The Measure-and-Reprogram Technique 2.0: Multi-Round Fiat-Shamir and More

CWI
Centrum Wiskunde & Informatica

QuSoft
Research Center for Quantum Software

Jelle Don, CWI Amsterdam
Joint work with Serge Fehr and Christian Majenz

Universiteit Leiden
Mathematisch Instituut

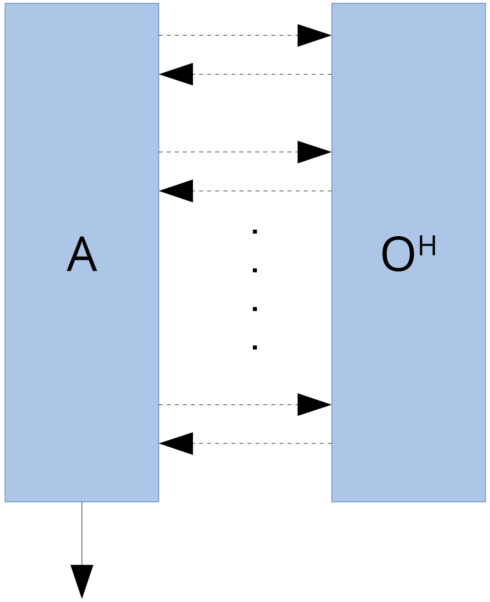
Introduction

- Proving *Fiat-Shamir* digital signatures and ZK proof systems secure against quantum attackers
- Secure in the *Quantum Random-Oracle Model* (QROM)
- Extending an existing QROM technique to a larger class of applications, notably
  - *Multi-round Fiat-Shamir signatures (Example: MQDSS)*
  - *Bulletproofs*
  - *Sequential-OR Proofs*
- Proving tightness

Quantum Random-Oracle Model

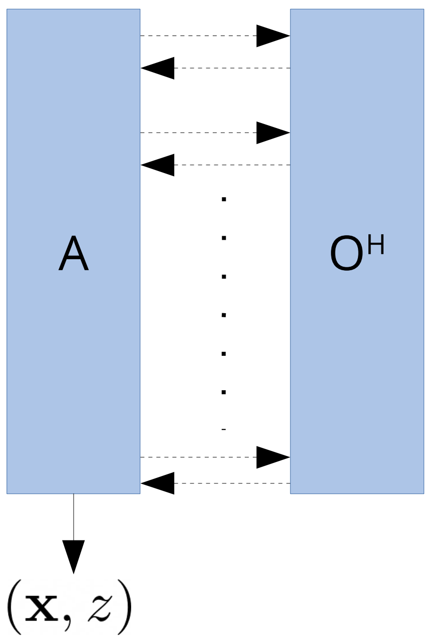
- We model the public hash function as an external random-oracle

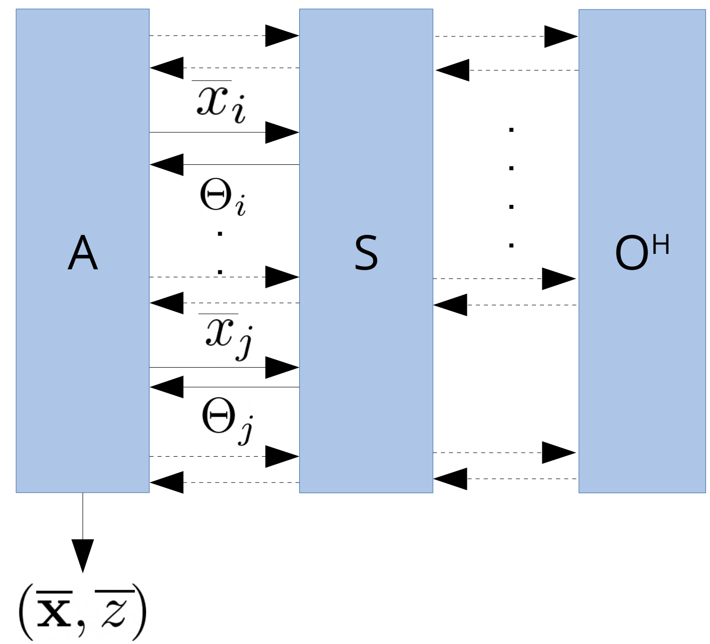
- All parties have quantum query access, which means that
  - The function cannot be computed locally
  - Parties can query a superposition of inputs



Main results

- Multi-input reprogrammability of the QROM:

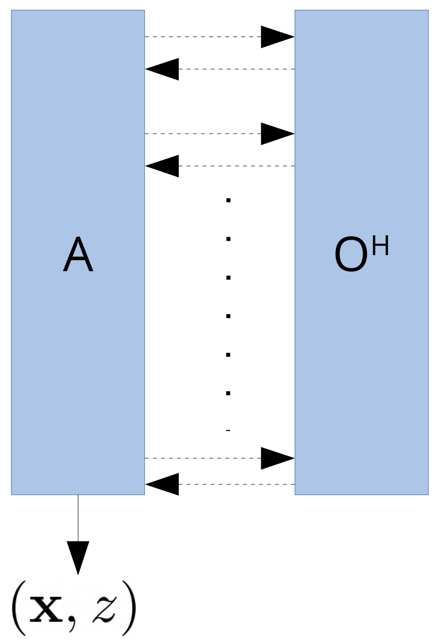


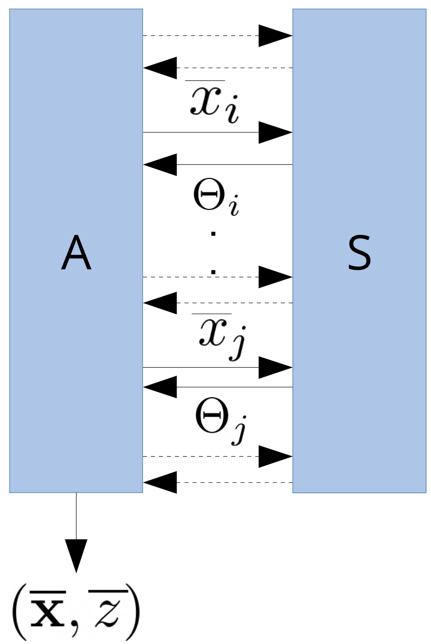


$$\frac{\Pr[\mathbf{x} = \mathbf{x}_\circ \wedge V(\mathbf{x}, \mathbf{H}(\mathbf{x}), z)]}{O(q^{2n})} \leq \Pr\left[\overline{\mathbf{x}} = \mathbf{x}_\circ \wedge V(\overline{\mathbf{x}}, \boldsymbol{\Theta}, \overline{z})\right]$$

Main results

- Multi-input reprogrammability of the QROM:





$$\frac{\Pr[\mathbf{x} = \mathbf{x}_\circ \wedge V(\mathbf{x}, \mathbf{H}(\mathbf{x}), z)]}{O(q^{2n})} \leq \Pr\left[\overline{\mathbf{x}} = \mathbf{x}_\circ \wedge V(\overline{\mathbf{x}}, \boldsymbol{\Theta}, \overline{z})\right]$$

Main results

- Security of multi-round Fiat-Shamir in the QROM:

$$ADV_{FS[\Pi_n]} \leq O(q^{2n}) \cdot ADV_{\Pi_n}$$

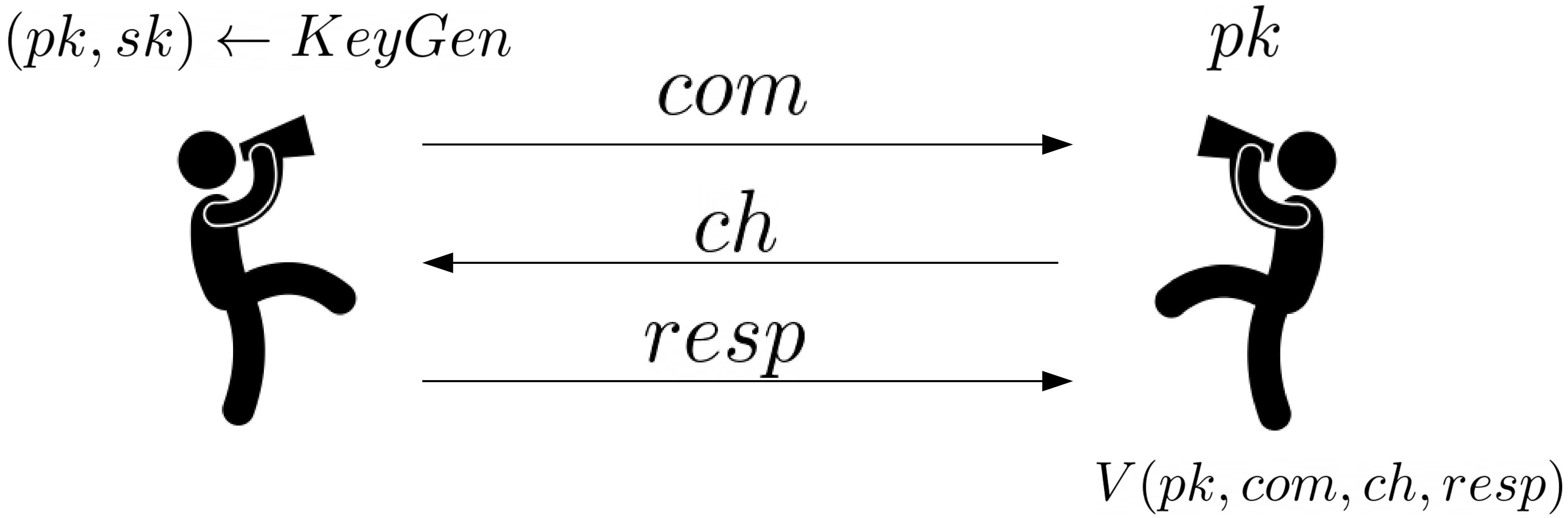
for any 2n+1-round public-coin proof system Π_n

- Tightness:
  - For typical 3-round schemes, there exists a FS attack that boosts the best interactive adversary by a factor q^2
  - The attack can be extended to an artificial multi-round scheme. This attack boosts the adversary's success by $n^{-2n}q^{2n}$

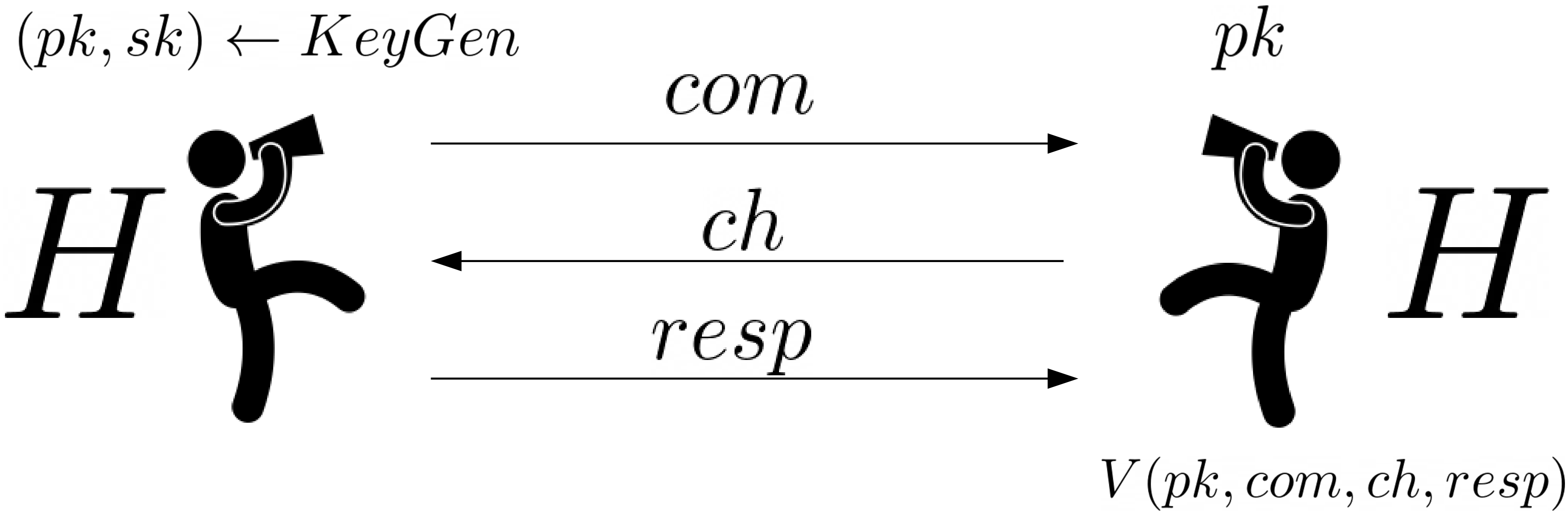
Outline of the talk

- Fiat-Shamir transformation
- How measure-and-reprogram 1.0 is applied
- Multi-round Fiat-Shamir; what we need
- Proof idea for multi-input reprogrammability
- Another application; sequential OR-proofs

The Fiat-Shamir transformation



The Fiat-Shamir transformation

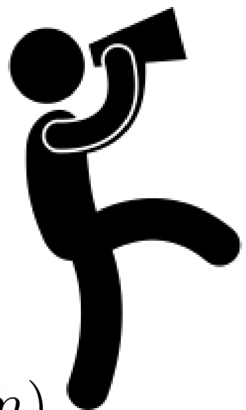


The Fiat-Shamir transformation

$(pk, sk) \leftarrow KeyGen$

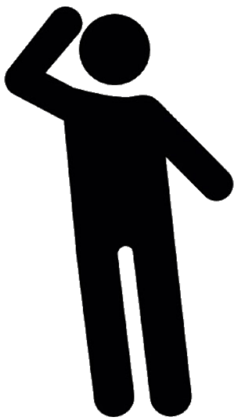
pk

H



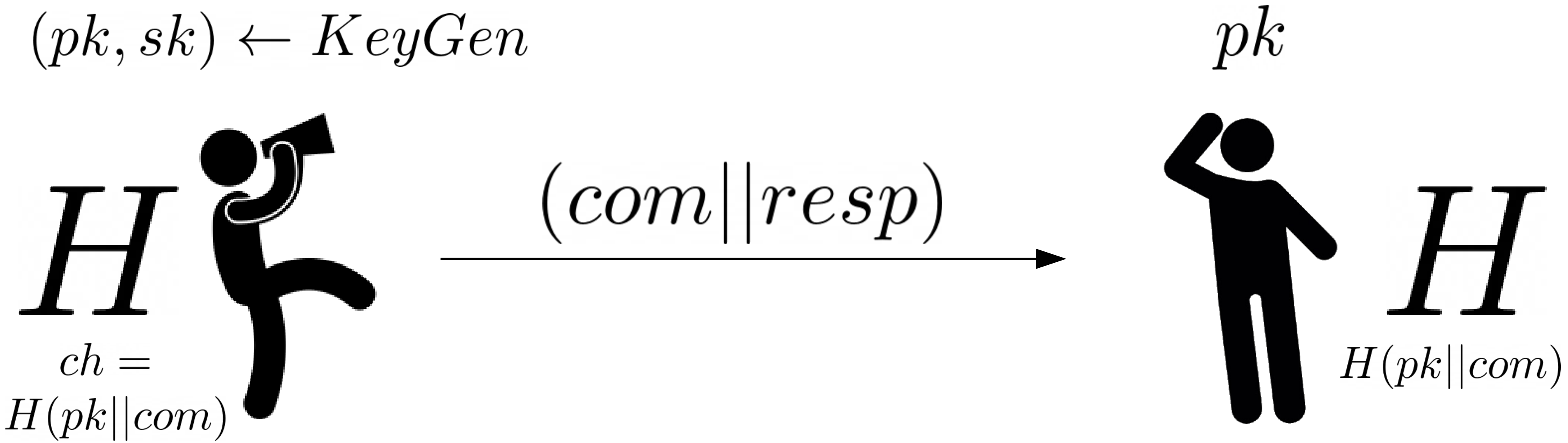
$ch = H(pk||com)$

$$\xrightarrow{(com||resp)}$$



H

The Fiat-Shamir transformation

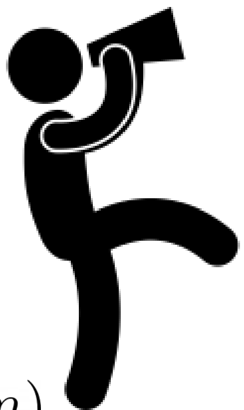


The Fiat-Shamir transformation

$(pk, sk) \leftarrow KeyGen$

pk

H



$(com||resp)$

H

$ch =$
$H(pk||com)$

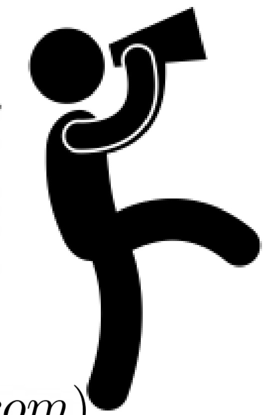
$H(pk||com)$

$V(pk, com, H(pk||com), resp)$

The Fiat-Shamir transformation

$(pk, sk) \leftarrow KeyGen$

pk

H 

$ch =$
$H(m||pk||com)$

$(m||com||resp)$

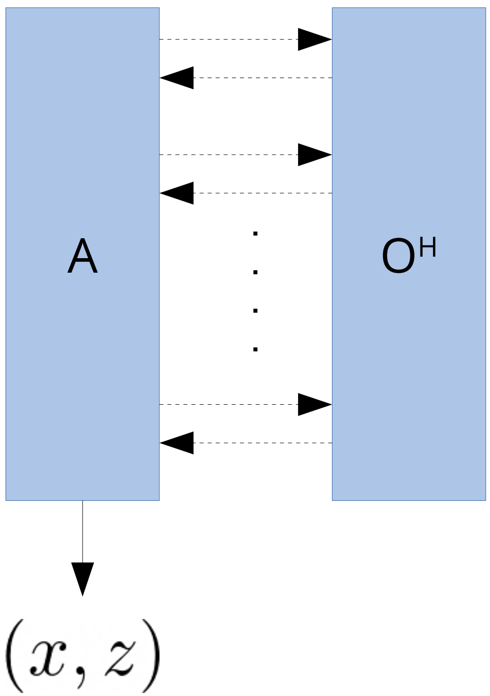
$\longrightarrow$

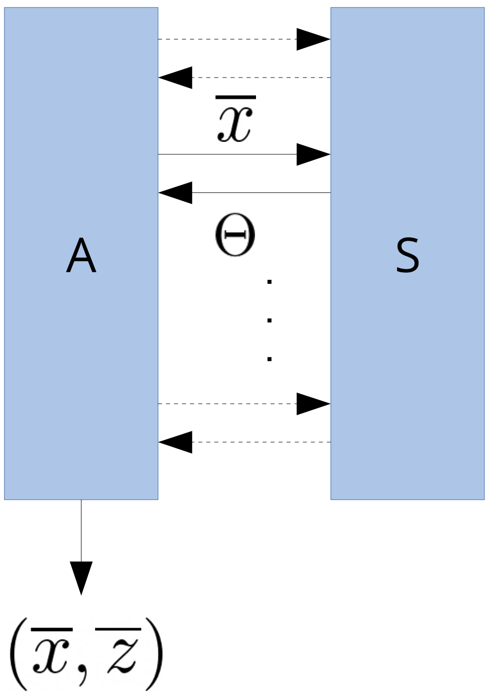
 H

$H(m||pk||com)$

$V(pk, com, H(m||pk||com), resp)$

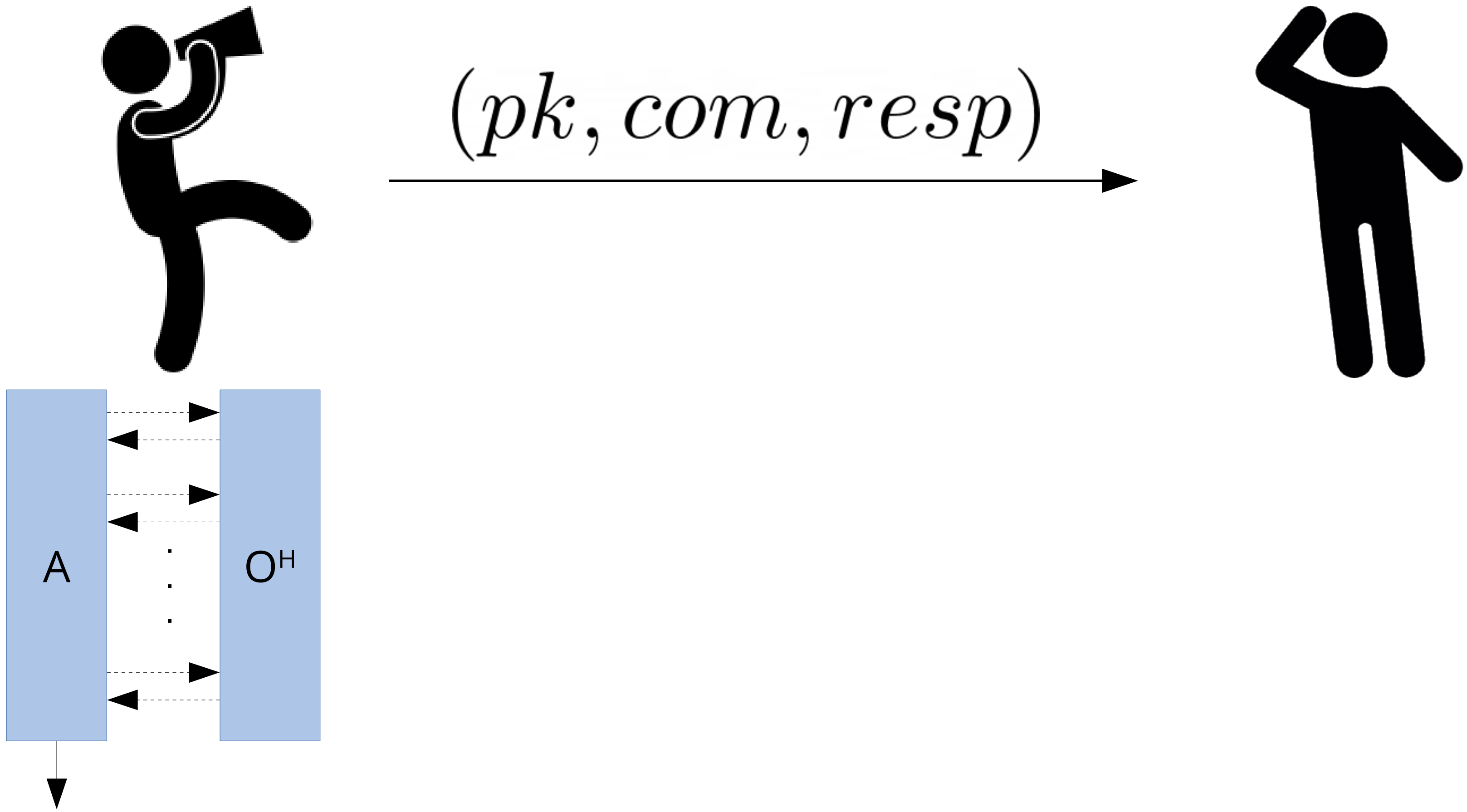
Measure-and-reprogram 1.0 [DFMS19]





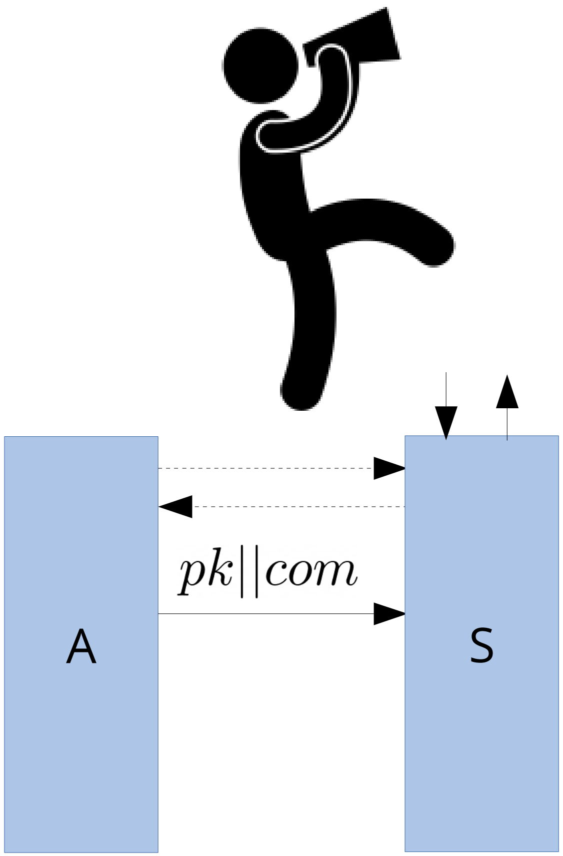
$$\frac{\Pr\left[x = x_\circ \wedge V(x, H(x), z)\right]}{O(q^2)} - \epsilon_{x_\circ} \leq \Pr\left[\overline{x} = x_\circ \wedge V(\overline{x}, \Theta, \overline{z})\right]$$

Application to plain Fiat-Shamir

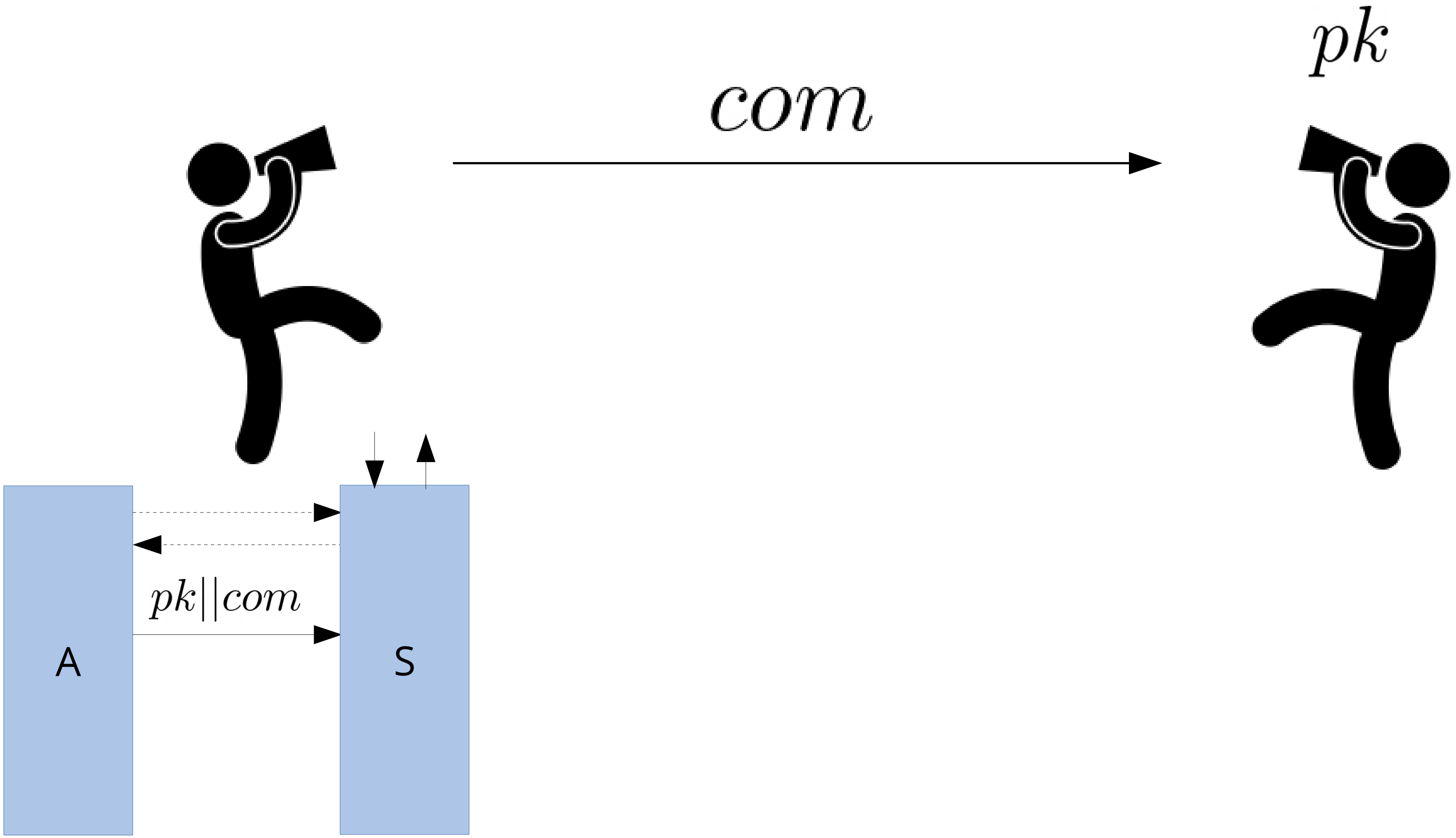


$$(pk, com, resp) = (x, z)$$

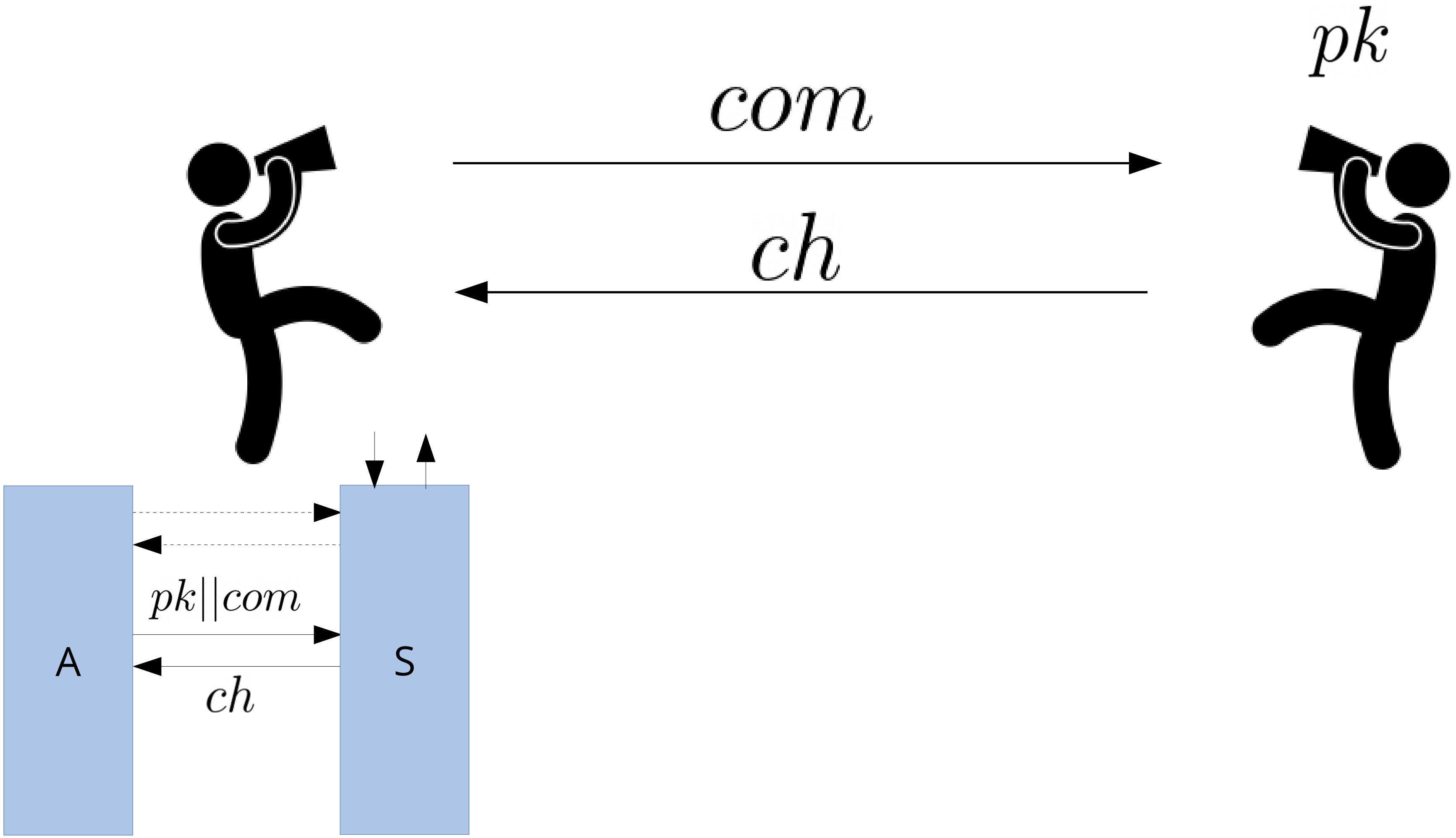
Application to plain Fiat-Shamir



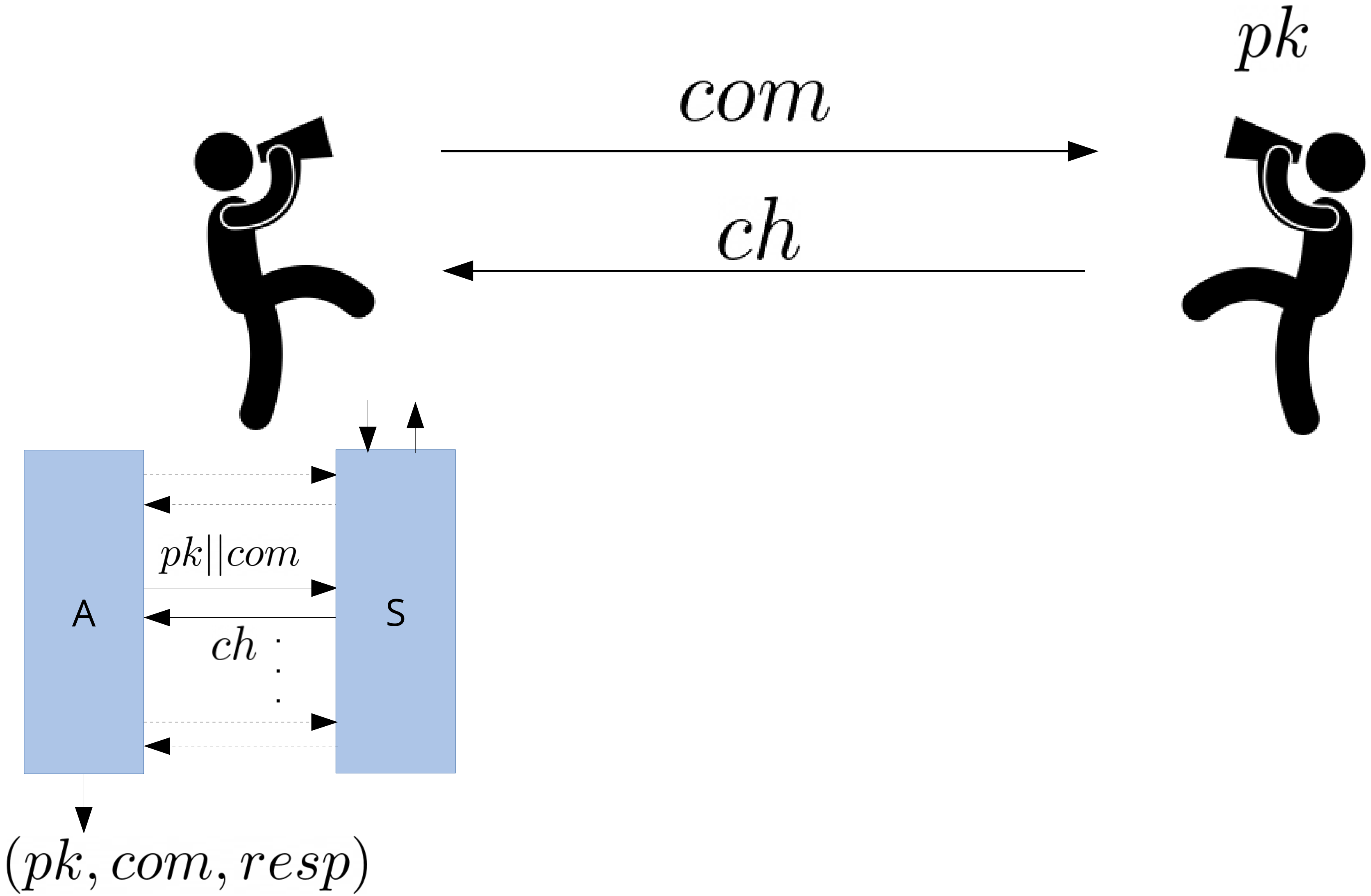
Application to plain Fiat-Shamir



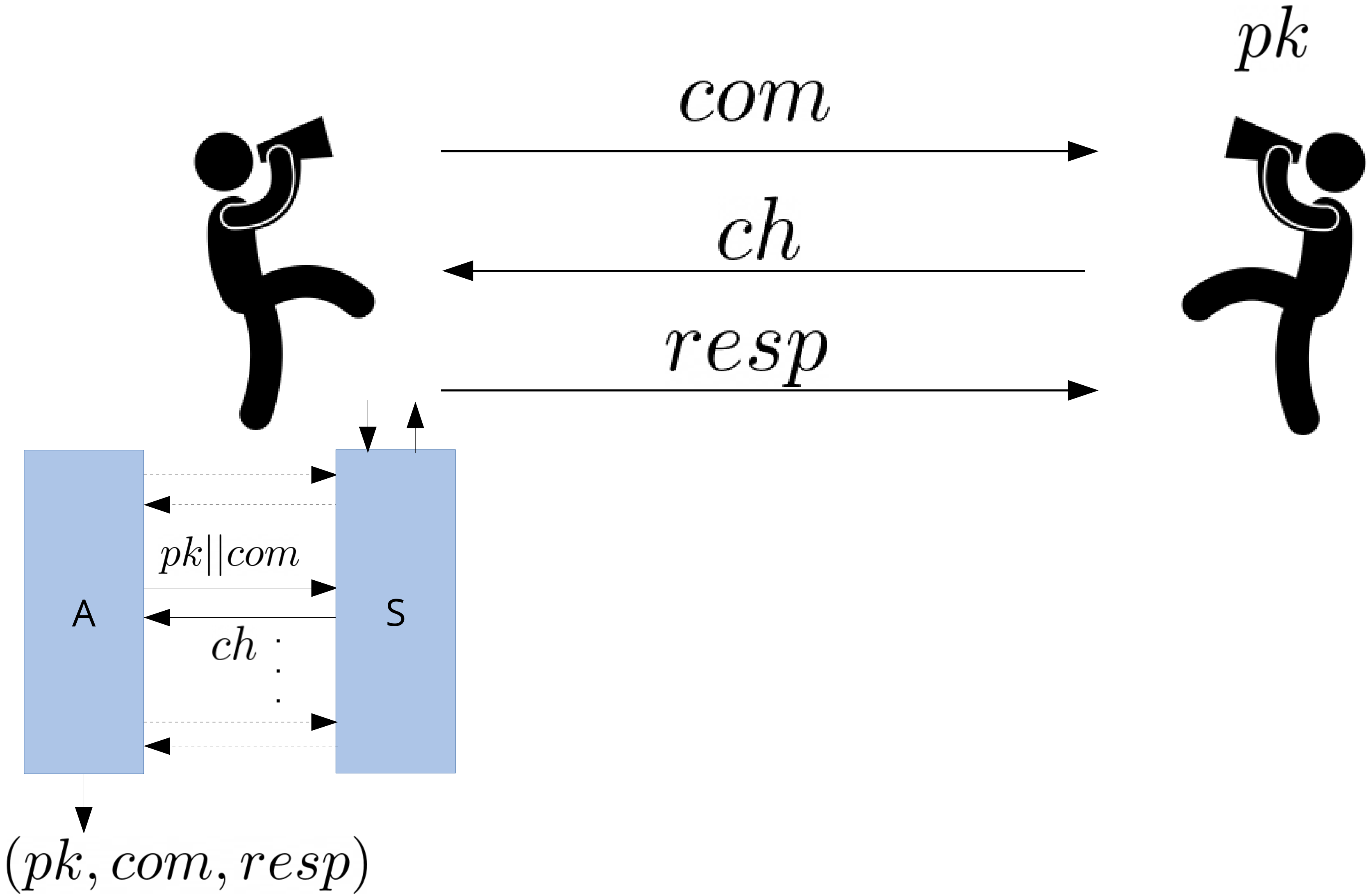
Application to plain Fiat-Shamir



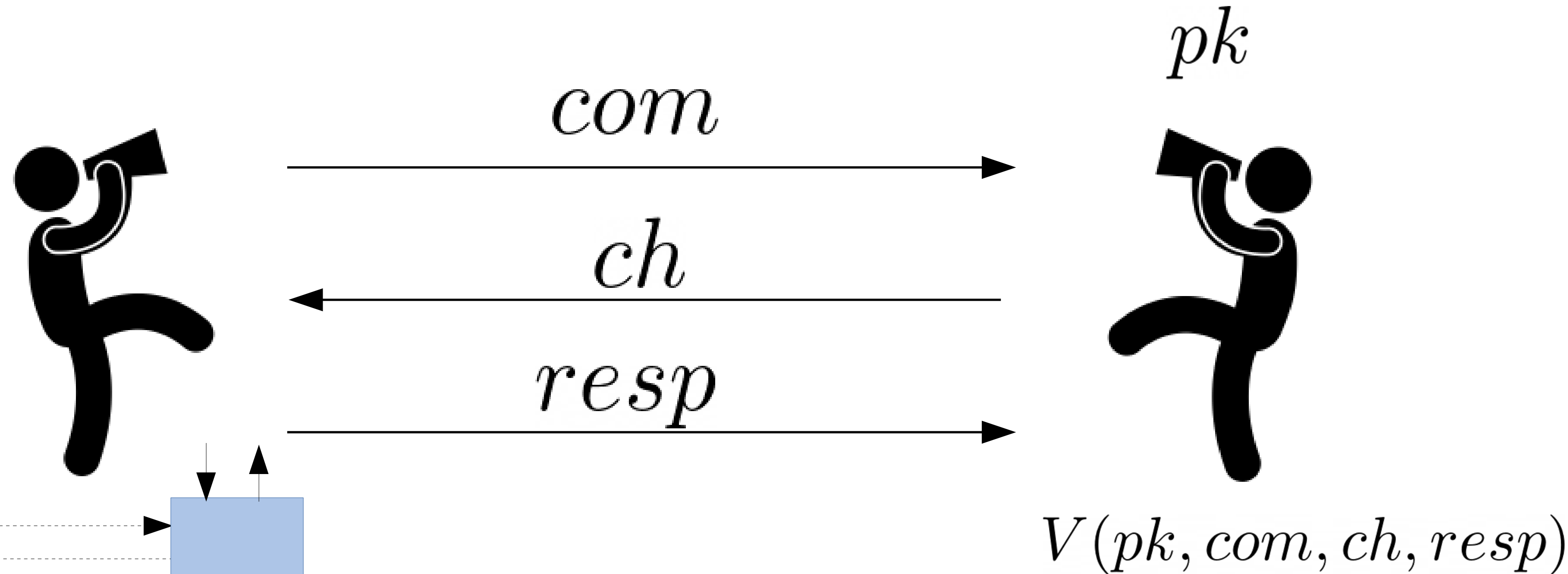
Application to plain Fiat-Shamir

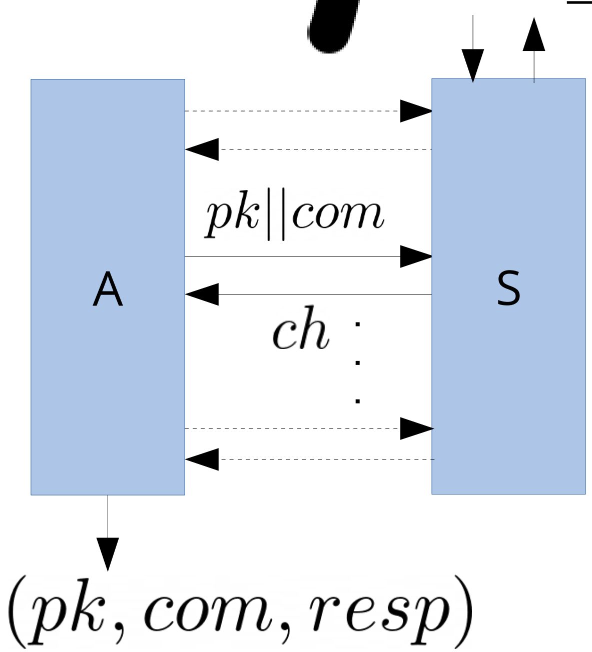


Application to plain Fiat-Shamir



Application to plain Fiat-Shamir





$$\frac{\Pr\left[x = x_\circ \wedge V(x, H(x), z)\right]}{O(q^2)} - \epsilon_{x_\circ} \leq \Pr\left[\overline{x} = x_\circ \wedge V(\overline{x}, \Theta, z)\right]$$

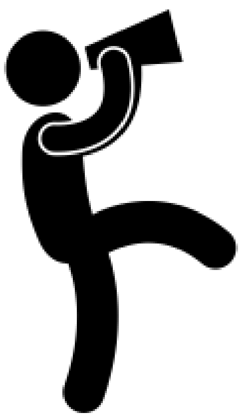
Multi-round Fiat-Shamir

- There exist 2n+1 round public coin interactive proof systems, for constant or logarithmic n.

- Generalized ‘multi-round’ FS transform takes away the interaction.

Multi-round Fiat-Shamir

$(pk, sk) \leftarrow KeyGen$ $\qquad\qquad$ pk



$$\xrightarrow{com_1}$$

$$\xleftarrow{ch_1}$$

$$\xrightarrow{com_2}$$

$$\vdots$$

$$\xrightarrow{com_n}$$

$$\xleftarrow{ch_n}$$

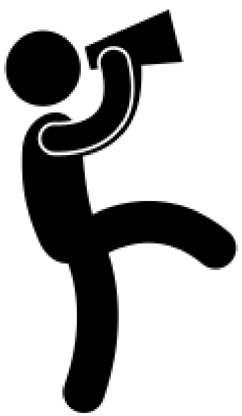
$$\xrightarrow{resp}$$

Multi-round Fiat-Shamir

$(pk, sk) \leftarrow KeyGen$

pk

$$\xrightarrow{\quad com_1 \quad}$$

H 

$$\xrightarrow{\quad com_2 \quad}$$

$$\vdots$$

$$\xrightarrow{\quad com_n \quad}$$

 H

$ch_i = H(com_i)$

$ch_i = H(com_i)$

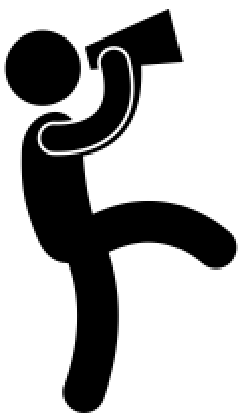
$$\xrightarrow{\quad resp \quad}$$

Multi-round Fiat-Shamir

$(pk, sk) \leftarrow KeyGen$

pk

H



$(com_1, \ldots, com_n, resp)$
$\longrightarrow$

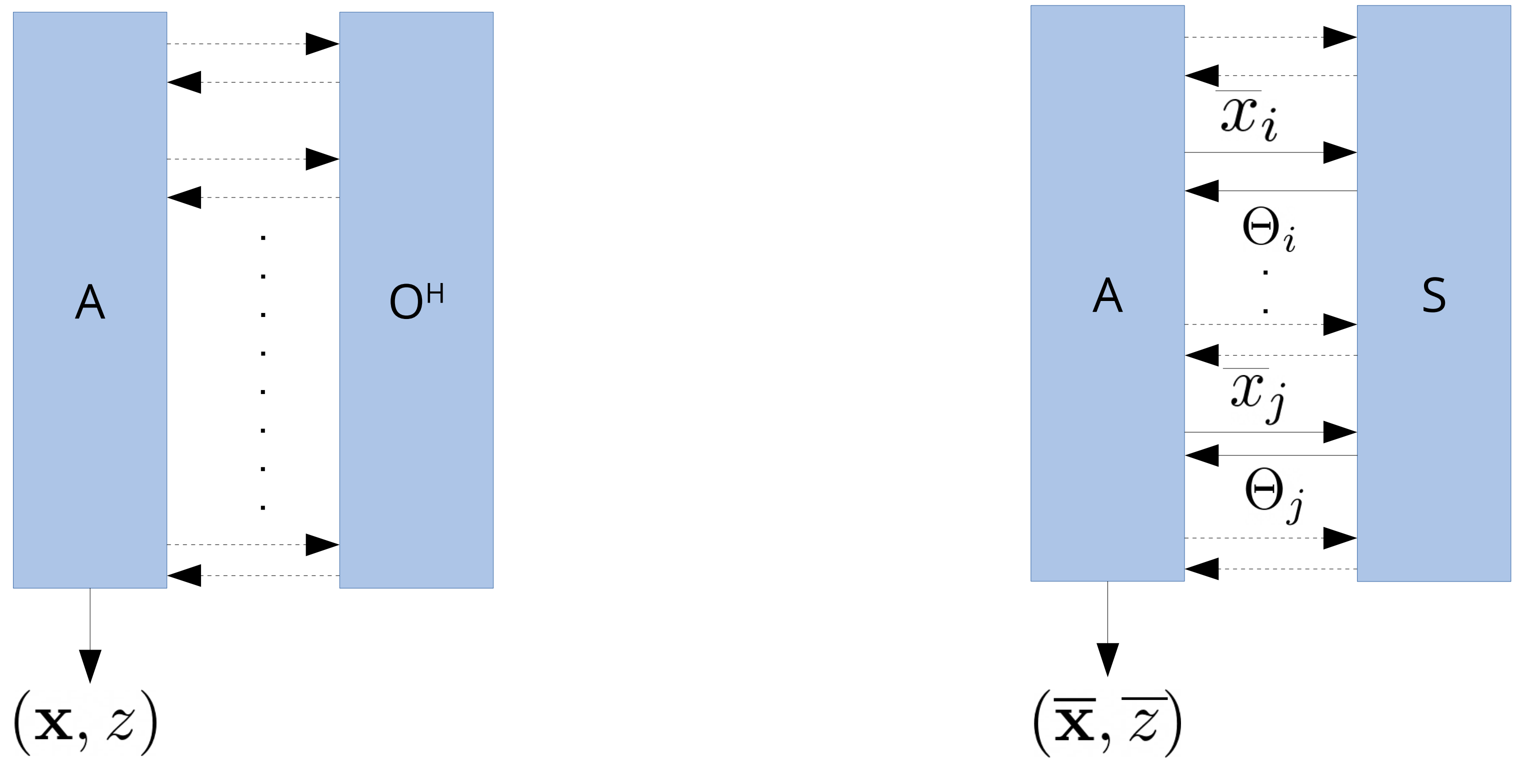
H

$ch_i = H(com_i)$

$ch_i = H(com_i)$

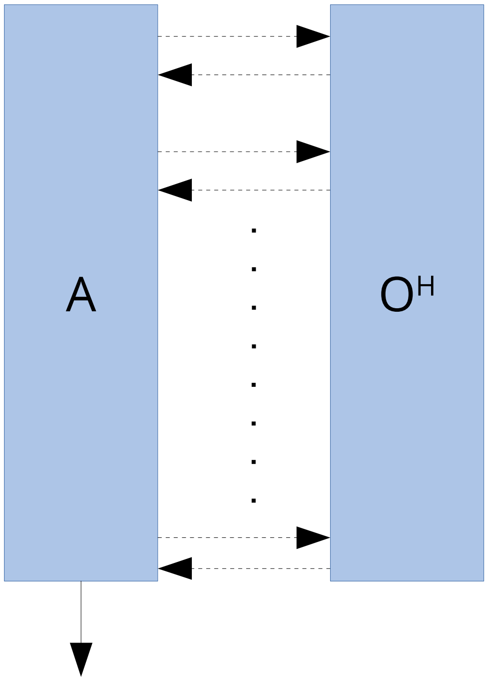
$V(x, \mathbf{com}, H(\mathbf{com}), resp)$

Multi-input reprogrammability



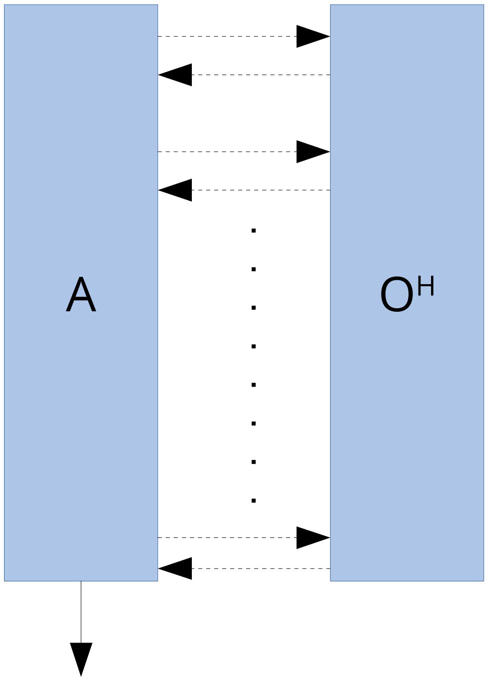
$$\frac{\Pr\left[\mathbf{x} = \mathbf{x}_\circ \wedge V(\mathbf{x}, H(\mathbf{x}), z)\right]}{?} - ? \leq \Pr\left[\overline{\mathbf{x}} = \overline{\mathbf{x}}_\circ \wedge V(\mathbf{x}, \mathbf{\Theta}, \overline{z})\right]$$

Multi-input reprogrammability



$(\mathbf{x}, z)$

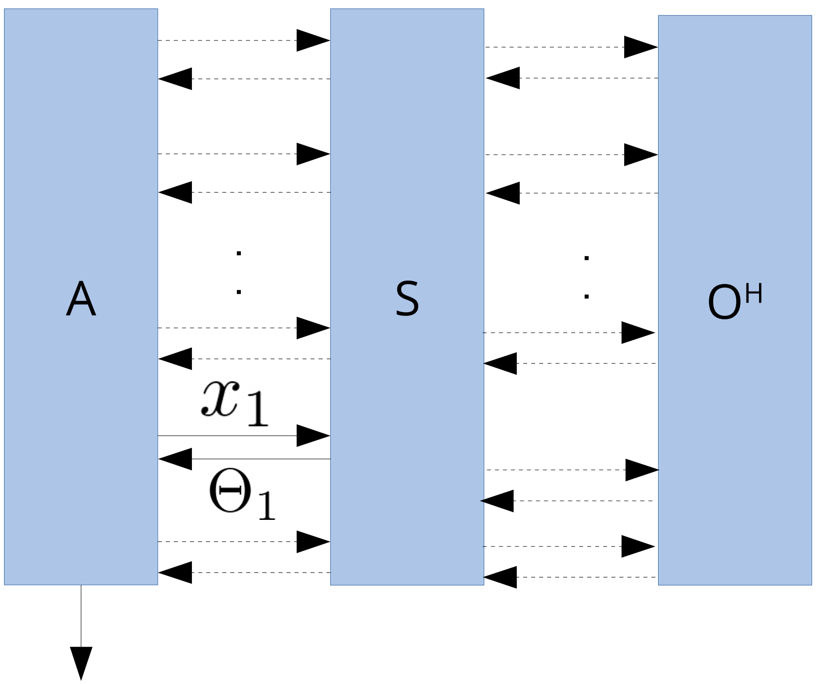
Multi-input reprogrammability



$$(x_1, z')$$

$$z' := (x_2, \ldots, x_n, z)$$

Multi-input reprogrammability

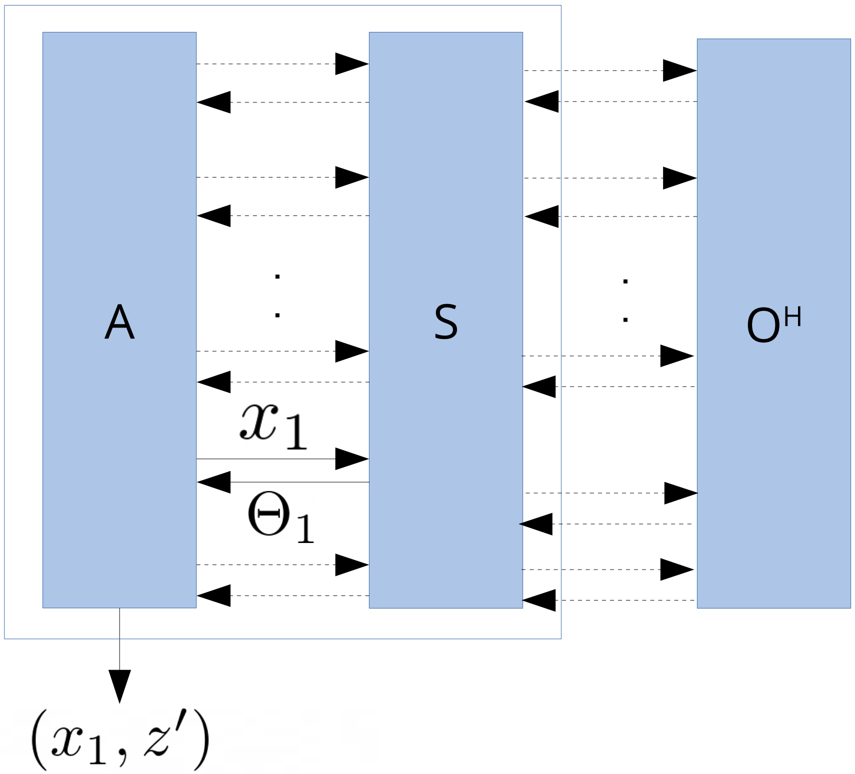


(x_1, z')

$z' := (x_2, \ldots, x_n, z)$

$$V(x_1, \Theta_1, x_2, H(x_2), \ldots, x_n, H(x_n), z)$$

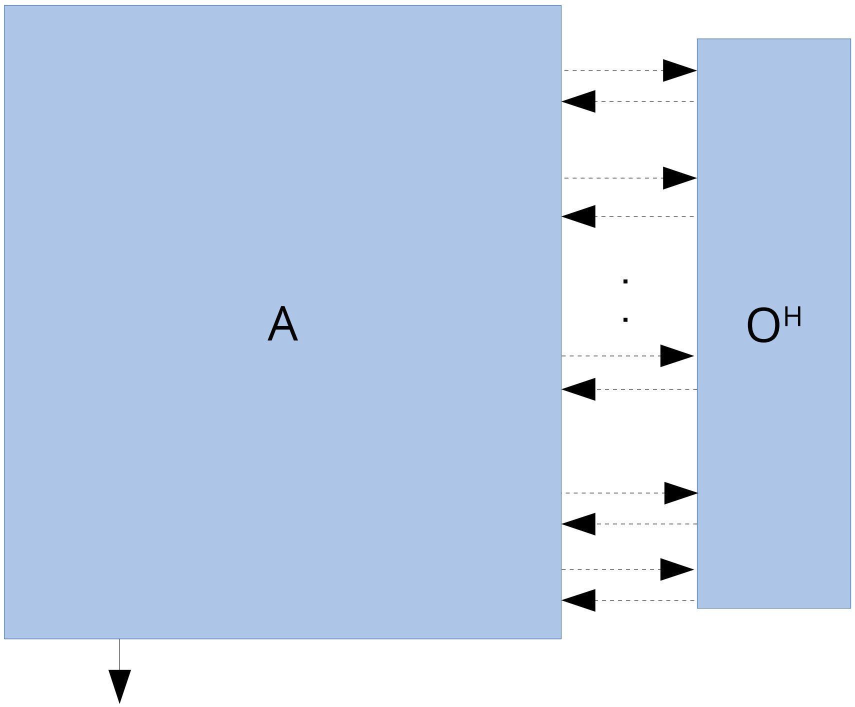
Multi-input reprogrammability



$$z' := (x_2, \ldots, x_n, z)$$

$$V(x_1, \Theta_1, x_2, H(x_2), \ldots, x_n, H(x_n), z)$$

Multi-input reprogrammability

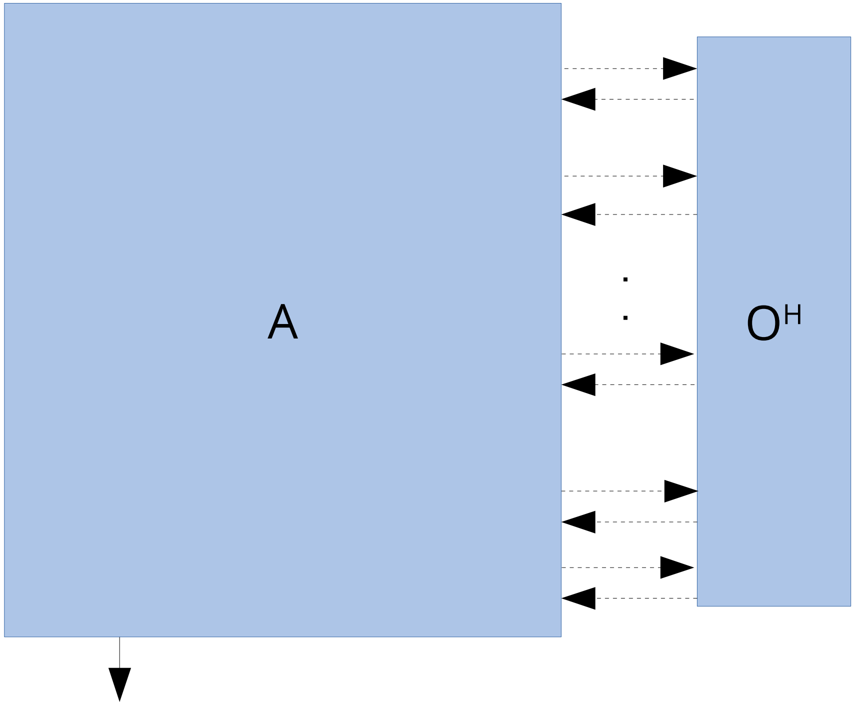


$$(x_1, z')$$

$$z' := (x_2, \ldots, x_n, z)$$

$$V(x_1, \Theta_1, x_2, H(x_2), \ldots, x_n, H(x_n), z)$$

Multi-input reprogrammability

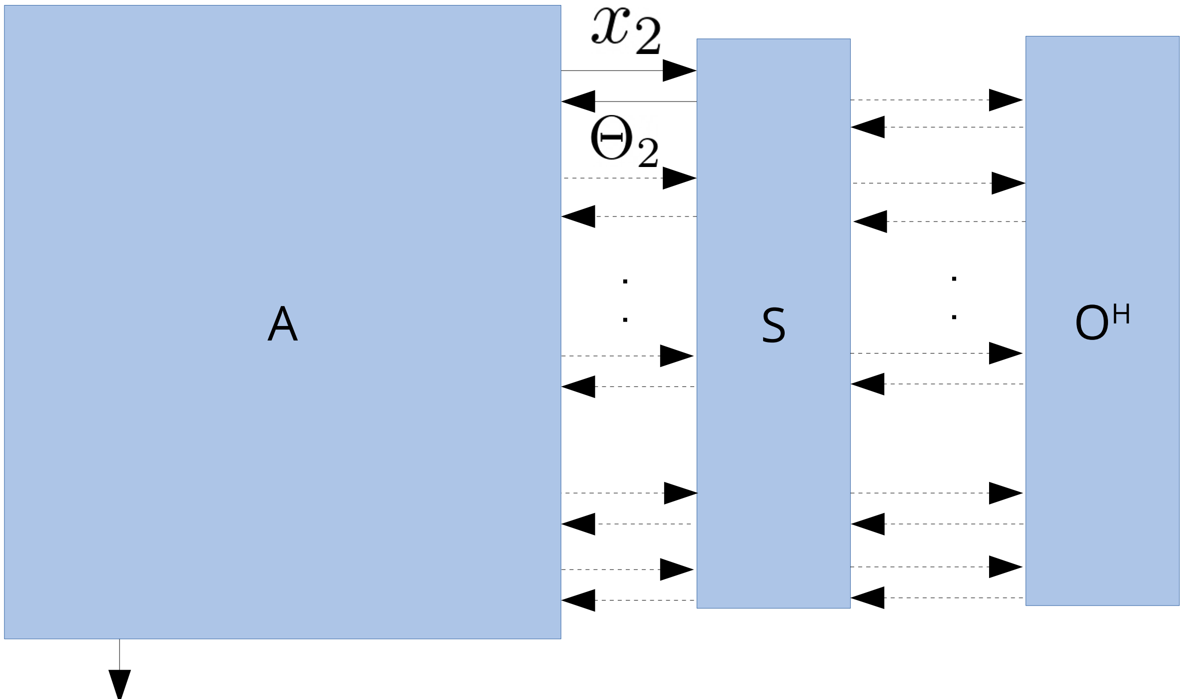


$$(x_1, z') = (x_2, z'')$$

$$z' := (x_2, \ldots, x_n, z) \qquad z'' := (x_1, x_3, \ldots, x_n, z)$$

$$V(x_1, \Theta_1, x_2, H(x_2), \ldots, x_n, H(x_n), z)$$

Multi-input reprogrammability

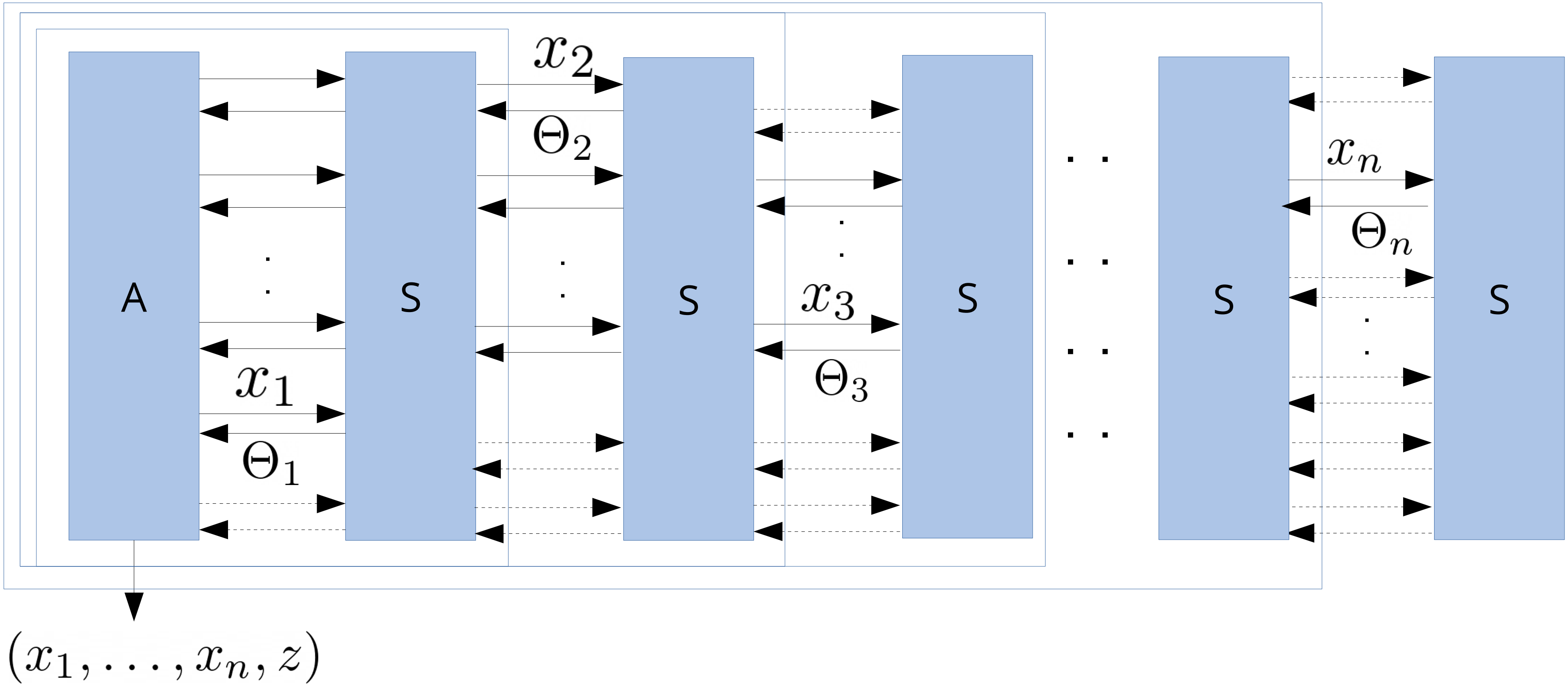


$$(x_1, z') = (x_2, z'')$$

$$z' := (x_2, \ldots, x_n, z) \qquad z'' := (x_1, x_3, \ldots, x_n, z)$$

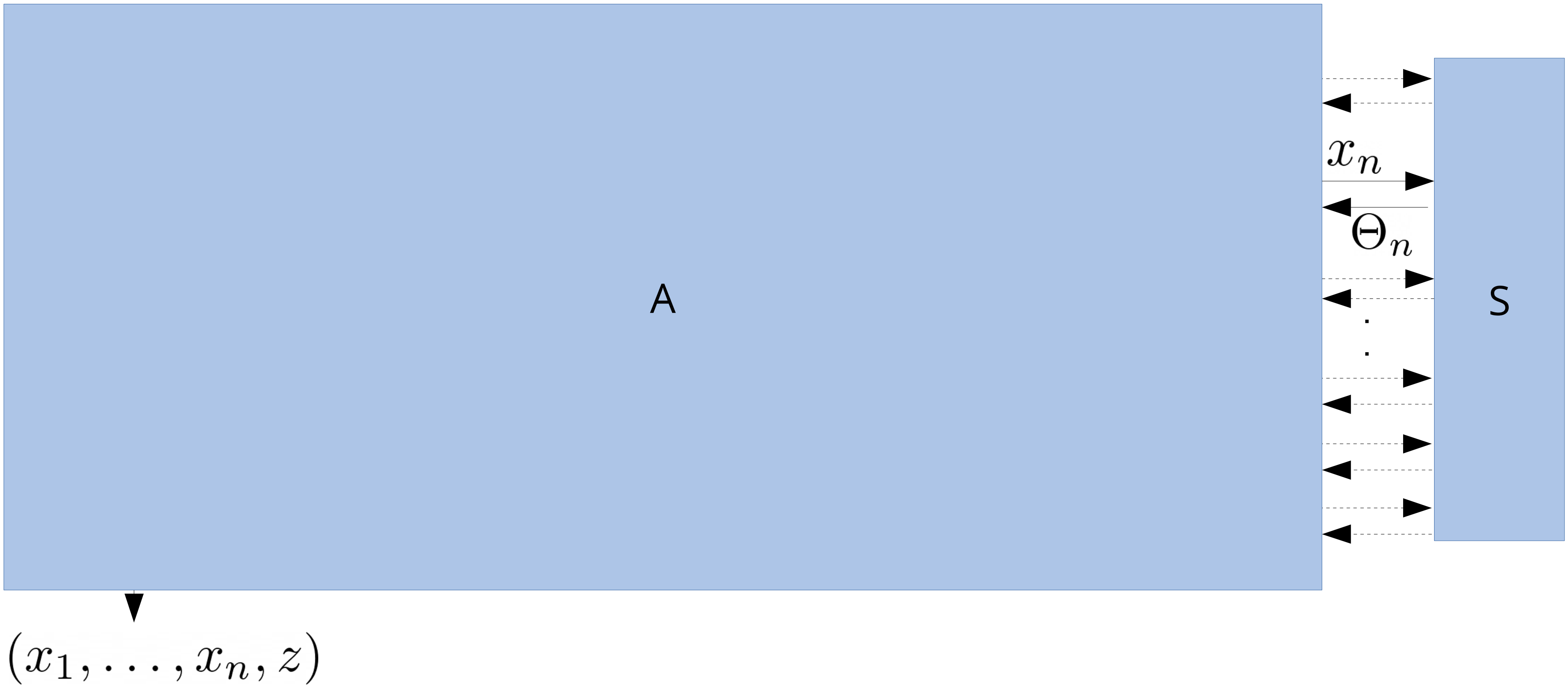
$$V(x_1, \Theta_1, x_2, {\color{red}\Theta_2}, \ldots, x_n, H(x_n), z)$$

Multi-input reprogrammability



$$V(x_1, \Theta_1, x_2, \Theta_2, \ldots, x_n, \Theta_n, z)$$

Multi-input reprogrammability



$$V(x_1, \Theta_1, x_2, \Theta_2, \ldots, x_n, \Theta_n, z)$$

Multi-input reprogrammability

$$\frac{\Pr\left[x_1 = x_1^\circ \wedge V(x_1, H(x_1), z')\right]}{O(q^2)} - \epsilon_{x_1^\circ} \leq \Pr\left[\overline{x_1} = x_1^\circ \wedge V(\overline{x_1}, \Theta_1, z')\right]$$

$$\frac{\Pr\left[\mathbf{x} = \mathbf{x}_\circ \wedge V(\mathbf{x}, H(\mathbf{x}), z)\right]}{?} - ? \leq \Pr\left[\overline{\mathbf{x}} = \overline{\mathbf{x}}_\circ \wedge V(\mathbf{x}, \boldsymbol{\Theta}, z)\right]$$

Multi-input reprogrammability

$$\frac{\Pr\left[x_1 = x_1^\circ \wedge V(x_1, H(x_1), z')\right]}{O(q^2)} - \epsilon_{x_1^\circ} \leq \Pr\left[\overline{x_1} = x_1^\circ \wedge V(\overline{x_1}, \Theta_1, z')\right]$$

$$\frac{\Pr\left[x_1 = x_1^\circ \wedge x_2 = x_2^\circ \wedge V(x_1, x_2, H(x_1), H(x_2), z'')\right]}{O(q^4)} - \epsilon_{x_1^\circ} - \epsilon_{x_2^\circ} \leq \Pr\left[\overline{x_1} = x_1^\circ \wedge \overline{x_2} = x_2^\circ \wedge V(\overline{x_1}, \overline{x_2}, \Theta_1, \Theta_2, z'')\right]$$

$$\frac{\Pr\left[\mathbf{x} = \mathbf{x}_\circ \wedge V(\mathbf{x}, H(\mathbf{x}), z)\right]}{?} - ? \leq \Pr\left[\overline{\mathbf{x}} = \overline{\mathbf{x}}_\circ \wedge V(\mathbf{x}, \boldsymbol{\Theta}, z)\right]$$

Multi-input reprogrammability

$$\frac{\Pr\left[x_1 = x_1^\circ \wedge V(x_1, H(x_1), z')\right]}{O(q^2)} - \epsilon_{x_1^\circ} \leq \Pr\left[\overline{x_1} = x_1^\circ \wedge V(\overline{x_1}, \Theta_1, z')\right]$$

$$\frac{\Pr\left[x_1 = x_1^\circ \wedge x_2 = x_2^\circ \wedge V(x_1, x_2, H(x_1), H(x_2), z'')\right]}{O(q^4)} - \epsilon_{x_1^\circ} - \epsilon_{x_2^\circ} \leq \Pr\left[\overline{x_1} = x_1^\circ \wedge \overline{x_2} = x_2^\circ \wedge V(\overline{x_1}, \overline{x_2}, \Theta_1, \Theta_2, z'')\right]$$

$$\vdots$$

$$\frac{\Pr\left[\mathbf{x} = \mathbf{x}_\circ \wedge V(\mathbf{x}, H(\mathbf{x}), z)\right]}{O(q^{2n})} - \sum_{i=1}^{n} \epsilon_{x_i^\circ} \leq \Pr\left[\overline{\mathbf{x}} = \overline{\mathbf{x}}_\circ \wedge V(\mathbf{x}, \boldsymbol{\Theta}, z)\right]$$

Multi-input reprogrammability

$\mathrm{Pr}\left[x_1\right.$ … $\left.\Theta_1, z')\right]$

$\mathrm{Pr}\left[x_1 = x_1^\circ \wedge x_2 = \right.$ … $\left. V(\overline{x_1}, \overline{x_2}, \Theta_1, \Theta_2, z'')\right]$

$$\forall i : \quad \sum_{x_i^\circ} \epsilon_{x_i^\circ} \leq negl(\eta)$$

$$\frac{\mathrm{Pr}\left[\mathbf{x} = \mathbf{x}_\circ \wedge V(\mathbf{x}, H(\mathbf{x}), z)\right]}{O(q^{2n})} - \sum_{i=1}^{n} \epsilon_{x_i^\circ} \leq \mathrm{Pr}\left[\overline{\mathbf{x}} = \overline{\mathbf{x}}_\circ \wedge V(\mathbf{x}, \boldsymbol{\Theta}, z)\right]$$

Multi-input reprogrammability

$\mathrm{Pr}\left[x_1\right.$ … $\left.\Theta_1, z')\right]$

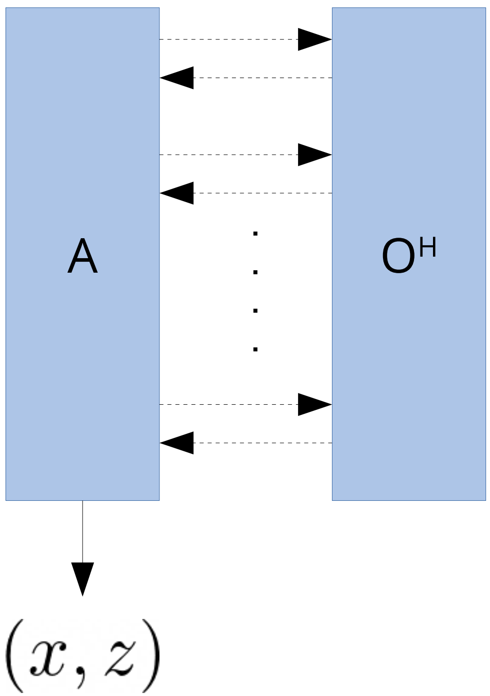
$\mathrm{Pr}\left[x_1 = x_1^\circ \wedge x_2 = \right.$ … $\left.\wedge V(\overline{x_1}, \overline{x_2}, \Theta_1, \Theta_2, z'')\right]$

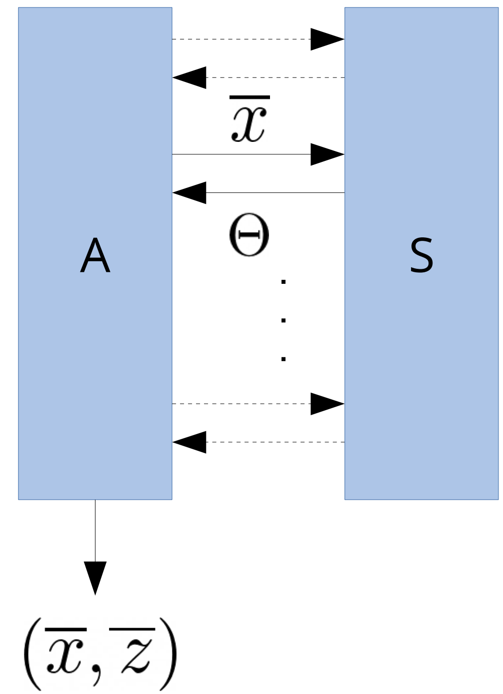
$$\sum_{i=1}^{n} \sum_{x_i^\circ} \epsilon_{x_i^\circ} \leq negl(\eta)$$

$$\sum_{\mathbf{x}_\circ} \sum_{i=1}^{n} \epsilon_{x_i^\circ} \leq \;???$$

$$\frac{\mathrm{Pr}\left[\mathbf{x} = \mathbf{x}_\circ \wedge V(\mathbf{x}, H(\mathbf{x}), z)\right]}{O(q^{2n})} - \sum_{i=1}^{n} \epsilon_{x_i^\circ} \leq \mathrm{Pr}\left[\overline{\mathbf{x}} = \overline{\mathbf{x}}_\circ \wedge V(\mathbf{x}, \mathbf{\Theta}, z)\right]$$

Measure-and-reprogram 2.0





$$\frac{\Pr\left[x = x_\circ \wedge V(x, H(x), z)\right]}{O(q^2)} \leq \Pr\left[\overline{x} = x_\circ \wedge V(\overline{x}, \Theta, \overline{z})\right]$$

Measure-and-reprogram 2.0

$$\frac{\Pr\left[x_1 = x_1^\circ \wedge V(x_1, H(x_1), z')\right]}{O(q^2)} - \epsilon_{x_1^\circ} \leq \Pr\left[\overline{x_1} = x_1^\circ \wedge V(\overline{x_1}, \Theta_1, z')\right]$$

$$\frac{\Pr\left[x_1 = x_1^\circ \wedge x_2 = x_2^\circ \wedge V(x_1, x_2, H(x_1), H(x_2), z'')\right]}{O(q^4)} - \epsilon_{x_1^\circ} - \epsilon_{x_2^\circ} \leq \Pr\left[\overline{x_1} = x_1^\circ \wedge \overline{x_2} = x_2^\circ \wedge V(\overline{x_1}, \overline{x_2}, \Theta_1, \Theta_2, z'')\right]$$

$$\vdots$$

$$\frac{\Pr\left[\mathbf{x} = \mathbf{x}_\circ \wedge V(\mathbf{x}, H(\mathbf{x}), z)\right]}{O(q^{2n})} - \sum_{i=1}^{n} \epsilon_{x_i^\circ} \leq \Pr\left[\overline{\mathbf{x}} = \overline{\mathbf{x}}_\circ \wedge V(\mathbf{x}, \boldsymbol{\Theta}, z)\right]$$

Measure-and-reprogram 2.0

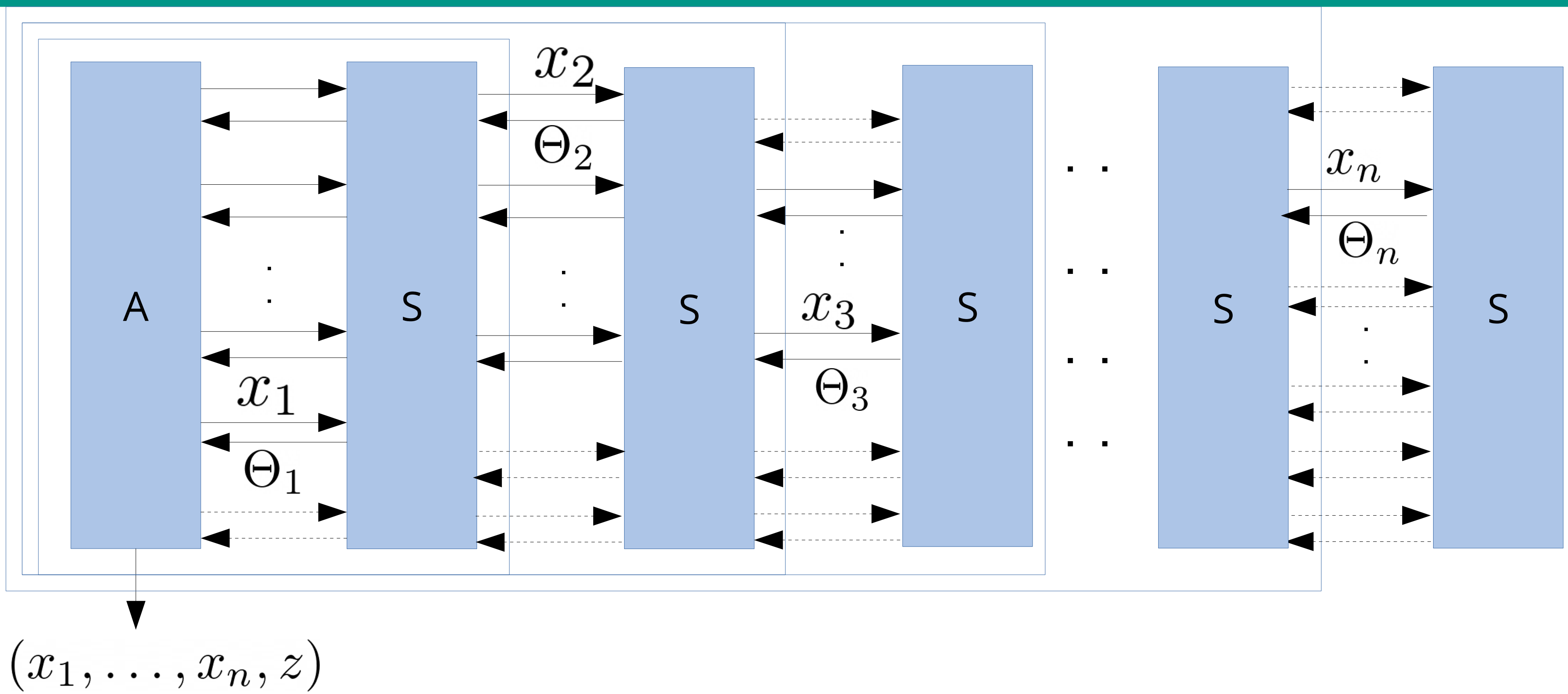
$$\frac{\Pr\left[x_1 = x_1^\circ \wedge V(x_1, H(x_1), z')\right]}{O(q^2)} \qquad \leq \Pr\left[\overline{x_1} = x_1^\circ \wedge V(\overline{x_1}, \Theta_1, z')\right]$$

$$\frac{\Pr\left[x_1 = x_1^\circ \wedge x_2 = x_2^\circ \wedge V(x_1, x_2, H(x_1), H(x_2), z'')\right]}{O(q^4)} \qquad \leq \Pr\left[\overline{x_1} = x_1^\circ \wedge \overline{x_2} = x_2^\circ \wedge V(\overline{x_1}, \overline{x_2}, \Theta_1, \Theta_2, z'')\right]$$

$$\vdots$$

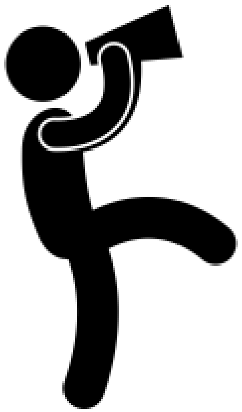
$$\frac{\Pr\left[\mathbf{x} = \mathbf{x}_\circ \wedge V(\mathbf{x}, H(\mathbf{x}), z)\right]}{O(q^{2n})} \qquad \leq \Pr\left[\overline{\mathbf{x}} = \overline{\mathbf{x}}_\circ \wedge V(\mathbf{x}, \boldsymbol{\Theta}, z)\right]$$

Multi-round Fiat-Shamir



Multi-round Fiat-Shamir

$(pk, sk) \leftarrow KeyGen$ $\qquad\qquad$ pk



$$\xrightarrow{\quad com_1 \quad}$$

$$\xleftarrow{\quad ch_1 \quad}$$

$$\xrightarrow{\quad com_2 \quad}$$

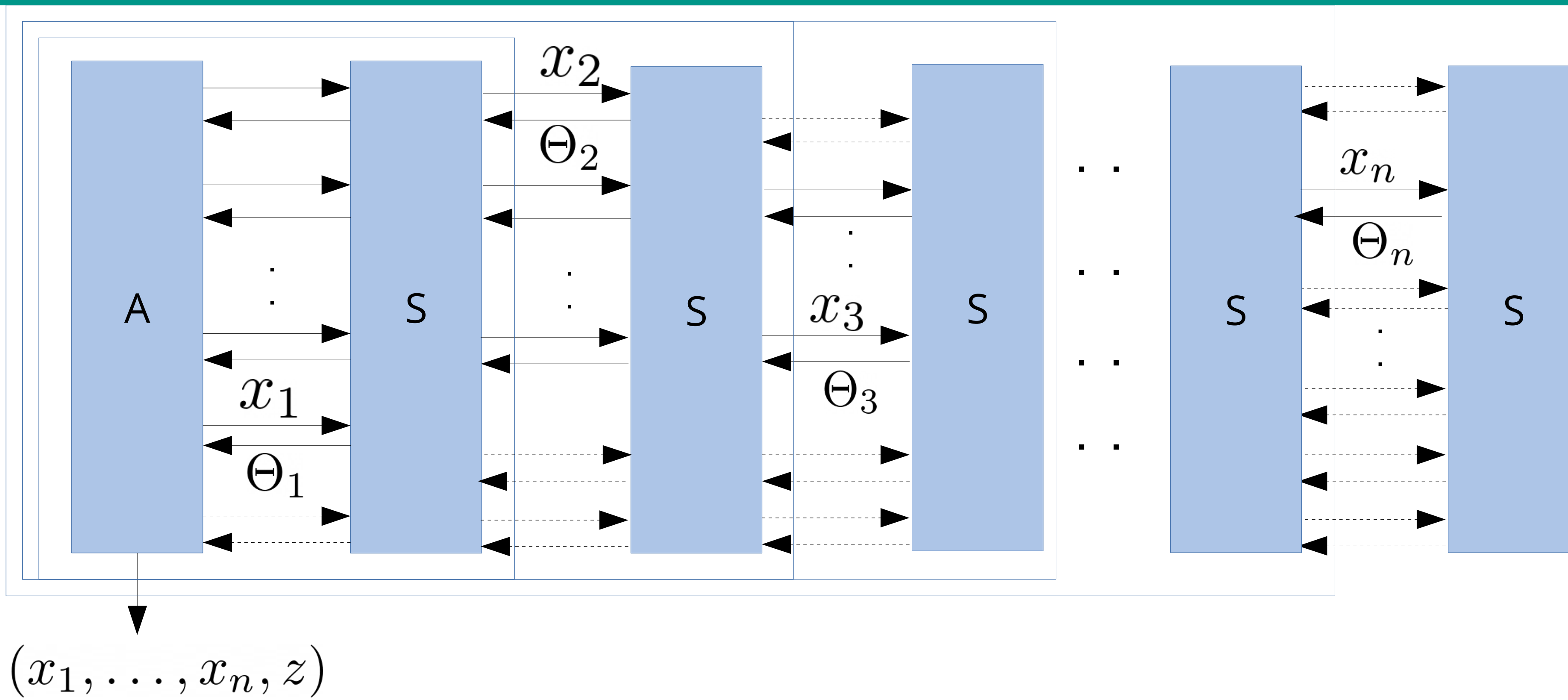
$$\vdots$$

$$\xrightarrow{\quad com_n \quad}$$

$$\xleftarrow{\quad ch_n \quad}$$

$$\xrightarrow{\quad resp \quad}$$

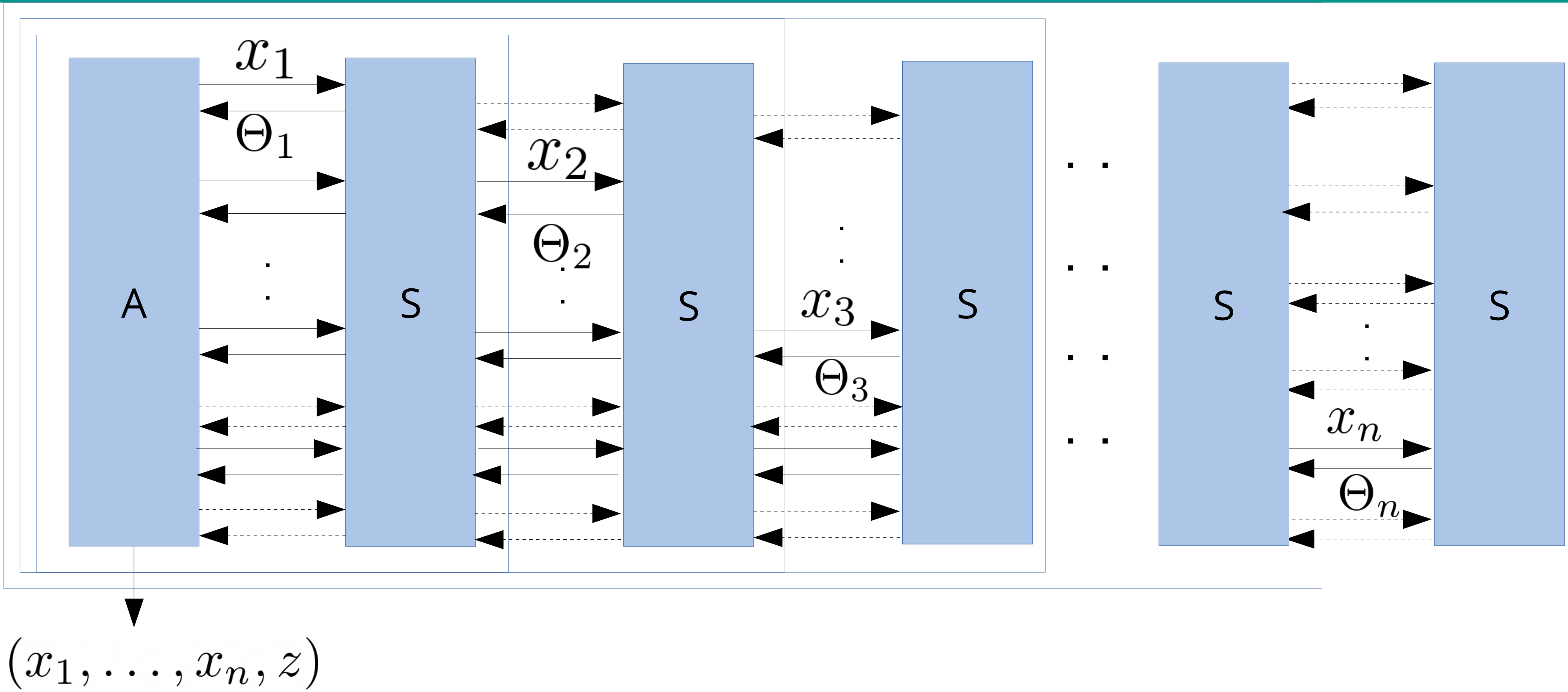
Multi-round Fiat-Shamir



Solution: include previous challenge in the hash:

$$ch_1 = H(0, x, com_1)$$
$$ch_i = H(i-1, ch_{i-1}, com_i)$$

Multi-round Fiat-Shamir



Solution: include previous challenge in the hash:

$$ch_1 = H(0, x, com_1)$$
$$ch_i = H(i-1, ch_{i-1}, com_i)$$

Sequential OR-proofs

- Introduced by Liu, Wei and Wong in 2004
  - Proves at least one of two statements x1,x2 is true, without revealing which one:

$$V(x_1, com_1, H(com_2), resp_1)$$
$$V(x_2, com_2, H(com_1), resp_2)$$

The end

Thank you for listening. Questions?