Improved Alternating-Moduli PRFs and Post-Quantum Signatures

Navid Alamati, **Guru Vamsi Policharla**, Srinivasan Raghuraman, and Peter Rindal

Designing Crypto Primitives

Provable security

Heuristic constructions

Designing Crypto Primitives

Provable security

- Security from hardness of DDH, SXDH, LPN, LWE, etc.

Heuristic constructions

- Security from resisting the best known attacks - AES, SHA etc.

Designing Crypto Primitives

Provable security

- Security from hardness of DDH, SXDH, LPN, LWE, etc.
- Generally slower

Heuristic constructions

- Security from resisting the best known attacks - AES, SHA etc.
- Designed to be fast

Designing Crypto Primitives

Provable security

- Security from hardness of DDH, SXDH, LPN, LWE, etc.
- Generally slower
- Simple to describe

Heuristic constructions

- Security from resisting the best known attacks - AES, SHA etc.
- Designed to be fast
- Complicated, deep circuits

Designing Crypto Primitives

Provable security

- Security from hardness of DDH, SXDH, LPN, LWE, etc.
- Generally slower
- Simple to describe
- Efficient evaluation in MPC/ZK

Heuristic constructions

- Security from resisting the best known attacks - AES, SHA etc.
- Designed to be fast
- Complicated, deep circuits
- Expensive to evaluate in MPC/ZK

Designing Crypto Primitives

Provable security

- Security from hardness of DDH, SXDH, LPN, LWE, etc.
- Genera
- Simple
- Efficient evaluation in MPC/ZK

Heuristic constructions

- Security from resisting the best known attacks - AES, SHA etc.
- s
- Expensive to evaluate in MPC/ZK

Can we have fast, simple to describe, crypto primitives that are MPC/ZK friendly?

The Alternating-Moduli Paradigm

The Alternating-Moduli Paradigm [BIP+18]

The Alternating-Moduli Paradigm [BIP+18]

Goal: Simple, shallow MPC friendly crypto primitives — OWFs, PRFs

The Alternating-Moduli Paradigm [BIP+18]

Goal: Simple, shallow MPC friendly crypto primitives — OWFs, PRFs

tldr; Alternating linear functions over different fields

The Alternating-Moduli Paradigm [BIP+18]

Goal: Simple, shallow MPC friendly crypto primitives — OWFs, PRFs

tldr; Alternating linear functions over different fields

Great for MPC / ZK !

The Alternating-Moduli Paradigm [BIP+18]

Goal: Simple, shallow MPC friendly crypto primitives — OWFs, PRFs

tldr; Alternating linear functions over different fields

Great for MPC / ZK !

"alterations" $\implies$ # rounds. As low as 1!

The Alternating-Moduli Paradigm [BIP+18]

Goal: Simple, shallow MPC friendly crypto primitives — OWFs, PRFs

tldr; Alternating linear functions over different fields

Great for MPC / ZK !

"alterations" $\Longrightarrow$ # rounds. As low as 1!

Why do they resist cryptanalysis?

The Alternating-Moduli Paradigm [BIP+18]

Goal: Simple, shallow MPC friendly crypto primitives — OWFs, PRFs

tldr; Alternating linear functions over different fields

Great for MPC / ZK !

"alterations" $\implies$ # rounds. As low as 1!

Why do they resist cryptanalysis?

High algebraic degree when represented in a single field

What do they look like?

What do they look like?

[BIP+18]: weak PRF

What do they look like?

[BIP+18]: weak PRF

$$y = B \cdot_3 (K \cdot_2 x)$$

What do they look like?

[BIP+18]: weak PRF

Input

$$y = B \cdot_3 (K \cdot_2 x)$$

What do they look like?

[BIP+18]: weak PRF

$$y = B \cdot_3 (\underbrace{K}_{\text{Secret Key}} \cdot_2 \overbrace{x}^{\text{Input}})$$

What do they look like?

[BIP+18]: weak PRF

$$y = B \cdot_3 (\underbrace{K}_{\text{Secret Key}} \cdot_2 \overbrace{x}^{\text{Input}})$$

Map $\mathbb{F}_2 \to \mathbb{F}_3$

What do they look like?

[BIP+18]: weak PRF

$$y = \underbrace{B}_{\mathbb{F}_3} \; \underbrace{K}_{\mathbb{F}_2} \; \underbrace{x}_{\mathbb{F}_2}$$

- $K \sim 384 \times 384$
- Can be circulant for faster evaluation
- Cryptanalysis + fixes in [CCKK21]. More variants in [BIP+18, DGI+21].

What do they look like?

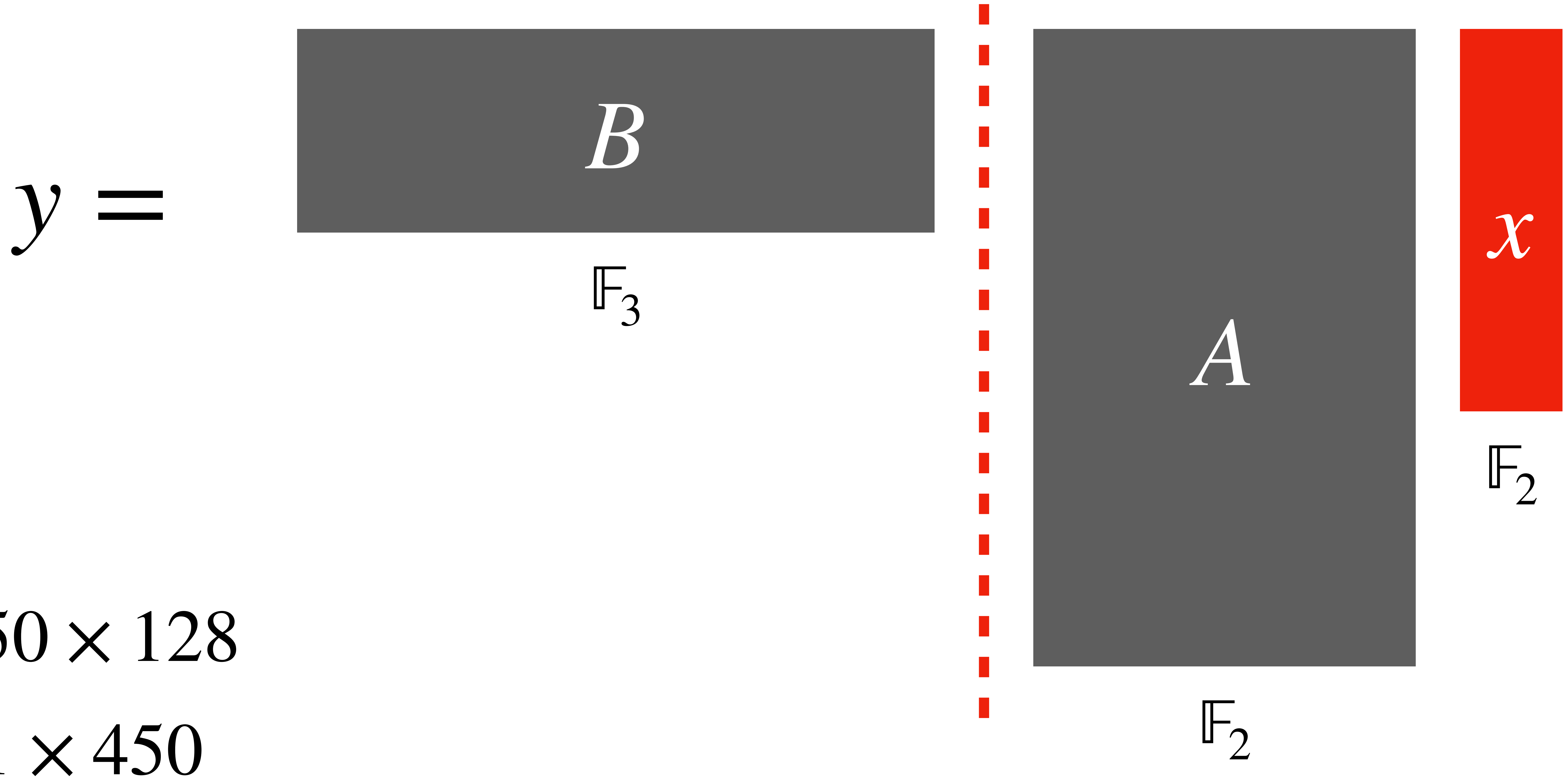
[DGH+21]: OWF

Input

$$y = B \cdot_3 (A \cdot_2 x)$$

What do they look like?

[DGH+21]: OWF



- $A \sim 450 \times 128$
- $B \sim 81 \times 450$

Efficient PQ Signatures

MPC-in-the-Head [IKOS07]

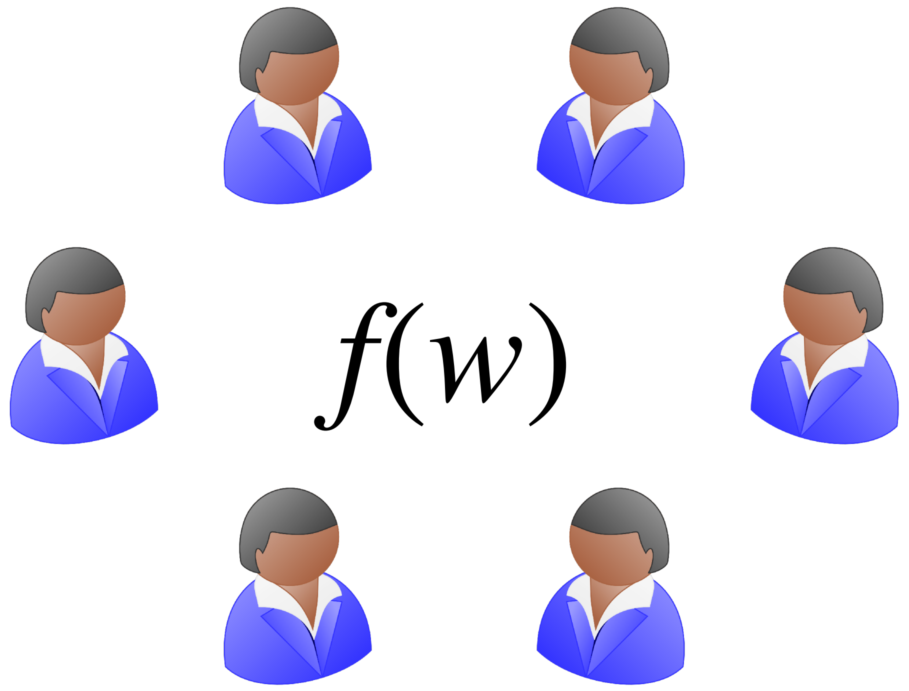
MPC-in-the-Head [IKOS07]

MPCitH: Convert an MPC protocol into a zero-knowledge proof

MPC-in-the-Head [IKOS07]

MPCitH: Convert an MPC protocol into a zero-knowledge proof

Each party has a "view" containing inputs/randomness/messages



MPC-in-the-Head [IKOS07]

MPCitH: Convert an MPC protocol into a zero-knowledge proof

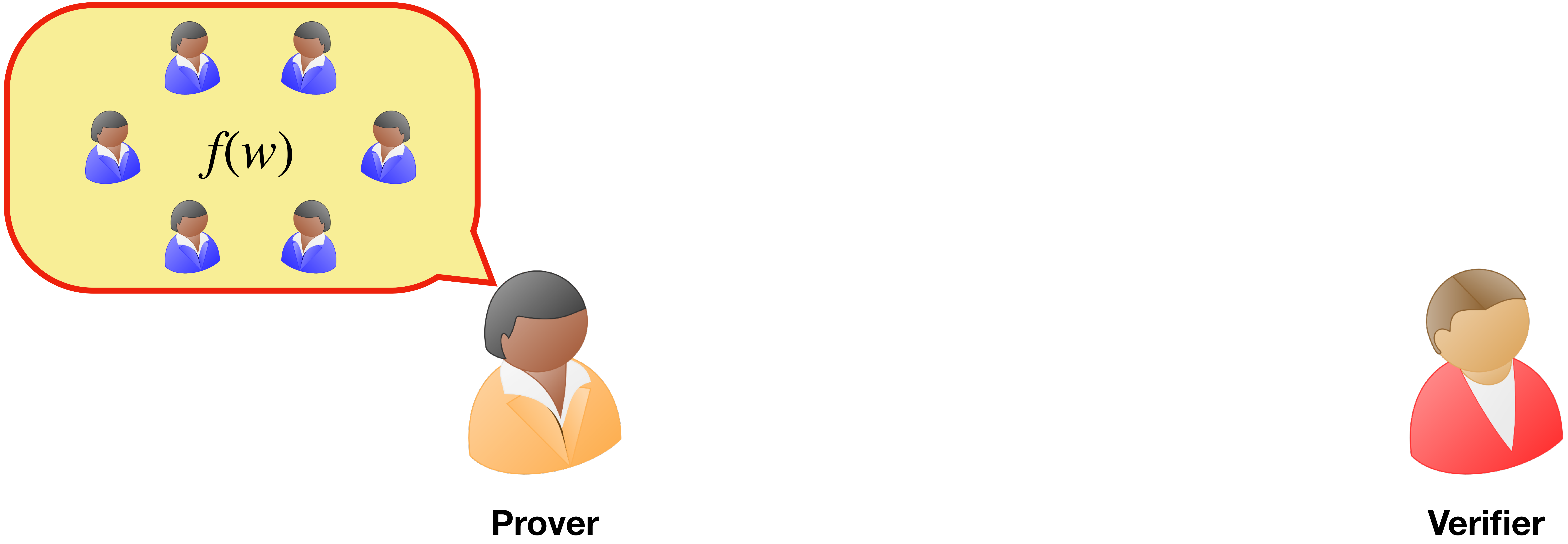
Each party has a "view" containing inputs/randomness/messages

Prover **Verifier**

MPC-in-the-Head [IKOS07]

MPCitH: Convert an MPC protocol into a zero-knowledge proof

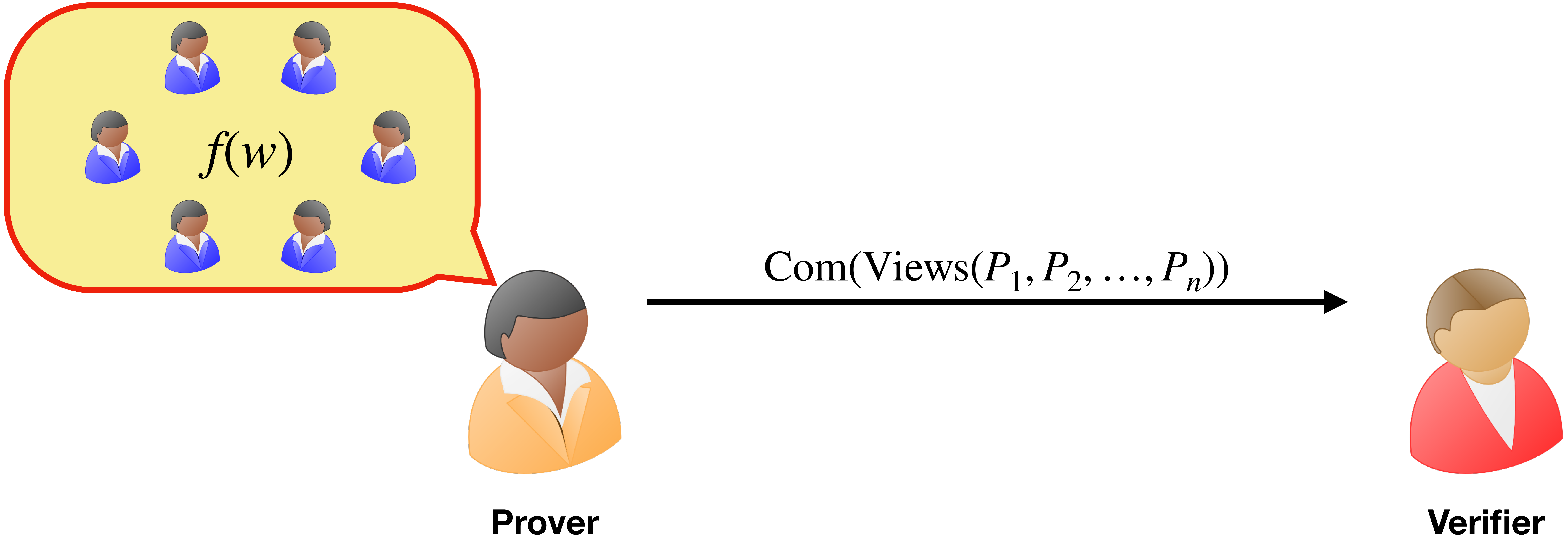
Each party has a "view" containing inputs/randomness/messages



MPC-in-the-Head [IKOS07]

MPCitH: Convert an MPC protocol into a zero-knowledge proof

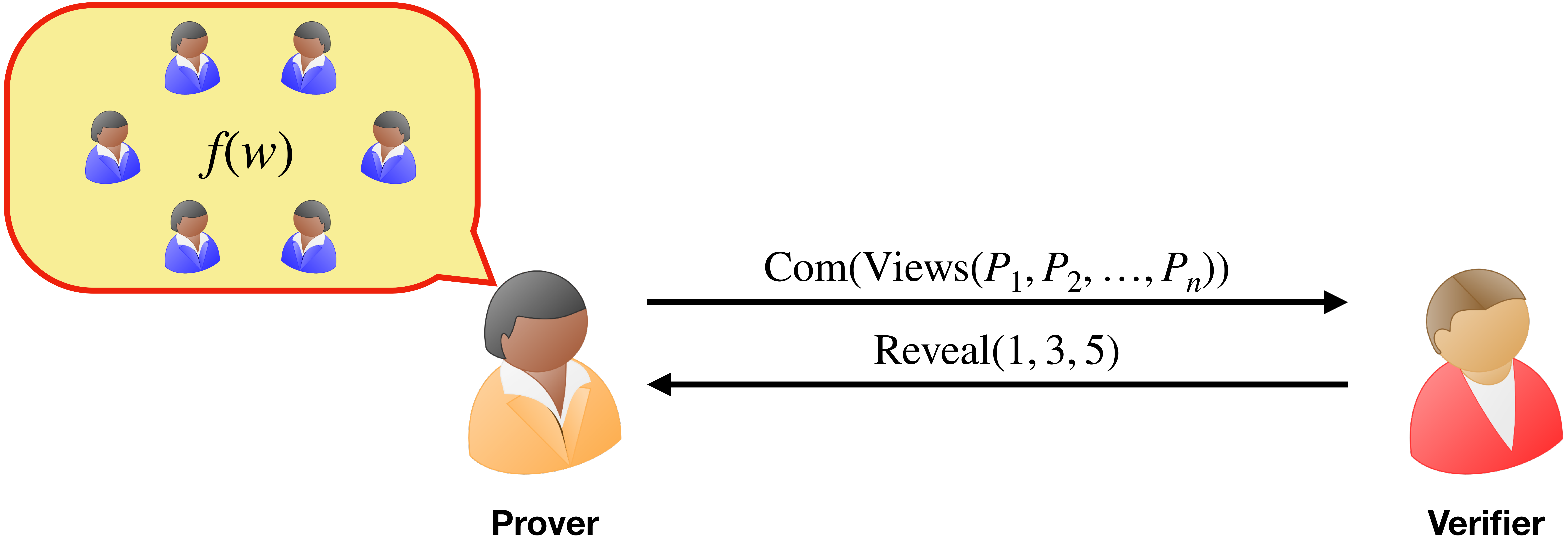
Each party has a "view" containing inputs/randomness/messages



MPC-in-the-Head [IKOS07]

MPCitH: Convert an MPC protocol into a zero-knowledge proof

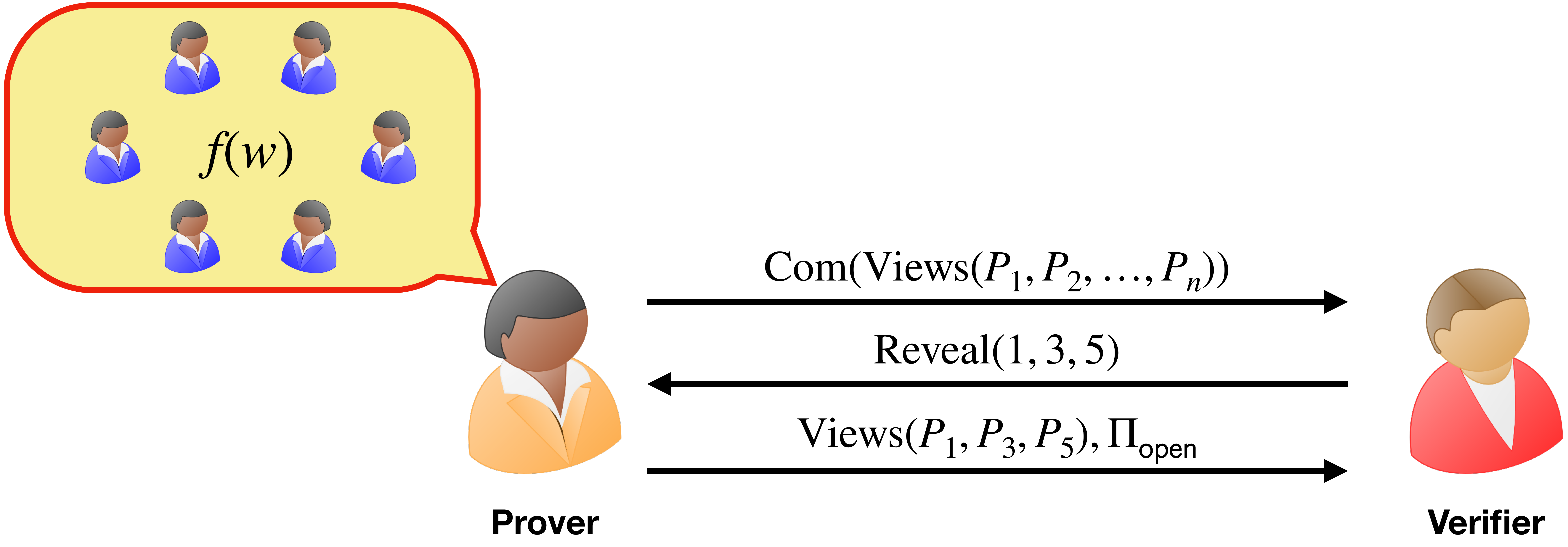
Each party has a "view" containing inputs/randomness/messages



MPC-in-the-Head [IKOS07]

MPCitH: Convert an MPC protocol into a zero-knowledge proof

Each party has a “view” containing inputs/randomness/messages



OWF → Signature

Can build a signature scheme given a OWF and a NIZK:

$$\Pi = \{\textsf{sk} \mid \textsf{pk} = f(\textsf{sk}) \wedge m\}$$

OWF $\rightarrow$ Signature

Can build a signature scheme given a OWF and a NIZK:

$$\Pi = \{\mathsf{sk} \mid \mathsf{pk} = f(\mathsf{sk}) \wedge m\}$$

- [DGH+21] introduce a OWF in the alternating-modulus paradigm

OWF → Signature

Can build a signature scheme given a OWF and a NIZK:

$$\Pi = \{\mathsf{sk} \mid \mathsf{pk} = f(\mathsf{sk}) \wedge m\}$$

- [DGH+21] introduce a OWF in the alternating-modulus paradigm
- Signatures $\approx$ 10 KB using [KKW18] (off the shelf MPCitH)

OWF $\to$ Signature

Can build a signature scheme given a OWF and a NIZK:

$$\Pi = \{\mathsf{sk} \mid \mathsf{pk} = f(\mathsf{sk}) \wedge m\}$$

- [DGH+21] introduce a OWF in the alternating-modulus paradigm
- Signatures $\approx$ 10 KB using [KKW18] (off the shelf MPCitH)
- Signature with AES + <u>custom</u> proof system, signatures $\approx$ 5 KB [BBD+23]

OWF → Signature

Can build a signature scheme given a OWF and a NIZK:

$$\Pi = \{\mathsf{sk} \mid \mathsf{pk} = f(\mathsf{sk}) \wedge m\}$$

- [DGH+21] introduce a OWF in the alternating-modulus paradigm
- Signatures $\approx$ 10 KB using [KKW18] (of Unsatisfactory ☹️ H)
- Signature with AES + custom proof system, signatures $\approx$ 5 KB [BBD+23]

OWF → Signature

Can build a signature scheme given a OWF and a NIZK:

$$\Pi = \{\mathsf{sk} \mid \mathsf{pk} = f(\mathsf{sk}) \wedge m\}$$

- [DGH+21] introduce a OWF in the alternating-modulus paradigm
- Signatures ≈ 10 KB using [KKW18] (of Unsatisfactory ☹️ H)
- Signature with AES + custom proof system, signatures ≈ 5 KB [BBD+23]

Can we do better with a custom proof for the AM-OWF? 🤔

MPCitH for AM-OWF

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

MPCitH for AM-OWF

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

- Linear operations are “free”

MPCitH for AM-OWF

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

- Linear operations are “free”
- **Observation:** Only non-linear operation: $\mathbb{F}_2 \to \mathbb{F}_3$

MPCitH for AM-OWF

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

- Linear operations are "free"

- **Observation**: Only non-linear operation: $\mathbb{F}_2 \to \mathbb{F}_3$

  1. Given correlations $([r]_2, [r]_3)$, and $[m]_2$. Reveal $z = m +_2 r$

MPCitH for AM-OWF

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

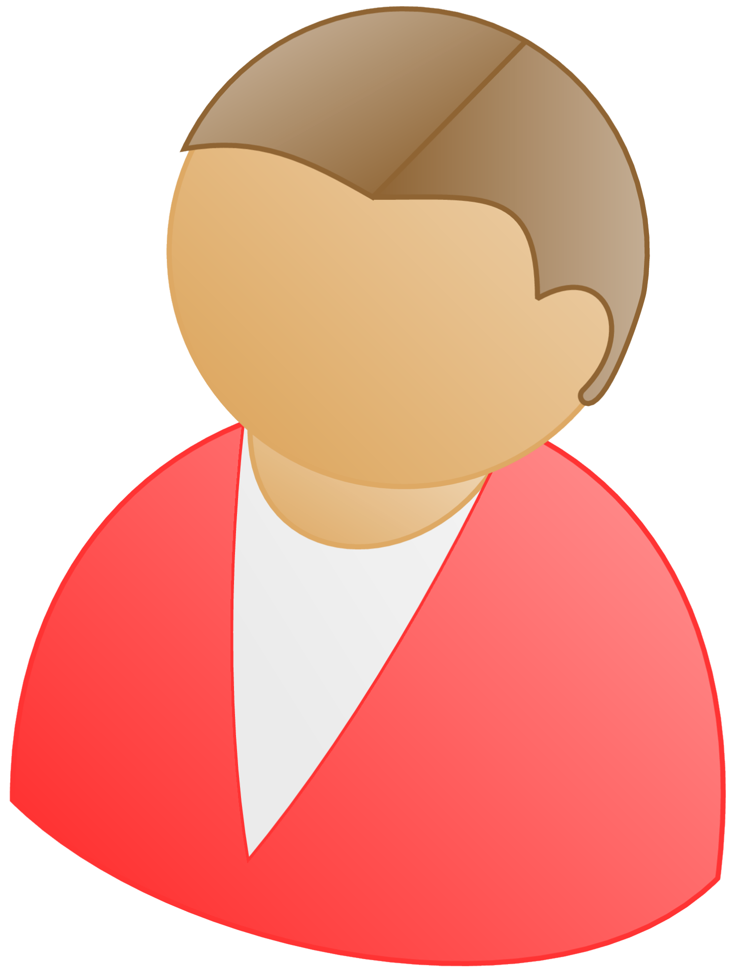
- Linear operations are "free"
- **Observation:** Only non-linear operation: $\mathbb{F}_2 \to \mathbb{F}_3$

1. Given correlations $([r]_2, [r]_3)$, and $[m]_2$. Reveal $z = m +_2 r$
2. $[m]_3 = z + (1 - 2z) \odot [r]_3$

MPCitH for AM-OWF [DHG+21]

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

Prover



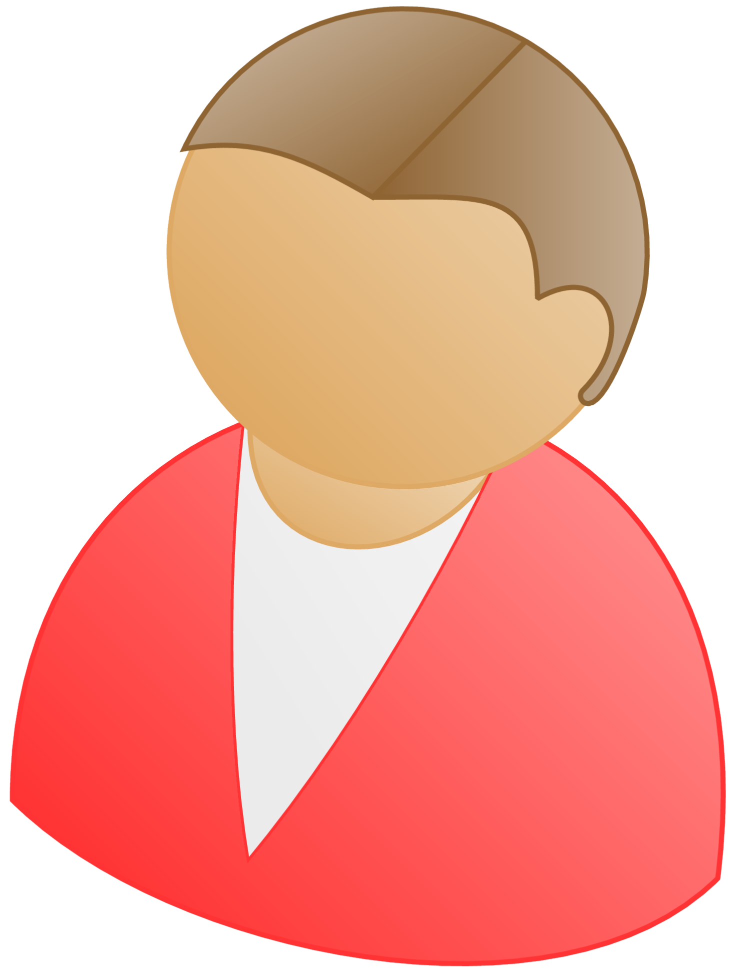
Verifier

MPCitH for AM-OWF [DHG+21]

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

1 $\xrightarrow[]{[x^{(i)}] \quad ([r^{(i)}]_2, [r^{(i)}]_3)}$

Prover



Verifier

MPCitH for AM-OWF [DHG+21]

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

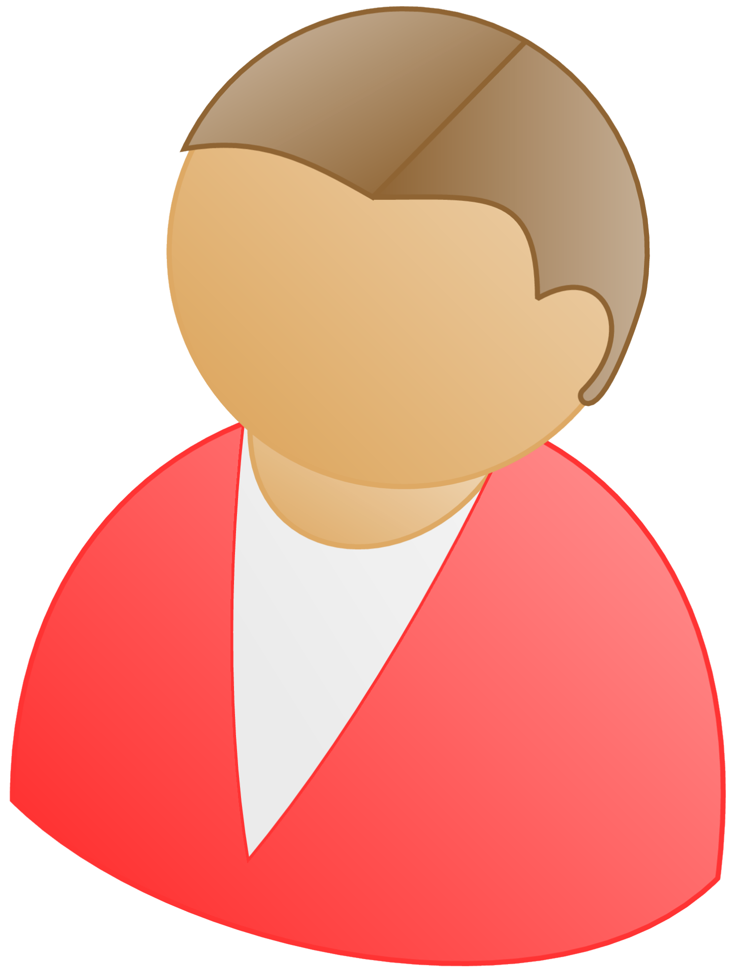
$[x^{(i)}]$

$\boxed{([r^{(i)}]_2, [r^{(i)}]_3)}$

Could be malformed

1

Prover



Verifier

MPCitH for AM-OWF [DHG+21]

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

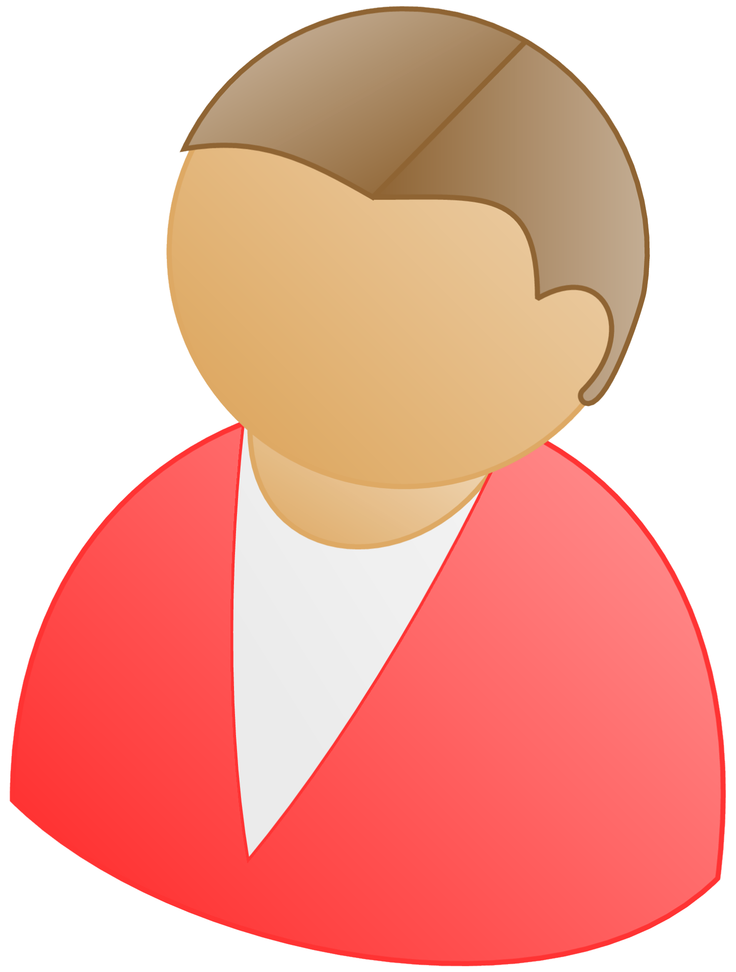
$[x^{(i)}]$

1 $\boxed{([r^{(i)}]_2, [r^{(i)}]_3)}$ Could be malformed

Check $([r^{(i)}]_2, [r^{(i)}]_3)$
via Cut-and-Choose

2

Prover



Verifier

MPCitH for AM-OWF [DHG+21]

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

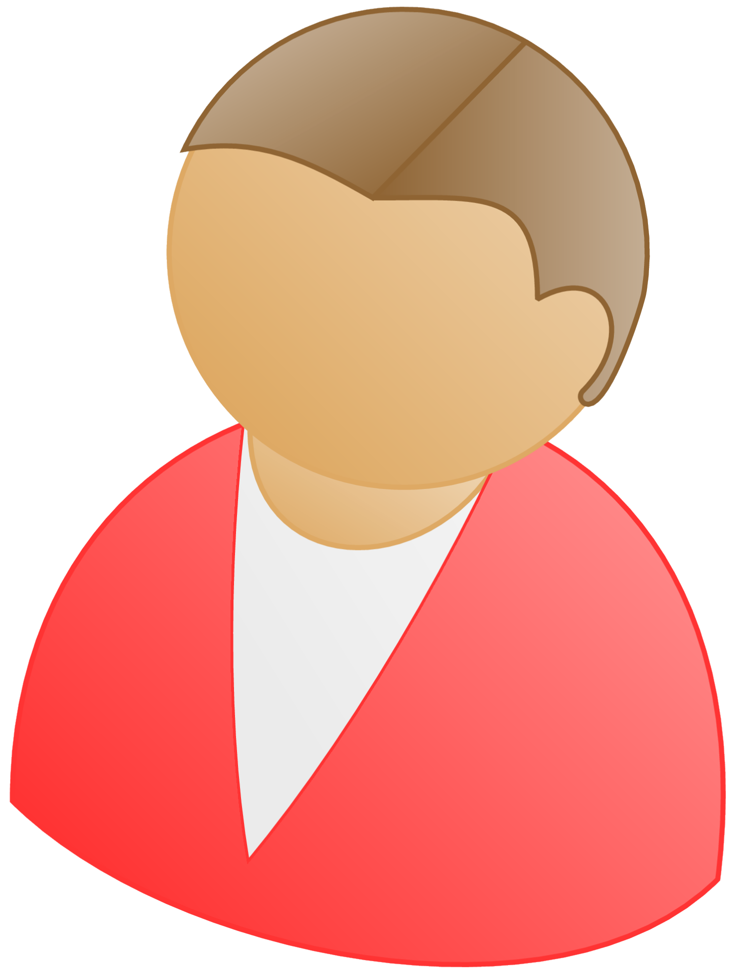
Prover

1 $[x^{(i)}]$

$\boxed{([r^{(i)}]_2, [r^{(i)}]_3)}$ Could be malformed

2 Check $([r^{(i)}]_2, [r^{(i)}]_3)$ via Cut-and-Choose

3 Send transcript of “online phase”



Verifier

MPCitH for AM-OWF [DHG+21]

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

Prover

1 $[x^{(i)}]$

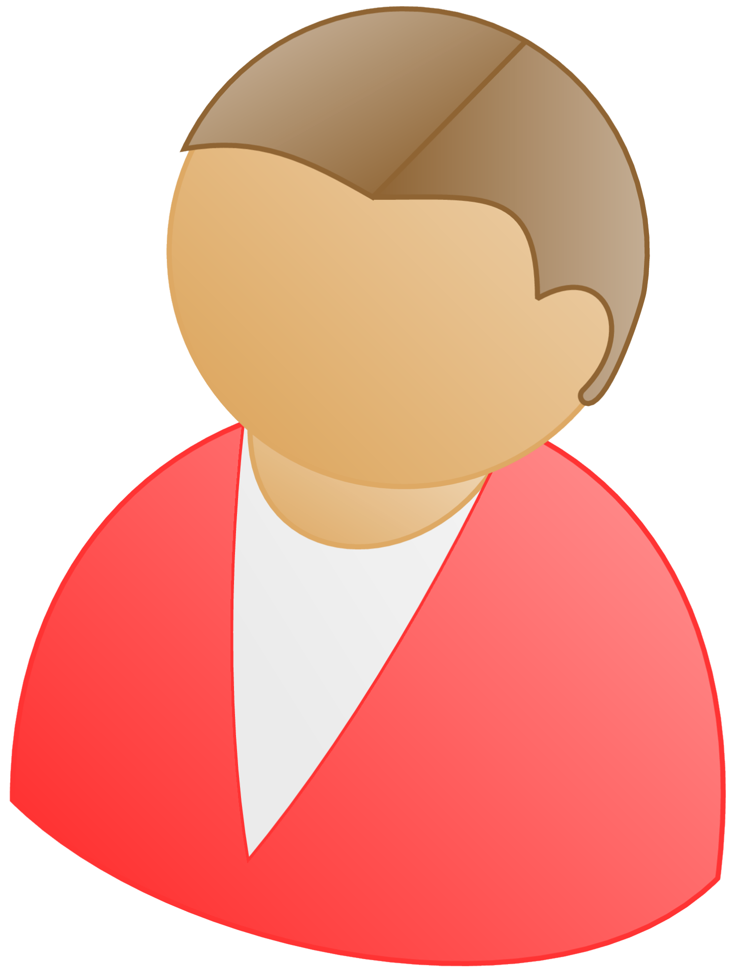
$\boxed{([r^{(i)}]_2, [r^{(i)}]_3)}$

Could be malformed

2 Check $([r^{(i)}]_2, [r^{(i)}]_3)$ via Cut-and-Choose

3 Send transcript of "online phase"

Total size: 10-13 KB



Verifier

MPCitH for AM-OWF [DHG+21]

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

$[x^{(i)}]$

Could be malformed

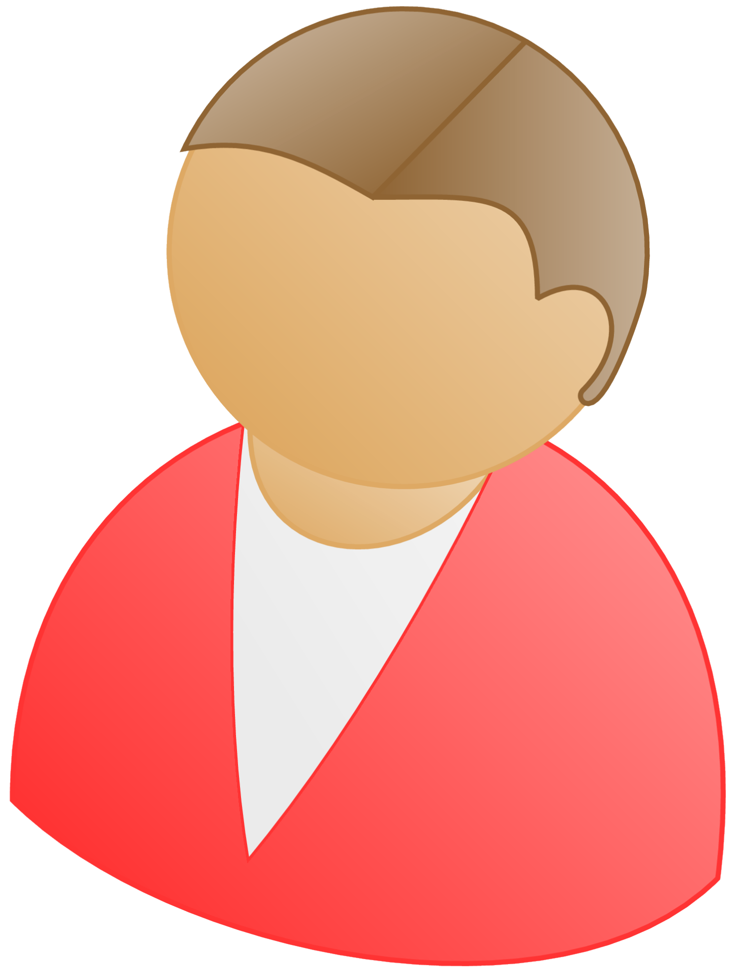
1 $\boxed{([r^{(i)}]_2, [r^{(i)}]_3)}$

Prover

2 Check $([r^{(i)}]_2, [r^{(i)}]_3)$ via Cut-and-Choose

Costs 5-7 KB! 😞

3 Send transcript of “online phase”



Verifier

Total size: 10-13 KB

MPCitH for AM-OWF [DHG+21]

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

Prover

$[x^{(i)}]$

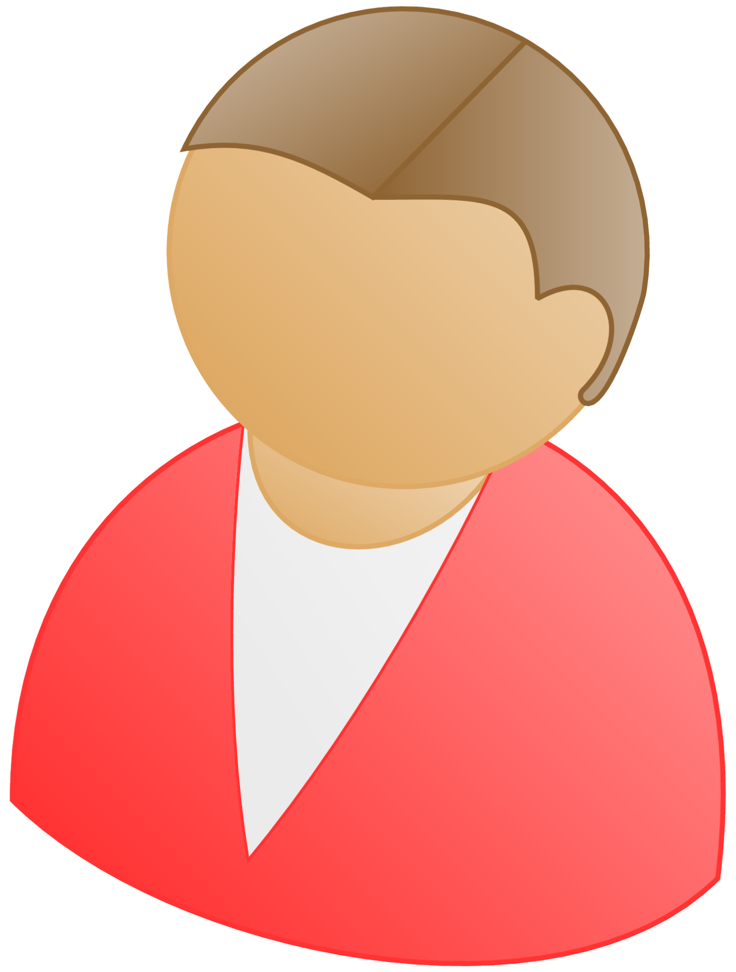
① $\boxed{([r^{(i)}]_2, [r^{(i)}]_3)}$ $\longrightarrow$ Could be malformed

Check $([r^{(i)}]_2, [r^{(i)}]_3)$ via Cut-and-Choose

② Costs 5-7 KB! 😞

Send transcript of "online phase"

③ $\longrightarrow$



Verifier

Can we avoid Cut-and-Choose?

MPCitH for AM-OWF [This Work]

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

$[x^{(i)}]$

Prover

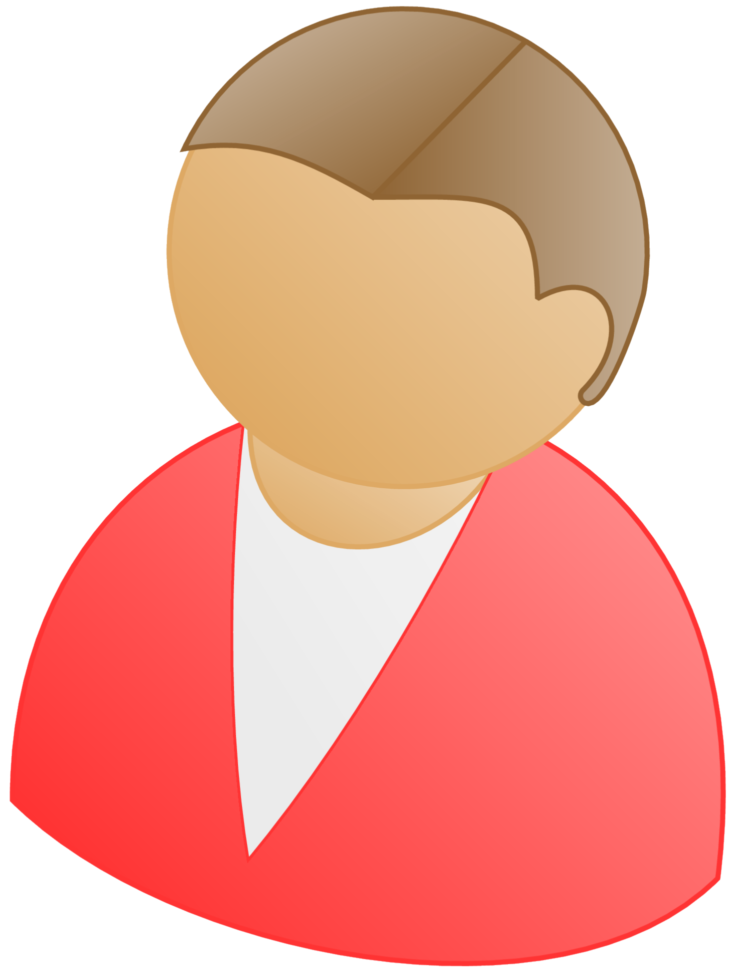
1 $([r^{(i)}]_2, [r^{(i)}]_3)$

Permute $([r^{(i)}]_2, [r^{(i)}]_3)$

2

Send transcript of “online phase”

3



Verifier

MPCitH for AM-OWF [This Work]

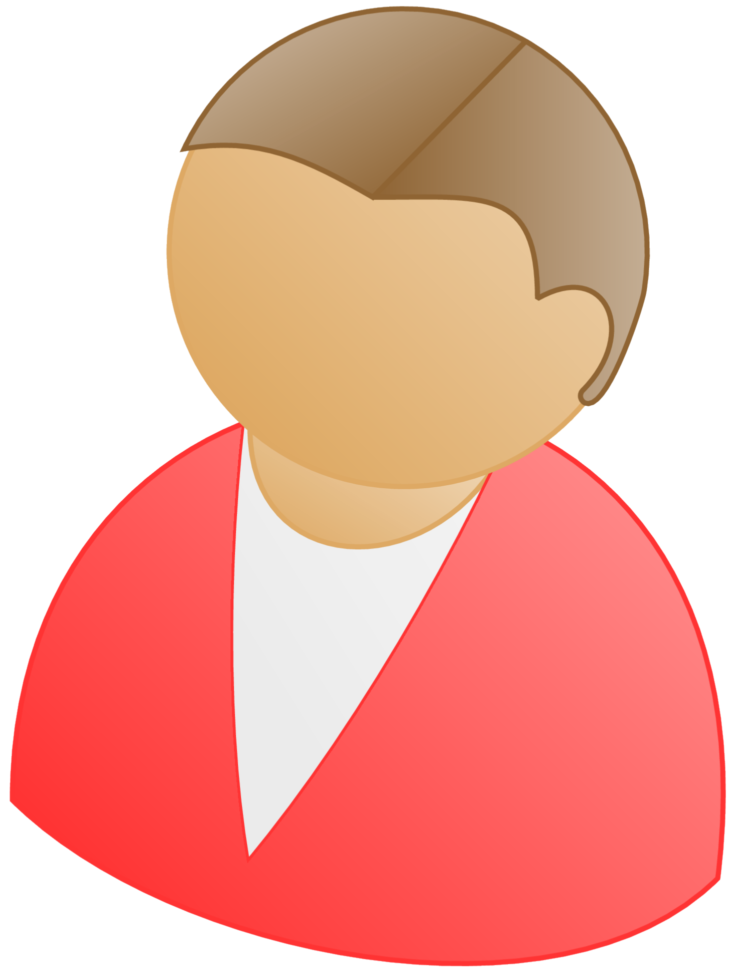
$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

Prover

1 $[x^{(i)}]$ $([r^{(i)}]_2, [r^{(i)}]_3)$ $\longrightarrow$

2 Permute $([r^{(i)}]_2, [r^{(i)}]_3)$ $\longleftarrow$

3 Send transcript of "online phase" $\longrightarrow$



Verifier

Soundness via a careful analysis.
Similar techniques in [CCJ23]

MPCitH for AM-OWF [This Work]

$$\Pi = \{x \mid y = B \cdot_3 (A \cdot_2 x)\}$$

$[x^{(i)}]$

1 $([r^{(i)}]_2, [r^{(i)}]_3)$

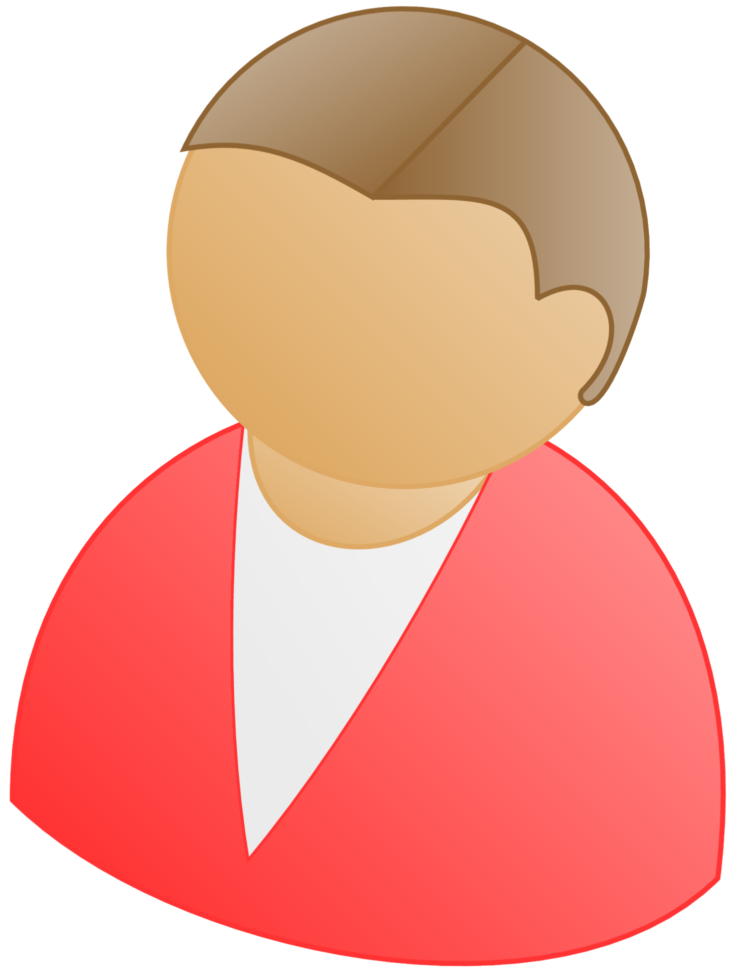
Permute $([r^{(i)}]_2, [r^{(i)}]_3)$

2 Free! 😃

Send transcript of "online phase"

3

Prover



Verifier

Soundness via a careful analysis.
Similar techniques in [CCJ23]

Comparison

	Fast (KB)	Short (KB)	Assumption
SPHINCS+	16.7	7.7	SHA256
CCJ23	11.3	7.8	f-almost RSD
AGH+23	9.7	4.5	SD over GF(256)
BBdSG+22	5.6	4.5	EM-AES
KZ22	5.8	4.4	Rain
ARZV23	7.7	4.4	MinRank
KHS23	5.8	3.8	AIM
Our Work	**5.5**	**4.0**	**AM-OWF**

Many more works! Dropped due to lack of space ☹️

New wPRF

Why do we want a new wPRF?

Secret Key Matrix

[BIP+18]: $$y = B \cdot_3 (\underbrace{K \cdot_2 x}_{})$$

Requires $O(\lambda^2)$ multiplications in MPC

Why do we want a new wPRF?

Secret Key Matrix

[BIP+18]: $y = B \cdot_3 (K \cdot_2 x)$

Requires $O(\lambda^2)$ multiplications in MPC

Can reduce communication by using circulant matrices

Why do we want a new wPRF?

Secret Key Matrix

[BIP+18]: $$y = B \cdot_3 \underbrace{(K \cdot_2 x)}$$

Requires $O(\lambda^2)$ multiplications in MPC

Can reduce communication by using circulant matrices

But work is still $\omega(\lambda)$ ☹️

New wPRF

Input

[BIP+18]: $y = B \cdot_3 (K \cdot_2 x)$

Secret Key Matrix

Input

Ours: $y = B \cdot_3 (A \cdot_2 (k \odot_2 x))$

Secret Key Vector

New wPRF

Input

[BIP+18]: $y = B \cdot_3 (\mathbf{K} \cdot_2 x)$

Secret Key Matrix

Input

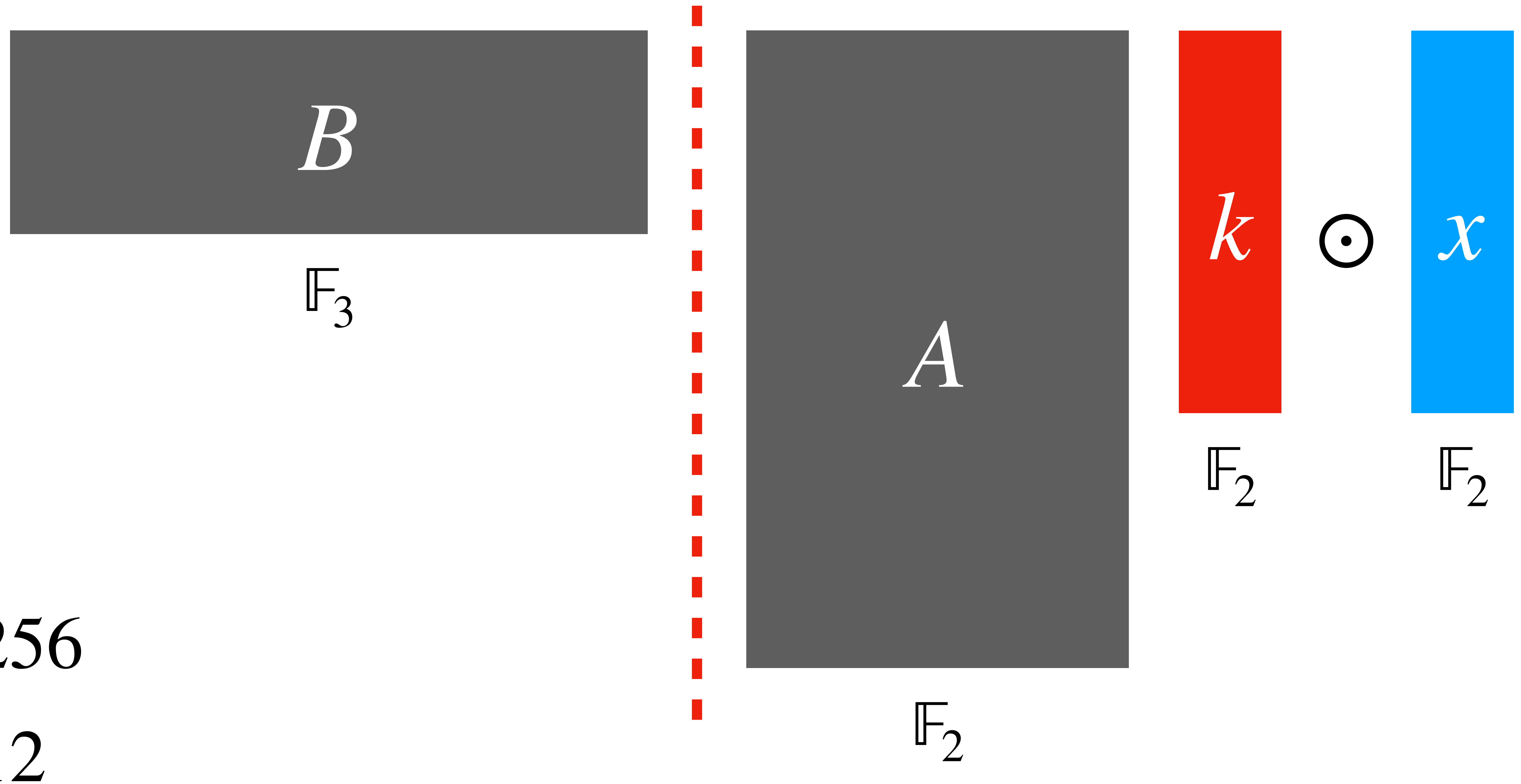
Ours: $y = B \cdot_3 (A \cdot_2 (k \odot_2 x))$

Linear time

Secret Key Vector

New wPRF

$y =$



- $A \sim 512 \times 256$
- $B \sim 81 \times 512$

OPRF Protocol

OPRF

OPRF

$$\mathsf{PRF}(k, x) \to y$$

OPRF

$$\mathsf{PRF}(k, x) \rightarrow y$$

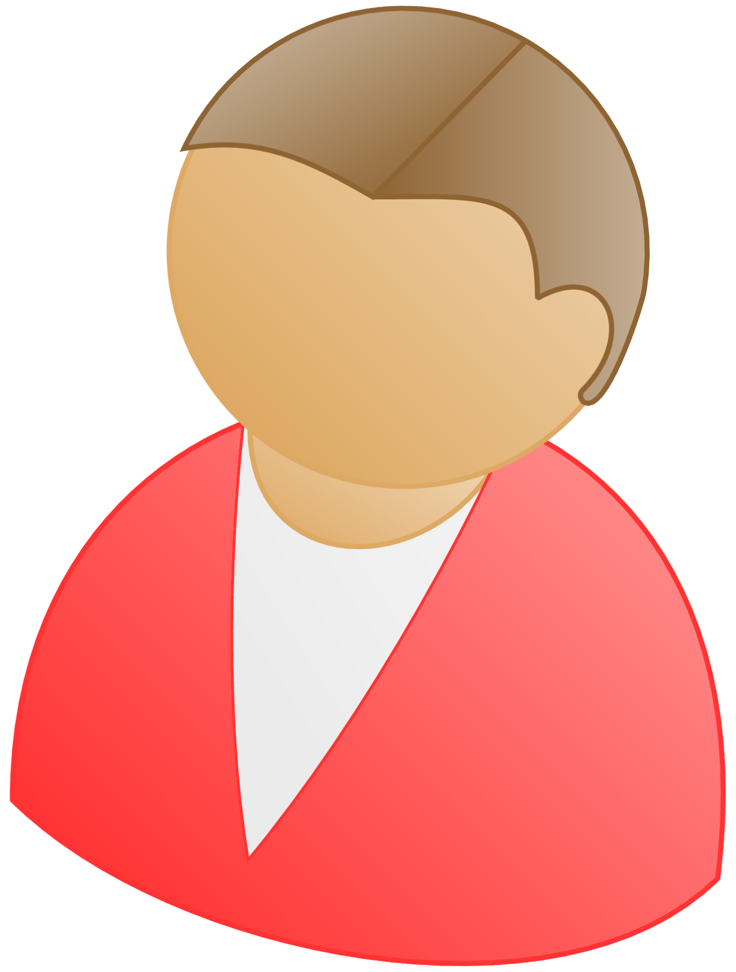
x

OPRF

$$\mathrm{PRF}(k, x) \rightarrow y$$

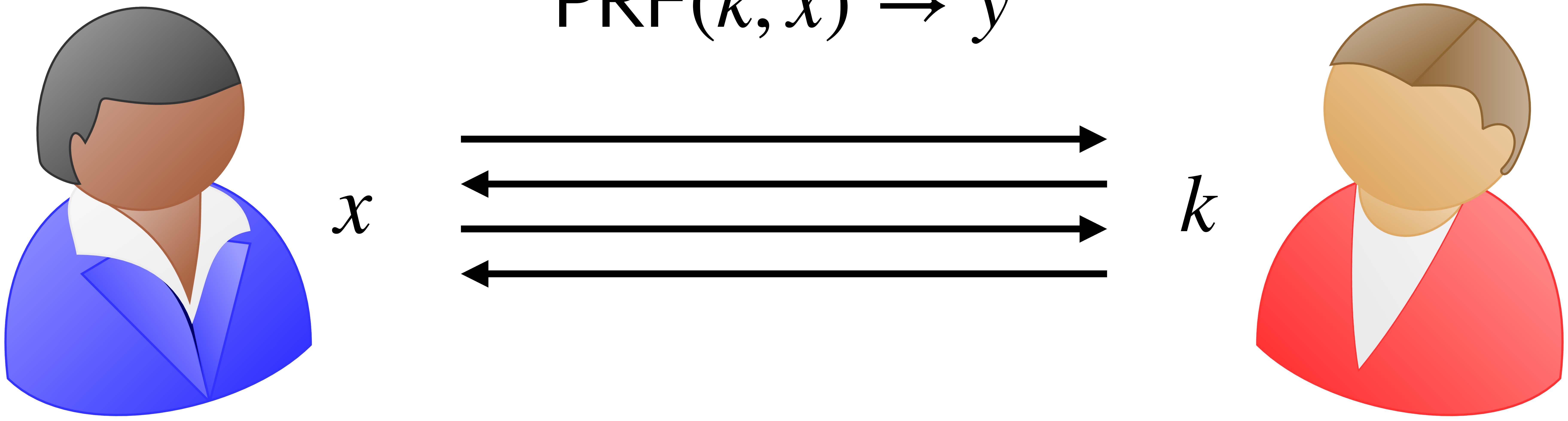
x

k



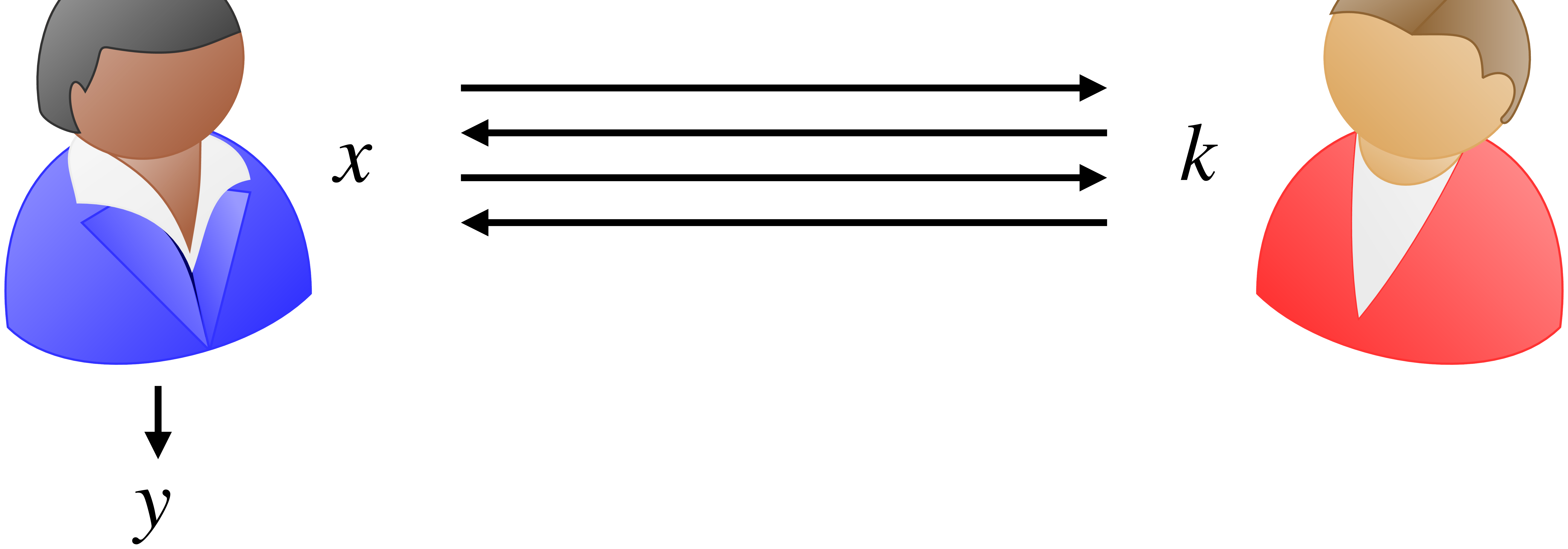
OPRF

$$\mathsf{PRF}(k, x) \to y$$

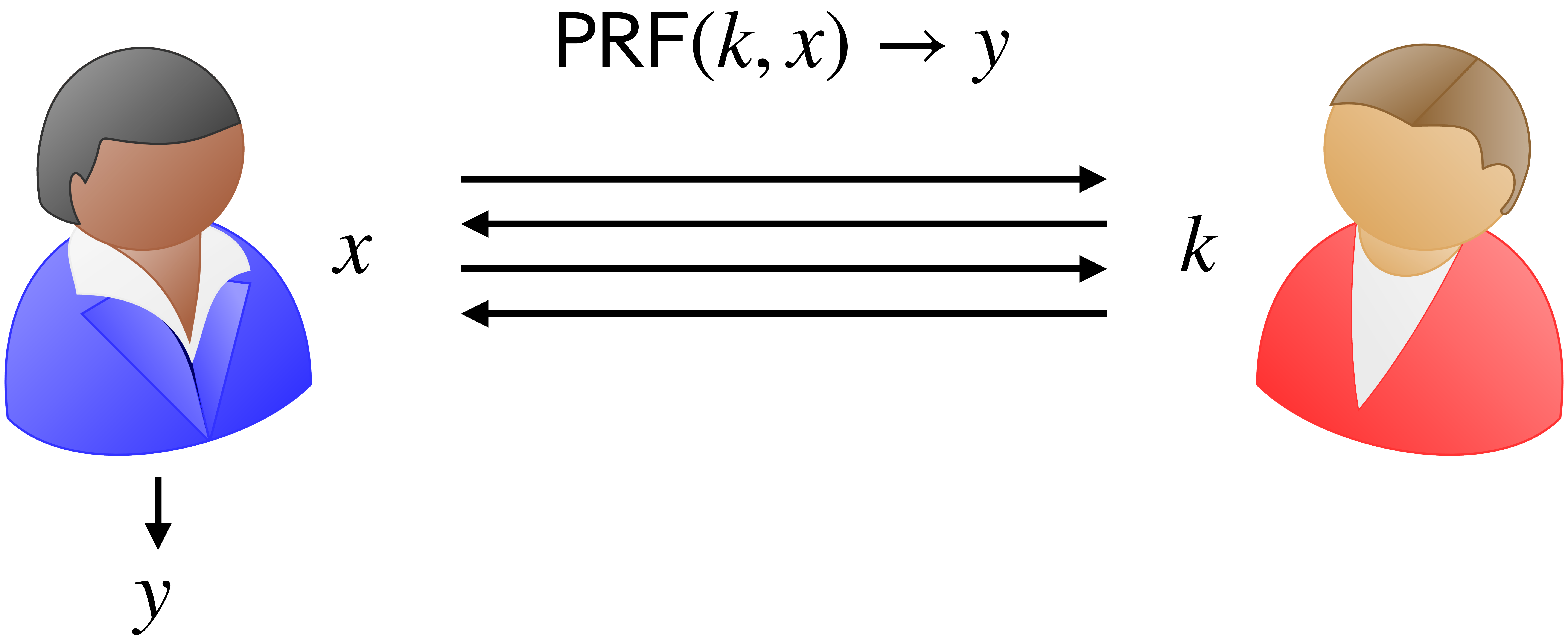


OPRF

$\mathsf{PRF}(k, x) \rightarrow y$



OPRF



Learns nothing about k

Learns nothing about x

Distributed wPRF evaluation

$$y = B \cdot_3 (A \cdot_2 (k \odot_2 x))$$

Distributed wPRF evaluation

$$y = B \cdot_3 (A \cdot_2 (k \odot_2 x))$$

Non-Linear

Distributed wPRF evaluation

$$y = B \cdot_3 (A \cdot_2 (k \odot_2 x))$$

Non-Linear

Implementing $k \odot x$:

Distributed wPRF evaluation

$$y = B \cdot_3 (A \cdot_2 (k \odot_2 x))$$

Non-Linear

Implementing $k \odot x$:

- **Observation:** k is the same across all evaluations

Distributed wPRF evaluation

$$y = B \cdot_3 (A \cdot_2 (k \odot_2 x))$$

Non-Linear

Implementing $k \odot x$:

- **Observation:** k is the same across all evaluations

$\Longrightarrow$ Can **reuse** OT correlations across evaluations!

Distributed wPRF evaluation

$$y = B \cdot_3 (A \cdot_2 (k \odot_2 x))$$

Non-Linear

Two approaches to implement $\mathbb{F}_2 \to \mathbb{F}_3$:

Distributed wPRF evaluation

$$y = B \cdot_3 (A \cdot_2 (k \odot_2 x))$$

Non-Linear

Two approaches to implement $\mathbb{F}_2 \rightarrow \mathbb{F}_3$:

- OT - Less communication but “consumes” OTs

Distributed wPRF evaluation

$$y = B \cdot_3 (A \cdot_2 (\textcolor{red}{k} \odot_2 \textcolor{blue}{x}))$$

Non-Linear

Two approaches to implement $\mathbb{F}_2 \rightarrow \mathbb{F}_3$:

- OT - Less communication but "consumes" OTs
- Garbling - More communication but no correlations needed

Evaluation

	Rounds	Comm. (bits)	Time (μs)
DDH [Mea86]	2	512	121
[DHG+21]	2*	65 + 1252	$25.4^{\dagger}$ + 6.1
Our Work (OT)	2*	38 + 916	7.0 + 0.4
Our Work (Garble)	2*	2^{15}	0.0 + $4.0^{\dagger}$
Our Work (Shared output)	1*	2^{15}	0.0 + $4.0^{\dagger}$

** excludes preprocessing rounds*
† denotes estimates

Wish List 🧞

Wish List 🧞

1. **More cryptanalysis!**
    - Better ways to analyze functions over alternating fields?
    - Post-Quantum cryptanalysis

Wish List 🧞

1. **More cryptanalysis!**
   - Better ways to analyze functions over alternating fields?
   - Post-Quantum cryptanalysis
2. **New primitives?**
   - We have OWFs and (w)PRFs. Can we have CRH? … or maybe even a Random Oracle?

Wish List 🧞

1. **More cryptanalysis!**
   - Better ways to analyze functions over alternating fields?
   - Post-Quantum cryptanalysis
2. **New primitives?**
   - We have OWFs and (w)PRFs. Can we have CRH? … or maybe even a Random Oracle?
3. **Better protocols!**
   - Only scratched the surface in terms of optimizing protocols
   - Also need better implementations!

Thank you!