Zero-Knowledge IOPs with Linear-Time Prover and Polylogarithmic-Time Verifier

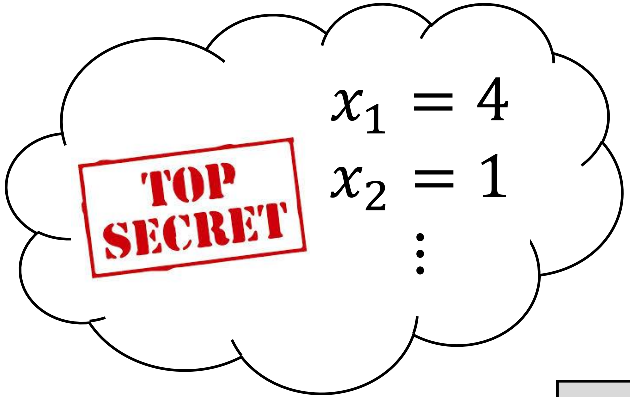
Jonathan Bootle (IBM Research – Zurich)

Joint work with Alessandro Chiesa (EPFL) and Siqi Liu (UC Berkeley)

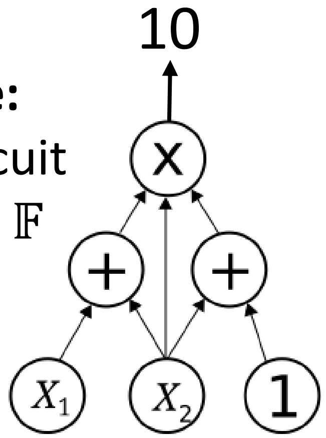
ia.cr/2020/1527


Zero-knowledge proofs and arguments

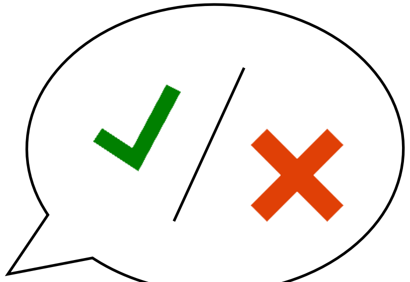
Witness:

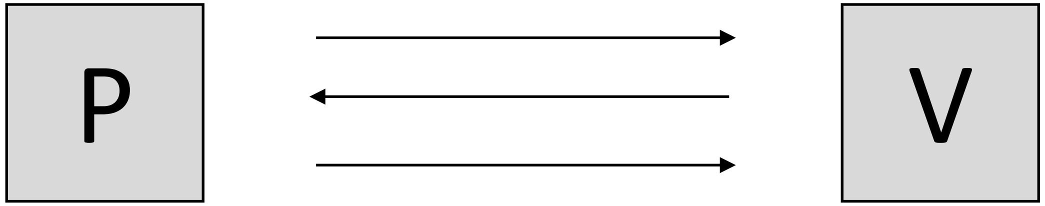


Instance:
N-gate circuit
over field $\mathbb{F}$



Completeness:
valid witness ⇒ accept





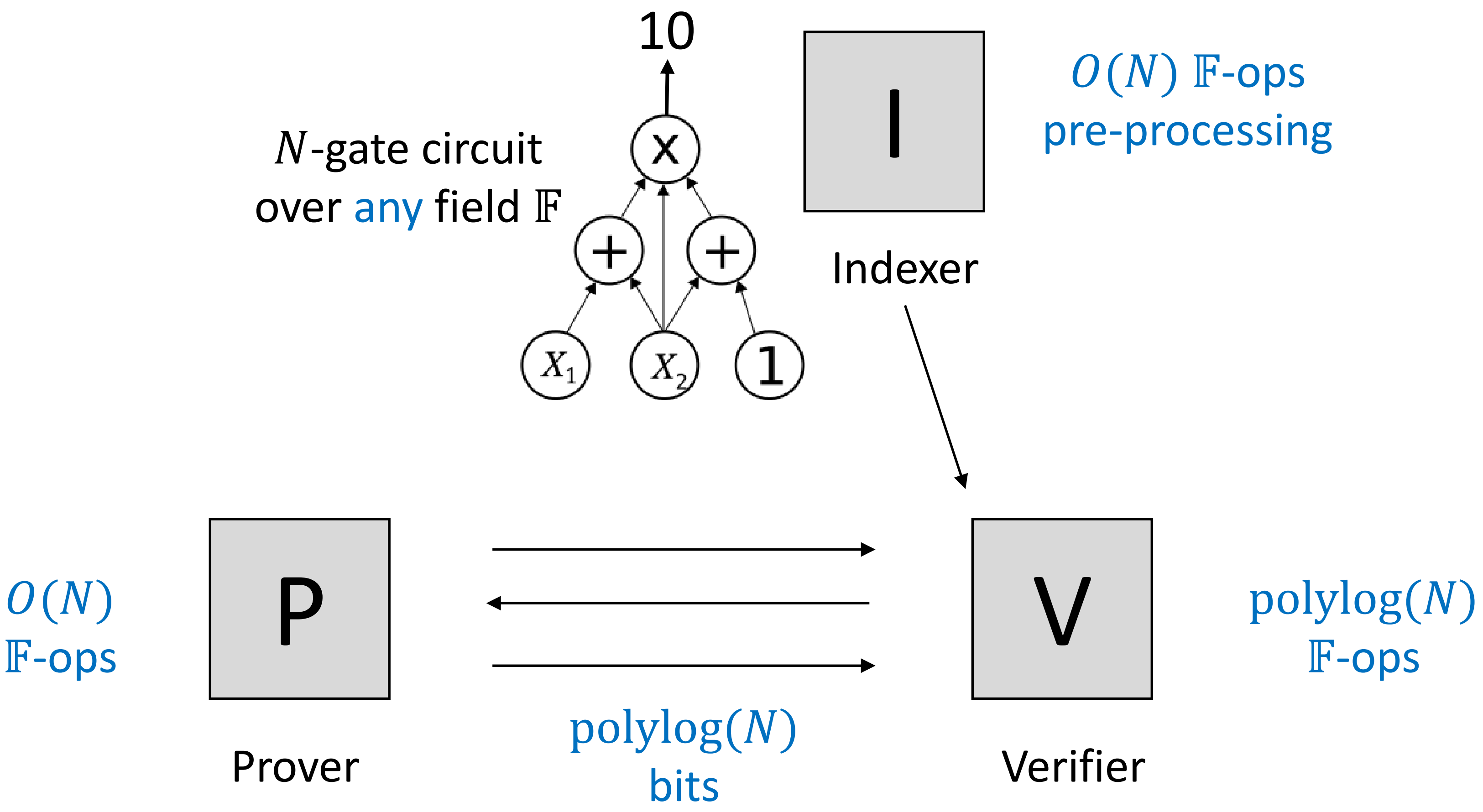
Prover

Verifier

Soundness:
invalid witness ⇒ reject

Zero-knowledge:
learns nothing about witness

The holy grail for efficient zero-knowledge



Obstacles to linear-time provers

Fast Fourier transforms

$(w_1, w_2 \dots, w_M)$
$O(N)$ wire values

$p(X), q(X)$
degree $O(N)$ polynomials

$O(N \log N)$
$\mathbb{F}$ -ops

$(p(\omega_1), \dots, p(\omega_k))$
RS encodings

$p(X) \cdot q(X) = r(X)$
multiplication

Algebraic commitments

$(w_1, w_2, \dots, w_M)$
$O(N)$ wire values

$(g_1, g_2 \dots, g_M)$
$O(N)$ group elements

$O(N)$ group exponentiations
$= O(\lambda N)$ $\mathbb{F}$-ops

$c = g_1^{w_1} g_2^{w_2} \cdots g_M^{w_M}$
commitment

Prior work

- **Arguments:** given any linear-time CRH as a black-box, CSAT over any field $\mathbb{F}$ of size $\Omega(N)$ has an argument system with

Work	Indexer complexity	Prover complexity	Verifier complexity	Proof size	Zero knowledge
[BCG20], any $\epsilon \in (0,1)$	$O(N)$ $\mathbb{F}$-ops	$O(N)$ $\mathbb{F}$-ops	$O(N^{\epsilon})$ $\mathbb{F}$-ops	$O(N^{\epsilon})$	✗

[AHIKV17] hashes
hashing $O(N)$ $\mathbb{F}$-elements
dominated by $O(N)$ $\mathbb{F}$-ops

- **IOPs:** CSAT over any field $\mathbb{F}$ of size $\Omega(N)$ has a point-query IOP with

Work	Indexer complexity	Prover complexity	Verifier complexity	#queries	Zero knowledge
[BCG20], any $\epsilon \in (0,1)$	$O(N)$ $\mathbb{F}$-ops	$O(N)$ $\mathbb{F}$-ops	$O(N^{\epsilon})$ $\mathbb{F}$-ops	$O(N^{\epsilon})$	✗

Information theoretic

Challenge: can we construct linear-time IOPs with better query complexity and ZK?

Results

Results

- **Arguments:** given any linear-time CRH as a black-box, CSAT over any field $\mathbb{F}$ of size $\Omega(N)$ has an argument system with

Work	Indexer complexity	Prover complexity	Verifier complexity	Proof size	Zero knowledge
[BCG20], any $\epsilon \in (0,1)$	$O(N)$ $\mathbb{F}$-ops	$O(N)$ $\mathbb{F}$-ops	$O(N^{\epsilon})$ $\mathbb{F}$-ops	$O(N^{\epsilon})$	✗
This work	$O(N)$ $\mathbb{F}$-ops	$O(N)$ $\mathbb{F}$-ops	$\text{polylog}(N)$ $\mathbb{F}$-ops	$O(\log N)$	✓

- **IOPs:** CSAT over any field $\mathbb{F}$ of size $\Omega(N)$ has a point-query IOP with

Work	Indexer complexity	Prover complexity	Verifier complexity	#queries	Zero knowledge
[BCG20], any $\epsilon \in (0,1)$	$O(N)$ $\mathbb{F}$-ops	$O(N)$ $\mathbb{F}$-ops	$O(N^{\epsilon})$ $\mathbb{F}$-ops	$O(N^{\epsilon})$	✗
This work	$O(N)$ $\mathbb{F}$-ops	$O(N)$ $\mathbb{F}$-ops	$\text{polylog}(N)$ $\mathbb{F}$-ops	$O(\log N)$	✓

Information theoretic

Results

- **Arguments:** given any linear-time CRH as a black-box, CSAT over any field $\mathbb{F}$ of size $\Omega(N)$ has an argument system with

Work	Indexer complexity	Prover complexity	Verifier complexity	Proof size	Zero knowledge
[BCG20], any $\epsilon \in (0,1)$	$O(N)$ $\mathbb{F}$-ops	$O(N)$ $\mathbb{F}$-ops	$O(N^{\epsilon})$ $\mathbb{F}$-ops	$O(N^{\epsilon})$	✗
This work	$O(N)$ $\mathbb{F}$-ops	$O(N)$ $\mathbb{F}$-ops	$\text{polylog}(N)$ $\mathbb{F}$-ops	$O(\log N)$	✓
[LSTW20], [GLSTW21]	$O(N)$ $\mathbb{F}$-ops	$O(N)$ $\mathbb{F}$-ops	$\text{polylog}(N)$ $\mathbb{F}$-ops	$O(\log N)$	✓

assumptions about ROs

- **IOPs:** CSAT over any field $\mathbb{F}$ of size $\Omega(N)$ has a point-query IOP with

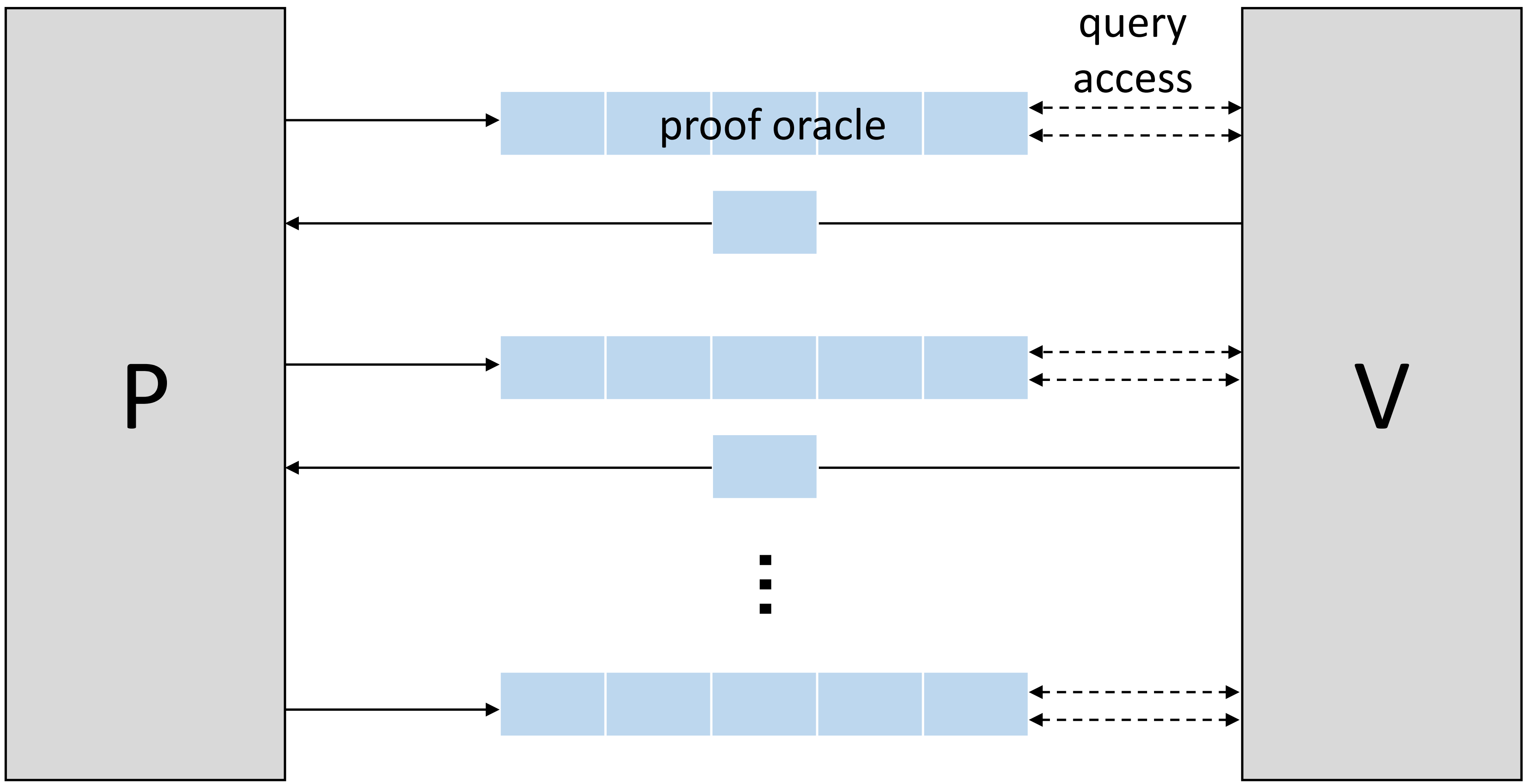
Work	Indexer complexity	Prover complexity	Verifier complexity	#queries	Zero knowledge
[BCG20], any $\epsilon \in (0,1)$	$O(N)$ $\mathbb{F}$-ops	$O(N)$ $\mathbb{F}$-ops	$O(N^{\epsilon})$ $\mathbb{F}$-ops	$O(N^{\epsilon})$	✗
This work	$O(N)$ $\mathbb{F}$-ops	$O(N)$ $\mathbb{F}$-ops	$\text{polylog}(N)$ $\mathbb{F}$-ops	$O(\log N)$	✓

Information theoretic

Overview of approach

Overview of approach

Interactive oracle proofs



Point queries:
$query(\pi, i) = \pi(i)$
(main result)

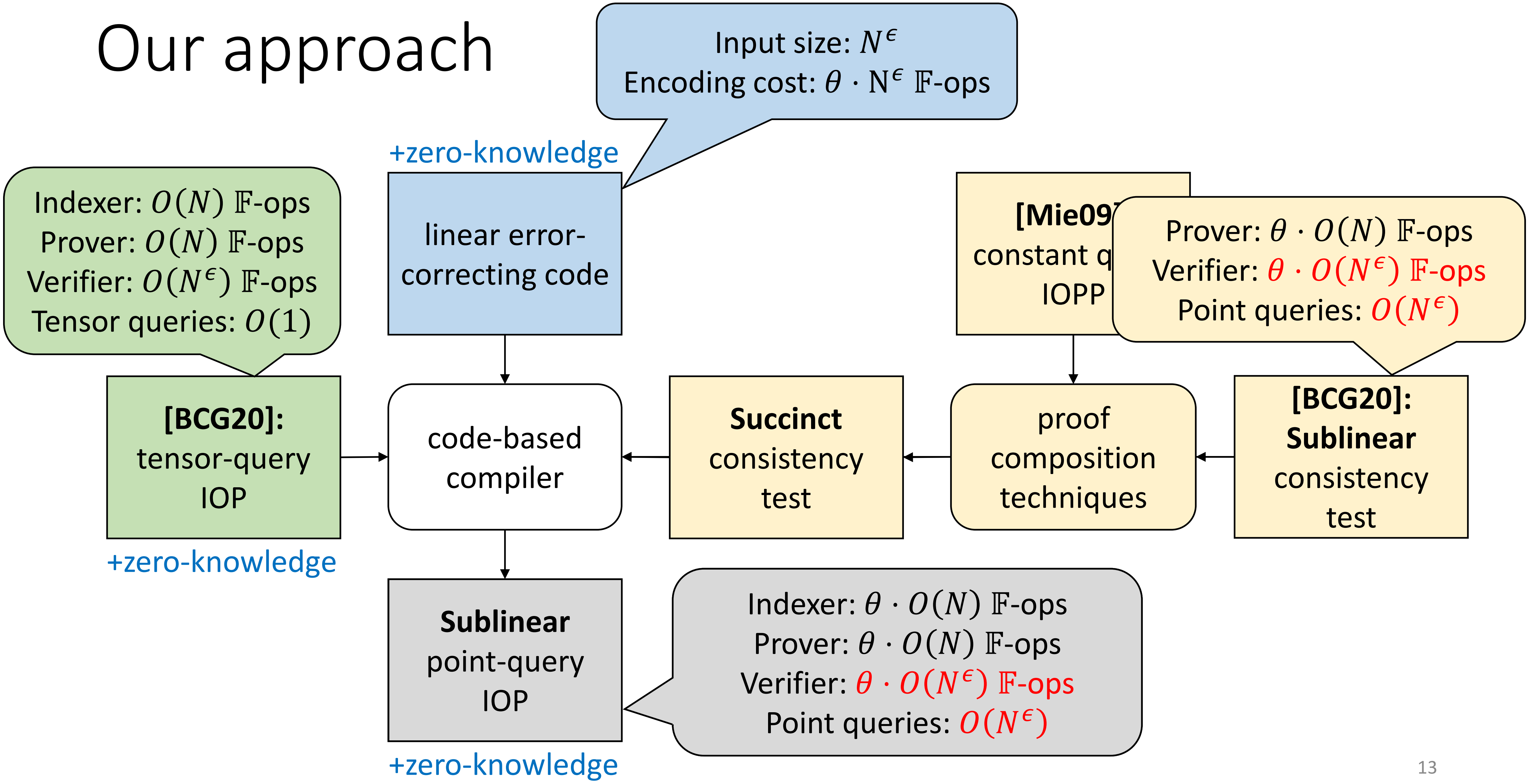
Tensor queries:
$query(\pi, q_1, q_2)$
$= \langle \pi, q_1 \otimes q_2 \rangle$

Linear queries:
$query(\pi, q) = \langle \pi, q \rangle$

proof oracle = committed data

answering query = opening commitment

Our approach

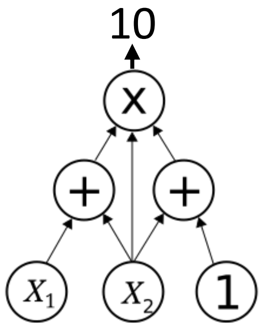


Zero-knowledge tensor IOPs

Tensor IOPs for circuit satisfiability

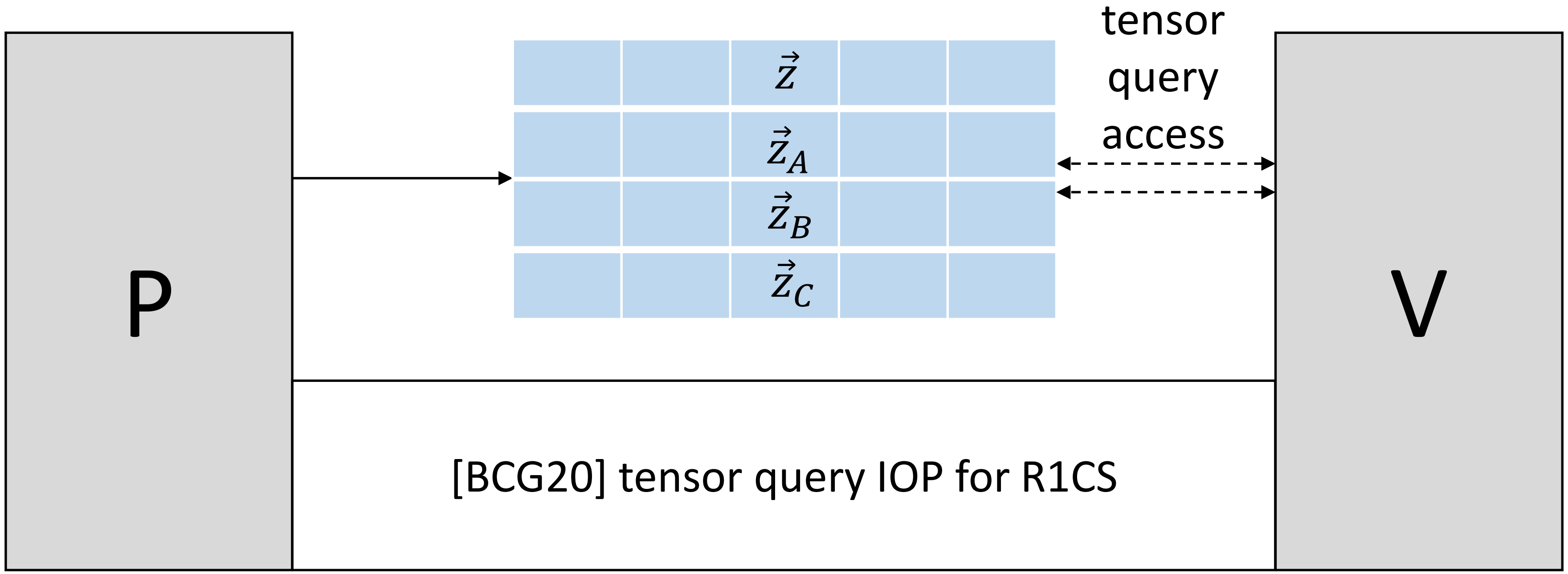
Instance:
- N-gate circuit over field $\mathbb{F}$

Witness:
- satisfying assignment



R1CS instance:
- $A, B, C \in \mathbb{F}^{N \times N}$

R1CS witness:
- $\vec{z}, \vec{z}_A, \vec{z}_B, \vec{z}_C \in \mathbb{F}^N$
- $\vec{z}_A = A\vec{z}, \vec{z}_B = B\vec{z}, \vec{z}_C = C\vec{z}, \vec{z}_A \circ \vec{z}_B = \vec{z}_C$

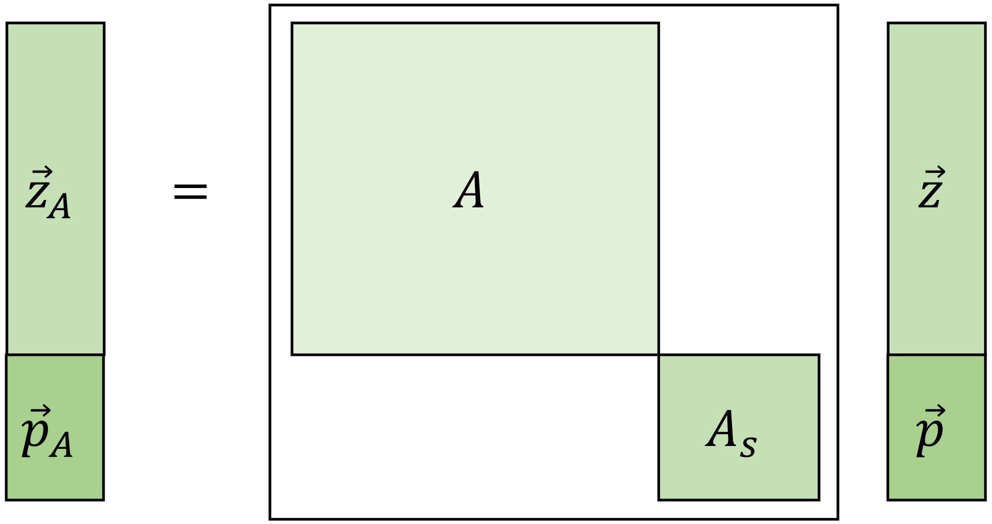


$query(\pi, q_1, q_2) = \langle \pi, q_1 \otimes q_2 \rangle$

Queries to $\vec{z}, \vec{z}_A, \vec{z}_B, \vec{z}_C$ leak information!

Making tensor queries look random

1. Pad R1CS instance with randomness



2. Run the same tensor IOP as before

R1CS gadget, random solution with $a, b \leftarrow \mathbb{F}$

$$\begin{pmatrix}1 & 0 & 0\end{pmatrix}\begin{pmatrix}a \\ b \\ ab\end{pmatrix} \circ \begin{pmatrix}0 & 1 & 0\end{pmatrix}\begin{pmatrix}a \\ b \\ ab\end{pmatrix} = \begin{pmatrix}0 & 0 & 1\end{pmatrix}\begin{pmatrix}a \\ b \\ ab\end{pmatrix}$$

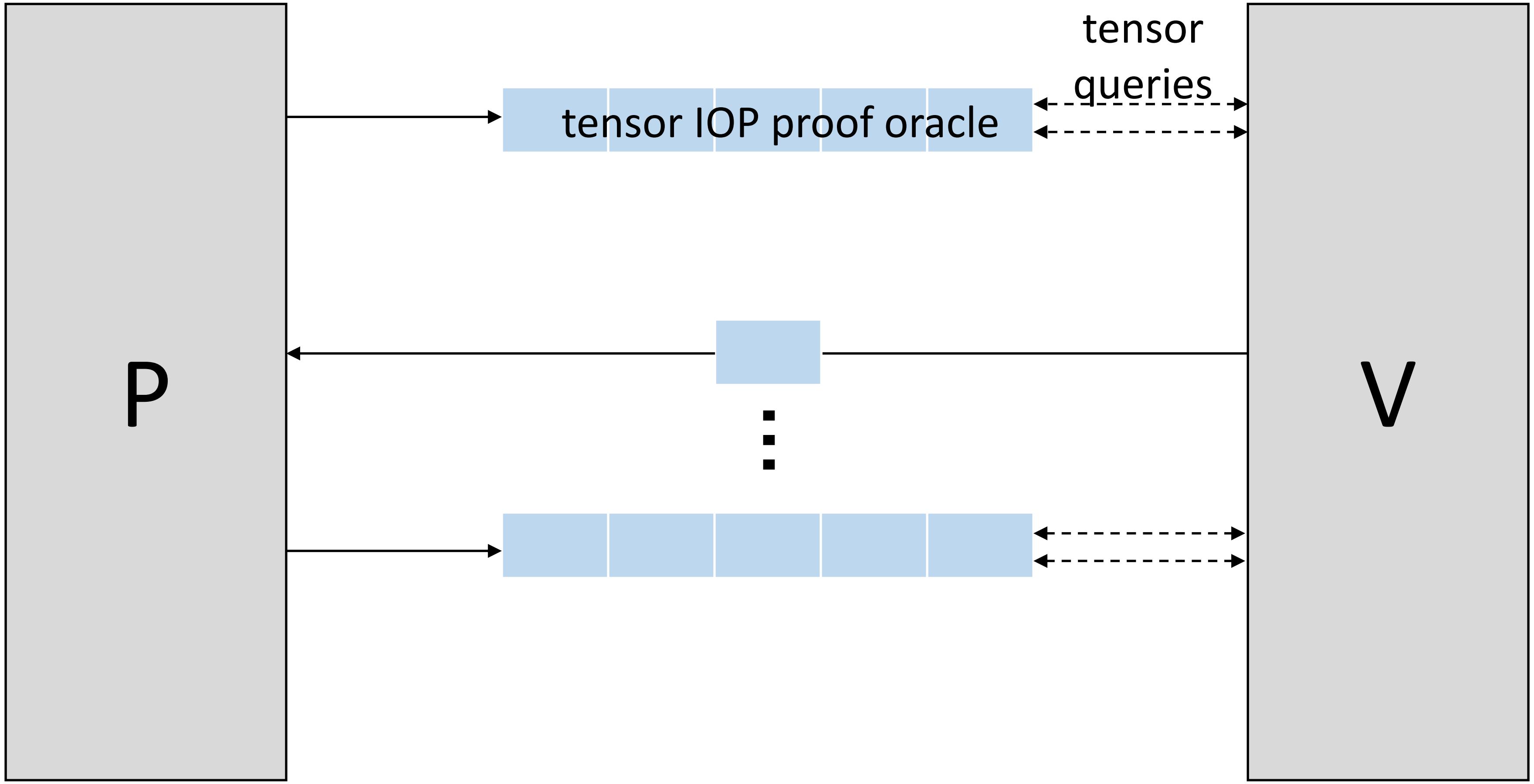
Repeat s times $\rightarrow$ R1CS instance $A_s, B_s, C_s \in \mathbb{F}^{3s\times 3s}$

$\vec{p}, \vec{p}_A$ make tensor queries look random

Zero-knowledge codes

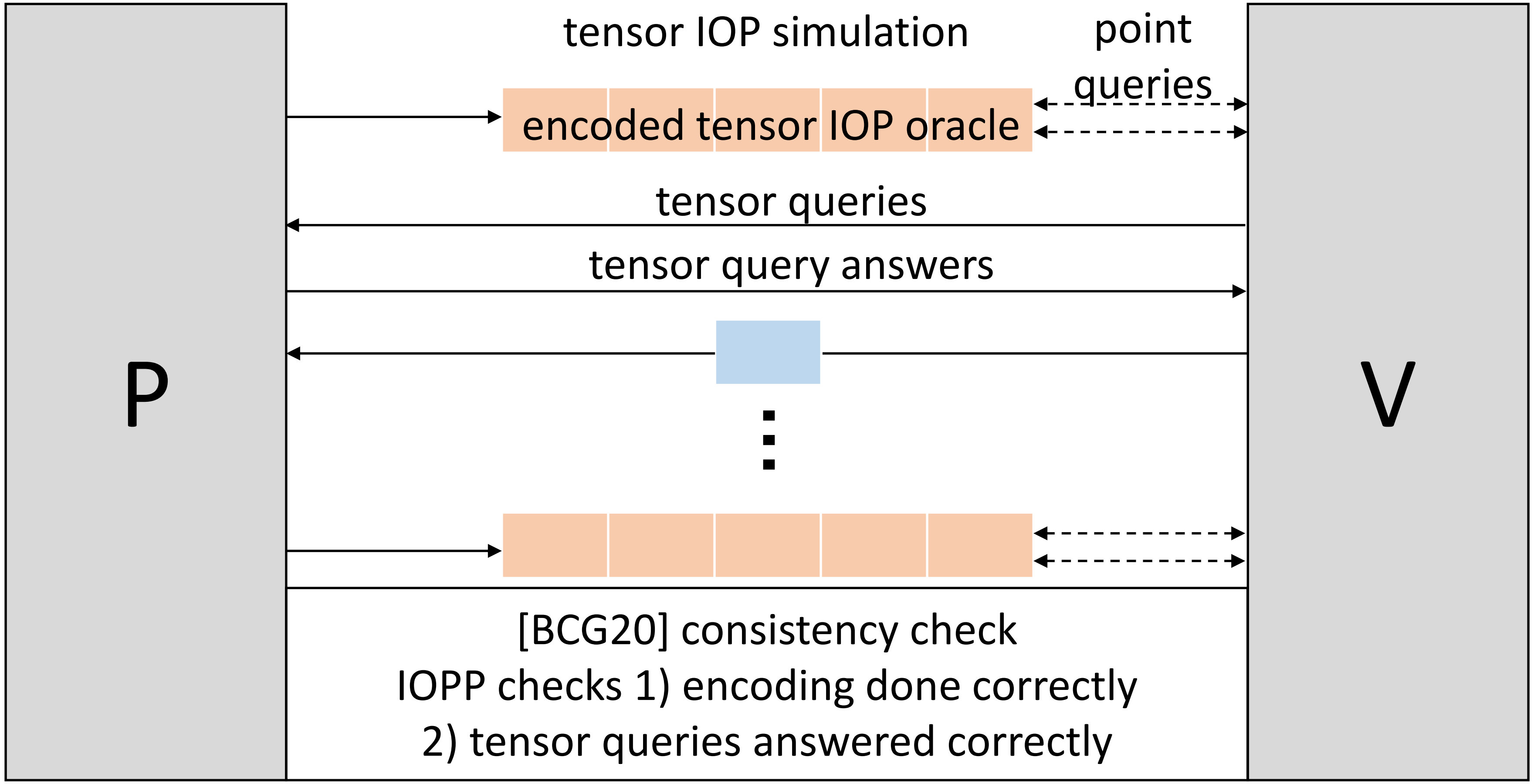
$$query(\pi, q_1, q_2) = \langle \pi, q_1 \otimes q_2 \rangle$$

Tensor IOP before code-based compiler

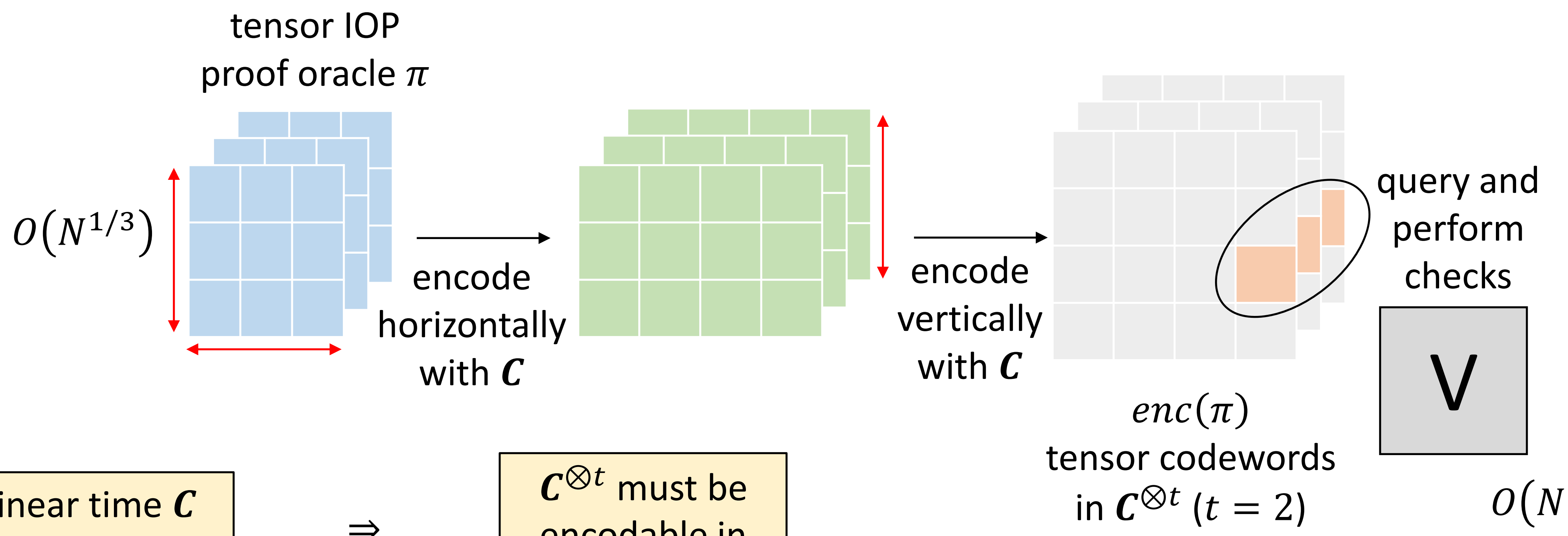


Tensor IOP after code-based compiler

$query(\pi, i) = \pi(i)$



Choice of encoding in consistency check



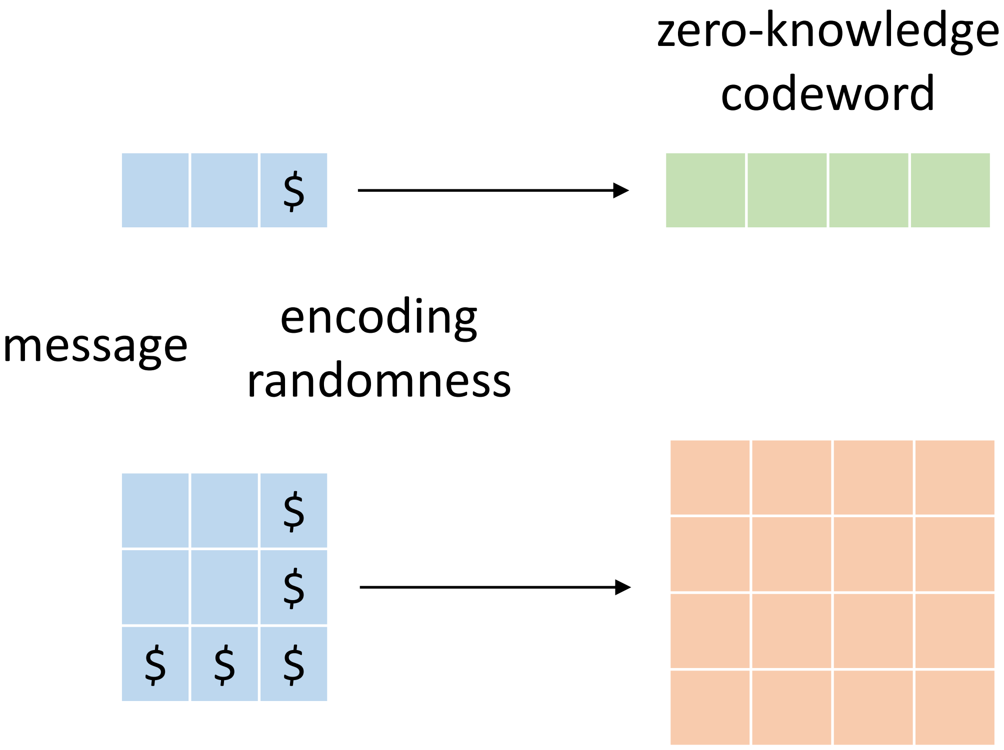
$O(N^{1/3})$
queries and
verification

Linear time $\boldsymbol{C}$ [Spi96], [DI14]	$\Rightarrow$	$\boldsymbol{C}^{\otimes t}$ must be encodable in linear time
?	$\Rightarrow$	Queries to $enc(\pi)$ must not leak information

Constructing linear-time ZK tensor codes

Bonus result:
new linear-time and
ZK base code

Theorem: ZK is
preserved under
tensor products

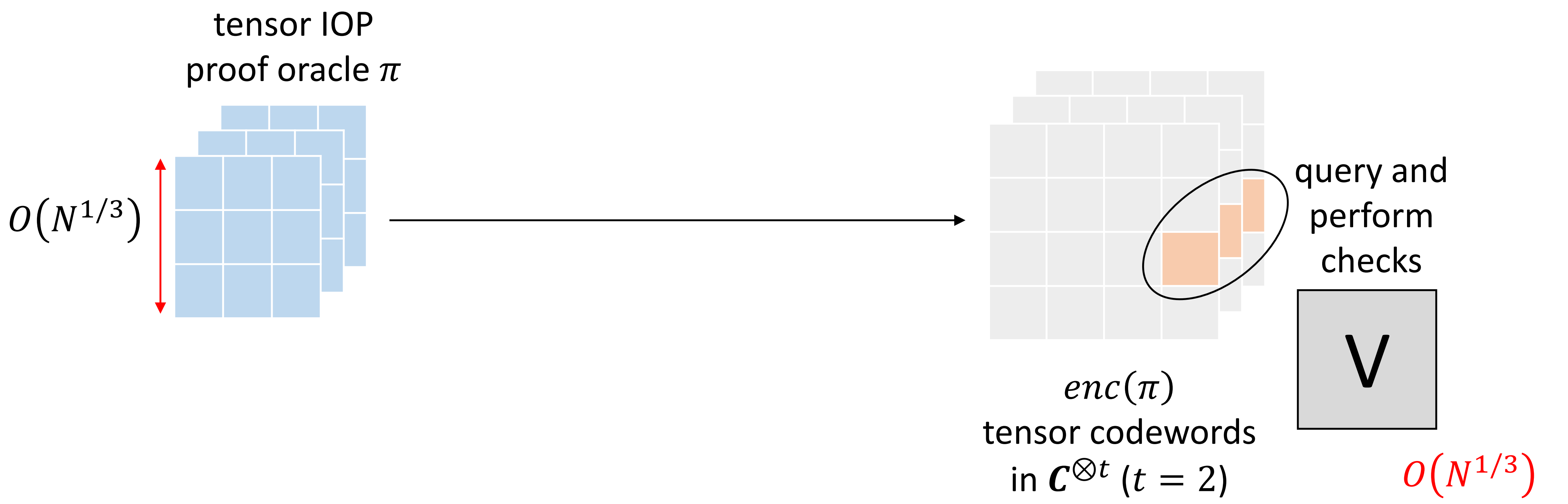


up to b queries to C look random

up to b queries to $C \otimes C$
look random

Reducing query complexity

Achieving succinct verification



queries and verification

Use another proof to show that V would have accepted!

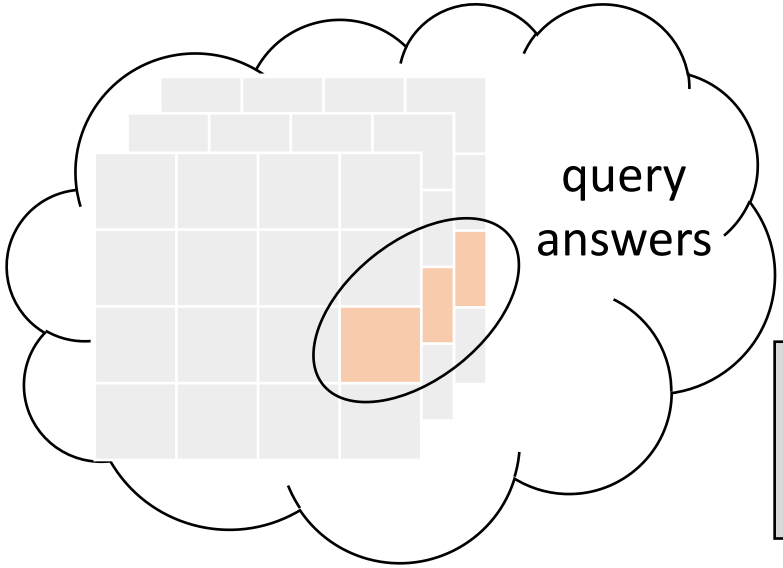
Query reduction through proof composition

Theorem: ZK is preserved under proof composition

P | [BCG20] consistency check minus $O(N^{\epsilon})$ point queries | **V**

Prover time $O(N)$

New witness:



New instance:

V

Size $n = O(N^{\epsilon})$

P* | [Mie09] IOPP $O(1)$ point queries | **V***

Prover time $O(n^c)$
$= O(N)$

New prover

New verifier

Summary

Summary

- **IOPs:** CSAT over any field $\mathbb{F}$ of size $\Omega(N)$ has a point-query IOP with

Work	Indexer complexity	Prover complexity	Verifier complexity	#queries	Zero knowledge
[BCG20], any $\epsilon \in (0,1)$	$O(N)$ $\mathbb{F}$-ops	$O(N)$ $\mathbb{F}$-ops	$O(N^{\epsilon})$ $\mathbb{F}$-ops	$O(N^{\epsilon})$	✗
This work	$O(N)$ $\mathbb{F}$-ops	$O(N)$ $\mathbb{F}$-ops	$\mathrm{polylog}(N)$ $\mathbb{F}$-ops	$O(\log N)$	✓

- Similar results for arguments
- New tools:

R1CS gadgets

ZK codes under tensor products

ZK under proof composition

Thanks!

ia.cr/2020/1527