{x}^{[\![1]\!]}, \ldots, \vec{x}^{[\![N]\!]}\right)$$

$$\vec{x} = \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

$$\left(\vec{x}, \vec{y}\right) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

$$[\![s]\!] = \left([\![\vec{x}]\!], [\![\vec{y}]\!], [\![X_1]\!], [\![X_2]\!], [\![Y_1]\!], [\![Y_2]\!], [\![A]\!], [\![B]\!]\right)$$



MPC protocol:

Create a random $t_0 = \sum_{i=1}^{N} t_0^{[\![i]\!]}$

Evaluate $F(t_0)$

Evaluate $A + Bt_0$

Check if $F(t_0) = A + Bt_0$

$N - 1$ private:

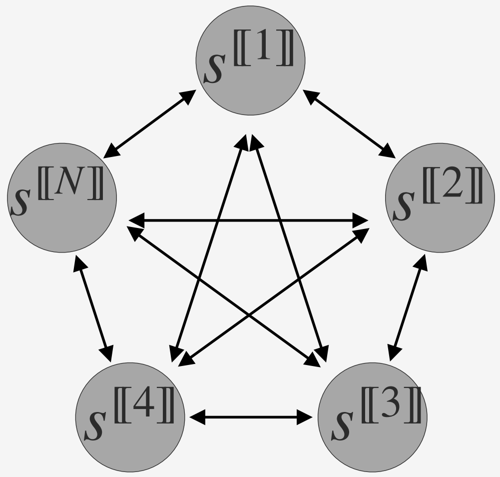
MPC protocol for the polynomial testing

$$[\![\vec{x}]\!] = \left(\vec{x}^{[\![1]\!]}, \ldots, \vec{x}^{[\![N]\!]}\right)$$

$$\vec{x} = \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

$$\left(\vec{x}, \vec{y}\right) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

$$[\![s]\!] = \left([\![\vec{x}]\!], [\![\vec{y}]\!], [\![X_1]\!], [\![X_2]\!], [\![Y_1]\!], [\![Y_2]\!], [\![A]\!], [\![B]\!]\right)$$



MPC protocol:

Create a random $t_0 = \sum_{i=1}^{N} t_0^{[\![i]\!]}$

Evaluate $F(t_0)$

Evaluate $A + Bt_0$

Check if $F(t_0) = A + Bt_0$

$N - 1$ private:

The views of $N - 1$ parties reveal no information about $\left(\vec{x}, \vec{y}\right)$

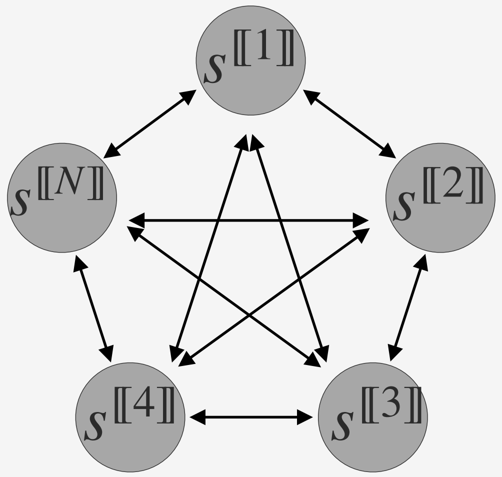
MPC protocol for the polynomial testing

$$[\![\vec{x}]\!] = \left(\vec{x}^{[\![1]\!]}, \ldots, \vec{x}^{[\![N]\!]}\right)$$

$$\vec{x} = \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

$$\left(\vec{x}, \vec{y}\right) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

$$[\![s]\!] = \left([\![\vec{x}]\!], [\![\vec{y}]\!], [\![X_1]\!], [\![X_2]\!], [\![Y_1]\!], [\![Y_2]\!], [\![A]\!], [\![B]\!]\right)$$



MPC protocol:

Create a random $t_0 = \sum_{i=1}^{N} t_0^{[\![i]\!]}$

Evaluate $F(t_0)$

Evaluate $A + Bt_0$

Check if $F(t_0) = A + Bt_0$

$N - 1$ private:

The views of $N - 1$ parties reveal no information about $\left(\vec{x}, \vec{y}\right)$

False positive probability:

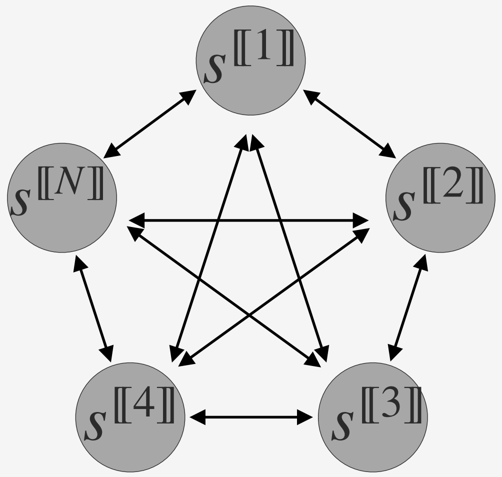
MPC protocol for the polynomial testing

$$[\![\vec{x}]\!] = \left(\vec{x}^{[\![1]\!]}, \ldots, \vec{x}^{[\![N]\!]}\right)$$

$$\vec{x} = \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

$$\left(\vec{x}, \vec{y}\right) \in \mathrm{SBC}\left[\vec{u}, \vec{v}\right]$$

$$[\![s]\!] = \left([\![\vec{x}]\!], [\![\vec{y}]\!], [\![X_1]\!], [\![X_2]\!], [\![Y_1]\!], [\![Y_2]\!], [\![A]\!], [\![B]\!]\right)$$



MPC protocol:

Create a random $t_0 = \sum_{i=1}^{N} t_0^{[\![i]\!]}$

Evaluate $F(t_0)$

Evaluate $A + Bt_0$

Check if $F(t_0) = A + Bt_0$

$N - 1$ private:

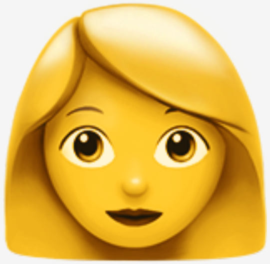
The views of $N - 1$ parties reveal no information about $\left(\vec{x}, \vec{y}\right)$

False positive probability:

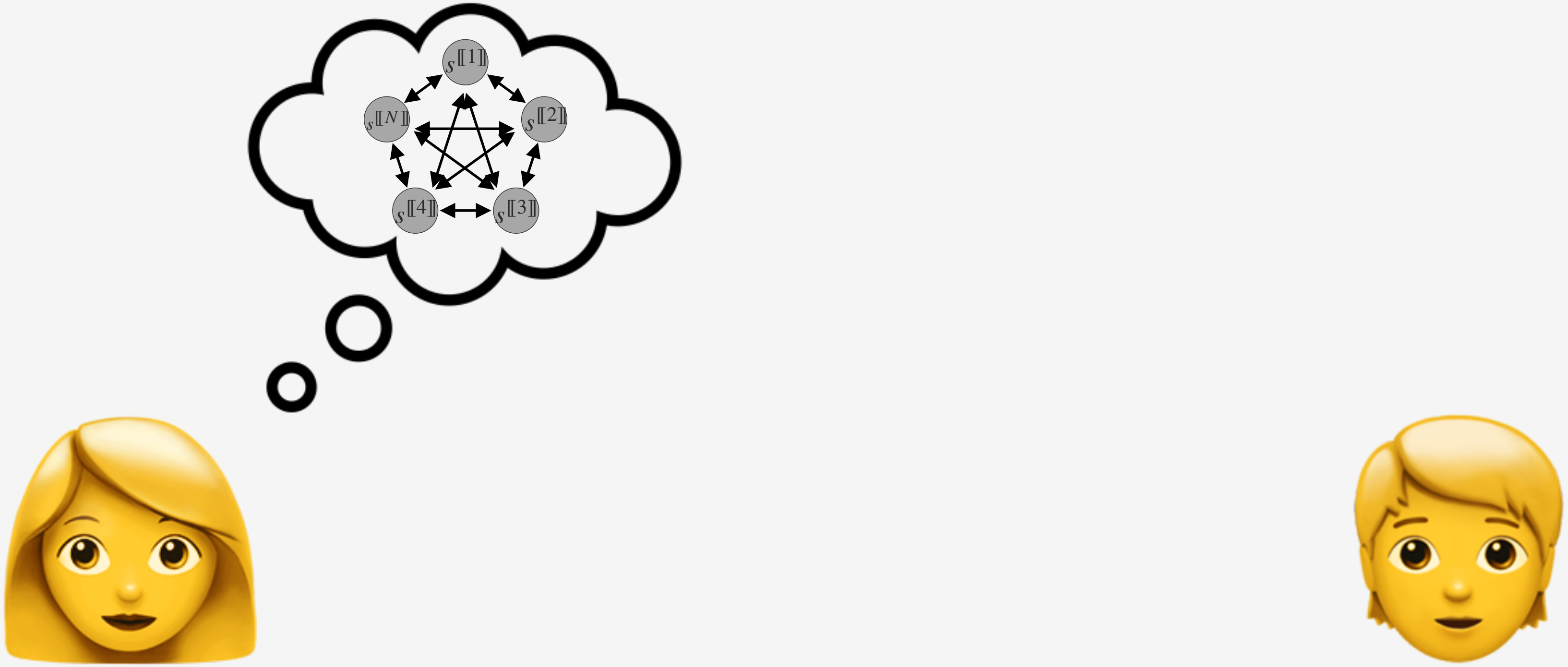
$$\Pr[\text{false positive}] \leq \frac{2}{q^k}$$

MPCitH protocol

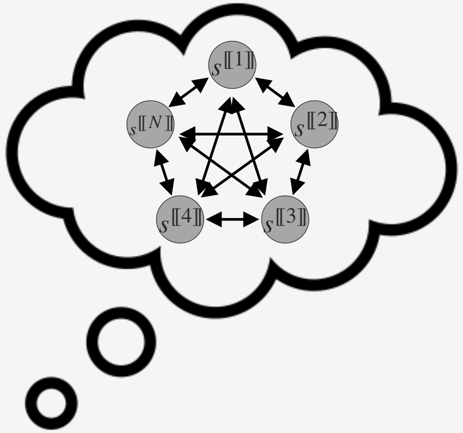
MPCitH protocol

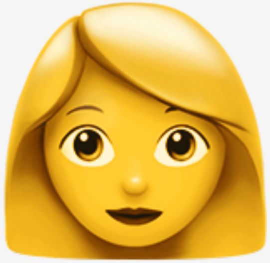


MPCitH protocol



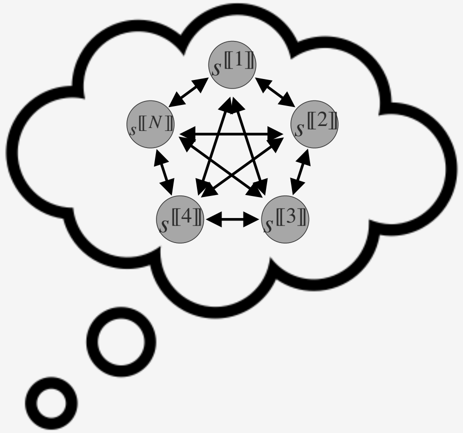
MPCitH protocol

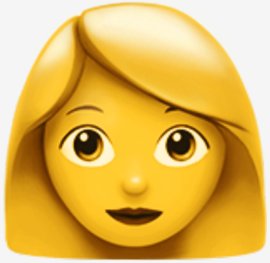




<u>commit:</u>

MPCitH protocol

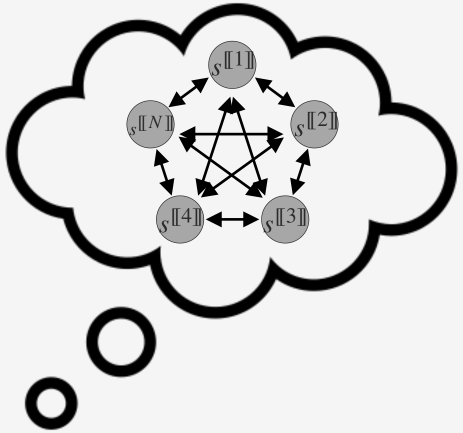


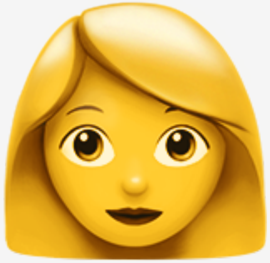


<u>commit:</u>

- $\text{com}\left(\text{View}^{[\![i]\!]}\right)$

MPCitH protocol

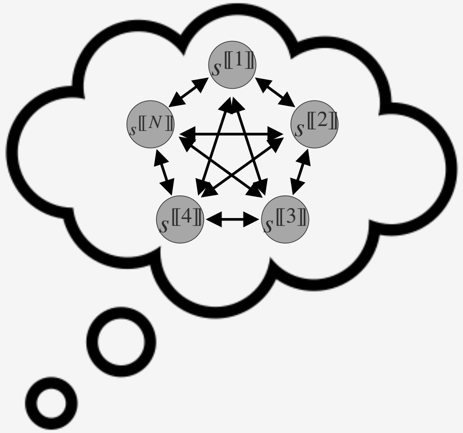


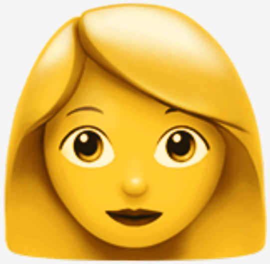


<u>commit:</u>

- $\mathrm{com}\left(\mathrm{View}^{[\![i]\!]}\right)$
- $\left(X_1 + t_0\left(\vec{u}\cdot\vec{x}\right)\right), \left(Y_1 + t_0\left(\vec{v}\cdot\vec{y}\right)\right)$
- $\left(X_2 + t_0\left(\vec{v}\cdot\vec{x}\right)\right), \left(Y_2 + t_0\left(\vec{u}\cdot\vec{y}\right)\right)$

MPCitH protocol

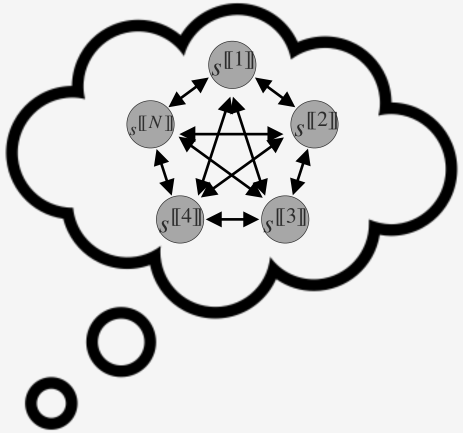


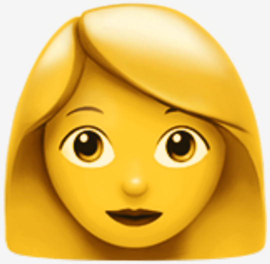


<u>commit:</u>

- $\text{com}\left(\text{View}^{[\![i]\!]}\right)$
- $\left(X_1 + t_0\left(\vec{u}\cdot\vec{x}\right)\right), \left(Y_1 + t_0\left(\vec{v}\cdot\vec{y}\right)\right)$
- $\left(X_2 + t_0\left(\vec{v}\cdot\vec{x}\right)\right), \left(Y_2 + t_0\left(\vec{u}\cdot\vec{y}\right)\right)$
- t_0

MPCitH protocol



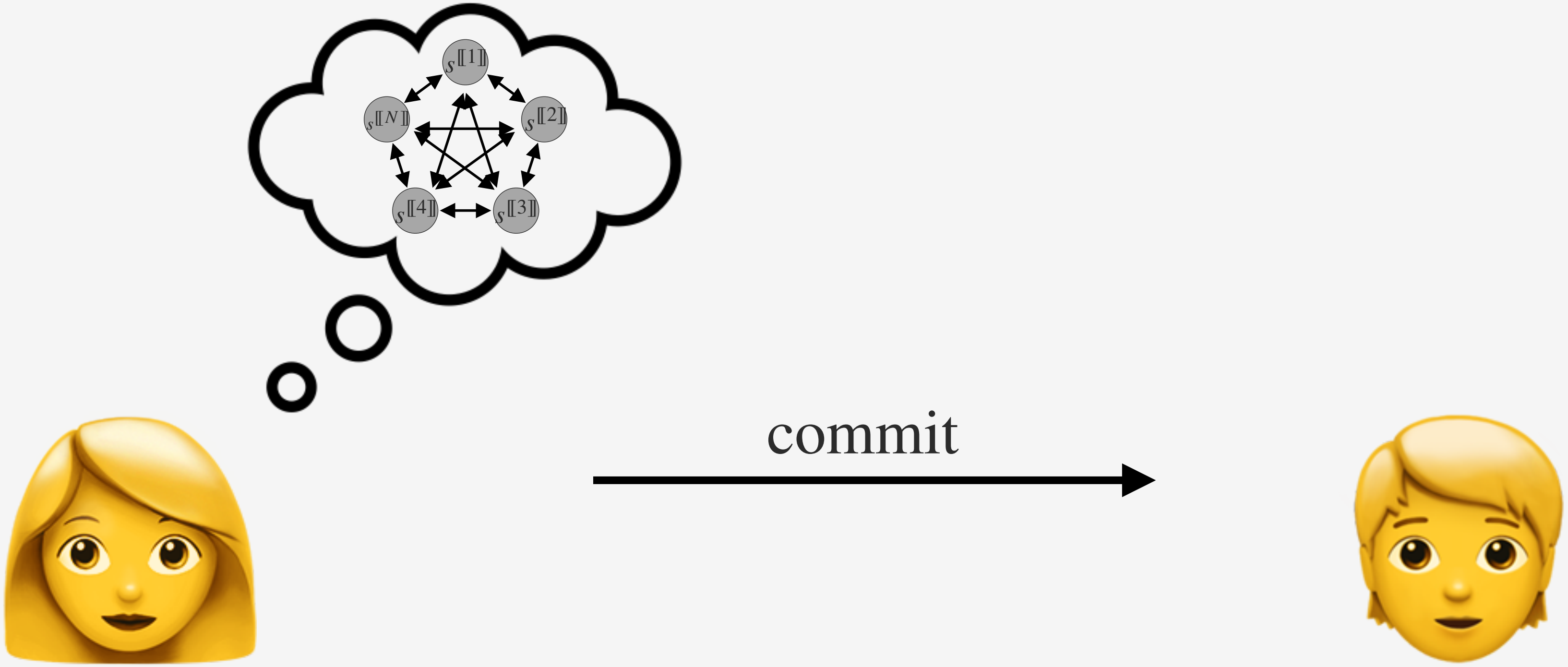


commit →

<u>commit:</u>

- $\mathrm{com}\left(\mathrm{View}^{[\![i]\!]}\right)$
- $\left(X_1 + t_0\left(\vec{u}\cdot\vec{x}\right)\right), \left(Y_1 + t_0\left(\vec{v}\cdot\vec{y}\right)\right)$
- $\left(X_2 + t_0\left(\vec{v}\cdot\vec{x}\right)\right), \left(Y_2 + t_0\left(\vec{u}\cdot\vec{y}\right)\right)$
- t_0

MPCitH protocol

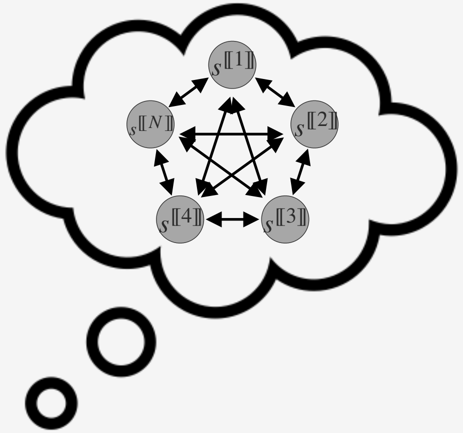


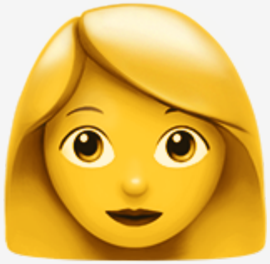
commit:

- $\text{com}\left(\text{View}^{[\![i]\!]}\right)$
- $\left(X_1 + t_0\left(\vec{u}\cdot\vec{x}\right)\right), \left(Y_1 + t_0\left(\vec{v}\cdot\vec{y}\right)\right)$
- $\left(X_2 + t_0\left(\vec{v}\cdot\vec{x}\right)\right), \left(Y_2 + t_0\left(\vec{u}\cdot\vec{y}\right)\right)$
- t_0

$i^* \xleftarrow{\$} \{1, \cdots, N\}$

MPCitH protocol





commit →

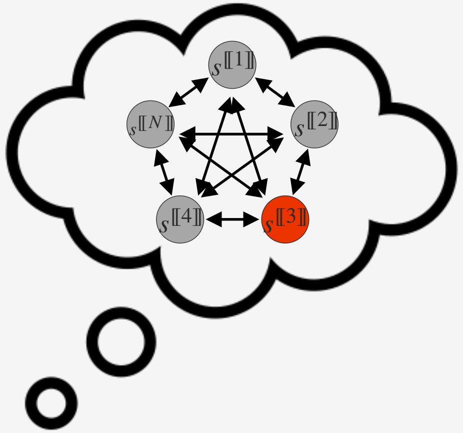
i^* ←

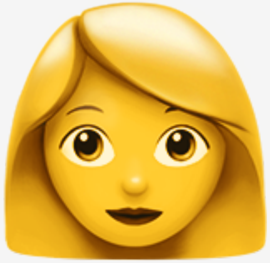
<u>commit:</u>

- $\text{com}\left(\text{View}^{[\![i]\!]}\right)$
- $\left(X_1 + t_0\left(\vec{u}\cdot\vec{x}\right)\right), \left(Y_1 + t_0\left(\vec{v}\cdot\vec{y}\right)\right)$
- $\left(X_2 + t_0\left(\vec{v}\cdot\vec{x}\right)\right), \left(Y_2 + t_0\left(\vec{u}\cdot\vec{y}\right)\right)$
- t_0

$$i^* \xleftarrow{\$} \{1, \cdots, N\}$$

MPCitH protocol





commit →

← i^*

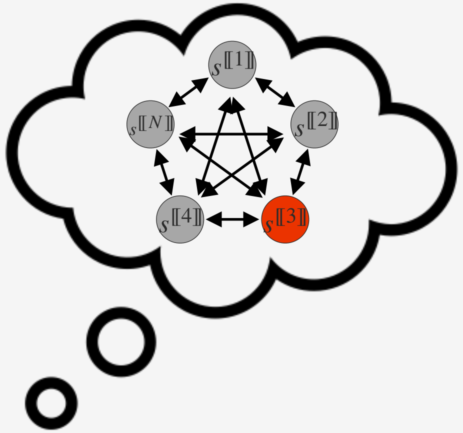
$\text{View}^{[\![i]\!]}$ for $i \neq i^*$ →

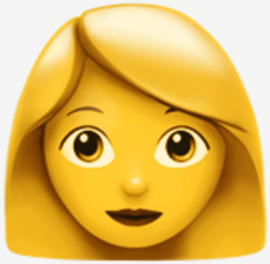
$i^* \xleftarrow{\$} \{1, \cdots, N\}$

<u>commit:</u>

- $\text{com}\left(\text{View}^{[\![i]\!]}\right)$
- $\left(X_1 + t_0\left(\vec{u}\cdot\vec{x}\right)\right), \left(Y_1 + t_0\left(\vec{v}\cdot\vec{y}\right)\right)$
- $\left(X_2 + t_0\left(\vec{v}\cdot\vec{x}\right)\right), \left(Y_2 + t_0\left(\vec{u}\cdot\vec{y}\right)\right)$
- t_0

MPCitH protocol





commit →

← i^*

$\mathrm{View}^{[\![i]\!]}$ for $i \neq i^*$ →

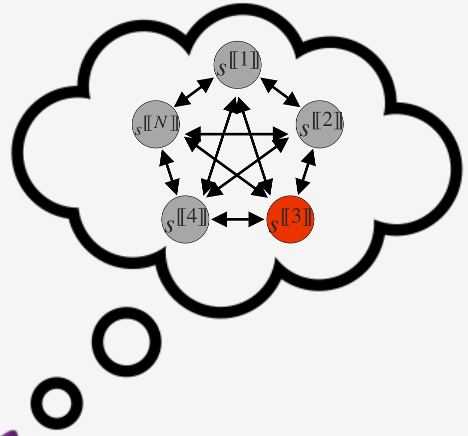
$i^* \xleftarrow{\$} \{1, \cdots, N\}$

<u>commit:</u>

- $\mathrm{com}\left(\mathrm{View}^{[\![i]\!]}\right)$
- $\left(X_1 + t_0\left(\vec{u} \cdot \vec{x}\right)\right), \left(Y_1 + t_0\left(\vec{v} \cdot \vec{y}\right)\right)$
- $\left(X_2 + t_0\left(\vec{v} \cdot \vec{x}\right)\right), \left(Y_2 + t_0\left(\vec{u} \cdot \vec{y}\right)\right)$
- t_0

Check if $F(t_0) = A + Bt_0$

MPCitH protocol



commit →

i^* ←

$\text{View}^{[\![i]\!]}$ for $i \neq i^*$ →

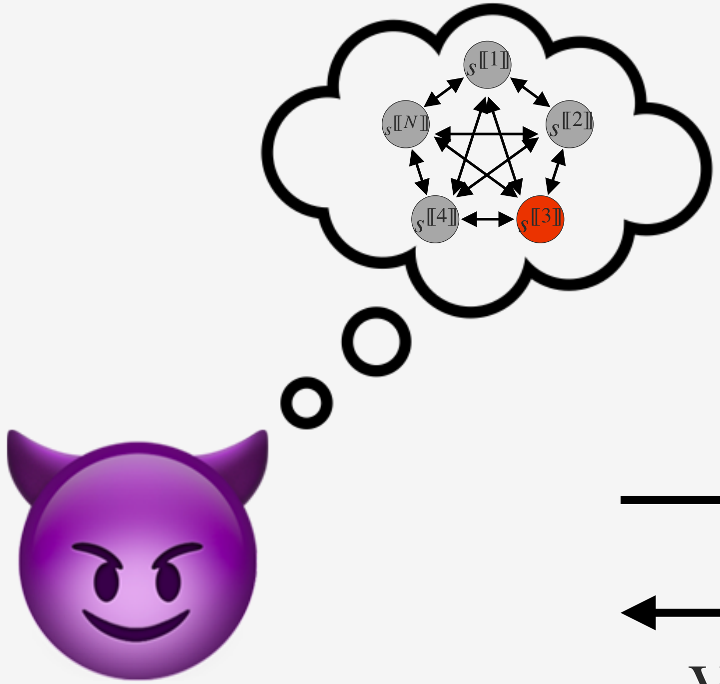
$i^* \xleftarrow{\$} \{1, \cdots, N\}$

Check if $F(t_0) = A + Bt_0$

<u>commit:</u>

- $\text{com}\left(\text{View}^{[\![i]\!]}\right)$
- $\left(X_1 + t_0\left(\vec{u} \cdot \vec{x}\right)\right), \left(Y_1 + t_0\left(\vec{v} \cdot \vec{y}\right)\right)$
- $\left(X_2 + t_0\left(\vec{v} \cdot \vec{x}\right)\right), \left(Y_2 + t_0\left(\vec{u} \cdot \vec{y}\right)\right)$
- t_0

MPCitH protocol



commit →

← i^*

$\text{View}^{[\![i]\!]}$ for $i \neq i^*$ →

$i^* \xleftarrow{\$} \{1, \cdots, N\}$

<u>commit:</u>

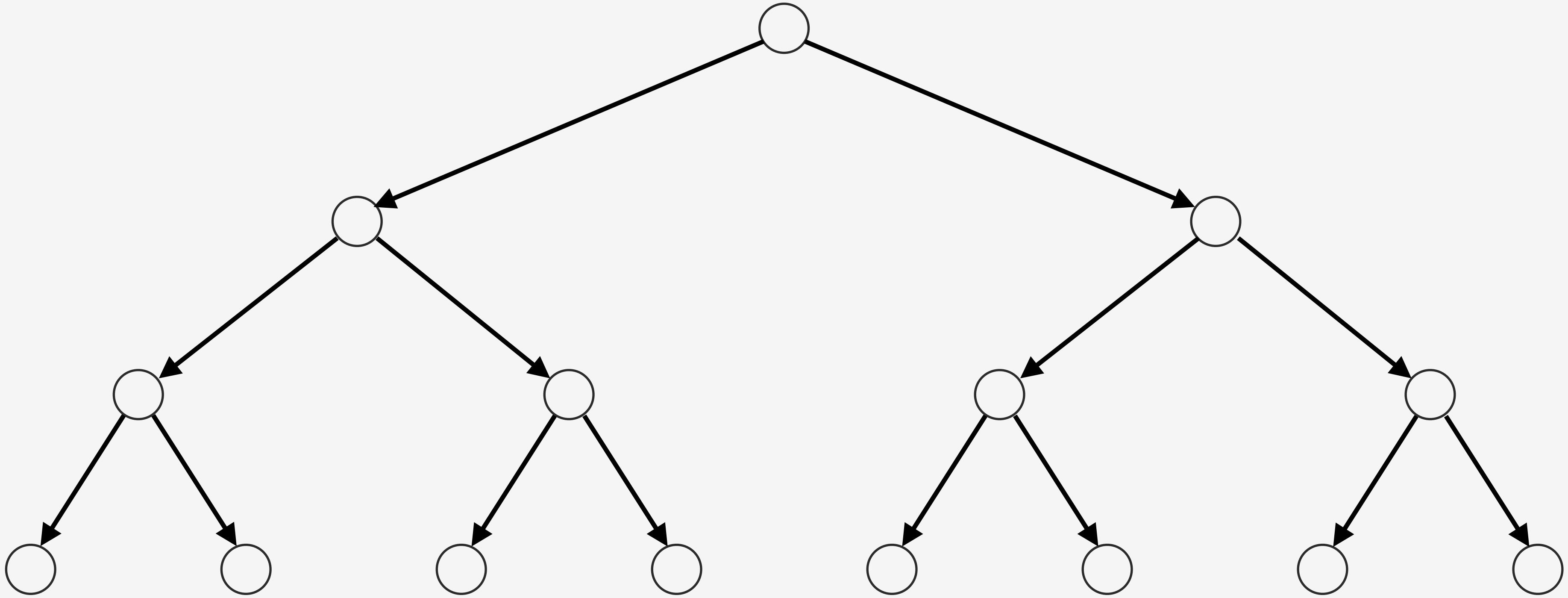
- $\text{com}\left(\text{View}^{[\![i]\!]}\right)$
- $\left(X_1 + t_0\left(\vec{u}\cdot\vec{x}\right)\right), \left(Y_1 + t_0\left(\vec{v}\cdot\vec{y}\right)\right)$
- $\left(X_2 + t_0\left(\vec{v}\cdot\vec{x}\right)\right), \left(Y_2 + t_0\left(\vec{u}\cdot\vec{y}\right)\right)$
- t_0

Soundness error $\dfrac{1}{N} + \dfrac{2}{q^k}$

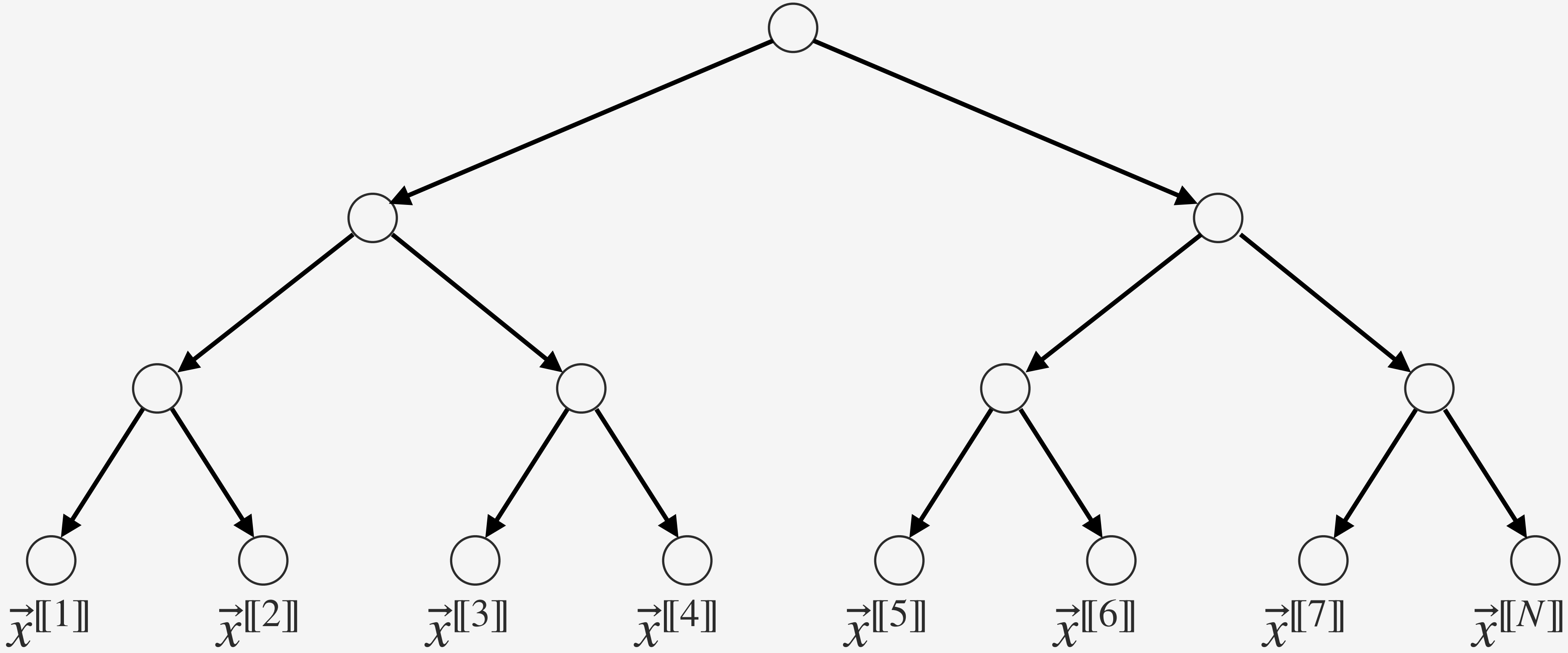
Check if $F(t_0) = A + Bt_0$

Commit using GGM trees

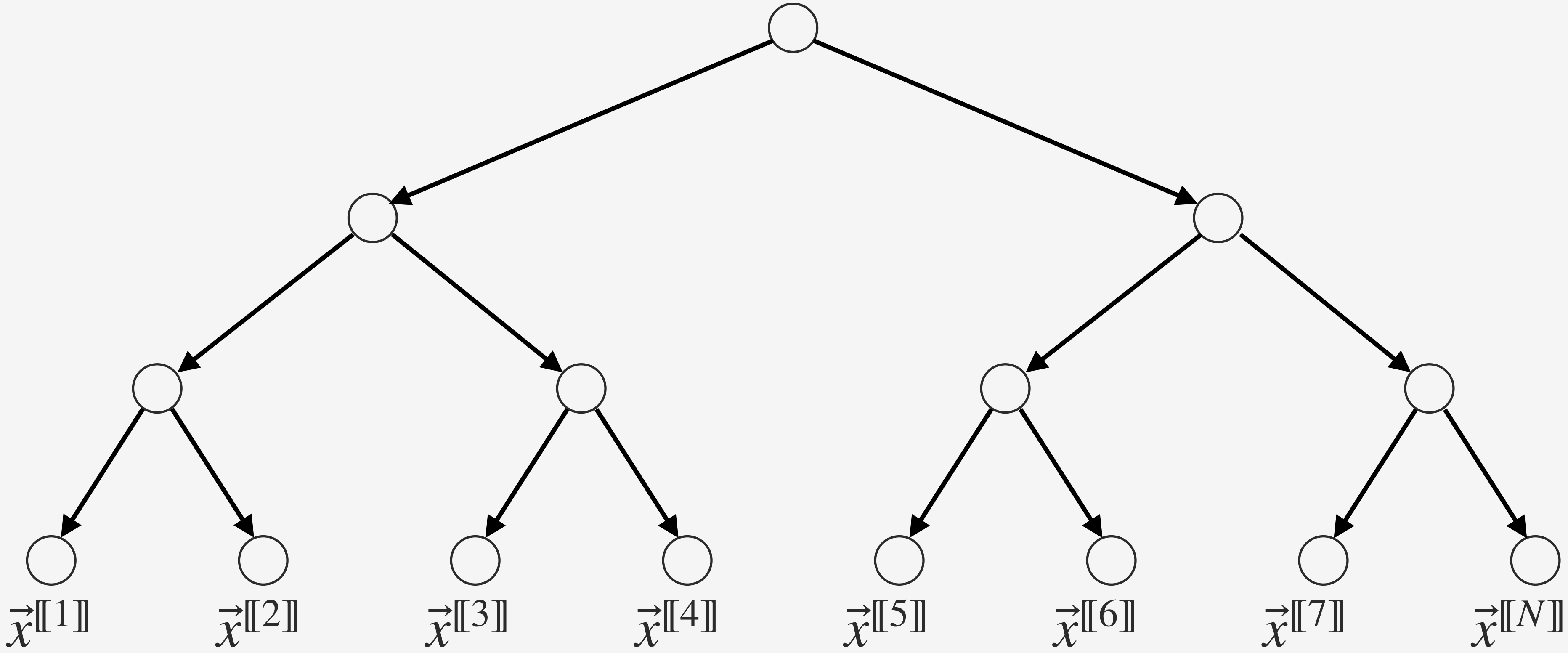
Commit using GGM trees



Commit using GGM trees



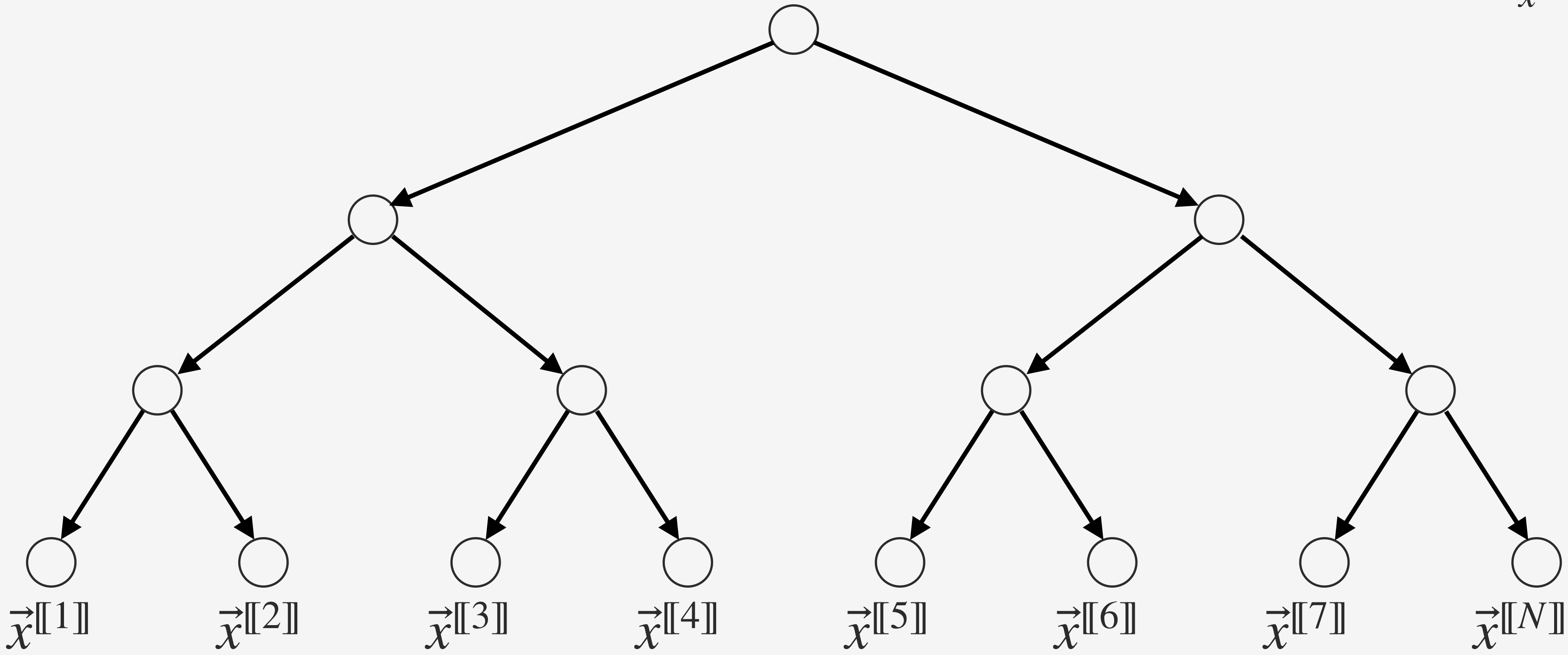
Commit using GGM trees



Derive $\vec{y}^{[\![i]\!]}, X_1^{[\![i]\!]}, X_2^{[\![i]\!]}, Y_1^{[\![i]\!]}, Y_2^{[\![i]\!]}, A^{[\![i]\!]}, B^{[\![i]\!]}$

Commit using GGM trees

$$\delta_{\vec{x}} = \vec{x} - \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

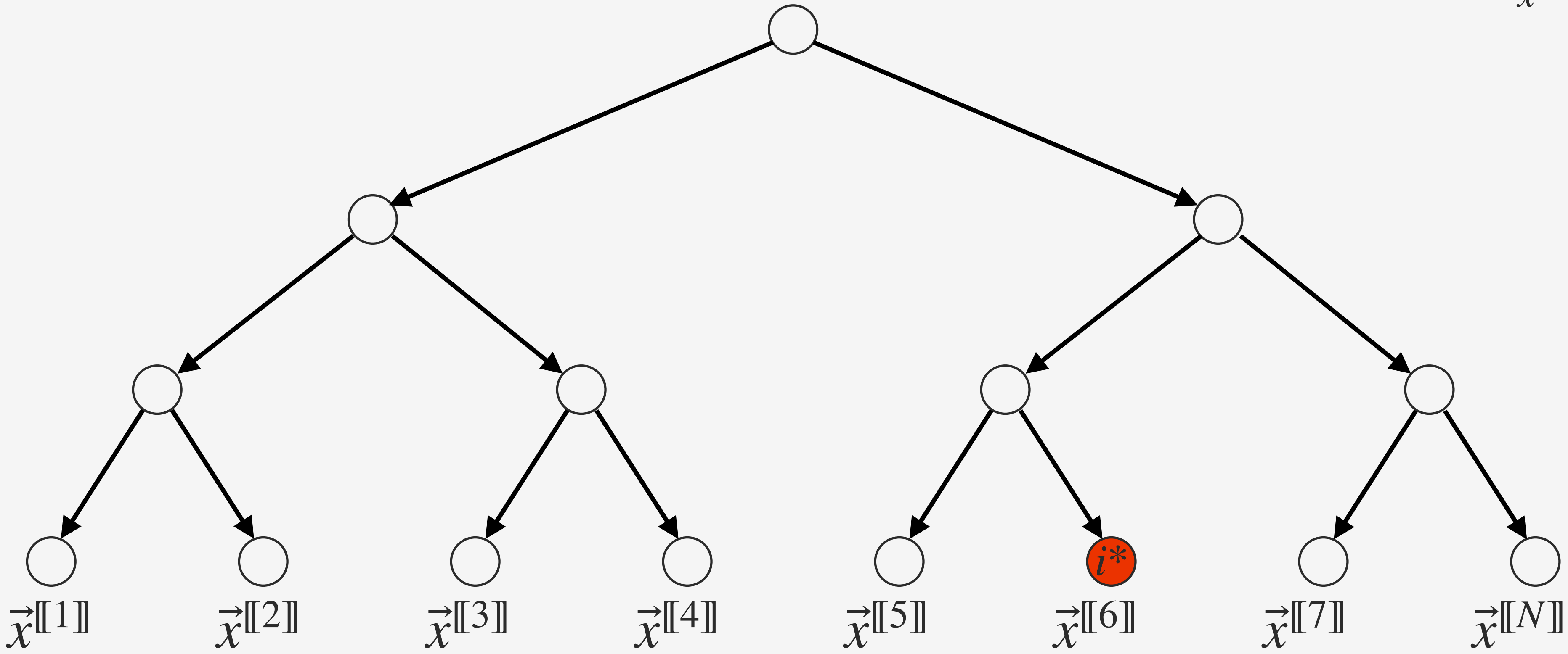


Derive $\vec{y}^{[\![i]\!]}, X_1^{[\![i]\!]}, X_2^{[\![i]\!]}, Y_1^{[\![i]\!]}, Y_2^{[\![i]\!]}, A^{[\![i]\!]}, B^{[\![i]\!]}$

Include offsets $\delta_{\vec{x}}, \delta_{\vec{y}}, \delta_A, \delta_B$ in commit

Commit using GGM trees

$$\delta_{\vec{x}} = \vec{x} - \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

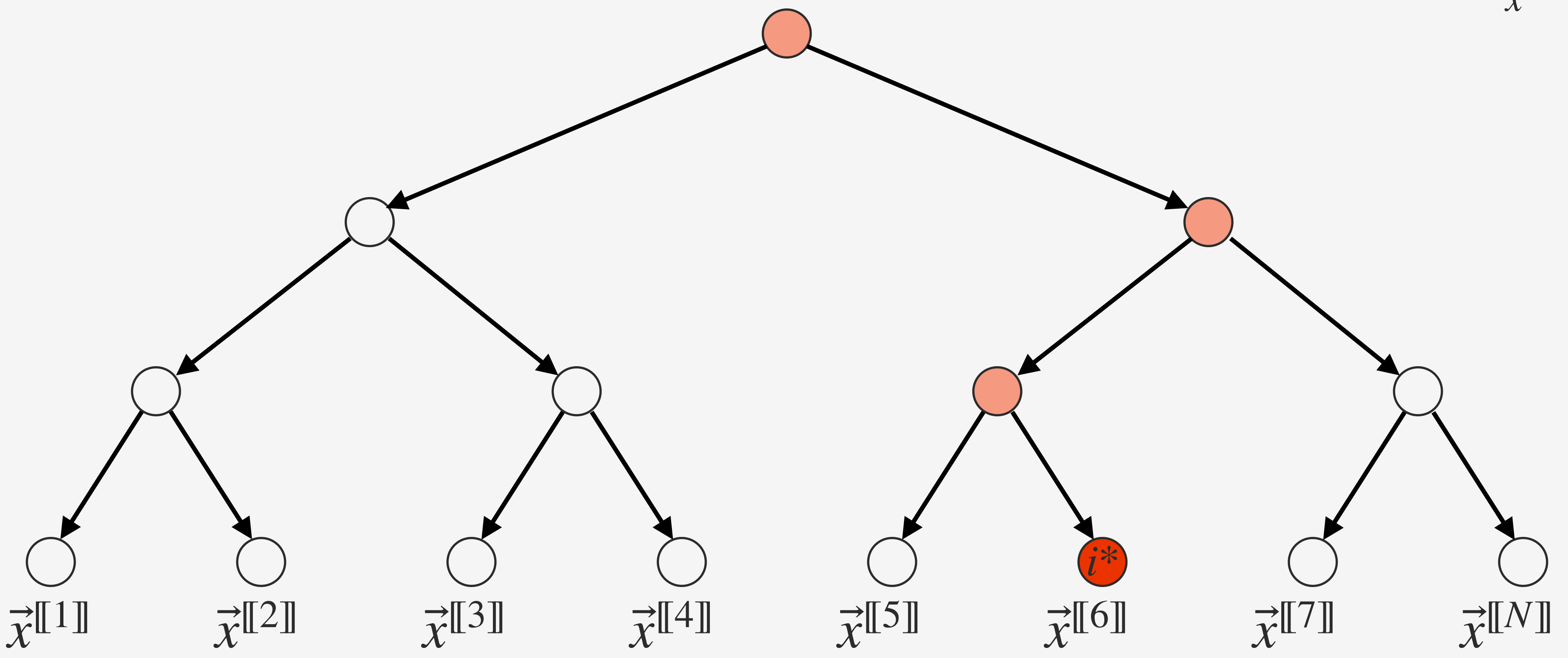


Derive $\vec{y}^{[\![i]\!]}, X_1^{[\![i]\!]}, X_2^{[\![i]\!]}, Y_1^{[\![i]\!]}, Y_2^{[\![i]\!]}, A^{[\![i]\!]}, B^{[\![i]\!]}$

Include offsets $\delta_{\vec{x}}, \delta_{\vec{y}}, \delta_A, \delta_B$ in commit

Commit using GGM trees

$$\delta_{\vec{x}} = \vec{x} - \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

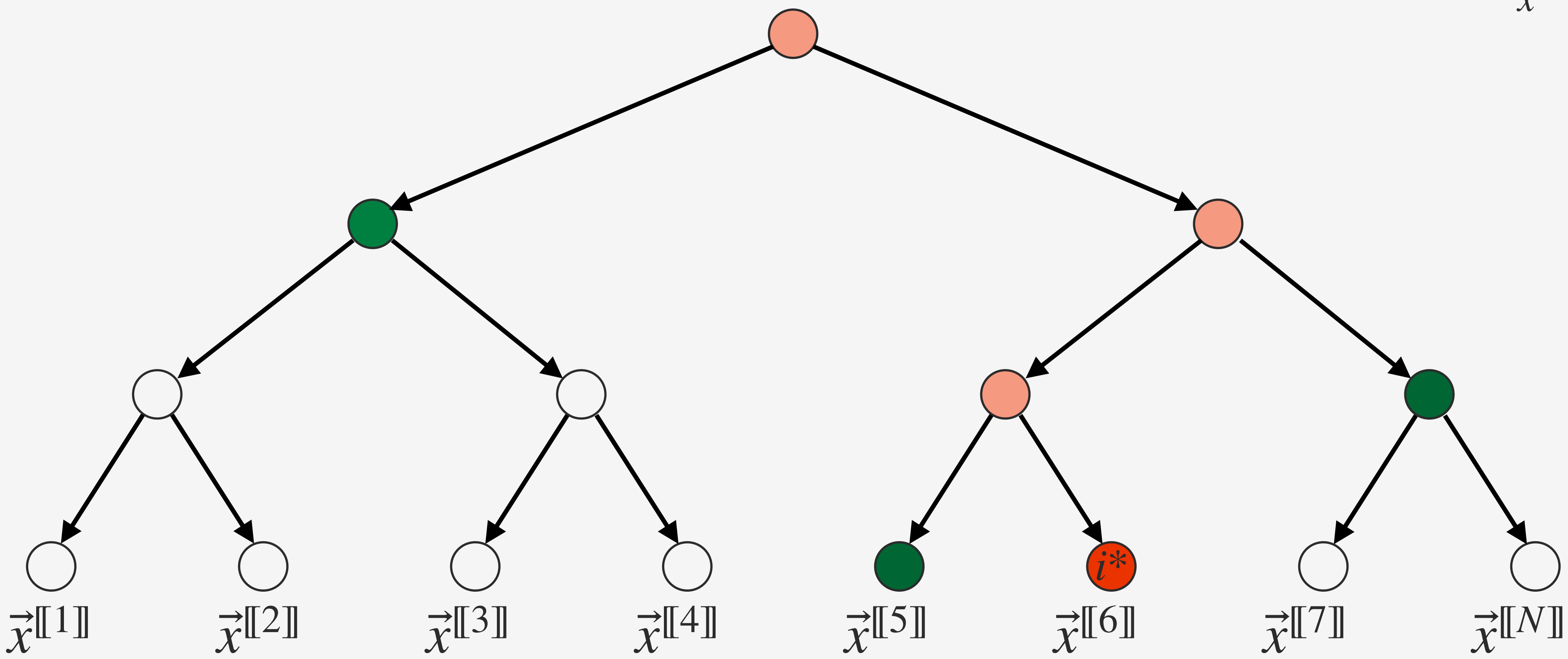


Derive $\vec{y}^{[\![i]\!]}, X_1^{[\![i]\!]}, X_2^{[\![i]\!]}, Y_1^{[\![i]\!]}, Y_2^{[\![i]\!]}, A^{[\![i]\!]}, B^{[\![i]\!]}$

Include offsets $\delta_{\vec{x}}, \delta_{\vec{y}}, \delta_A, \delta_B$ in commit

Commit using GGM trees

$$\delta_{\vec{x}} = \vec{x} - \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$

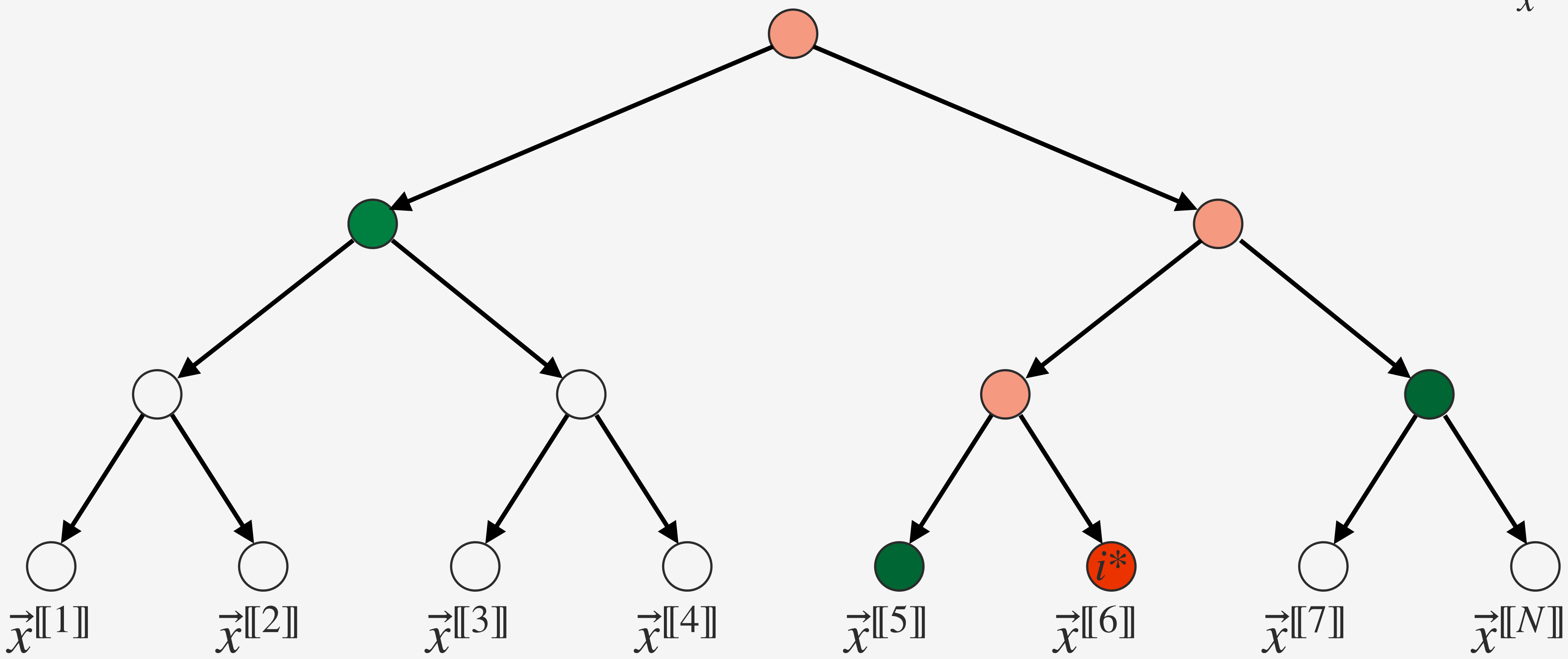


Derive $\vec{y}^{[\![i]\!]}, X_1^{[\![i]\!]}, X_2^{[\![i]\!]}, Y_1^{[\![i]\!]}, Y_2^{[\![i]\!]}, A^{[\![i]\!]}, B^{[\![i]\!]}$

Include offsets $\delta_{\vec{x}}, \delta_{\vec{y}}, \delta_A, \delta_B$ in commit

Commit using GGM trees

$$\delta_{\vec{x}} = \vec{x} - \sum_{i=1}^{N} \vec{x}^{[\![i]\!]}$$



Derive $\vec{y}^{[\![i]\!]}, X_1^{[\![i]\!]}, X_2^{[\![i]\!]}, Y_1^{[\![i]\!]}, Y_2^{[\![i]\!]}, A^{[\![i]\!]}, B^{[\![i]\!]}$

Include offsets $\delta_{\vec{x}}, \delta_{\vec{y}}, \delta_A, \delta_B$ in commit

Open $\log_2(N)$ nodes

Signature scheme

Signature scheme

τ repetitions

Signature scheme

τ repetitions

Fiat-Shamir transform $\rightarrow$ signature scheme

Signature scheme

τ repetitions

Fiat-Shamir transform → signature scheme

h_{com}

Signature scheme

τ repetitions

Fiat-Shamir transform → signature scheme

h_{com}

For each round:

Signature scheme

τ repetitions

Fiat-Shamir transform $\rightarrow$ signature scheme

h_{com}

For each round:

- $\delta_{\vec{x}}, \delta_{\vec{y}}, \delta_A, \delta_B$

Signature scheme

τ repetitions

Fiat-Shamir transform → signature scheme

h_{com}

For each round:

- $\delta_{\vec{x}}, \delta_{\vec{y}}, \delta_A, \delta_B$
- $\left(X_1 + t\left(\vec{u} \cdot \vec{x}\right)\right), \left(Y_1 + t\left(\vec{v} \cdot \vec{y}\right)\right)$

Signature scheme

τ repetitions

Fiat-Shamir transform → signature scheme

h_{com}

For each round:

- $\delta_{\vec{x}}, \delta_{\vec{y}}, \delta_A, \delta_B$
- $\left(X_1 + t\left(\vec{u}\cdot\vec{x}\right)\right), \left(Y_1 + t\left(\vec{v}\cdot\vec{y}\right)\right)$
- $\left(X_2 + t\left(\vec{v}\cdot\vec{x}\right)\right), \left(Y_2 + t\left(\vec{u}\cdot\vec{y}\right)\right)$

Signature scheme

τ repetitions

Fiat-Shamir transform → signature scheme

h_{com}

For each round:

- $\delta_{\vec{x}}, \delta_{\vec{y}}, \delta_A, \delta_B$
- $\left(X_1 + t\left(\vec{u} \cdot \vec{x}\right)\right), \left(Y_1 + t\left(\vec{v} \cdot \vec{y}\right)\right)$
- $\left(X_2 + t\left(\vec{v} \cdot \vec{x}\right)\right), \left(Y_2 + t\left(\vec{u} \cdot \vec{y}\right)\right)$
- t_0

Signature scheme

τ repetitions

Fiat-Shamir transform → signature scheme

h_{com}

For each round:

- $\delta_{\vec{x}}, \delta_{\vec{y}}, \delta_A, \delta_B$
- $\left(X_1 + t\left(\vec{u} \cdot \vec{x}\right)\right), \left(Y_1 + t\left(\vec{v} \cdot \vec{y}\right)\right)$
- $\left(X_2 + t\left(\vec{v} \cdot \vec{x}\right)\right), \left(Y_2 + t\left(\vec{u} \cdot \vec{y}\right)\right)$
- t_0
- GGM tree opening

Signature scheme

τ repetitions

Fiat-Shamir transform → signature scheme

h_{com}

For each round:

- $\delta_{\vec{x}}, \delta_{\vec{y}}, \delta_A, \delta_B$
- $\left(X_1 + t\left(\vec{u} \cdot \vec{x}\right)\right), \left(Y_1 + t\left(\vec{v} \cdot \vec{y}\right)\right)$
- $\left(X_2 + t\left(\vec{v} \cdot \vec{x}\right)\right), \left(Y_2 + t\left(\vec{u} \cdot \vec{y}\right)\right)$
- t_0
- GGM tree opening

$\rightarrow \sigma$

Signature size and running times

Signature size and running times

$\underline{\lambda = 128}$

Signature size and running times

$\underline{\lambda = 128}$

$q = 2$
$n = 130$
$k = 257$

Signature size and running times

$\underline{\lambda = 128}$

$q = 2$
$n = 130$
$k = 257$

N	τ	$\|\sigma\|$	t_{sign}	t_{verify}
2^8	16*	5.436 KB	0.76 ms	0.67 ms
2^9	15	5.340 KB	0.90 ms	0.81 ms
2^{10}	13	4.842 KB	1.05 ms	0.97 ms
2^{11}	12	4.665 KB	1.42 ms	1.34 ms
2^{12}	11	4.457 KB	2.10 ms	2.01 ms
2^{13}	10	4.216 KB	3.33 ms	3.23 ms
2^{15}	9	4.087 KB	11.85 ms	10.81 ms
2^{16}	8*	3.766 KB	19.32 ms	19.00 ms

Using an AMD EPYC 9374F running at 3.85 GHz
(*) $\lambda > 127.9999$

Signature size and running times

$\lambda = 128$

$q = 2$
$n = 130$
$k = 257$

Artifact versions:

N	τ	$\lvert\sigma\rvert$	t_{sign}	t_{verify}
2^8	16*	5.436 KB	0.76 ms	0.67 ms
2^9	15	5.340 KB	0.90 ms	0.81 ms
2^{10}	13	4.842 KB	1.05 ms	0.97 ms
2^{11}	12	4.665 KB	1.42 ms	1.34 ms
2^{12}	11	4.457 KB	2.10 ms	2.01 ms
2^{13}	10	4.216 KB	3.33 ms	3.23 ms
2^{15}	9	4.087 KB	11.85 ms	10.81 ms
2^{16}	8*	3.766 KB	19.32 ms	19.00 ms

Using an AMD EPYC 9374F running at 3.85 GHz
(*) $\lambda > 127.9999$

Signature size and running times

$\lambda = 128$

$q = 2$
$n = 130$
$k = 257$

Artifact versions:
- Correlated GGM trees

N	τ	$\|\sigma\|$	t_{sign}	t_{verify}
2^8	16*	5.436 KB	0.76 ms	0.67 ms
2^9	15	5.340 KB	0.90 ms	0.81 ms
2^{10}	13	4.842 KB	1.05 ms	0.97 ms
2^{11}	12	4.665 KB	1.42 ms	1.34 ms
2^{12}	11	4.457 KB	2.10 ms	2.01 ms
2^{13}	10	4.216 KB	3.33 ms	3.23 ms
2^{15}	9	4.087 KB	11.85 ms	10.81 ms
2^{16}	8*	3.766 KB	19.32 ms	19.00 ms

Using an AMD EPYC 9374F running at 3.85 GHz
(*) $\lambda > 127.9999$

Signature size and running times

$\lambda = 128$

$q = 2$
$n = 130$
$k = 257$

Artifact versions:
- Correlated GGM trees
- AES

N	τ	$\|\sigma\|$	t_{sign}	t_{verify}
2^8	16*	5.436 KB	0.76 ms	0.67 ms
2^9	15	5.340 KB	0.90 ms	0.81 ms
2^{10}	13	4.842 KB	1.05 ms	0.97 ms
2^{11}	12	4.665 KB	1.42 ms	1.34 ms
2^{12}	11	4.457 KB	2.10 ms	2.01 ms
2^{13}	10	4.216 KB	3.33 ms	3.23 ms
2^{15}	9	4.087 KB	11.85 ms	10.81 ms
2^{16}	8*	3.766 KB	19.32 ms	19.00 ms

Using an AMD EPYC 9374F running at 3.85 GHz
(*) $\lambda > 127.9999$

Signature size and running times

$\lambda = 128$

$q = 2$
$n = 130$
$k = 257$

Artifact versions:
- Correlated GGM trees
- AES
- Fast hypercube Folding

N	τ	$\|\sigma\|$	t_{sign}	t_{verify}
2^8	16*	5.436 KB	0.76 ms	0.67 ms
2^9	15	5.340 KB	0.90 ms	0.81 ms
2^{10}	13	4.842 KB	1.05 ms	0.97 ms
2^{11}	12	4.665 KB	1.42 ms	1.34 ms
2^{12}	11	4.457 KB	2.10 ms	2.01 ms
2^{13}	10	4.216 KB	3.33 ms	3.23 ms
2^{15}	9	4.087 KB	11.85 ms	10.81 ms
2^{16}	8*	3.766 KB	19.32 ms	19.00 ms

Using an AMD EPYC 9374F running at 3.85 GHz
(*) $\lambda > 127.9999$

Thank you

ePrint 2023/1685

Artifact