How to Delegate Computations: The Power of No-Signaling Proofs

Ran Raz

(Weizmann Institute & IAS)

Joint work with:

Yael Tauman Kalai

Ron Rothblum

Delegation of Computation

Delegation of Computation:

Alice has $x \in \{0,1\}^n$

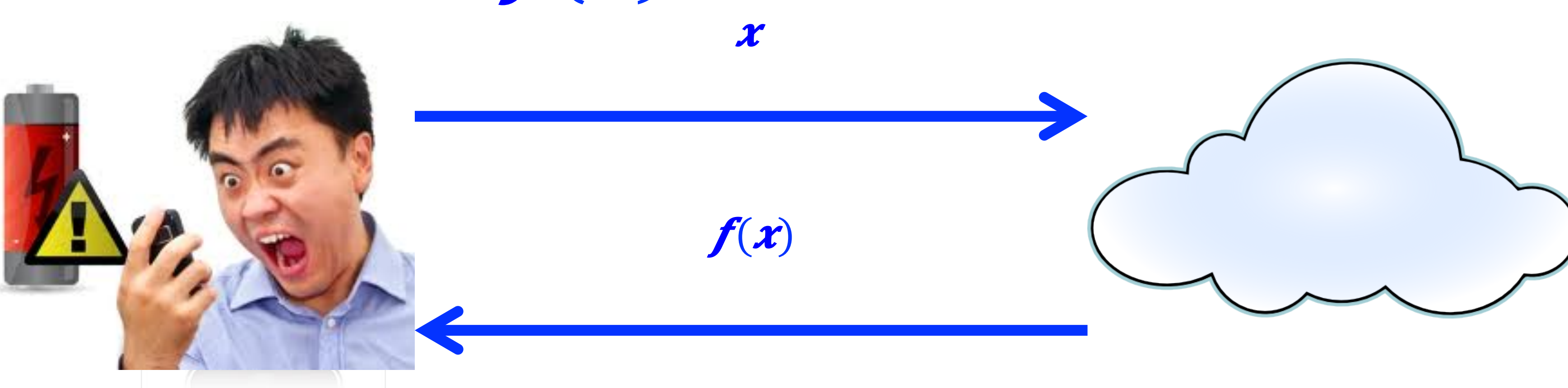
Alice needs to compute $f(x)$, where

f is publicly known

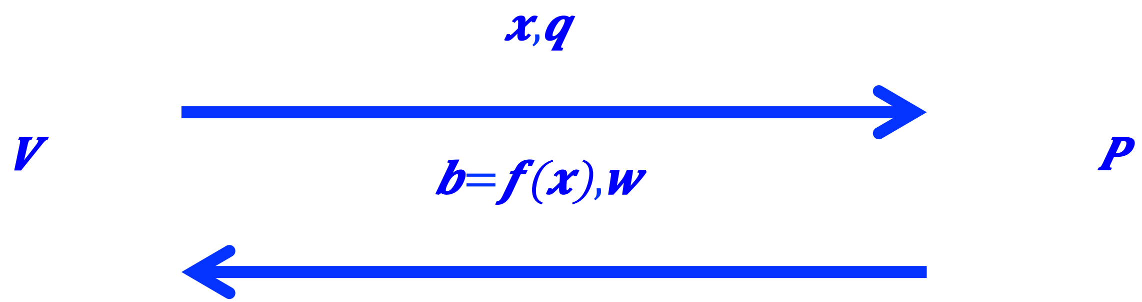
Bob offers to compute $f(x)$ for Alice

Alice sends x to Bob

Bob sends $f(x)$ to Alice



1-Round Delegation Scheme for f:



$f \in Time[t(n)]$

V *accepts* or **rejects**

1) Completeness: if P is honest:

$$\Pr[V \text{ accepts}] = 1 - neg$$

2) Soundness: $\forall P^* \in Time[t^*(n)]$, if $b \neq f(x)$:

$$\Pr[V \text{ rejects}] = 1 - neg$$

3) Running time of P: $poly(t(n))$

4) Running time of V: $\ll t(n)$

Previous Work [GKR+KR]:

If f is a logspace-uniform circuit of size t and depth d:

1-round delegation scheme s.t.:

Running time of P: poly(t)

Running time of V: $O(n+poly(d))$

(under exponential hardness assumptions)

Our Result:

If $f \in Time[t(n)]$

1-round delegation scheme s.t.:

Running time of P: **poly**$(t(n))$

Running time of V: $n \cdot polylog(t(n))$

(under exponential hardness assumptions)

Variants of Delegation Schemes:

1-Round or Interactive

Computational or Statistical soundness:

- 1-Round, Computational: This talk!
- 1-Round, Statistical: Impossible!
- Interactive, Computational: Solved! (with only 2-rounds) [Killian,Micali], (based on MIP=NEXP) [BFL]
- Interactive, Statistical: [GKR 08]

- Many other works, under unfalsifiable assumptions, or with preprocessing.

The Approach of Aiello et al.

2-Prover Interactive Proofs [BGKW]:

Provers A,B claim that $x \in L$

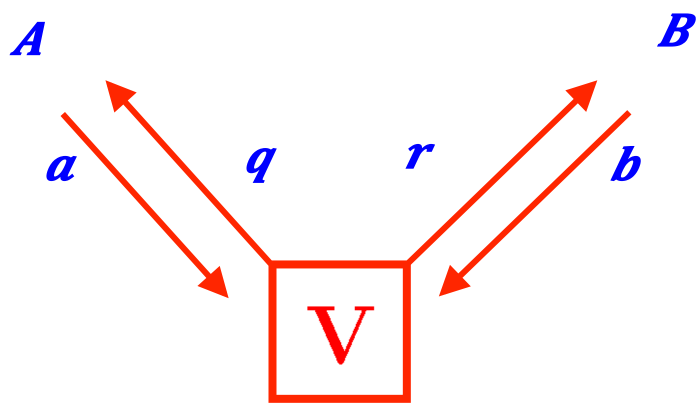
V sends a query q to A and r to B

no communication between A and B

A answers by $a = A(q)$

B answers by $b = B(r)$

V decides accept/reject by q,r,a,b



MIP=NEXP (scaled down) [BFL+FL]:

$\forall L \in Time[t(n)]$, $\exists$ 2-provers MIP s.t.:

1) Completeness: if A,B are honest:

$$\mathbf{Pr}[V\ accepts]=\mathbf{1}$$

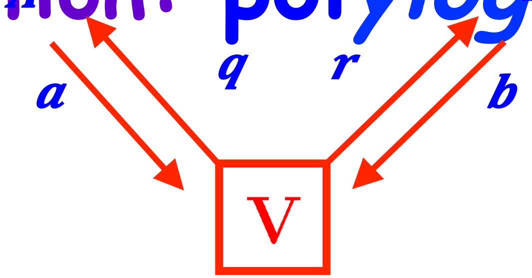
2) Soundness: $\forall A^*, B^*$ if $x \notin L$:

$$\mathbf{Pr}[V\ rejects]=\mathbf{1}-neg$$

3) Running time of A,B: $poly(t(n))$

4) Running time of V: $O(n)$

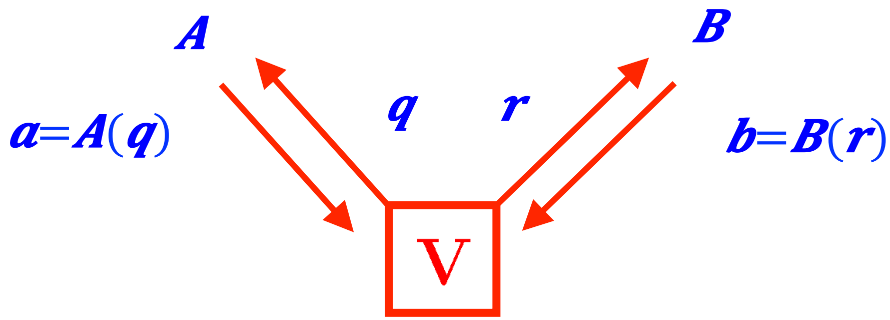
5) Communication: $polylog(t(n))$

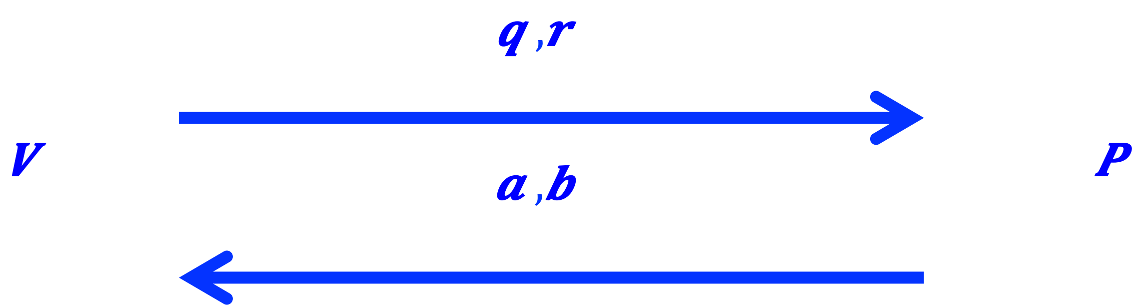


[Aiello Bhatt Ostrovsky Sivarama 00]:

MIP $\Longrightarrow$ 1-Round Argument ?!?

MIP:

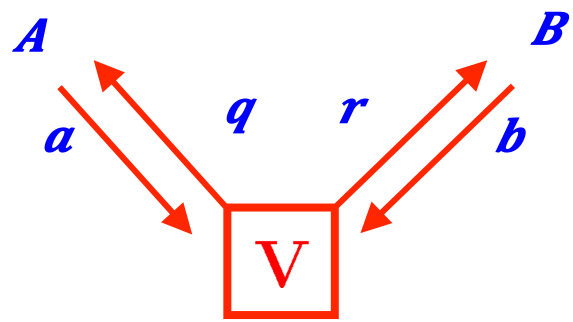




q,r = FHE of q,r (with different keys)

a,b = FHE of $\mathbf{a}=\mathbf{A}(\mathbf{q}), b=B(r)$

No-Signaling Strategies:



$a = A(q,r,z)$, $b = B(q,r,z)$

(where z is a shared random string):

Given q, the random variables a,r are independent

Given r, the random variables b,q are independent

No-Signaling Strategies for k provers:

queries: $q_1, \ldots, q_k$, answers $a_1, \ldots, a_k$

$a_i = A_i(q_1, \ldots, q_k, z)$, ($z$ = random string)

For every $S \subset [k]$: Given $\{q_i : i \in S\}$, $\{a_i : i \in S\}$, $\{q_i : i \notin S\}$, are independent

Soundness Against No-Signaling:

$\forall no-signaling \, (A_1, \ldots, A_k)^*$, if $x \notin L$:

$\mathbf{Pr}[V \, rejects] = \mathbf{1} - neg$

We Show (using [ABOS 00]):

MIP **with no-signaling soundness** $\Longrightarrow$ 1-Round Argument

(we need soundness for almost-no-signaling strategies)

Corollary:

Interactive Proof $\Longrightarrow$ 1-Round Argument

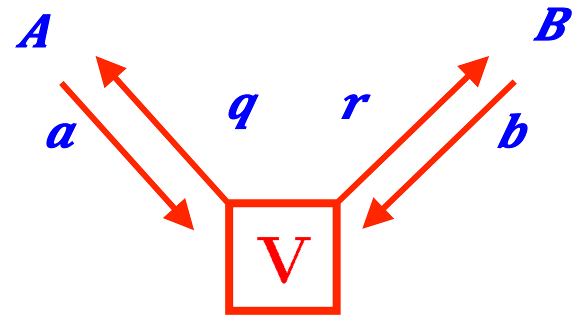
(under exponential hardness assumptions)

Gives a simpler proof for [KR 09]

Challenge: Show stronger MIPs with no-signaling soundness

No-Signaling Strategies

Entangled Strategies:



A,B share entangled quantum state $|$ $si{\downarrow}A,B$

A gets q, B gets r

A measures A, B measures B

A answers a, B answers b

Soundness Against Entangled Strategies:

$\forall entangled\,(A{\downarrow}1, \ldots, A{\downarrow}k){\uparrow}*$, if $x \notin L$:

$\mathbf{Pr}[V\ rejects] = \mathbf{1} - neg$

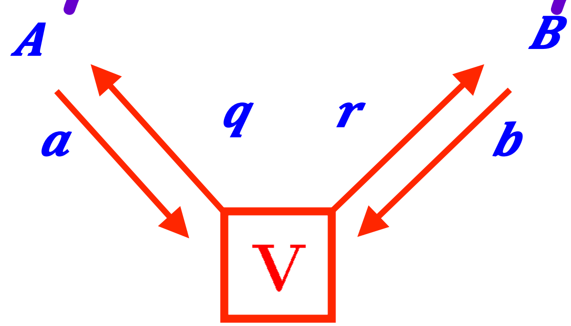
Entangled vs. No-Signaling:

Entangled strategies are no-signaling

Signaling $\Longrightarrow$
information travels faster than light

Hence, no-signaling is likely to hold in any future ultimate theory of physics

No-signaling soundness is likely to ensure soundness in any future physical theory



MIPs with No-Signaling Soundness:

No-Sig cheating provers are powerful:

$PSPACE \subseteq no\text{-}sig\ MIP \subseteq EXP$

$no\text{-}sig\ MIP(2)=PSPACE$ (by linear programing)

In particular, all known protocols for $MIP=NEXP$ are not sound for no-signaling

Example: Assume: V checks $a \oplus b = v\downarrow q,r$

Let $a = v\downarrow q,r \oplus z$. Let $b = z$. (z is random)

Then V always accepts

Our Result: no-*sig MIP* = *EXP*

If $\mathbf{L} \in Time[t(n)]$, MIP s.t.:

Running time of $P_1,\dots,P_k$:
poly($t(n)$)

Running time of V: $O(n)$

Number of provers: $\mathbf{k} = polylog(t(n))$

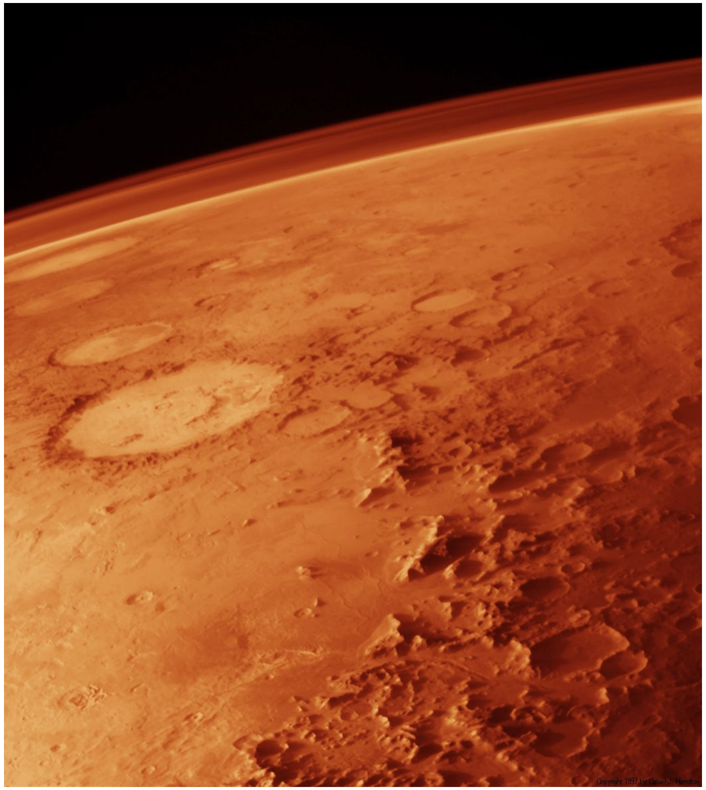
Communication: polylog($t(n)$)

Completeness: 1

Soundness: against no-sig strategies
(with negligible error)

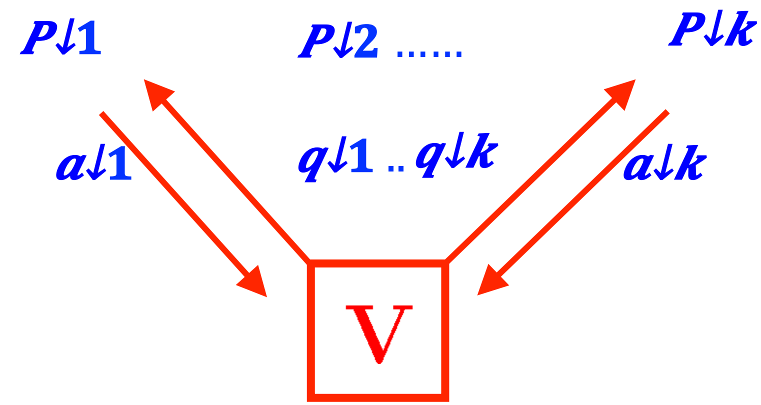
(gives soundness against entangled provers)

Delegating Computation to the Martians:



Delegating Computation to the Martians:

$\mathbf{L} \in Time[\boldsymbol{t}(\boldsymbol{n})]$



Running time of provers: **poly**($\boldsymbol{t}$)

Running time of $\boldsymbol{V}$: $\boldsymbol{O}(\boldsymbol{n})$

Number of provers: $\boldsymbol{k} = polylog(\boldsymbol{t})$

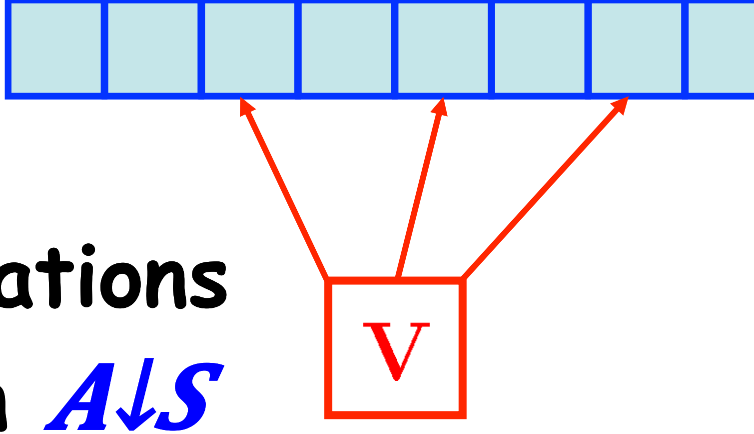
Number of provers: **polylog**($\boldsymbol{t}$)

Completeness: **1**

Soundness: against no-sig strategies

(with negligible error)

Steps of the Proof



No-Signaling PCPs:

For every subset S of locations s.t. $|S|\le K$, $\exists$ distribution A_S

If V queries locations $S=\{q_1,\dots,q_d\}$, the answers are given by $(a_1,\dots,a_d)\in_R A_S$

Guarantee: if $|S_1|,|S_2|\le K$, then A_{S_1}, A_{S_2} agree on their intersection

Step I: Switch to PCP:

Our Result:

$\mathbf{L} \in Time[t(n)]$ PCP s.t.:

Running time of prover: poly(t)

Running time of V: $O(n)$

Number of queries: $polylog(t)$

Completeness: 1

Soundness: against no-sig strategies

with $K =$ polylog(t)

(with negligible error)

Thank You!