Probabilistically Checkable Arguments

Yael Tauman Kalai
Microsoft Research

Ran Raz
Weizmann Institute

Our Results

Main Result:

public-coin IP ⇒ one-round argument

PSPACE = IP = Public-coin IP [LFKN, Shamir, Goldwasser-Sipser]

⇓

Corollary1: PSPACE $\subseteq$ 1-round arguments

Our Results (Cont.)

Main Result:

public-coin IP → one-round argument

Define: probabilistically checkable arguments (PCAs)

$\approx$ PCPs that are only computationally sound

Main Result with IP[Goldwasser-K-Rothblum08]

⇓

Corollary2: Short PCAs of size poly(|witness|)

Interactive Proofs (IP)
[Golwasser-Micali-Rackoff, Babai]

Proofs that use **interaction** and **randomization**

- **IP=PSPACE** [Lund-Fortnow-Karloff-Nissan, Shamir]
  - # rounds = poly(n)
- Can we reduce the number of rounds?
  - O(1)-round IP = 1-round IP
  - Believed: 1-round IP does not contain much…
    (1-round IP ≠ PSPACE)

Interactive Arguments (IA)

Interactive proofs that are only **computationally sound:**

Security holds only against comp. bounded cheating provers

Poly-time verifier

Honest prover's runtime T

Soundness against cheating provers of size 2^{κ}

Interactive Arguments (cont.)

IA=NEXP [Kilian,Micali]

 # rounds = 2 (4 messages)

What can be proved via 1-round interactive argument?

– [Micali]: In random oracle model
NEXP=1-round IA

– What about in the plain model??

PSPACE $\subseteq$ 1-round IA

public-coin: verifier only sends his coin tosses

[Goldwasser-Sipser]: IP = public-coin IP

public-coin IP → (PIR) → one-round argument

$msg_{V'}$

P — V

P' — V'

Independent of instance

public-coin: verifier only sends his coin tosses

[Goldwasser-Sipser]: IP = public-coin IP

public-coin IP —PIR→ one-round argument

Main Thm:

No blowup if we use fully-homomorphic encryption [Gentry09]

Under expo… …tions, any public-coin IP can … converted into a one-round argument (blowup in provers run-time)

Previous Attempts

- Fiat-Shamir88:

  Use hash-function to convert any public-coin IP into 1-round argument

- Barak01, Goldwasser-K03:

  Exhibit inherent difficulties in proving soundness

- Aiello-Bhatt-Ostrovsky-Rajagopalan00:

  Use PIR scheme to convert the two-round Kilian/Micali argument for NEXP into a (short) one-round argument

- Dwork-Langberg-Naor-Nissim-Reingold04:

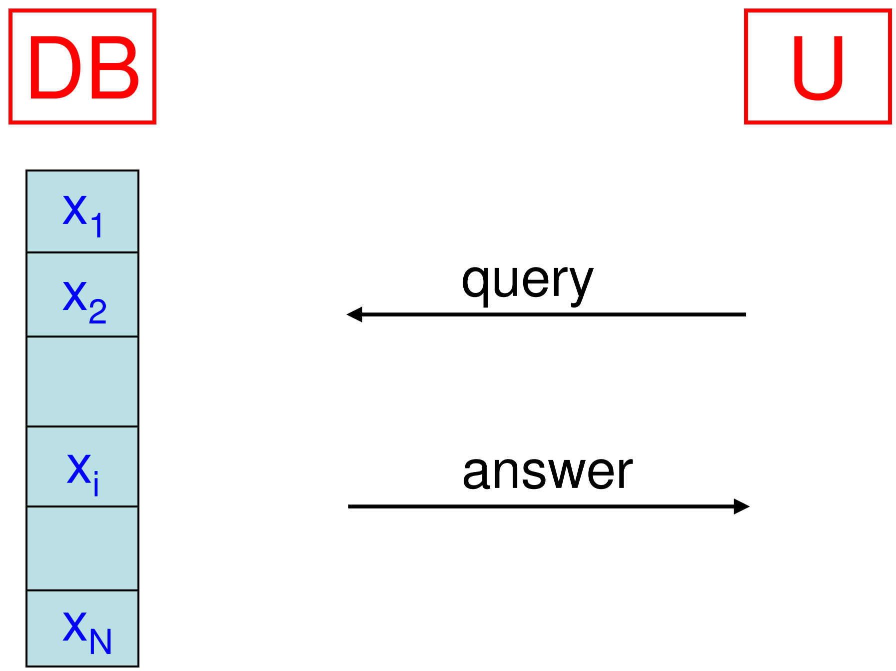
  Exhibit inherent difficulties in proving soundness

Proof Idea

Public-coin interactive proof → (PIR) → 1-round argument

PIR Scheme

[Chor-Goldreich-Kushilevitz-Sudan95, Kushilevitz-Ostrovsky97]



PIR Scheme

[Chor-Goldreich-Kushilevitz-Sudan95, Kushilevitz-Ostrovsky97]

Secrecy: $\forall i,j \in \{1,\dots,N\}$

$$q(i) \approx q(j)$$

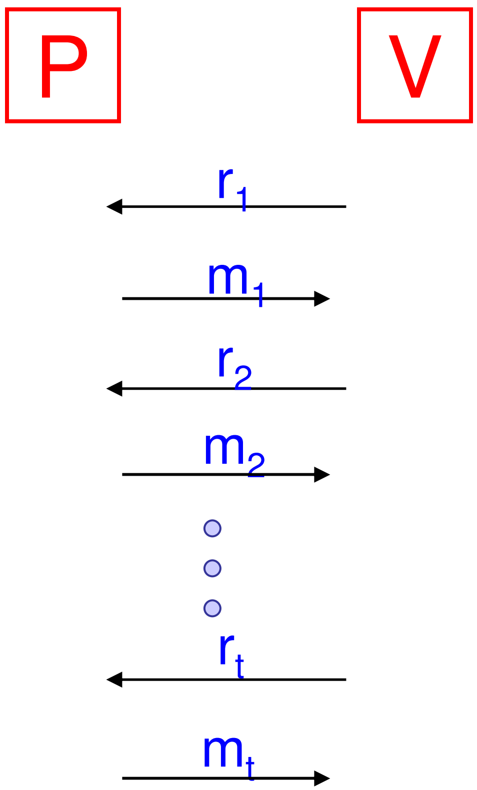
For distinguishers of size poly(N)

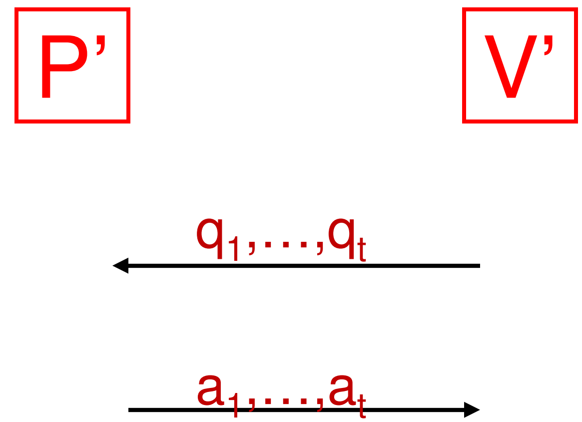
polylog PIR Scheme [CMS99]:

Communication complexity = poly(κ, log N)

User run-time poly(κ, log N)

Public-coin interactive proof → 1-round argument



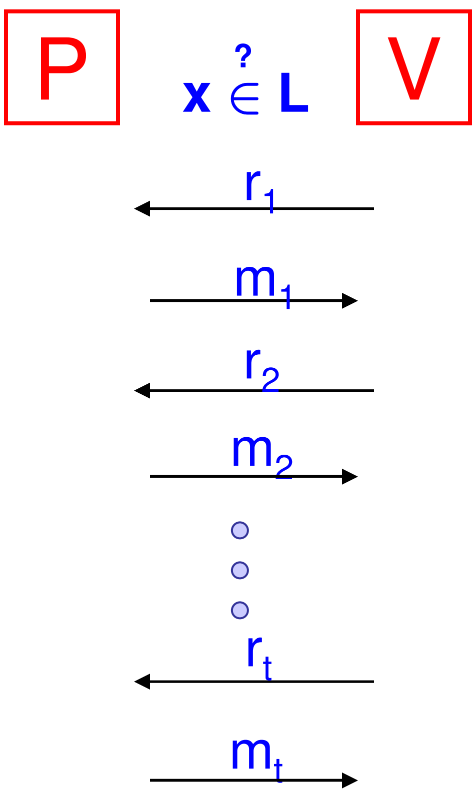


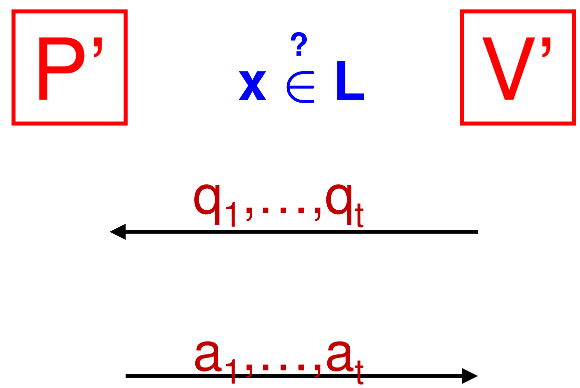
- q_i=query$(r_1,\ldots,r_i)$
- a_i=answer(q_i,DB_i), where the $(r_1,\ldots,r_i)$ entry of DB_i is $m_i(r_1,\ldots,r_i)$

Proof Idea

Fix x not in L. Suppose $\exists$ P^* of size $\leq 2^\kappa$ s.t.

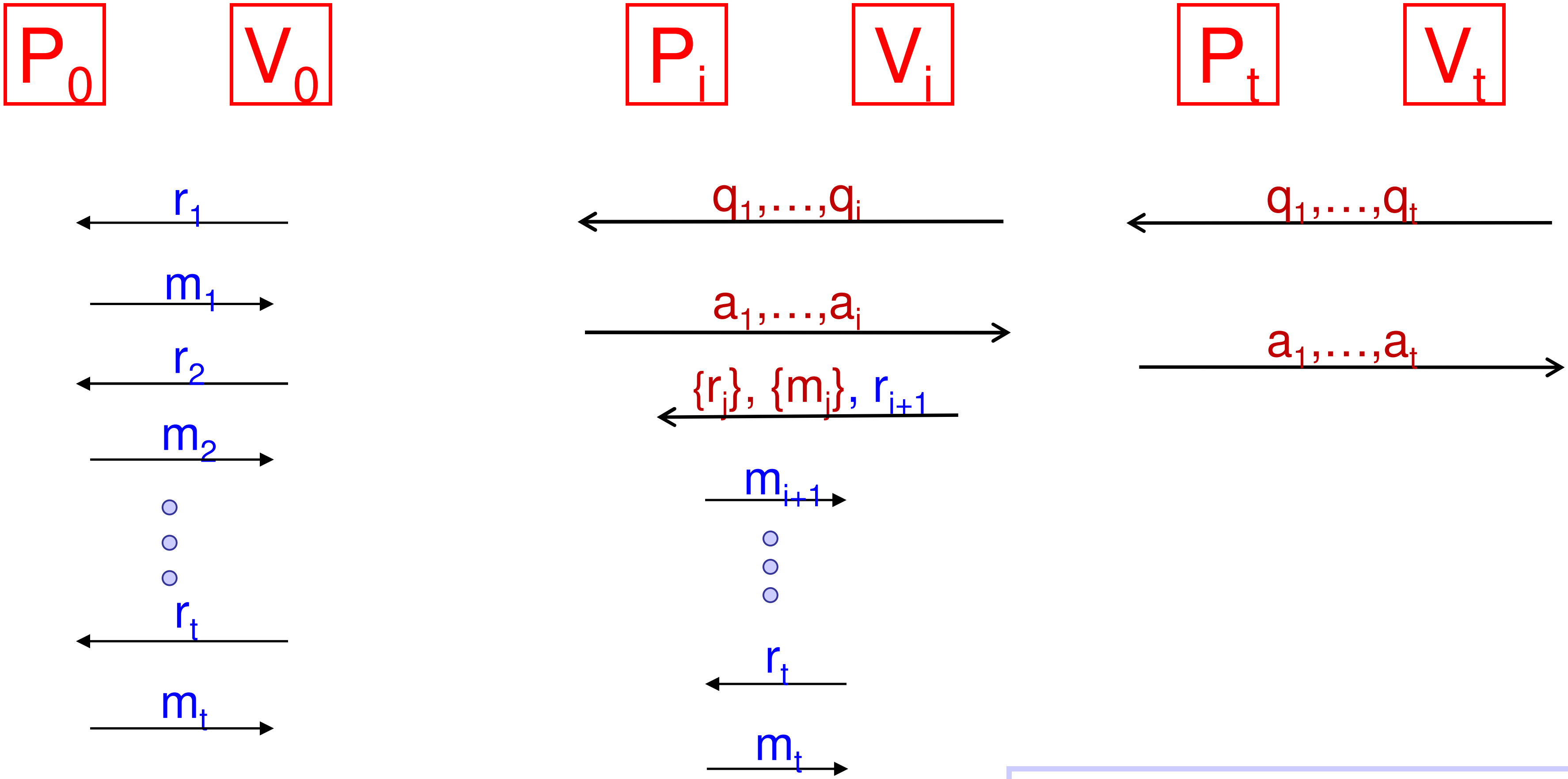
$$\Pr[(P^*,V')(x)=1] \geq s+\varepsilon$$





- q_i=query$(r_1,\ldots,r_i)$
- a_i=answer(q_i,DB_i), where the $(r_1,\ldots,r_i)$ entry of DB_i is $m_i(r_1,\ldots,r_i)$

Proof Idea

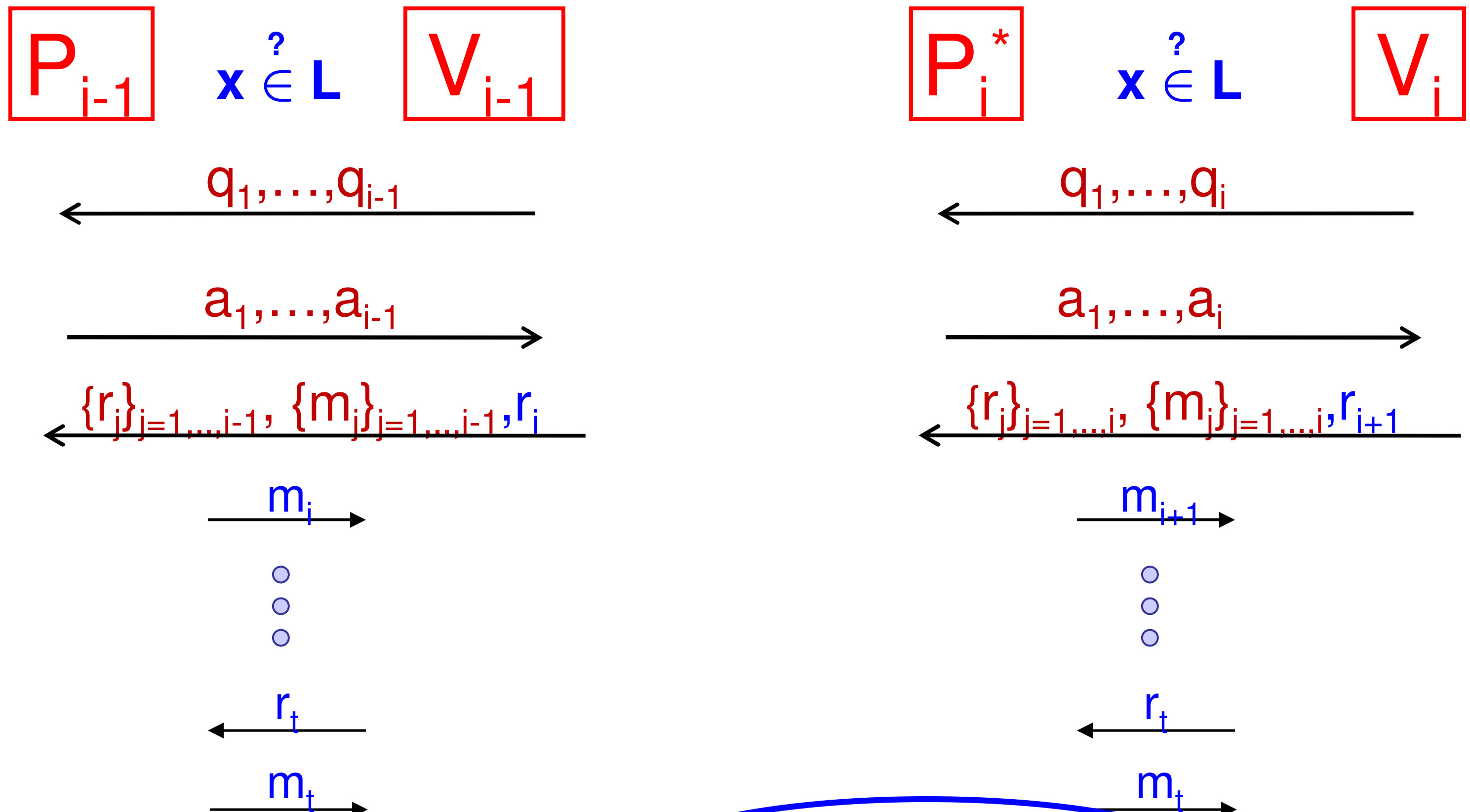


soundness $\leq$ s against any cheating prover

$\exists P^*$ of size 2^κ s.t.

$\Pr[(P^*,V_t)(x)=1] \geq s+\varepsilon$

Proof Idea (Cont.)



soundness $\leq s^*$ against a cheating prover of size 2^{κ}

$\approx |P^*_i| + 2^{O(cc)}$

$i(x)=1] \geq s^* + \varepsilon/t$

Use P^*_i to break PIR in time $2^{O(\kappa)}$

Summary

public-coin IP → (PIR) → one-round argument

Corollary: PSPACE $\subseteq$ 1-round argument

Open: 1-round argument = PSPACE ? NEXP ?

Remark: This method does not seem to work when applied to interactive **arguments** (rather than proofs)

Interactive proof [GKR08] → PCA

Thanks !!