SNARGs for P, and more\textsuperscript{1},
from poly-secure PIR

Justin Holmgren

Joint work with Zvika Brakerski and Yael Kalai

\textsuperscript{1}With RAM efficiency for the prover
Verifiable Computation: What we want

Common Reference String

Hey! $f(x) = y$. Here's a proof

I believe you

Computationally bounded
What’s Known

**Assumptions**
- random oracle/knowledge
- super-polynomial assumptions or iO
- standard LWE

**Result**
- holy grail
- two-message schemes

**Our Result**
- public key + 1 message, secret verification key

Moreover, RAM efficiency
Adversarial Worker:
- Adaptively chooses DB, M, x, y, d', and pf
- \textit{Wins} if $M^{DB}(x) \nrightarrow y,d'$ and \textit{Verify} accepts
Theorem

Assume standard LWE.

Then there is a non-interactive RAM delegation scheme.

For simplicity, assume FHE

More generally, any succinct PIR suffices
Scheme Overview

MIP

Prover 0

M, x, y, d

Worker

Client

Non-Interactive Delegation

Consider alternate with responses $q'_1, \ldots, q'_k, a'_1, \ldots, a'_k$

If $q_1 = q'_1$ then $a_1 \cong_c a'_1$

If $q_S = q'_S$ then $a_S \cong_c a'_S$

Construct stronger MIP?

Statistical No-Signaling [KRR14]

Encrypted with independent FHE keys

Construct stronger FHE?

• “Spooky-free” [DHRW16]
• “homomorphism-extractable” [BC12]

Guarantees answers are no-signaling

Verifier

Sound if answers generated locally

Aiello-Bhat-Ostrovsky-Rajagopalan ‘00
Family of MIP-based schemes

<table>
<thead>
<tr>
<th>FHE Strength</th>
<th>MIP Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spooky-Free</td>
<td>Local</td>
</tr>
<tr>
<td>Super-poly</td>
<td>Statistical</td>
</tr>
<tr>
<td>IND-CPA</td>
<td>No-Signaling</td>
</tr>
<tr>
<td>IND-CPA</td>
<td>Computational</td>
</tr>
<tr>
<td></td>
<td>No-Signaling</td>
</tr>
</tbody>
</table>

Moreover, MIP is adaptive

This Work
MIP Overview

1. Lemma: “local soundness”

For any T-time $P^*$ which claims $M^{DB}(x) \rightarrow y, d'$ ($Pr[\text{win}] > \epsilon$)

- We can construct an algorithm
- Assign $P^*$ : Any $V$ such that $|V| \leq k$

Our focus today

2. Lemma: local soundness implies soundness.
### Tableau for RAMs

**Variables:**

<table>
<thead>
<tr>
<th>Layer 1</th>
<th>Layer 2</th>
<th>...</th>
<th>Layer t</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine state</td>
<td>Digest</td>
<td>Mem Op</td>
<td>Merkle Proof</td>
</tr>
</tbody>
</table>

- **Check initial state = q₀**
- **Check final output = y**
- **Check final digest = d’**
- **Check initial digest = d**

**poly(λ)**

Local constraints:

- Check Merkle proofs, check state transition (for all adj. layers)
Local to global

**Claim**

\[ M^{DB}(x) \rightarrow y, d' \]

With probability \( \epsilon \)

\[ M^{DB}(x) \not\rightarrow y, d' \]

By hybrid argument, for some \( i \):

---

### Variables

<table>
<thead>
<tr>
<th>Layer</th>
<th>Machine state</th>
<th>Merkle root</th>
<th>Mem Op</th>
<th>Merkle Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 1</td>
<td>( M.q_0 )</td>
<td>( d )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layer 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layer t</td>
<td>( y )</td>
<td>( d' )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Local to global

**Claim**

\[ M^{DB}(x) \rightarrow y, d' \]

Assign \[ P^* \]

= queries to Assign \[ P^* \]

**Variables**

<table>
<thead>
<tr>
<th>Machine state</th>
<th>Merkle root</th>
<th>Mem Op</th>
<th>Merkle Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer i</td>
<td>Correct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layer i+1</td>
<td>Incorrect</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

With probability \( \epsilon \)

\[ M^{DB}(x) \not\rightarrow y, d' \]

By hybrid argument, For some i...

with prob \( \epsilon/t \)
Local to global

Claim

\[ M_{DB}(x) \rightarrow y, d' \]

With probability \( \epsilon \)

\[ M_{DB}(x) \not\rightarrow y, d' \]

By hybrid argument, For some i...

Variables

<table>
<thead>
<tr>
<th>Machine state</th>
<th>Merkle root</th>
<th>Mem Op</th>
<th>Merkle Proof</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer i</td>
<td>Correct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layer i+1</td>
<td>Incorrect</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Locally Consistent

Hash Collision!

Assign

Assign \( P^* \)

= queries to Assign \( P^* \)
Application: NP Delegation

\[ \mathcal{L} = \{ x : \exists w \text{ s.t. } R_{\mathcal{L}}(x, w) \} \]

Prover

Verifier

With modifications, can prove many x's "for the price of one" x, w, proof that \( R_{\mathcal{L}}(x, w) = 1 \)

Optimal communication* [Gentry-Wichs]

running time \(|x| + |w|\)

For deterministic computations

Soundness follows from deterministic adaptive soundness

* from falsifiable assumptions
Thanks