

Zero-Knowledge Proofs for Syndrome Decoding from MPC-in-the-Head

Thibauld Feneuil

CRYPTOEXPERTS and SORBONNE UNIVERSITÉ

April 14, 2022

*Based on joint works with
Antoine Joux and Matthieu Rivain.*

Zero-Knowledge Proofs for Syndrome Decoding

Syndrome Decoding Problem on Random Linear Code

From (H, y) , find $x \in \mathbb{F}^m$ such that

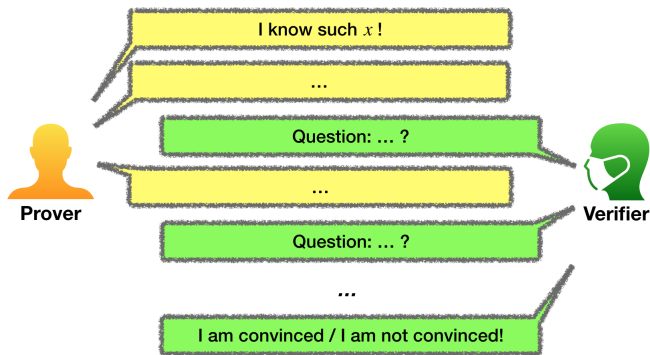
$$y = Hx \quad \text{and} \quad \text{wt}(x) = w.$$

Zero-Knowledge Proofs for Syndrome Decoding

Syndrome Decoding Problem on Random Linear Code

From (H, y) , find $x \in \mathbb{F}^m$ such that

$$y = Hx \quad \text{and} \quad \text{wt}(x) = w.$$

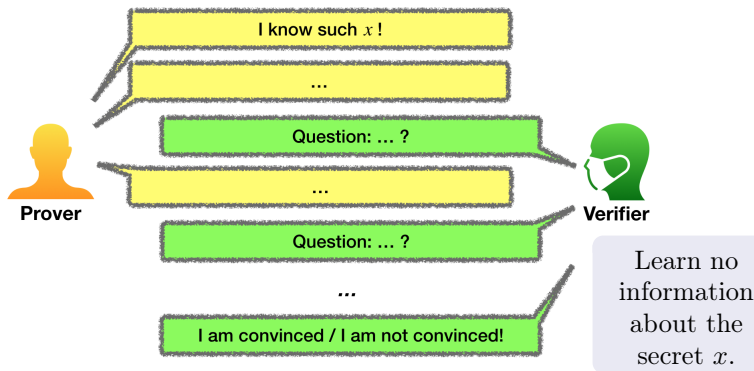


Zero-Knowledge Proofs for Syndrome Decoding

Syndrome Decoding Problem on Random Linear Code

From (H, y) , find $x \in \mathbb{F}^m$ such that

$$y = Hx \quad \text{and} \quad \text{wt}(x) = w.$$



MPC-in-the-Head Paradigm

MPC-in-the-Head Paradigm

- Generic technique to build *zero-knowledge protocols* using *multi-party computation*.
- Introduced in 2007 by:

[IKOS07] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai.
Zero-knowledge from secure multiparty computation. STOC 2007.

- Popularized in 2016 by *Picnic*, a candidate of the NIST Post-Quantum Cryptography Standardization.

Sharing of the secret

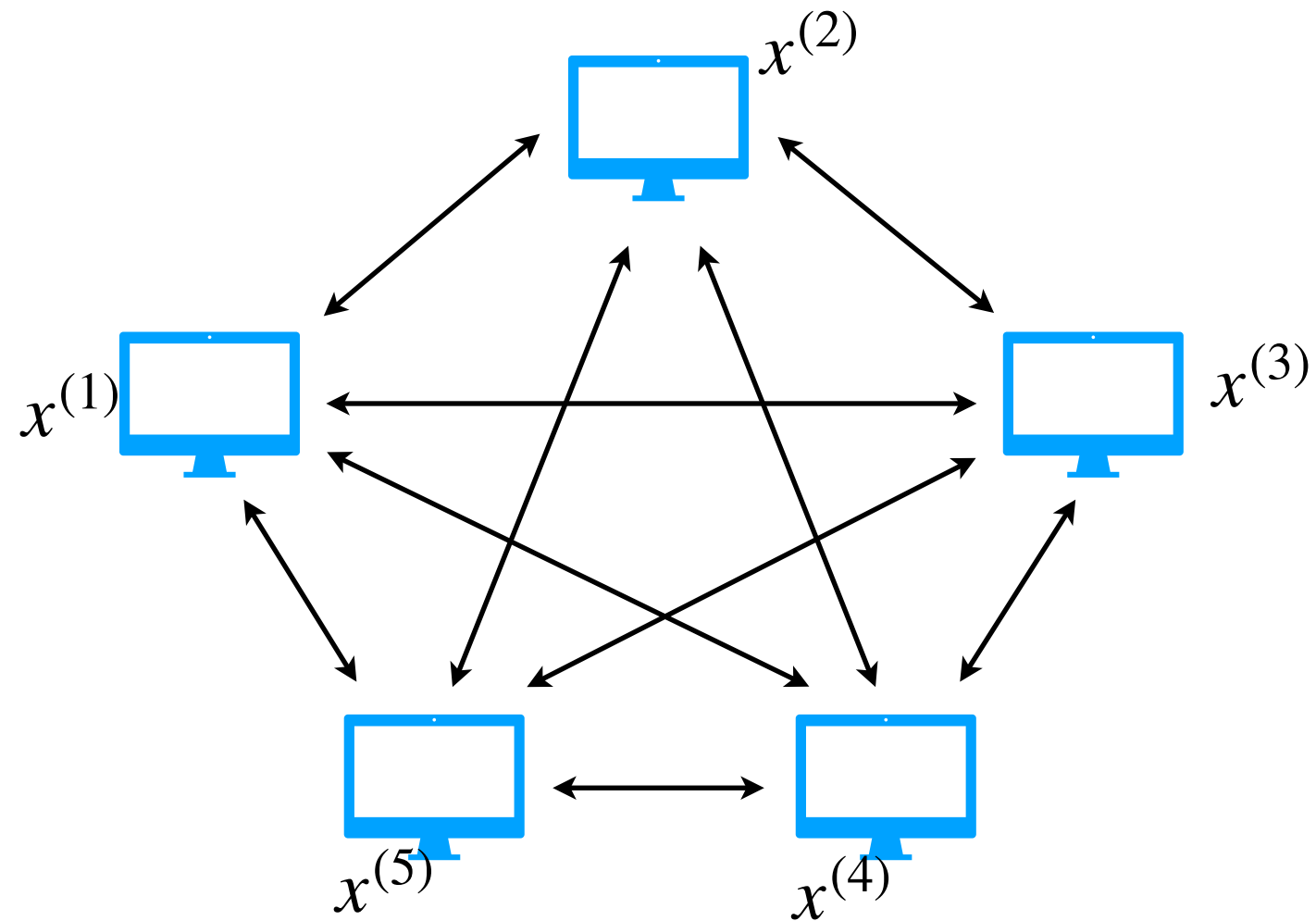
The secret x satisfies

$$y = Hx \quad \text{and} \quad \text{wt}(x) = w.$$

We share it in N parts:

$$x = x^{(1)} + x^{(2)} + \dots + x^{(N-1)} + x^{(N)}.$$

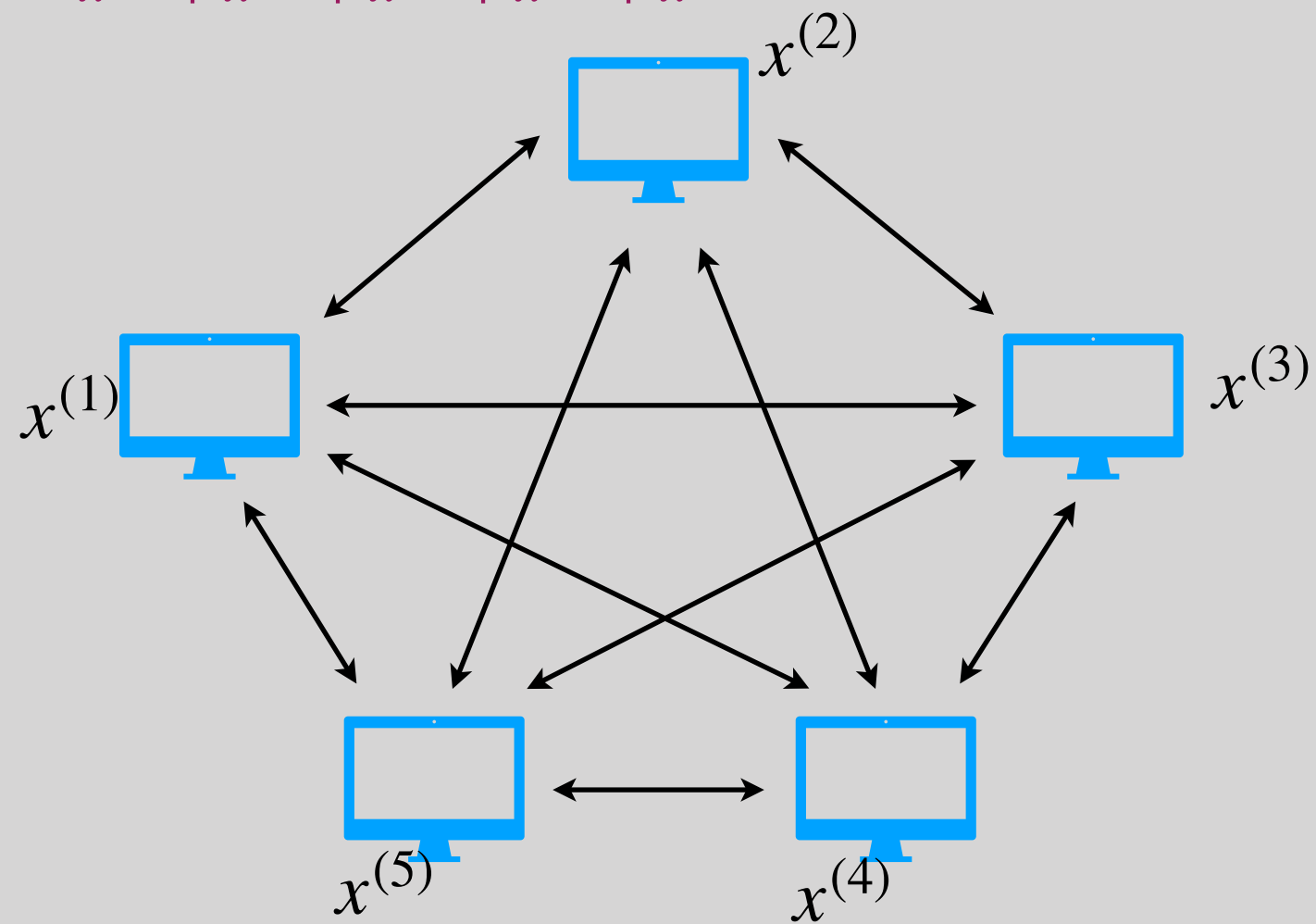
$$x = x^{(1)} + x^{(2)} + x^{(3)} + x^{(4)} + x^{(5)}$$



The multi-party computation outputs

- *Accept* if x is a syndrome decoding solution,
- *Reject* otherwise.

$$x = x^{(1)} + x^{(2)} + x^{(3)} + x^{(4)} + x^{(5)}$$

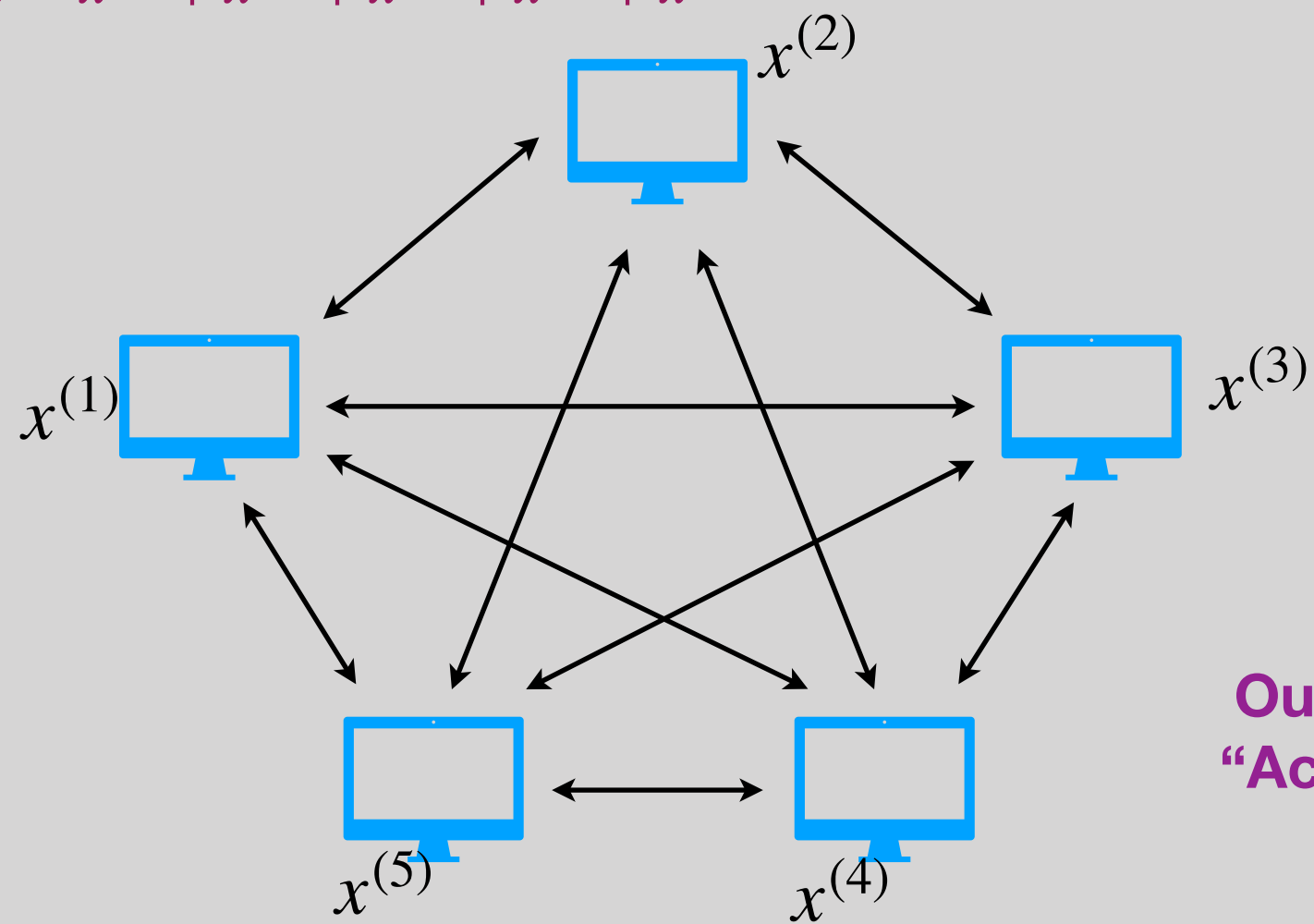


Honest Prover



Verifier

$$x = x^{(1)} + x^{(2)} + x^{(3)} + x^{(4)} + x^{(5)}$$



Outputs
“Accept”

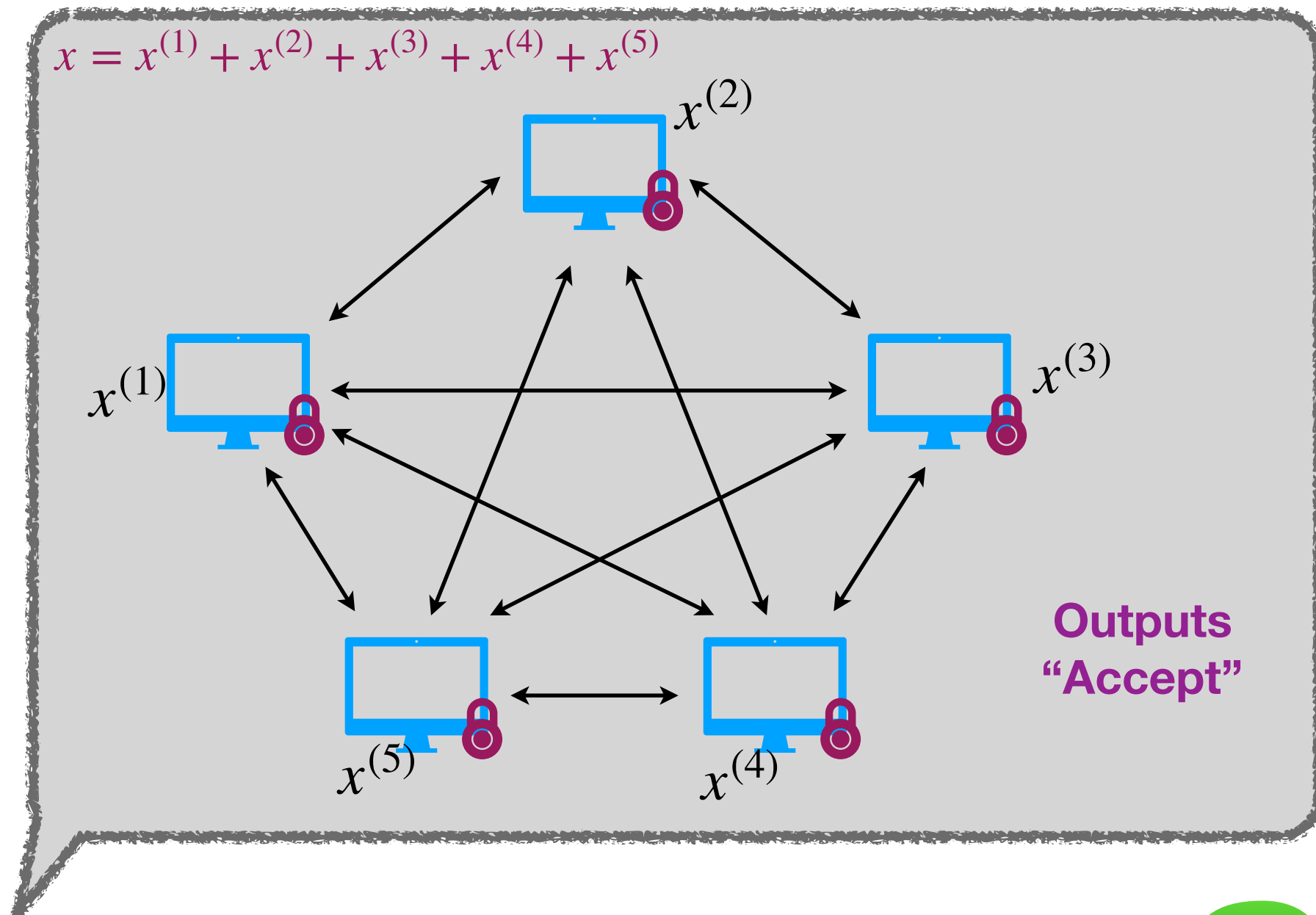


Honest Prover



Verifier

 = Commitment



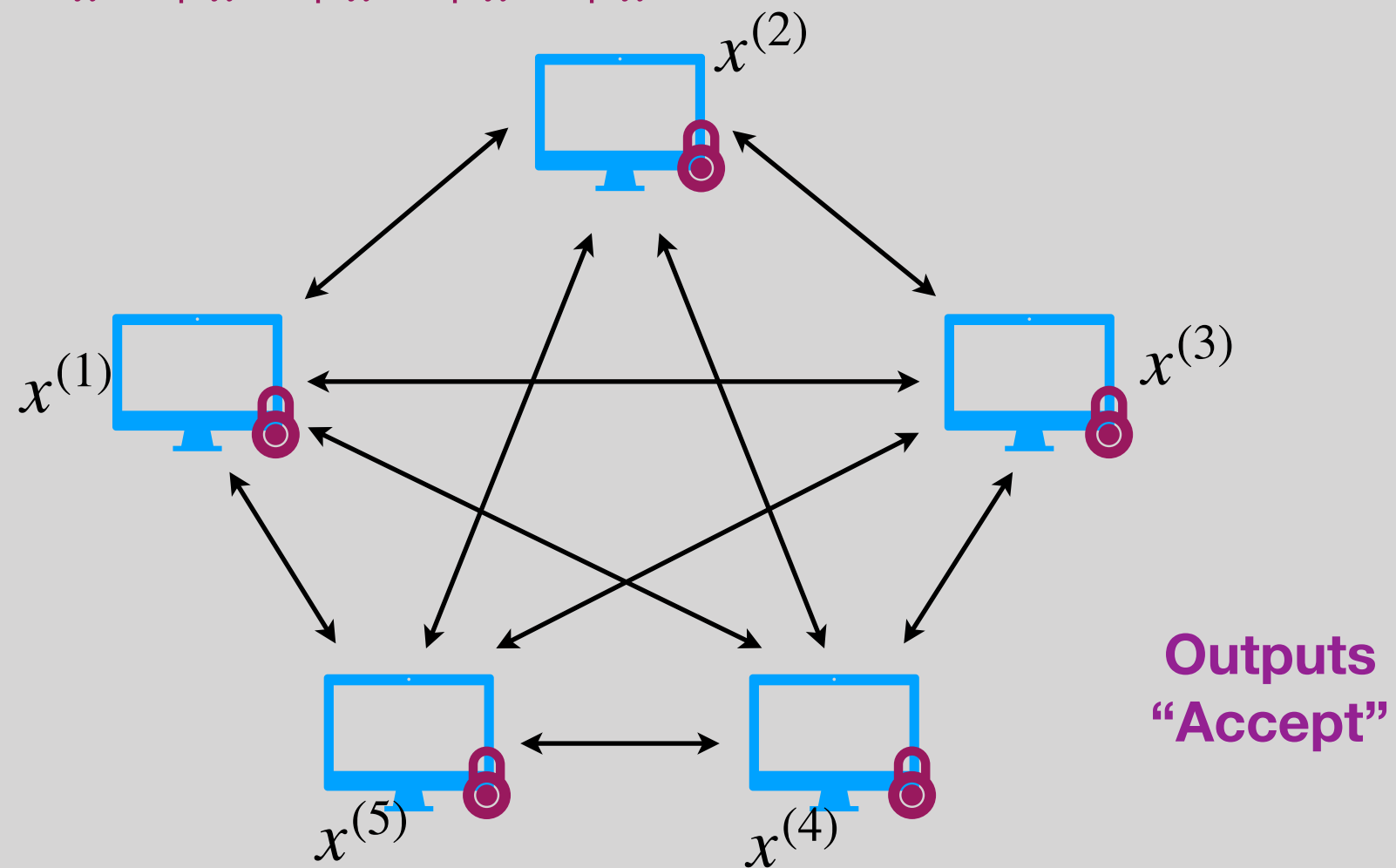
Honest Prover



Verifier

 = Commitment

$$x = x^{(1)} + x^{(2)} + x^{(3)} + x^{(4)} + x^{(5)}$$



Honest Prover

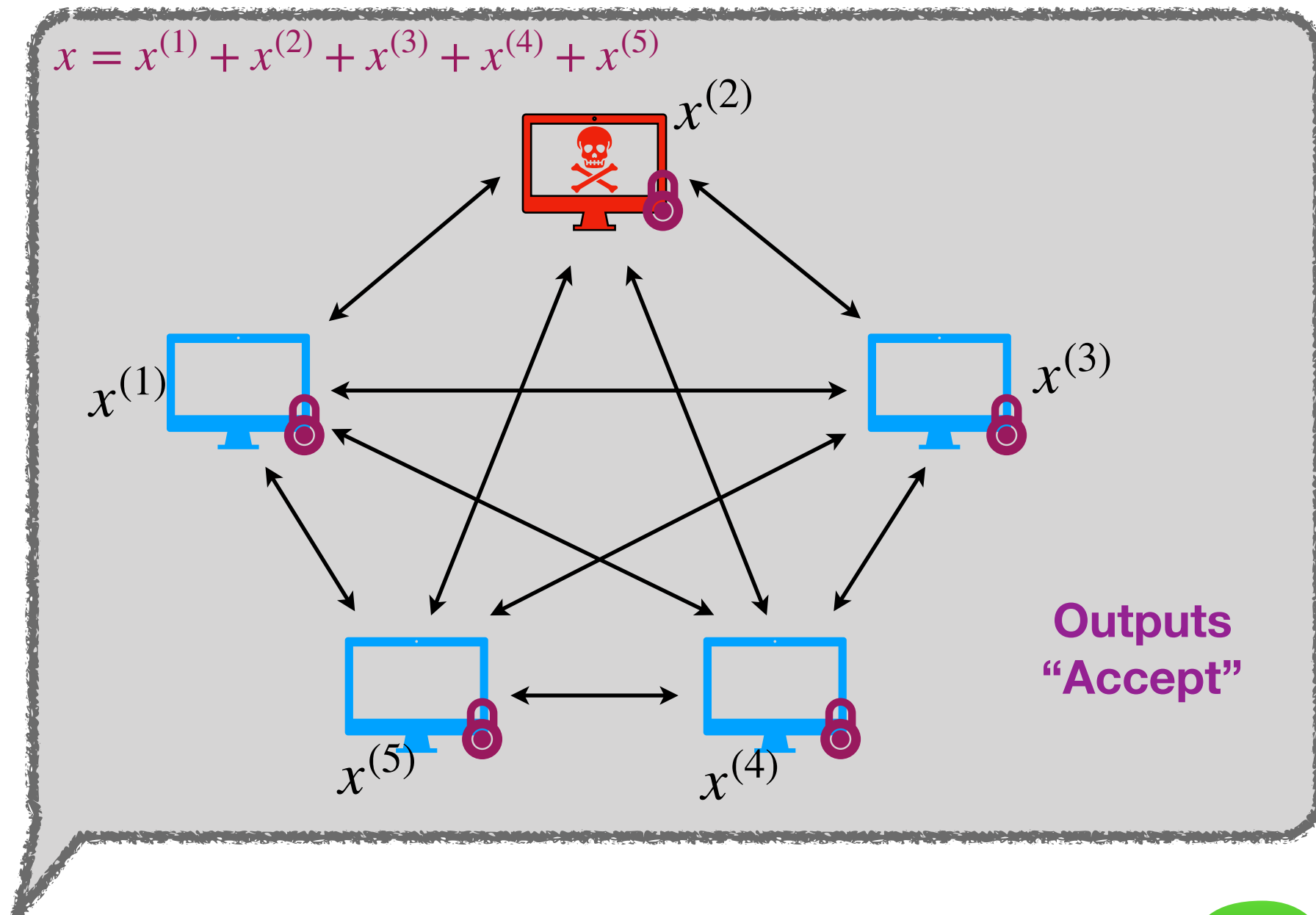
Reveal the views of every party
except Party 2.

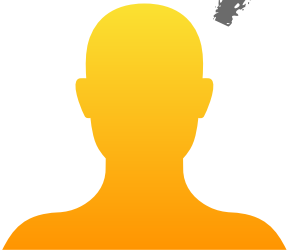
Seems OK...



Verifier

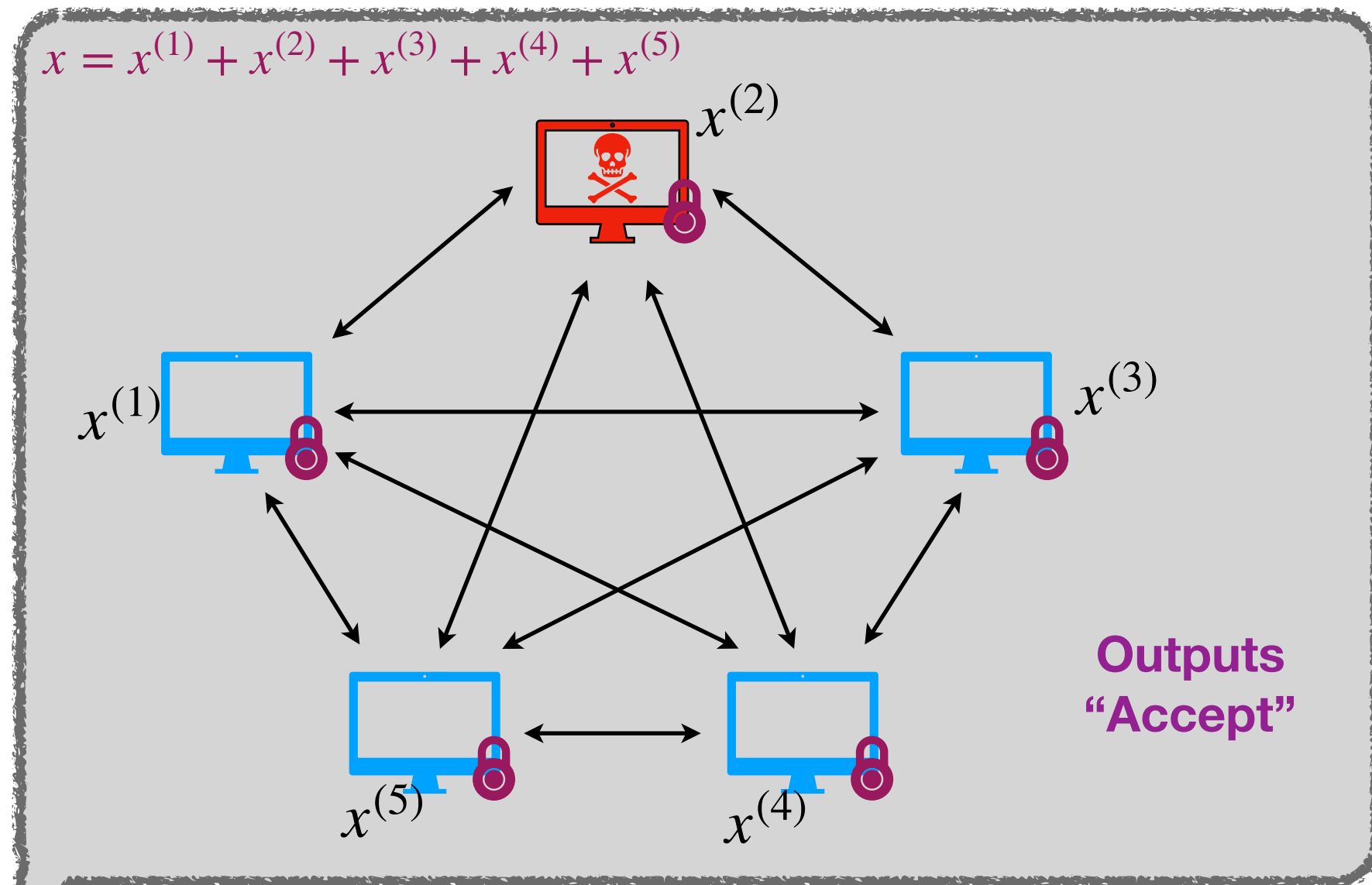
 = Commitment




Malicious Prover


Verifier

 = Commitment



Malicious Prover

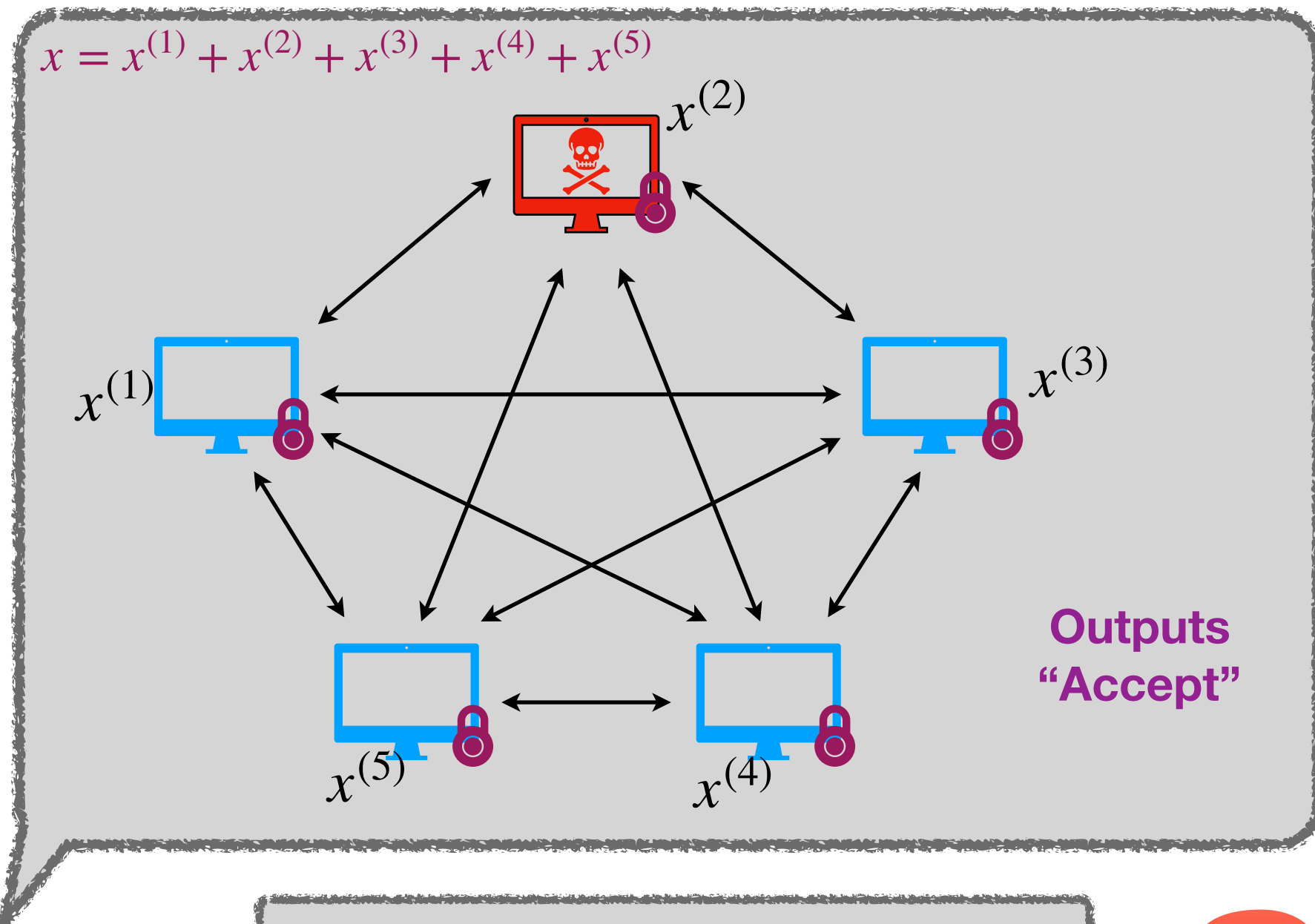
Reveal the views of every party
except Party 2.

Seems OK...



Verifier

 = Commitment



Malicious Prover

Reveal the views of every party
except Party 3.

You tried to cheat!!!!



Verifier

Zero-Knowledge Protocol

Soundness error:

$$\frac{1}{N}$$

Proof size: depends on the multi-party computation protocol

Two possible trade-offs:

- Repeat the protocol many times:
fast proofs, but large proofs
- Take a larger N :
short proofs, but slow proofs

State of the art about ZK PoK for SD

Protocol	Year	Assumption	Soundness err.
Stern's	1993	SD	$2/3$
Véron's	1997	SD	$2/3$
CVE's	2010	SD on $\mathbb{F}_q$	$\approx 1/2$
AGS's	2011	QCSD	$\approx 1/2$

State of the art about ZK PoK for SD

Protocol	Year	Assumption	Soundness err.
Stern's	1993	SD	$2/3$
Véron's	1997	SD	$2/3$
CVE's	2010	SD on $\mathbb{F}_q$	$\approx 1/2$
AGS's	2011	QCSD	$\approx 1/2$
GPS's	2021	SD on $\mathbb{F}_q$	$\approx 1/N$

[GPS21] Shay Gueron, Edoardo Persichetti, and Paolo Santini. *Designing a Practical Code-based Signature Scheme from Zero-Knowledge Proofs with Trusted Setup*. Eprint 2021/1020. Cryptography 2022.

State of the art about ZK PoK for SD

Protocol	Year	Assumption	Soundness err.
Stern's	1993	SD	$2/3$
Véron's	1997	SD	$2/3$
CVE's	2010	SD on $\mathbb{F}_q$	$\approx 1/2$
AGS's	2011	QCSD	$\approx 1/2$
GPS's	2021	SD on $\mathbb{F}_q$	$\approx 1/N$
BGKS's	2021	QCSD	$\approx 1/2$

[BGKS21] Loïc Bidoux, Philippe Gaborit, Mukul Kulkarni, Nicolas Sendrier.
Quasi-Cyclic Stern Proof of Knowledge. arXiv 2110.05005.

State of the art about ZK PoK for SD

Protocol	Year	Assumption	Soundness err.
Stern's	1993	SD	$2/3$
Véron's	1997	SD	$2/3$
CVE's	2010	SD on $\mathbb{F}_q$	$\approx 1/2$
AGS's	2011	QCSD	$\approx 1/2$
GPS's	2021	SD on $\mathbb{F}_q$	$\approx 1/N$
BGKS's	2021	QCSD	$\approx 1/2$
FJR21's	2021	SD	$\approx 1/N$

$$\sigma = \sigma_N \circ \sigma_{N-1} \circ \dots \circ \sigma_3 \circ \sigma_2 \circ \sigma_1$$

[FJR21] Thibauld Feneuil, Antoine Joux, and Matthieu Rivain. *Shared Permutation for Syndrome Decoding: New Zero-Knowledge Protocol and Code-Based Signature*. Eprint 2021/1576.

State of the art about ZK PoK for SD

Protocol	Year	Assumption	Soundness err.
Stern's	1993	SD	$2/3$
Véron's	1997	SD	$2/3$
CVE's	2010	SD on $\mathbb{F}_q$	$\approx 1/2$
AGS's	2011	QCSD	$\approx 1/2$
GPS's	2021	SD on $\mathbb{F}_q$	$\approx 1/N$
BGKS's	2021	QCSD	$\approx 1/2$
FJR21's	2021	SD	$\approx 1/N$
BGKM's	2022	SD	$\approx 1/N$

[BGKM22] Loïc Bidoux, Philippe Gaborit, Mukul Kulkarni, Victor Mateu.
Code-based Signatures from New Proofs of Knowledge for the Syndrome Decoding Problem. arXiv 2110.05005.

State of the art about ZK PoK for SD

Protocol	Year	Assumption	Soundness err.
Stern's	1993	SD	$2/3$
Véron's	1997	SD	$2/3$
CVE's	2010	SD on $\mathbb{F}_q$	$\approx 1/2$
AGS's	2011	QCSD	$\approx 1/2$
GPS's	2021	SD on $\mathbb{F}_q$	$\approx 1/N$
BGKS's	2021	QCSD	$\approx 1/2$
FJR21's	2021	SD	$\approx 1/N$
BGKM's	2022	SD	$\approx 1/N$
FJR22's	2022	SD	$\approx 1/N$

Prove $\text{wt}(x) \leq w$, not $\text{wt}(x) = w$.

$$Q(X) = \prod_{i: x_i \neq 0} (X - \gamma_i), \quad \deg Q = w$$

[FJR22] Thibault Feneuil, Antoine Joux, and Matthieu Rivain. *Syndrome Decoding in the Head: Shorter Signatures from Zero-Knowledge Proofs*. Eprint 2022/188.

Comparison Zero-Knowledge Protocol for SD

Name Protocol	Year	Instance 1	Instance 2
Stern	1993	37.4 KB	46.1 KB
Véron	1997	31.7 KB	38.7 KB
CVE10	2010	-	37.4 KB
GPS21 (fast)	2021	-	19.9 KB
GPS21 (short)	2021	-	15.2 KB
FJR21 (fast)	2021	20.7 KB	25.6 KB
FJR21 (short)	2021	13.6 KB	16.4 KB
FJR22 (fast)	2022	14.4 KB	9.7 KB
FJR22 (short)	2022	9.7 KB	6.9 KB
Field size q		2	256
Code length m		1280	208
Code dimension k		$m/2$	$m/2$
Hamming weight w		132	78
Security level λ		128	128

Prove only
an inequality

Comparison Code-based Signatures (1/2)

Scheme Name	sgn	pk	t_{sgn}	t_{verif}
BGS21	24.1 KB	0.1 KB	-	-
BGS21	22.5 KB	1.7 KB	-	-
GPS21 - 256	22.2 KB	0.11 KB	-	-
GPS21 - 1024	19.5 KB	0.12 KB	-	-
FJR21 (fast)	22.6 KB	0.09 KB	13 ms	12 ms
FJR21 (short)	16.0 KB	0.09 KB	62 ms	57 ms
BGKM22 - Sig1	23.7 KB	0.1 KB	-	-
BGKM22 - Sig2	20.6 KB	0.2 KB	-	-
FJR22 - $\mathbb{F}_2$ (fast)	15.6 KB	0.09 KB	-	-
FJR22 - $\mathbb{F}_2$ (short)	10.9 KB	0.09 KB	-	-
FJR22 - $\mathbb{F}_2$ (fast)	17.0 KB	0.09 KB	13 ms	13 ms
FJR22 - $\mathbb{F}_2$ (short)	11.8 KB	0.09 KB	64 ms	61 ms
FJR22 - $\mathbb{F}_{256}$ (fast)	11.5 KB	0.14 KB	6 ms	6 ms
FJR22 - $\mathbb{F}_{256}$ (short)	8.26 KB	0.14 KB	30 ms	27 ms

Comparison Code-based Signatures (2/2)

Scheme Name	$ \text{sgn} $	$ \text{pk} $	t_{sgn}	t_{verif}
Durandal - I	3.97 KB	14.9 KB	4 ms	5 ms
Durandal - II	4.90 KB	18.2 KB	5 ms	6 ms
LESS-FM - I	15.2 KB	9.78 KB	-	-
LESS-FM - II	5.25 KB	205 KB	-	-
LESS-FM - III	10.39 KB	11.57 KB	-	-
Wave	2.07 KB	3.2 MB	300 ms	-
FJR22 - $\mathbb{F}_2$ (fast)	15.6 KB	0.09 KB	-	-
FJR22 - $\mathbb{F}_2$ (short)	10.9 KB	0.09 KB	-	-
FJR22 - $\mathbb{F}_2$ (fast)	17.0 KB	0.09 KB	13 ms	13 ms
FJR22 - $\mathbb{F}_2$ (short)	11.8 KB	0.09 KB	64 ms	61 ms
FJR22 - $\mathbb{F}_{256}$ (fast)	11.5 KB	0.14 KB	6 ms	6 ms
FJR22 - $\mathbb{F}_{256}$ (short)	8.26 KB	0.14 KB	30 ms	27 ms

Conclusion

MPC-in-the-Head

- ☞ Useful combinatorial technique to produce zero-knowledge protocols.

MPC-in-the-Head for Syndrome Decoding

- ☞ Shorter proofs of knowledge.
- ☞ Currently gives the code-based signatures with the shortest “signature size + public key size”.

Remark: the applications of the MPC-in-the-Head paradigm are not limited to code-based problems.