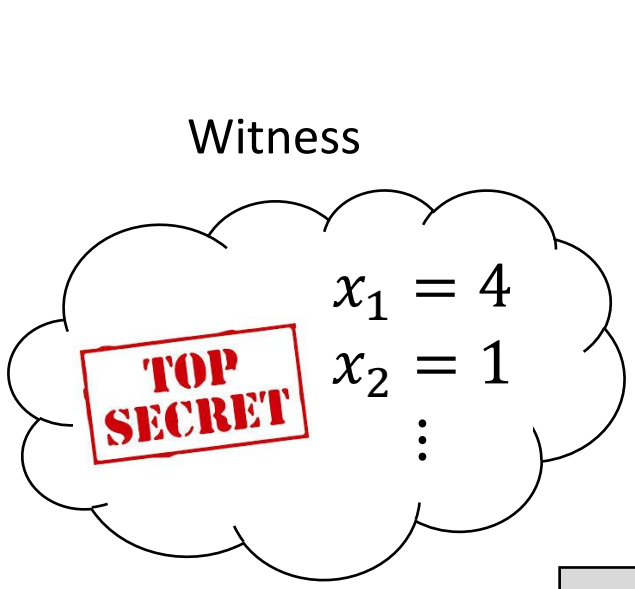
More Efficient Amortization of Exact Zero-Knowledge Proofs for LWE

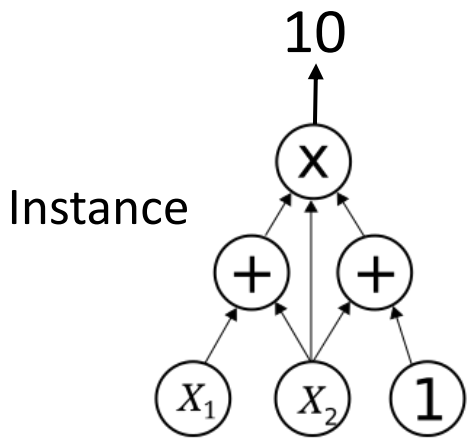
Jonathan Bootle

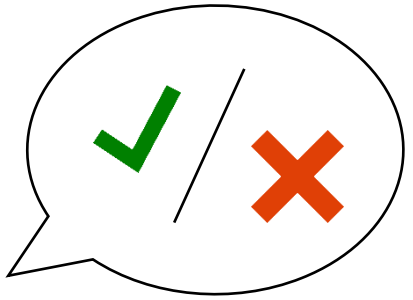
Joint work with Vadim Lyubashevsky, Ngoc Khanh Nguyen and Gregor Seiler

(IBM Research – Zurich)

Zero-knowledge proofs and arguments







P

V

Prover

Verifier

Completeness: if the witness is valid, the verifier accepts

Soundness: if the instance has no solution, the verifier rejects

Knowledge Soundness: the prover must know a witness

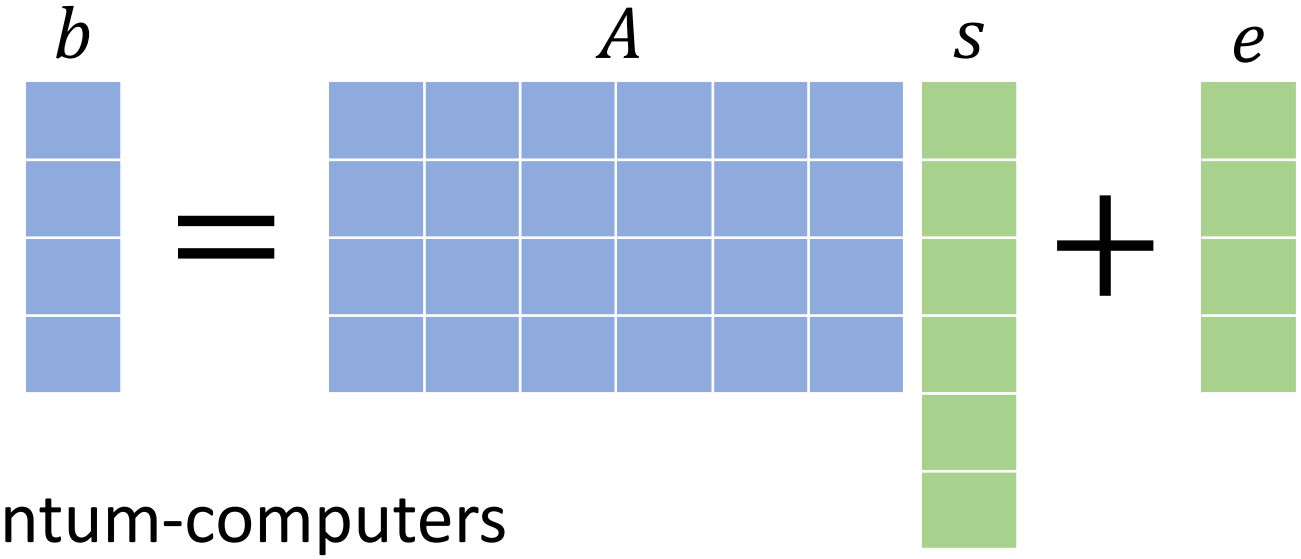
Zero-knowledge: the prover's messages leak nothing about the witness

The Search LWE Problem

Amortised case:

Prove knowledge of solutions to $(A, b_1), \ldots, (A, b_r)$

- Instance: $A \in \mathbb{Z}_p^{n \times m}$ and $b \in \mathbb{Z}_p^n$
- Witness: short $s \in \mathbb{Z}^m$ and $e \in \mathbb{Z}^n$ such that $b = As + e$

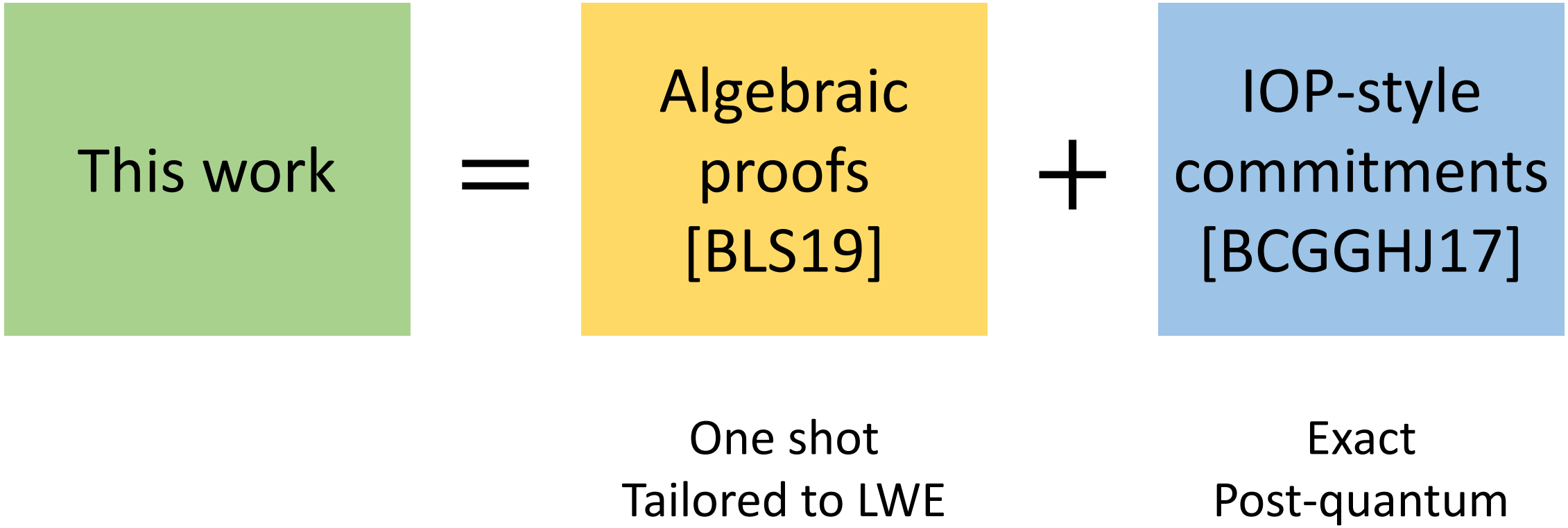


- Hard for quantum-computers
- Worst-to-average case reductions
- Used to construct signatures, encryption, FHE and much more

Types of Proofs

Algebraic	**Combinatorial**	**IOPs + Hash**	**Classical**
One shot	Multi shot	One shot	One shot
Relaxed	Exact	Exact	Exact
Relaxed: Shows prover knows less short (s, e) solution to (A, tb) **Multi shot:** Needs repeating to boost soundness		Target NP problems Post-quantum	Target many problems Quantum insecure

Overview of Approach



Results

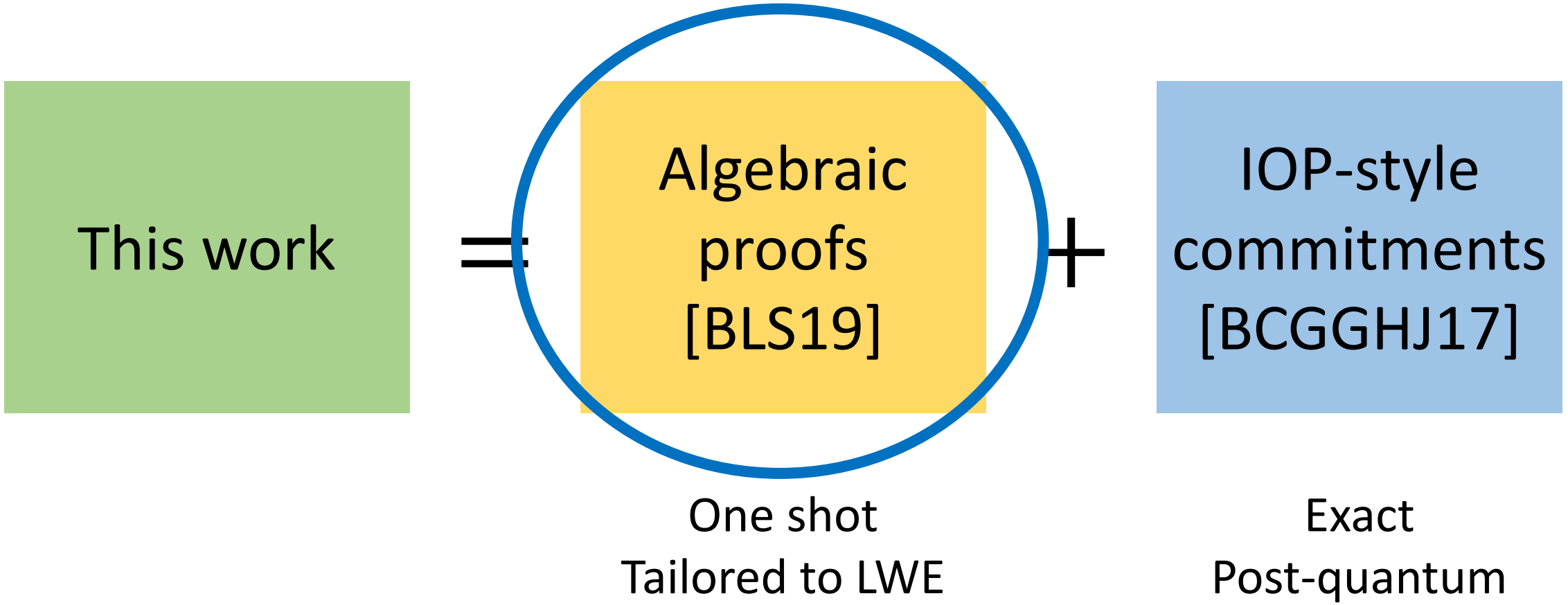
- Asymptotic ($n \times m$ matrix A)

# Instances	Prover time	Verifier time	Proof size
1	$O(mn)$ ops in $\mathbb{Z}_p$	$O(mn)$ ops in $\mathbb{Z}_p$	$O(m)$ elems in $\mathbb{Z}_p$
r	$O(rmn)$ ops in $\mathbb{Z}_p$	$O(mn + mr)$ ops in $\mathbb{Z}_p$	$O(m + r)$ elems in $\mathbb{Z}_p$

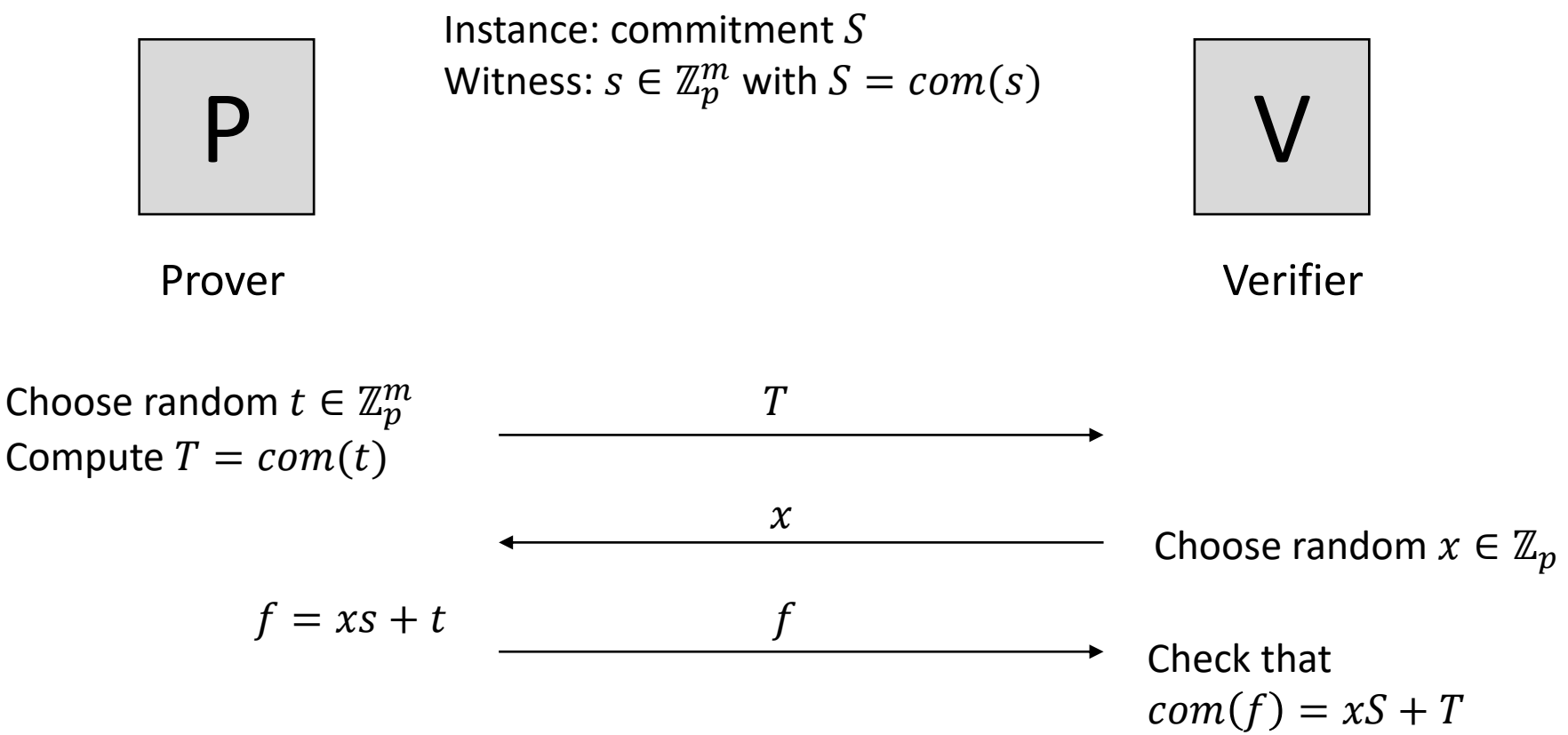
- Concrete proof size per instance

[ENS20]	[LNS21]	This work
47KB	33KB	2.3KB

Overview of Approach



A Basic Schnorr-like Proof



Extending to LWE instances

Prover commits to blue values before seeing x

- Use masked opening $f = sx + t$ to check useful conditions

$$s \in \{0,1\}^m$$
$$\Updownarrow$$
$$s \circ (1^m - s) = 0^m$$
$$\Updownarrow$$
$$f \circ (x \cdot 1^m - f) = x^2 \cdot 0^m + x \cdot u + v$$

Check $f \circ (x \cdot 1^m - f)$ is linear in x

$$b = As + e$$
$$\Updownarrow$$
$$e = b - As$$
$$\Updownarrow$$
$$g = x \cdot b - Af$$

Compute masked opening g of e from f

$$e \in \{0,1\}^n$$
$$\Updownarrow$$
$$e \circ (1^n - e) = 0^n$$
$$\Updownarrow$$
$$g \circ (x \cdot 1^n - g) = x^2 \cdot 0^n + x \cdot y + z$$

Check $g \circ (x \cdot 1^n - g)$ is linear in x

Proof for a Single LWE Instance

Instance: LWE instance (A, b)
Witness: s, e with $b = As + e$

P

Prover

V

Verifier

Proof for many instances embeds many secrets s into f using interpolation

Compute $S = com(s)$
Choose random $t \in \mathbb{Z}_p^m$, compute $T = com(t)$
Compute $f \circ (x \cdot 1^m - f) = x \cdot u + v$
Compute $g = x \cdot b - Af$
Compute $g \circ (x \cdot 1^n - g) = x \cdot y + z$
Compute commitments U, V, Y, Z to u, v, y, z

S, T, U, V, Y, Z →

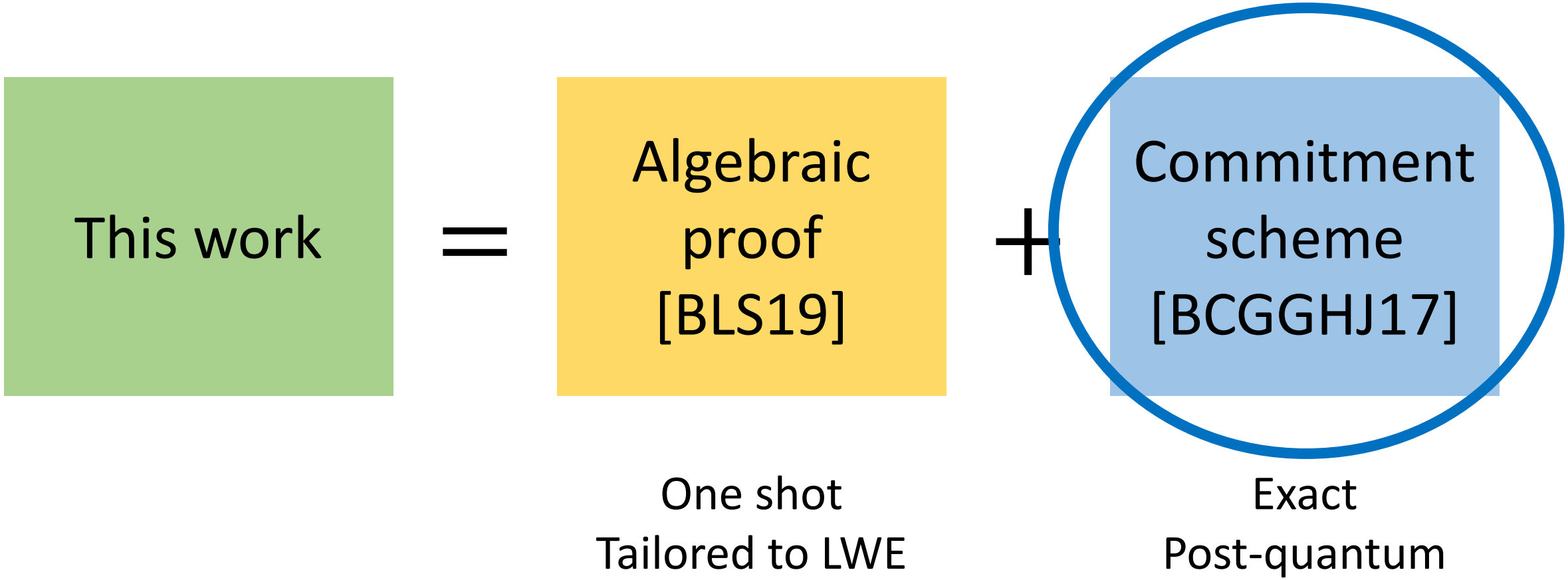
← x

Choose random $x \in \mathbb{Z}_p$

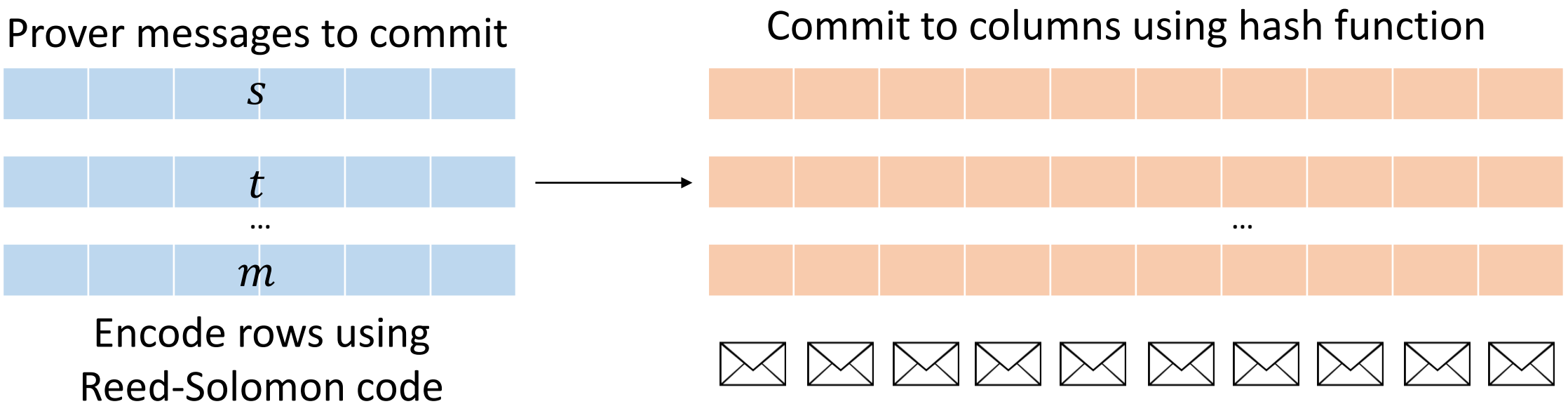
$f = xs + t$ → f

Compute $g = xb - Af$
Check that $com(f) = xS + T$
$com\big(f \circ (x1^m - f)\big) = xU + V$
$com\big(g \circ (x1^m - g)\big) = xY + Z$

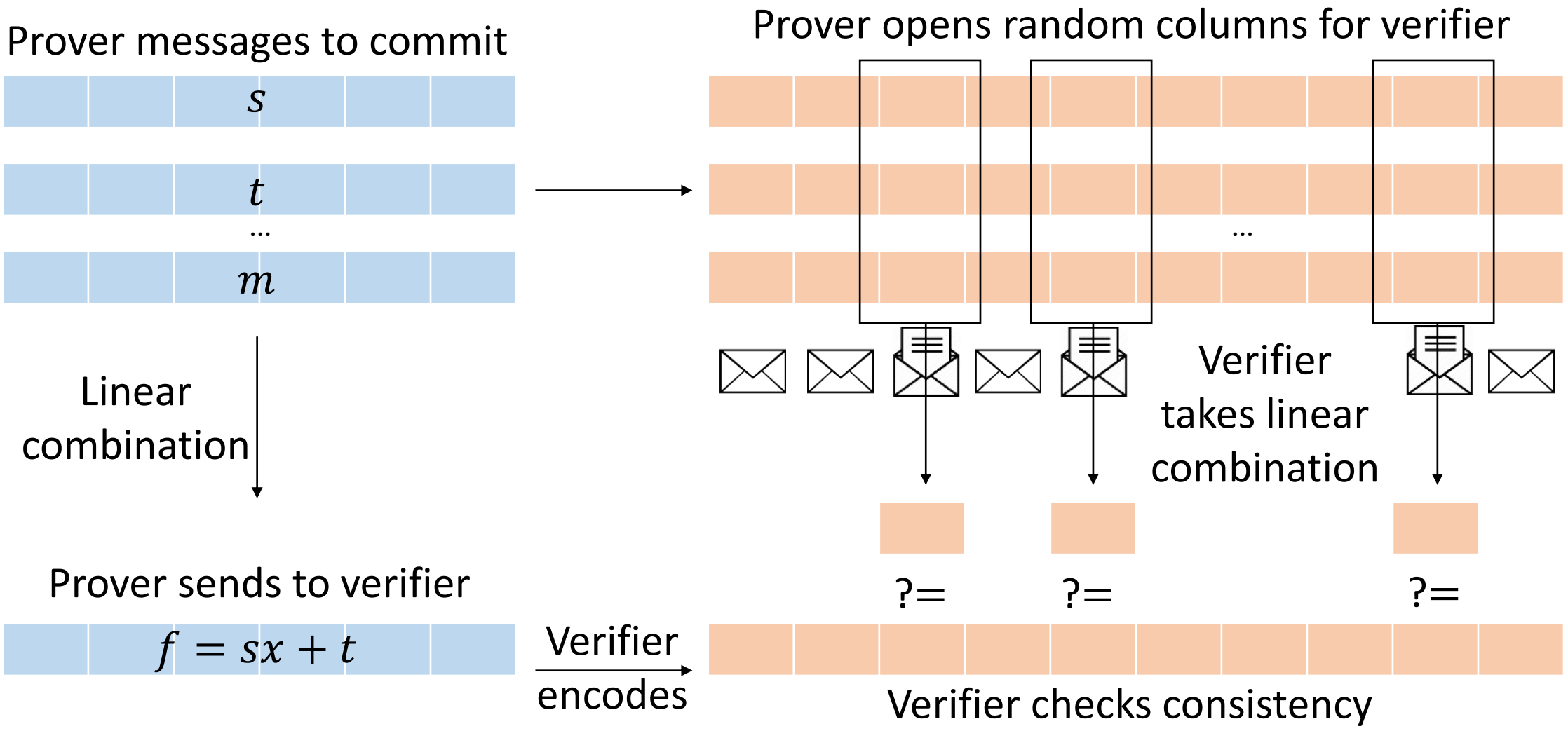
Overview of Approach



The commitment scheme

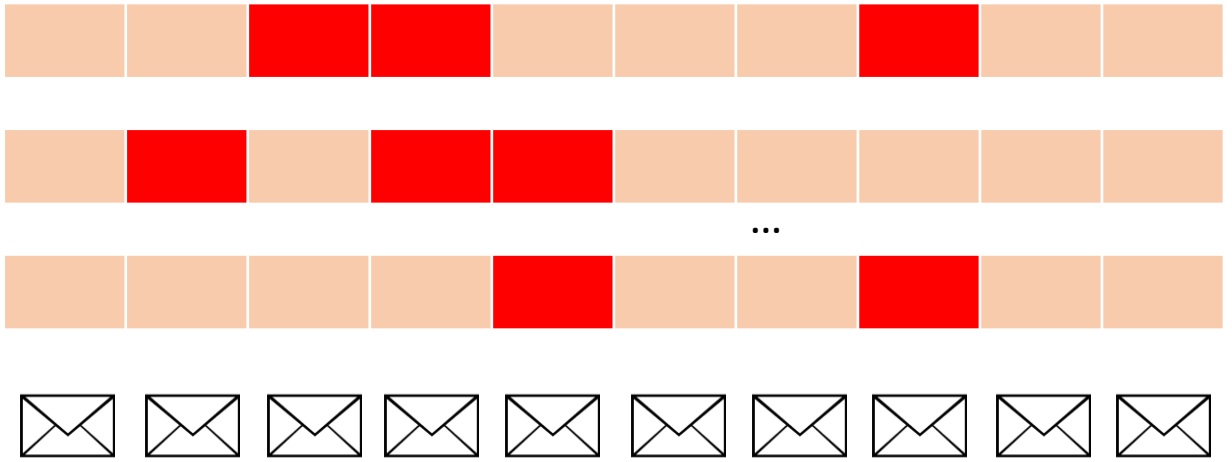


Commitment openings

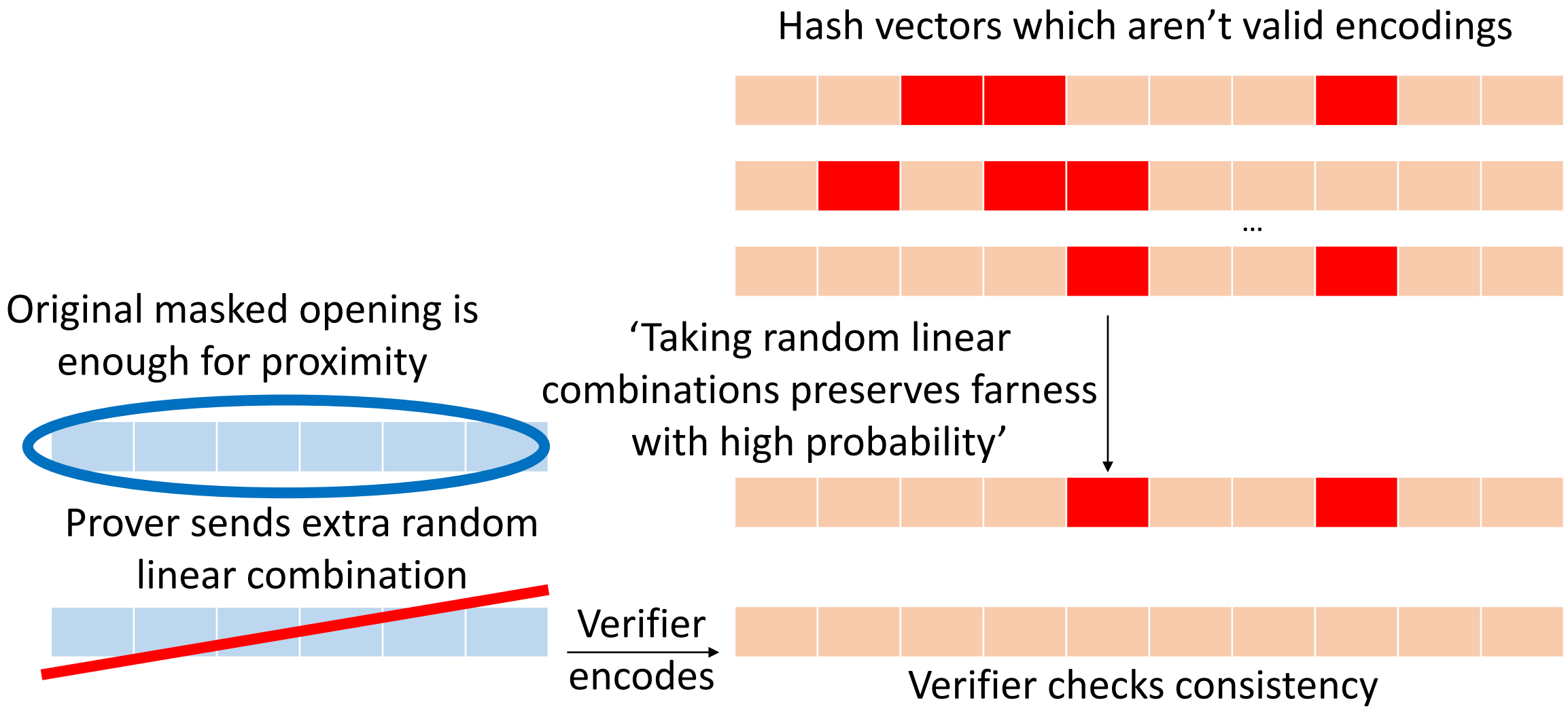


How can the prover cheat?

Hash vectors which aren’t valid encodings



Forcing valid encodings with a proximity test

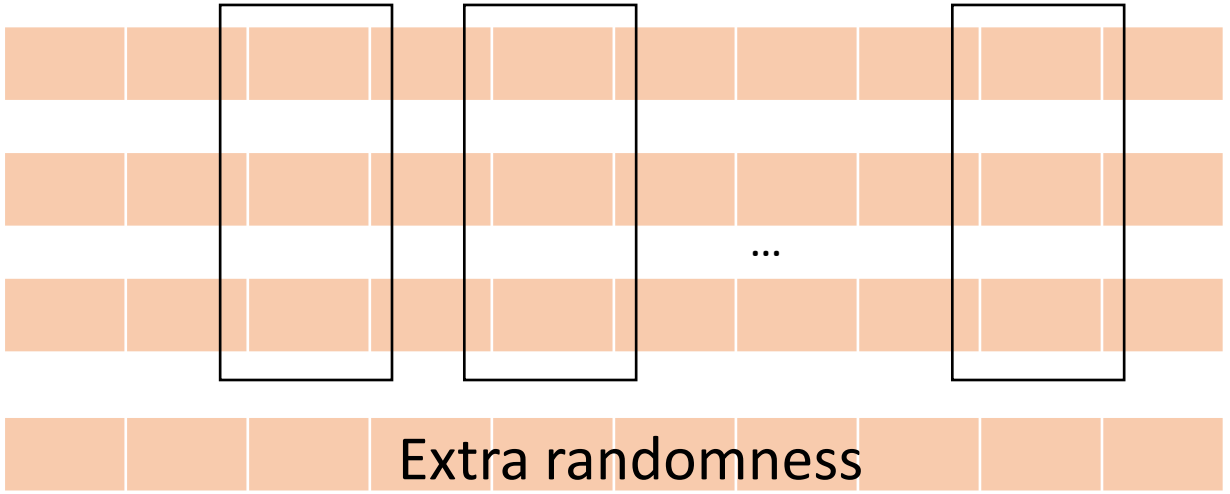


Zero Knowledge Sketch

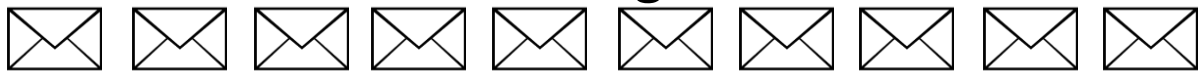
Prover messages to commit

Encode rows and extra randomness with Reed-Solomon code

Opening a few columns leaks no information on messages



Commit to columns and extra randomness using hash function



Unopened commitments leak no information on messages

Thanks!

- Asymptotic

# Instances	Prover time	Verifier time	Proof size
1	$O(mn)$ ops in $\mathbb{Z}_p$	$O(mn)$ ops in $\mathbb{Z}_p$	$O(m)$ elems in $\mathbb{Z}_p$
r	$O(rmn)$ ops in $\mathbb{Z}_p$	$O(mn + mr)$ ops in $\mathbb{Z}_p$	$O(m + r)$ elems in $\mathbb{Z}_p$

- Concrete proof size per instance

[ENS20]	[LNS21]	This work
47KB	33KB	2.3KB

- https://ia.cr/2020/1449