Linear-Time Zero-Knowledge Proofs for Arithmetic Circuit Satisfiability

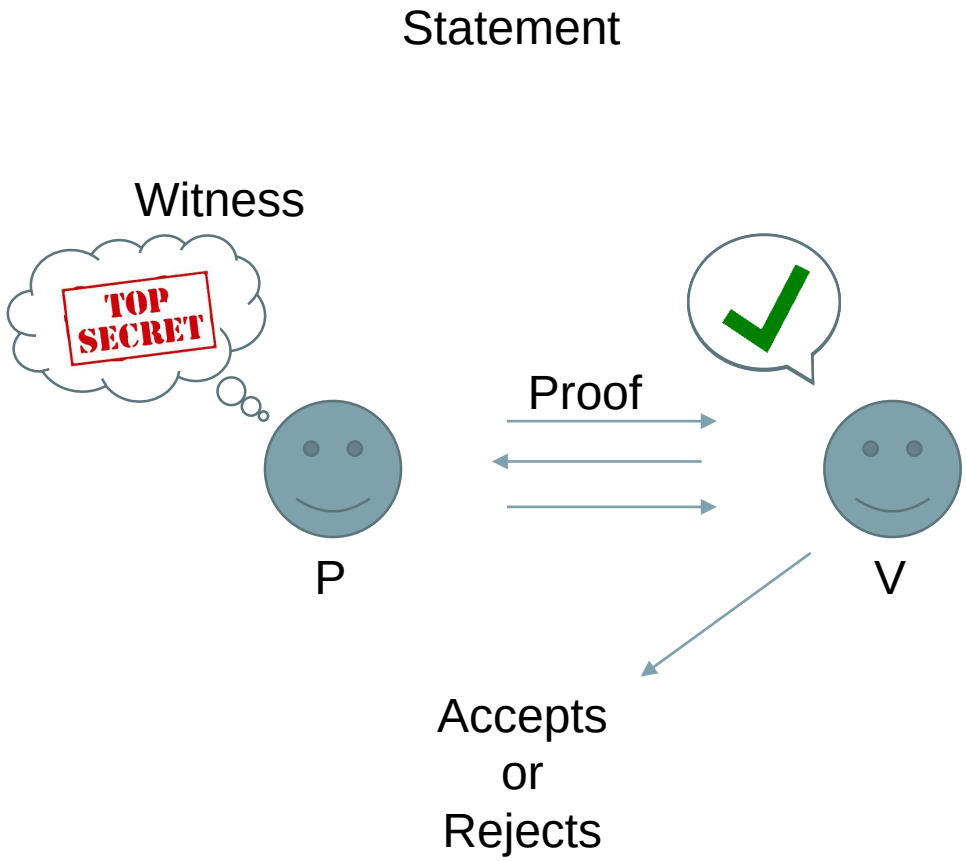
Jonathan Bootle, Andrea Cerulli, Essam Ghadafi, Jens Groth, Mohammad Hajiabadi and Sune K. Jakobsen

European Research Council
Established by the European Commission

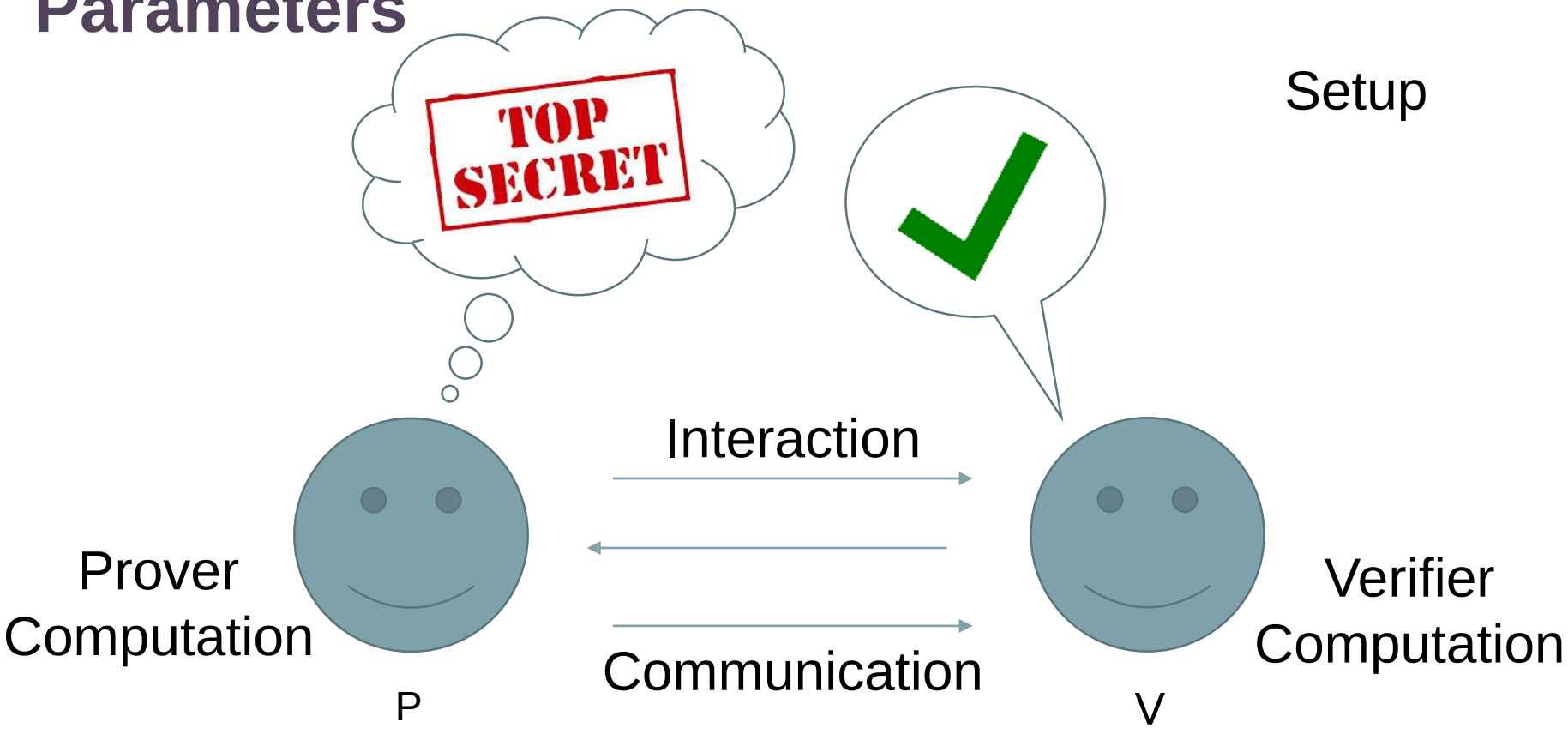
Zero Knowledge Proofs

- Completeness
- Soundness
- Zero-Knowledge

- Proof of Knowledge
- Interactive
- Public-coin



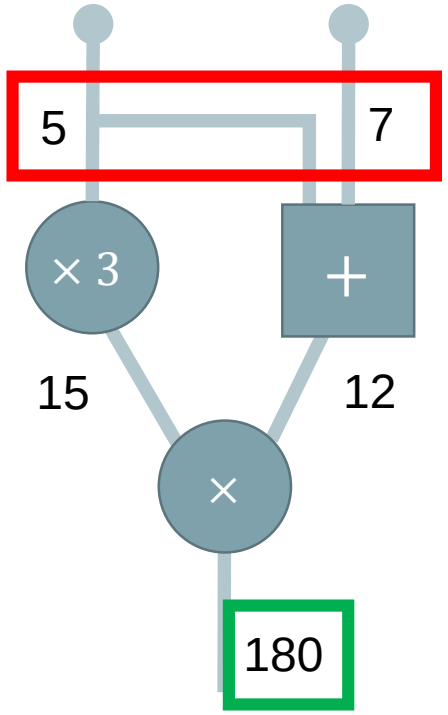
Parameters



Goal: constant computational overhead for the Prover

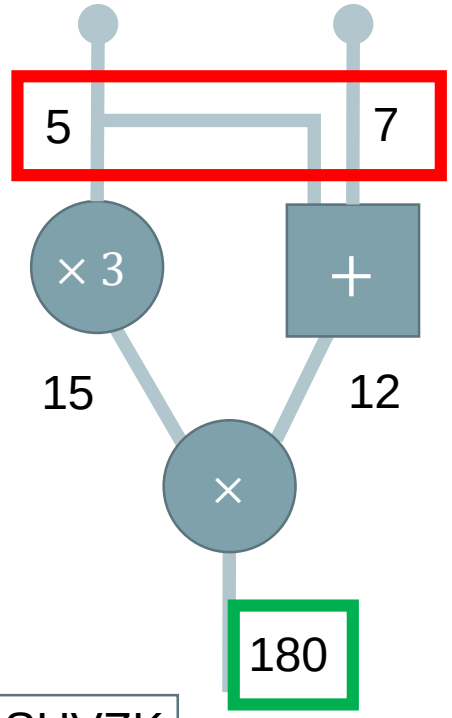
Arithmetic Circuits

- Prover knows inputs
- Publicly known outputs
- Check inputs give the correct outputs
- Do valid inputs exist? NP-Complete



Results

- Security parameter λ
- Finite field F, 2^{λ} elements
- Arithmetic circuit,
  N = poly(λ) gates
- Zero-knowledge arguments
  and proofs

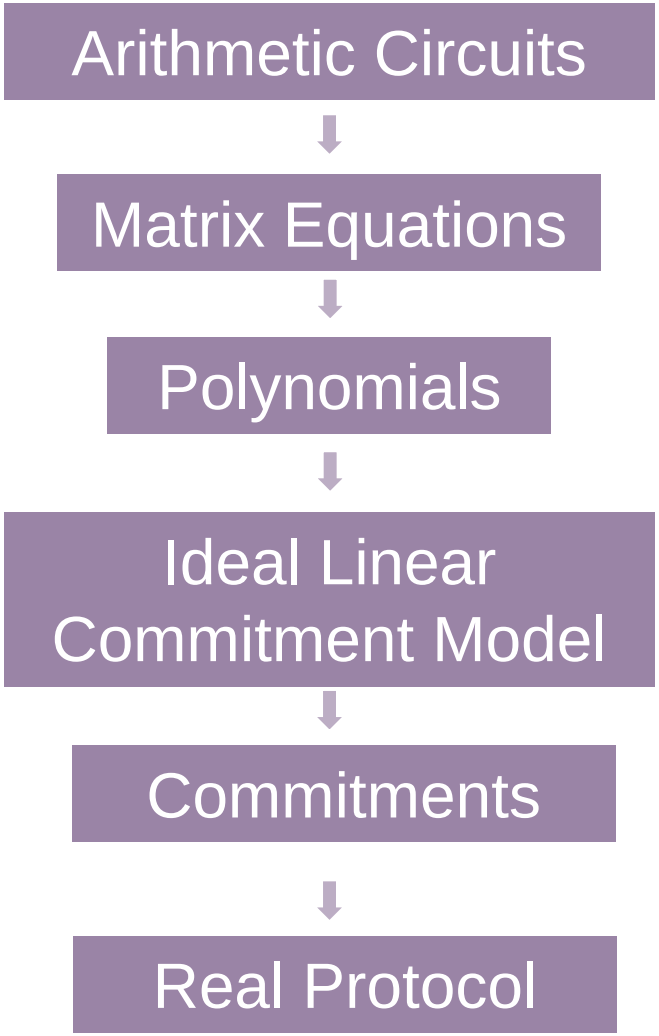


Statistical SHVZK

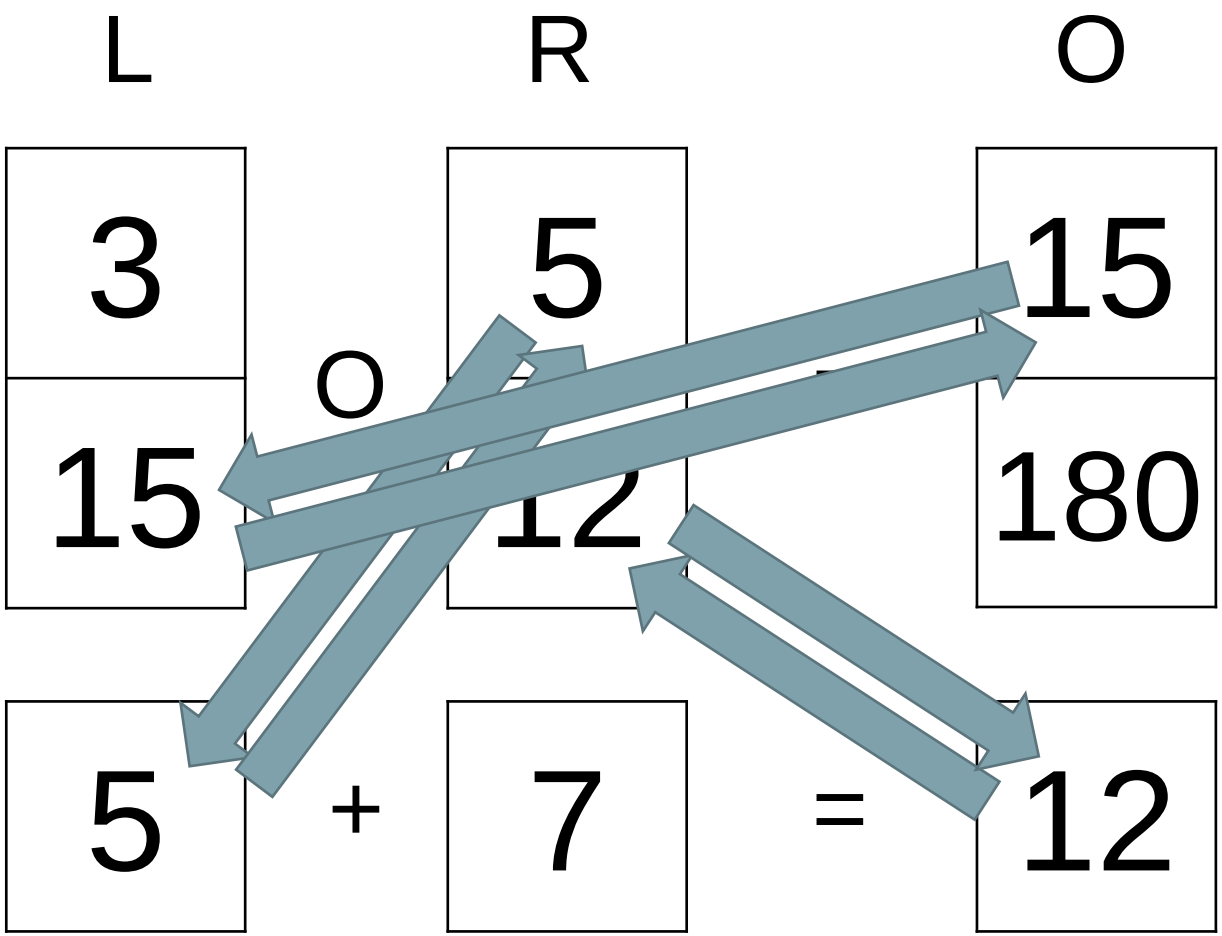
Prover	Verifier	Comm.	Rounds	Assumption
O(N) multiplications in F	o(N) multiplications in F	poly(λ)√N elements of F	O(loglog N)	lt-CRHF
O(N) multiplications in F	o(N) multiplications in F	O(N) elements of F	O(loglog N)	lt-OWF

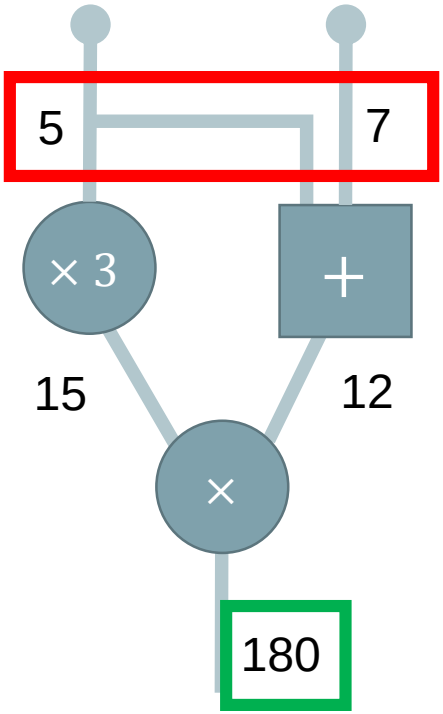
Statistical Soundness

Overview

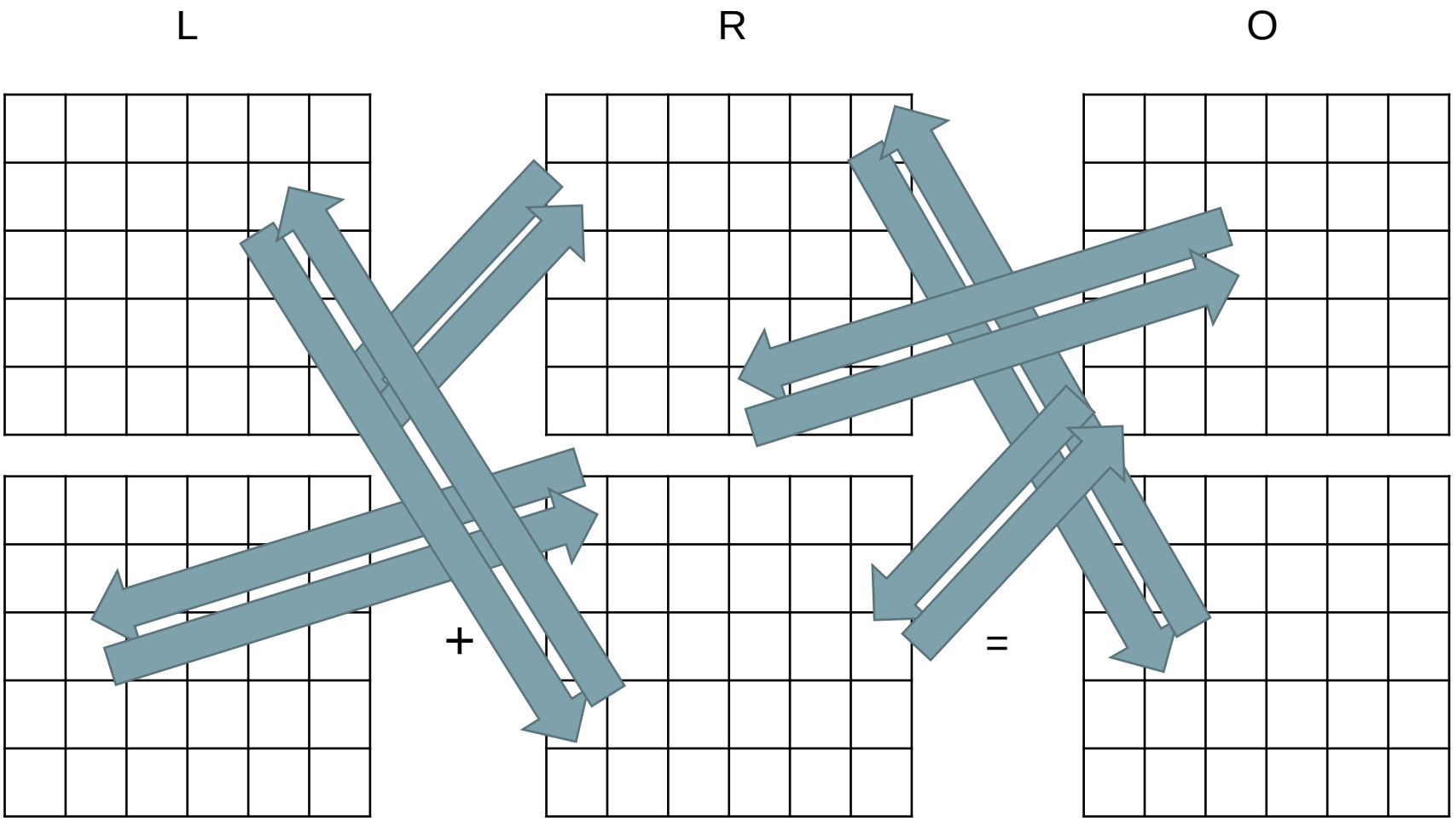

Arithmetic Circuits
Matrix Equations
Polynomials
Ideal Linear Commitment Model
Commitments
Real Protocol

High Level Structure

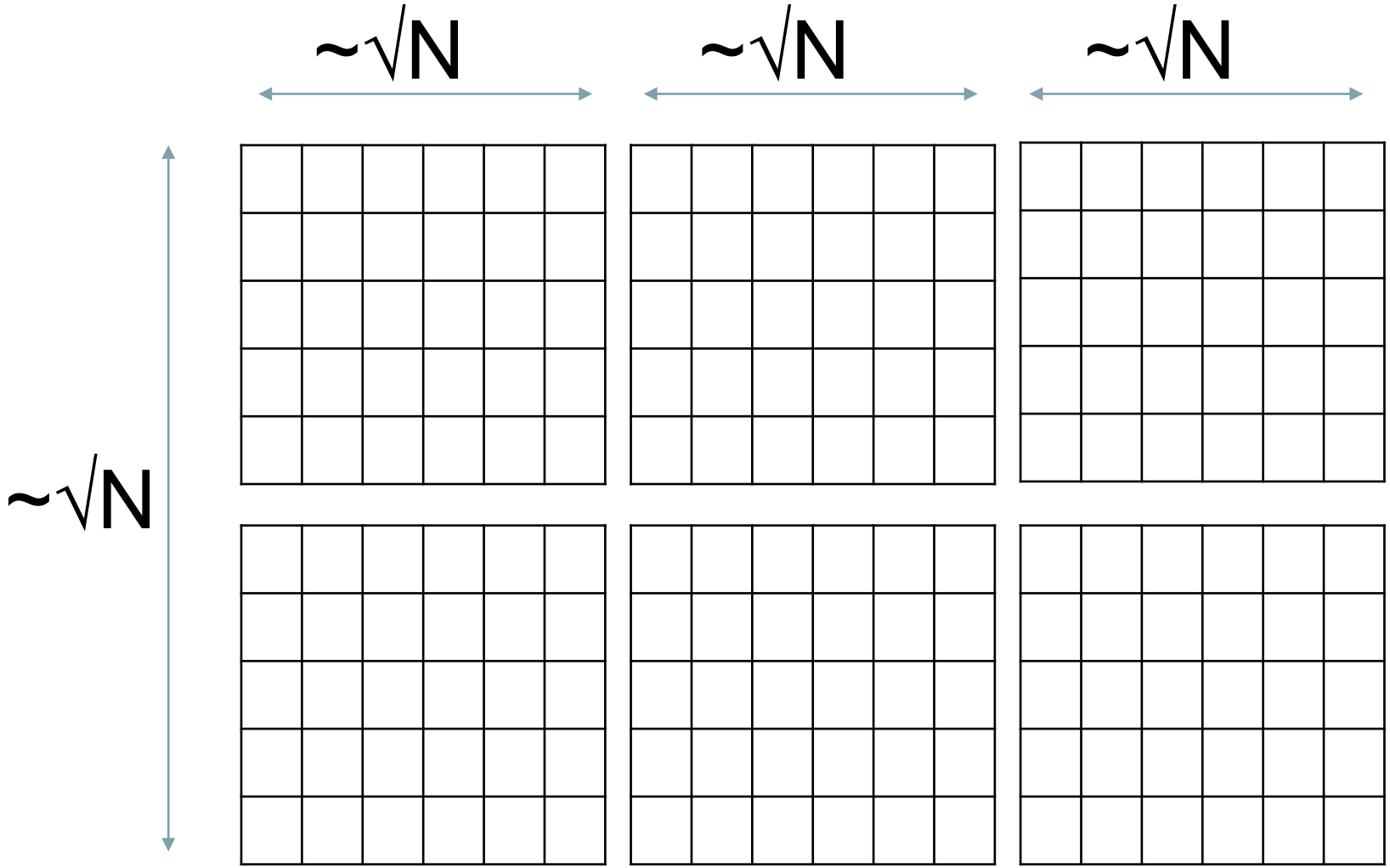




High Level Structure



Matrix Dimensions

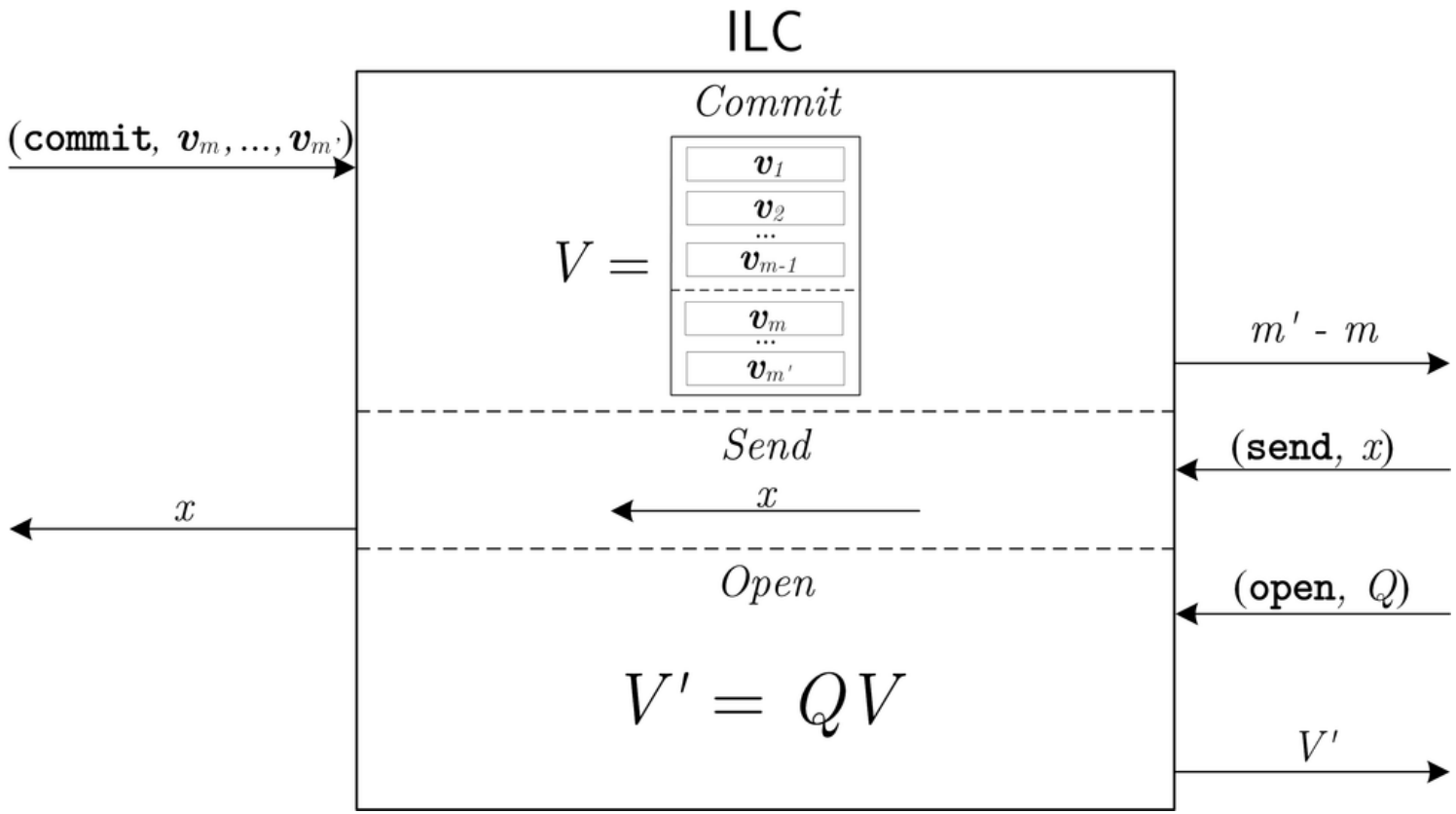


Previous Arguments

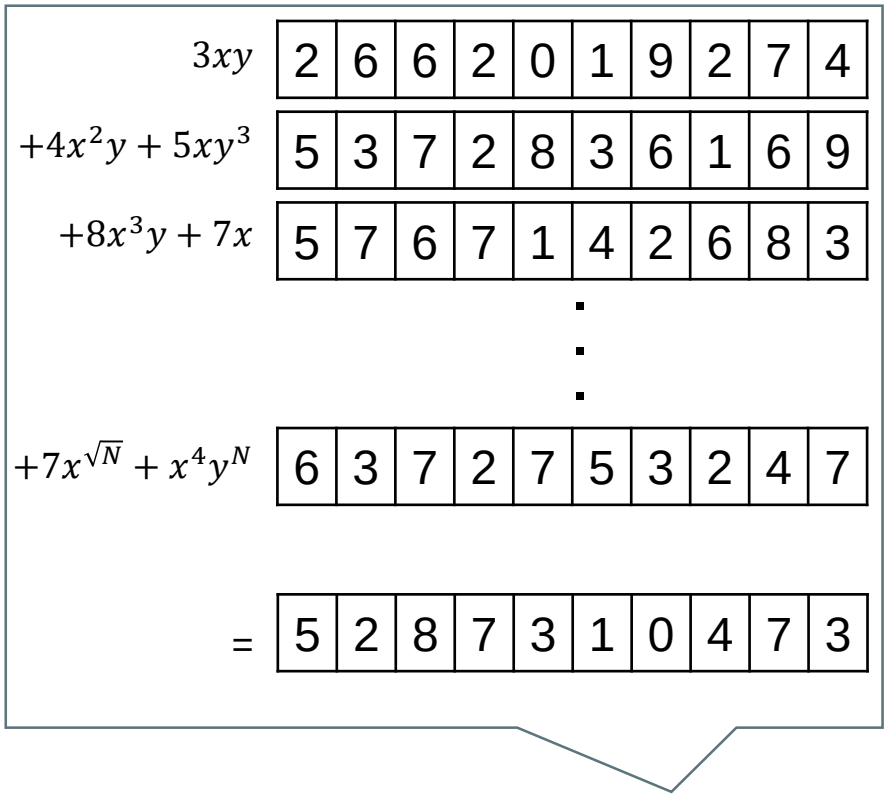
- Other protocols commit to vectors ([G09], [S09])
- Random challenge x
- Prover opens linear combinations
- Check openings are correct
- Embed AC-SAT into coefficients

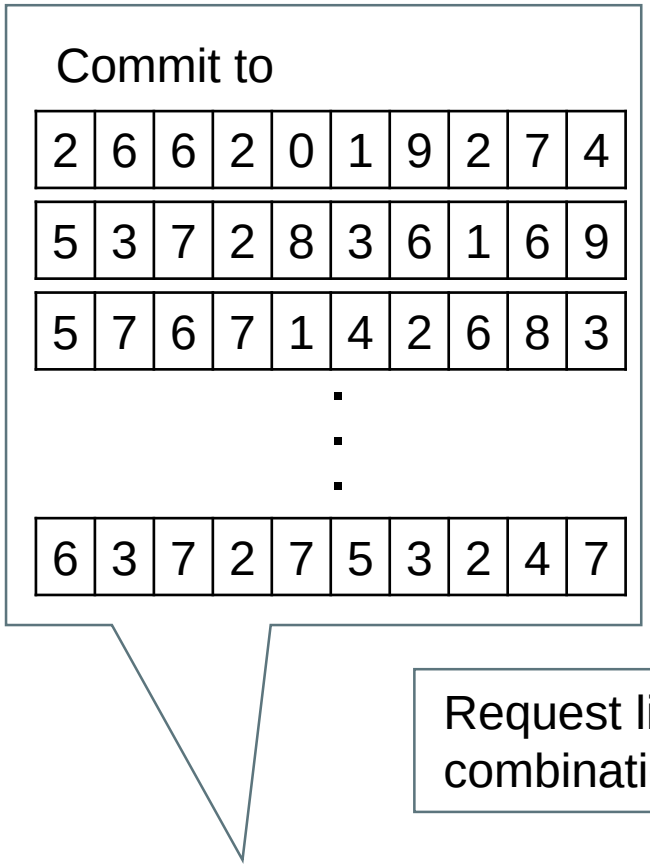
$3x$	2	6	6	2	0	1	9	2	7	4
$+4x^2$	5	3	7	2	8	3	6	1	6	9
$+8x^3$	5	7	6	7	1	4	2	6	8	3
$+7x^4$	6	3	7	2	7	5	3	2	4	7
=	5	2	8	7	3	1	0	4	7	3

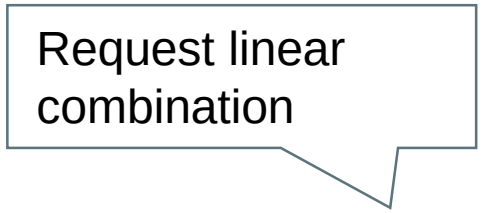
Ideal Linear Commitment Model



Sub-linear Verifier





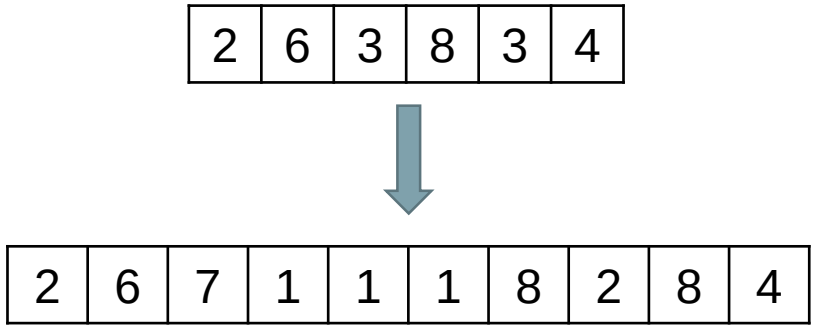


Commitment Ingredients

- Linear error-correcting code
- Example: [DI14]

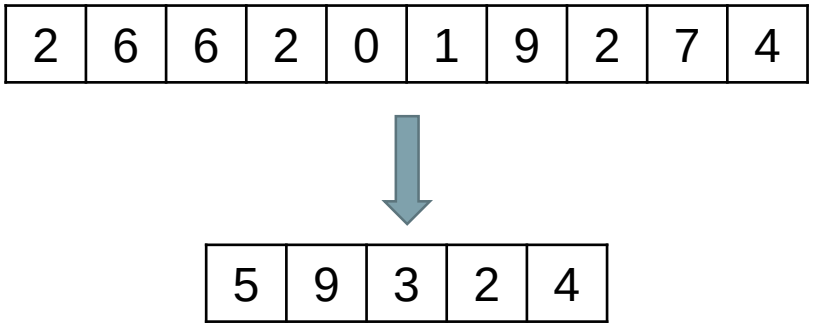
- Randomise for zero-knowledge

Linear code
Linear-time encoding
Linear Minimum Distance



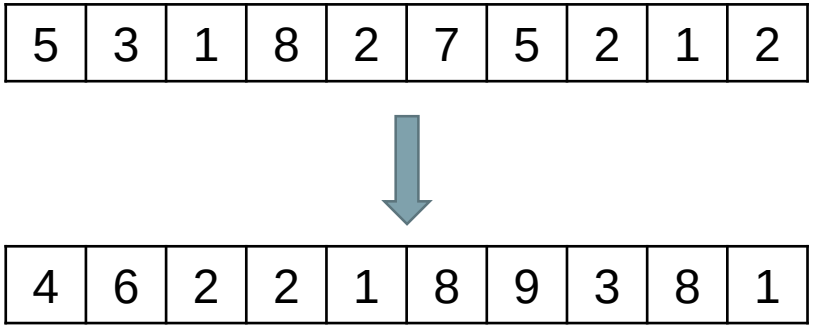
Commitment Ingredients

- **Hiding:**
- Collision-resistant hash function
- Example: [AHIKV17]



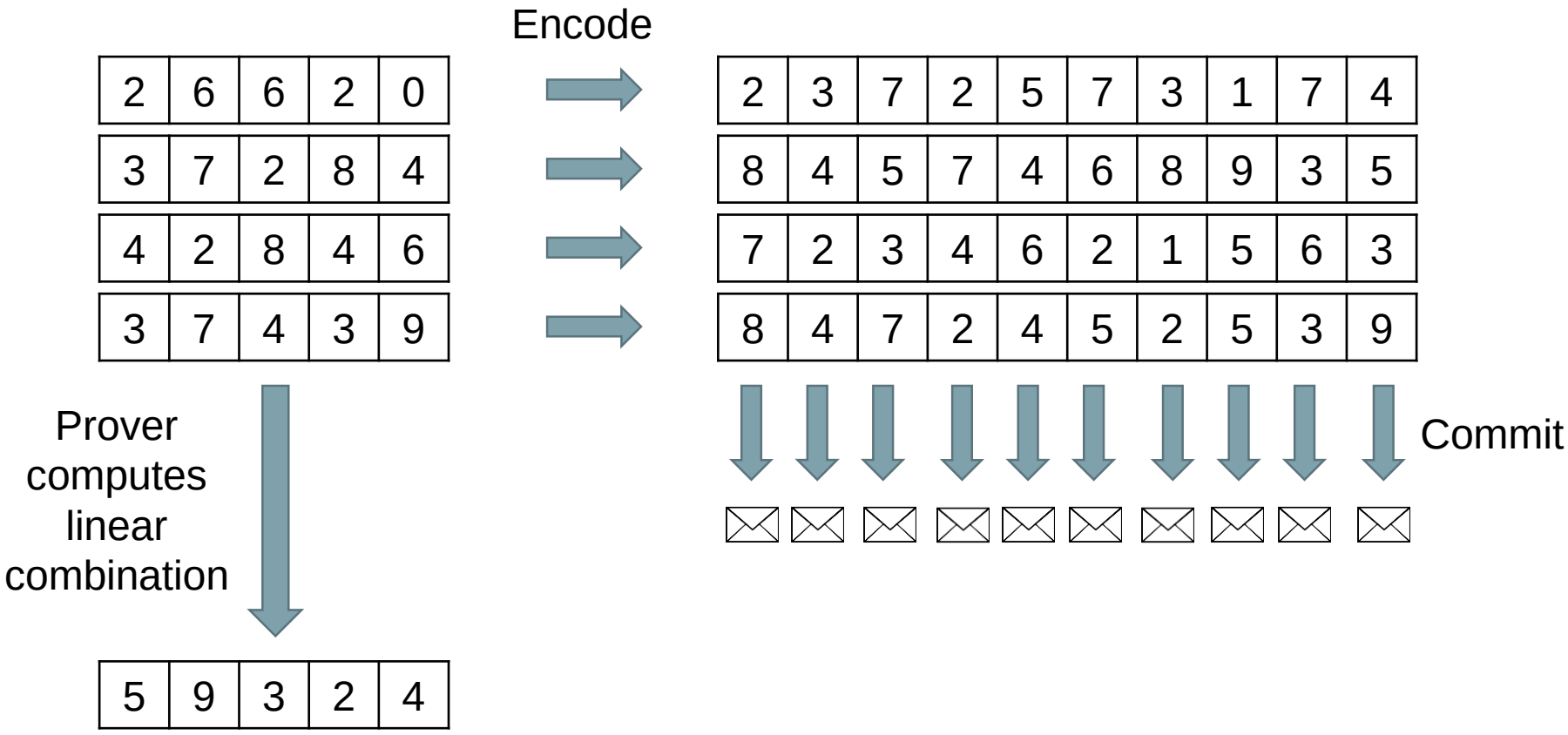
Linear-time computable

- **Binding:**
- One-way function
- Example: [IKOS08]

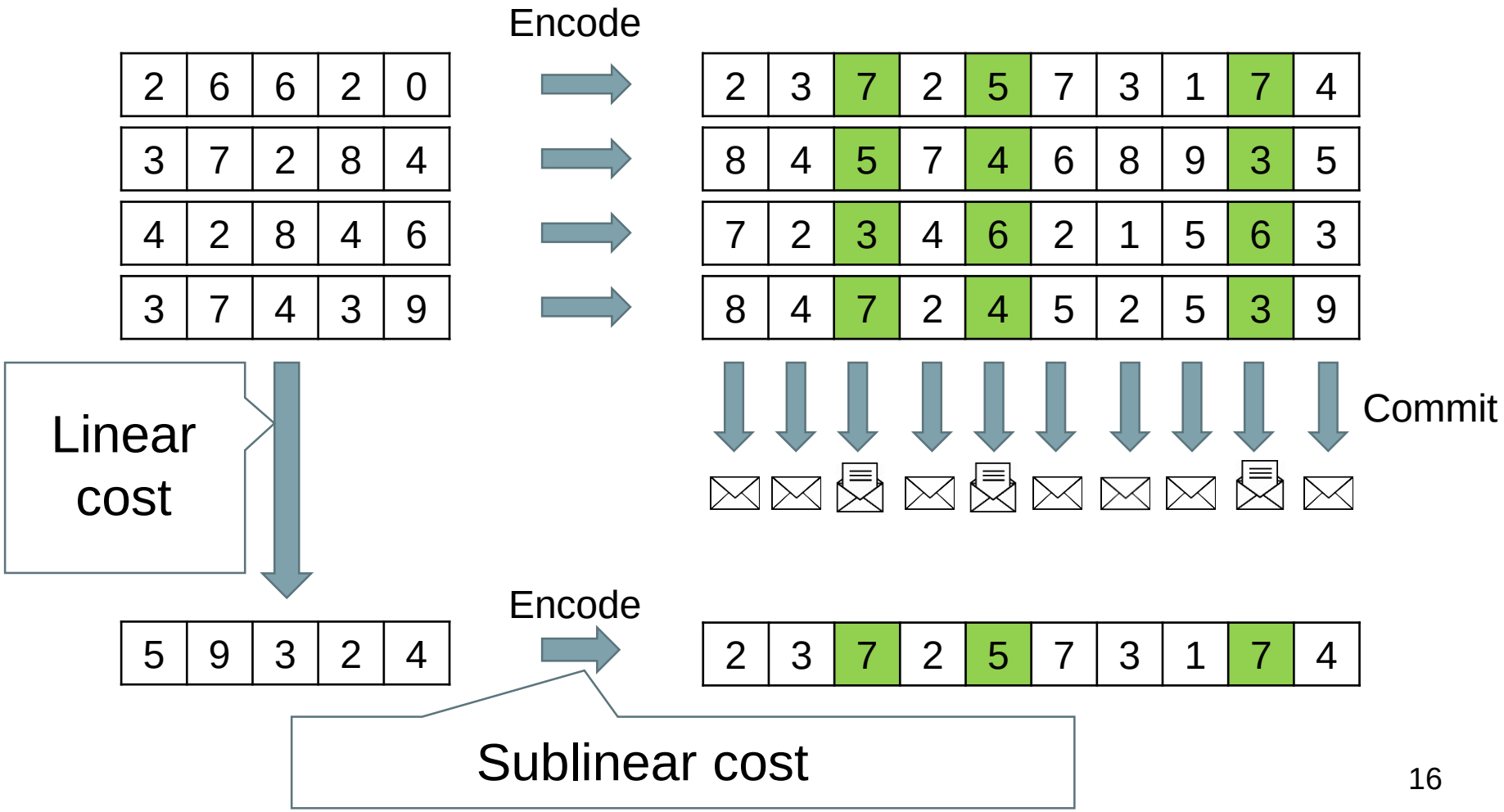


Linear-time computable

Opening Commitments



Opening Commitments



Ideal Protocols to Real Protocols

Arguments using [AHIKV17]

- Hiding commitments

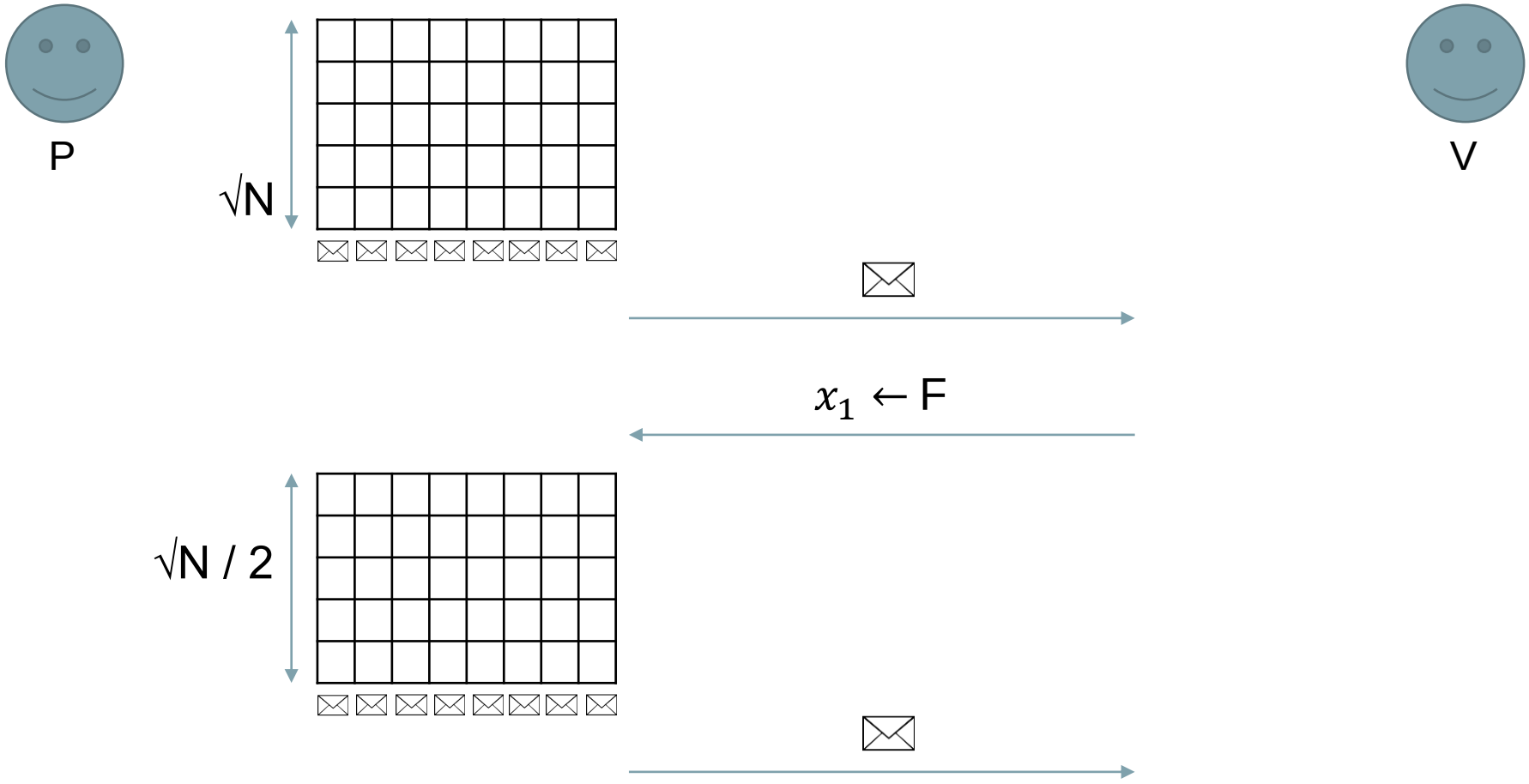
- Perfect Completeness
- Computational Soundness
- Statistical SHVZK

Proofs using [IKOS08]

- Binding commitments

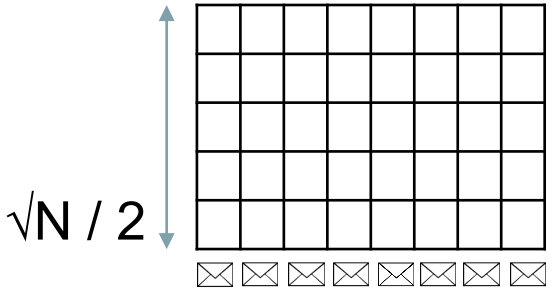
- Perfect Completeness
- Statistical Soundness
- Computational SHVZK

Protocol Flow



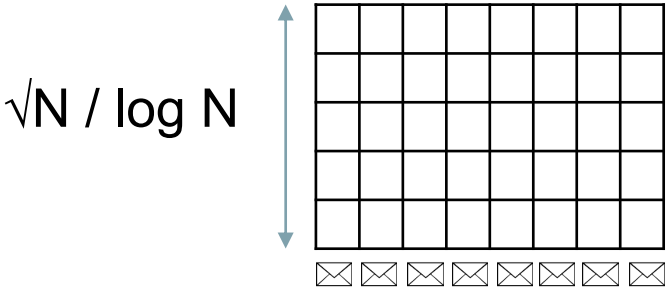
Protocol Flow

P

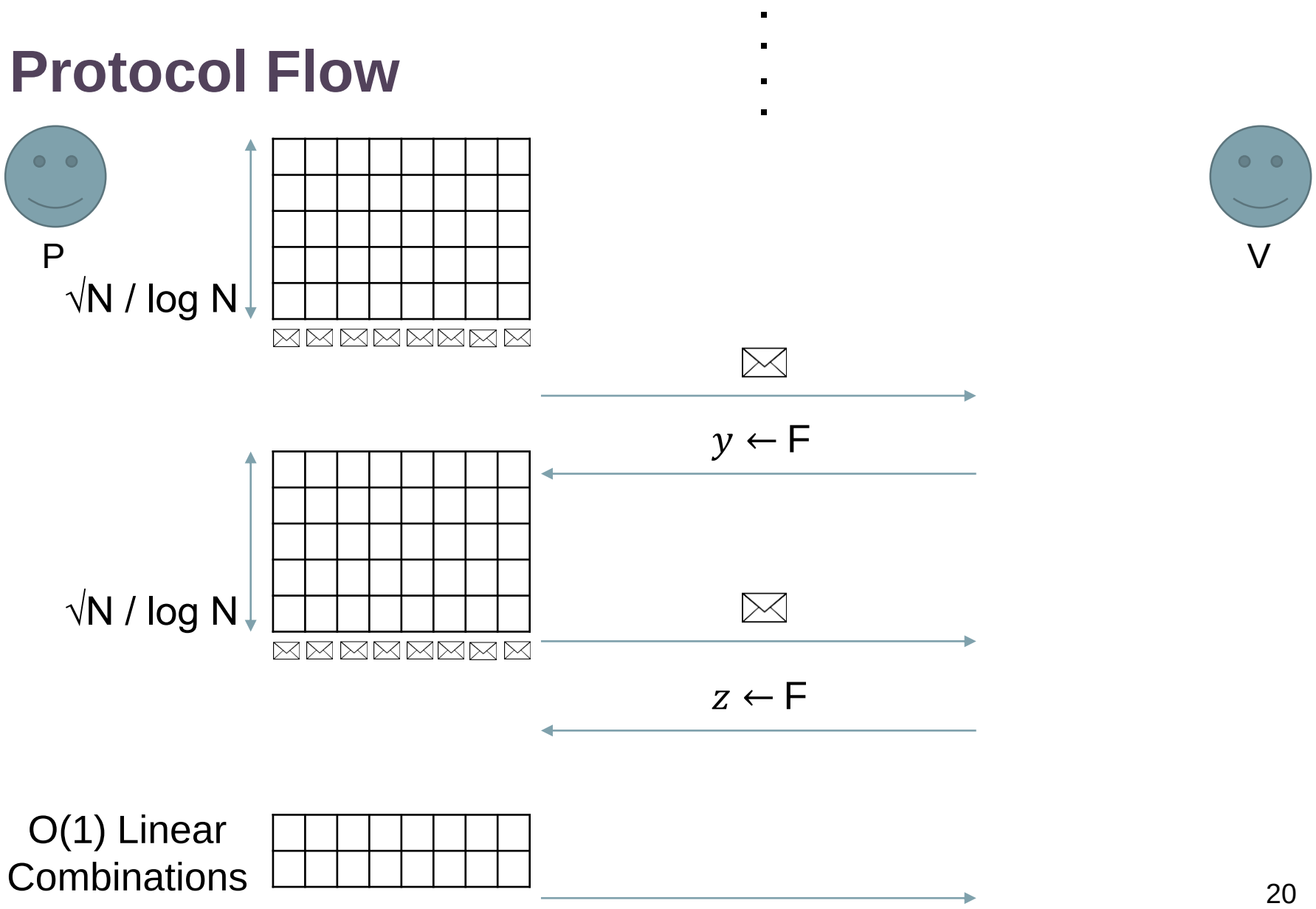


V

$x_{\log\log N} \leftarrow$ F



Protocol Flow

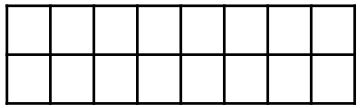


Protocol Flow

P

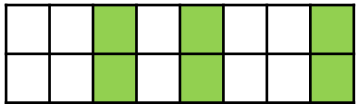
V

O(1) Linear Combinations



$I \subset \{1, \ldots, \sqrt{N}\}$

Open columns in I

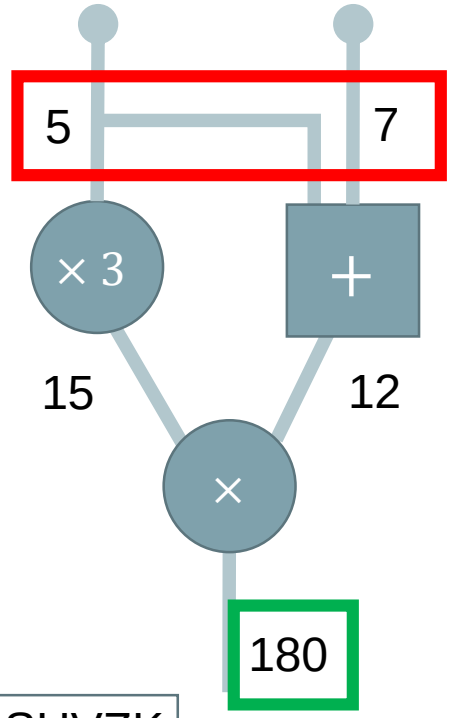


Comparison for Arguments

Previous work	Prover	Verifier	Comm.	Assumption
[CD96]	O(λN) mult	O(λN) mult	O(N) elem	DLOG
[G09], [S09]	O(λN/log N) mult	O(λN) mult	O(√N) elem	DLOG
SNARKs	O(λN) mult	O(λ) mult	O(1) elem	KOE, qPDH
[BSCS16]	$O(N^{1+c})$ mult	$O(N^{1+c})$ mult	poly(λ) log N elem	CRHF
Ligero 2017	O(N log N) mult	O(N) mult	poly(λ)√N elem	CRHF
This work	O(N) mult	o(N) mult	poly(λ)√N elem	CRHF

Thanks!

- Security parameter λ
- Finite field F, 2^{λ} elements
- Arithmetic circuit,
  N = poly(λ) gates
- Zero-knowledge arguments
  and proofs



Statistical SHVZK

Prover	Verifier	Comm.	Rounds	Assumption
O(N) multiplications in F	o(N) multiplications in F	poly(λ)$\sqrt{N}$ elements of F	O(loglog N)	lt-CRHF
O(N) multiplications in F	o(N) multiplications in F	O(N) elements of F	O(loglog N)	lt-OWF

Statistical Soundness