SNARGs for P, and more[1], from poly-secure PIR

Justin Holmgren

Joint work with Zvika Brakerski and Yael Kalai

[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		**Result**
random oracle/ knowledge		holy grail
super-polynomial assumptions or iO		two-message schemes
standard LWE	**Our Result**	public key+1 message, secret verification key

Moreover, RAM efficiency

Soundness:

P.P.T.  wins negligibly often

Worker | **Client**

pk

$pk, vk \leftarrow Gen(1^{\lambda})$

DB

DB

$d = Digest(DB)$

M,x

$y, d' \leftarrow M^{DB}(x)$

M,x,y,d',pf

Verify(M,d,x,y,d',pf)

Accept?

Adversarial Worker:

- Adaptively chooses DB, M, x, y, d', and pf
- *Wins* if $M^{DB}(x) \not\to y,d'$ **and** Verify accepts

Theorem

For simplicity, assume FHE

More generally, any succinct PIR suffices

Assume standard LWE.

Then there is a non-interactive RAM delegation scheme.

Scheme Overview

Aiello-Bhat-Ostrovsky-Rajagopalan '00

MIP

q_1 q_k

Prover 0

M,x,y,

Verifier

Construct stronger MIP?

Statistical No-Signaling [KRR14]

Sound if answers generated **locally**

Non-Interactive Delegation

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

If $q_1 = q'_1$ then $a_1 \approx_c a'_1$
If $q_S = q'_S$ then $a_S \approx_c a'_S$

Construct stronger FHE?

- "Spooky-free" [DHRW16])
- "homomorphism-extractable" [BC12]

Encrypted with independent FHE keys

Guarantees answers are **no-signaling**

Family of MIP-based schemes

	FHE Strength	MIP Strength
More Crypto	Spooky-Free	Local
	Super-poly IND-CPA	Statistical No-Signaling
More MIP	IND-CPA	Computational No-Signaling

Moreover, MIP is adaptive

This Work

MIP Overview

Redo [KRR14] and more

1. Lemma: "local soundness"

distribution

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

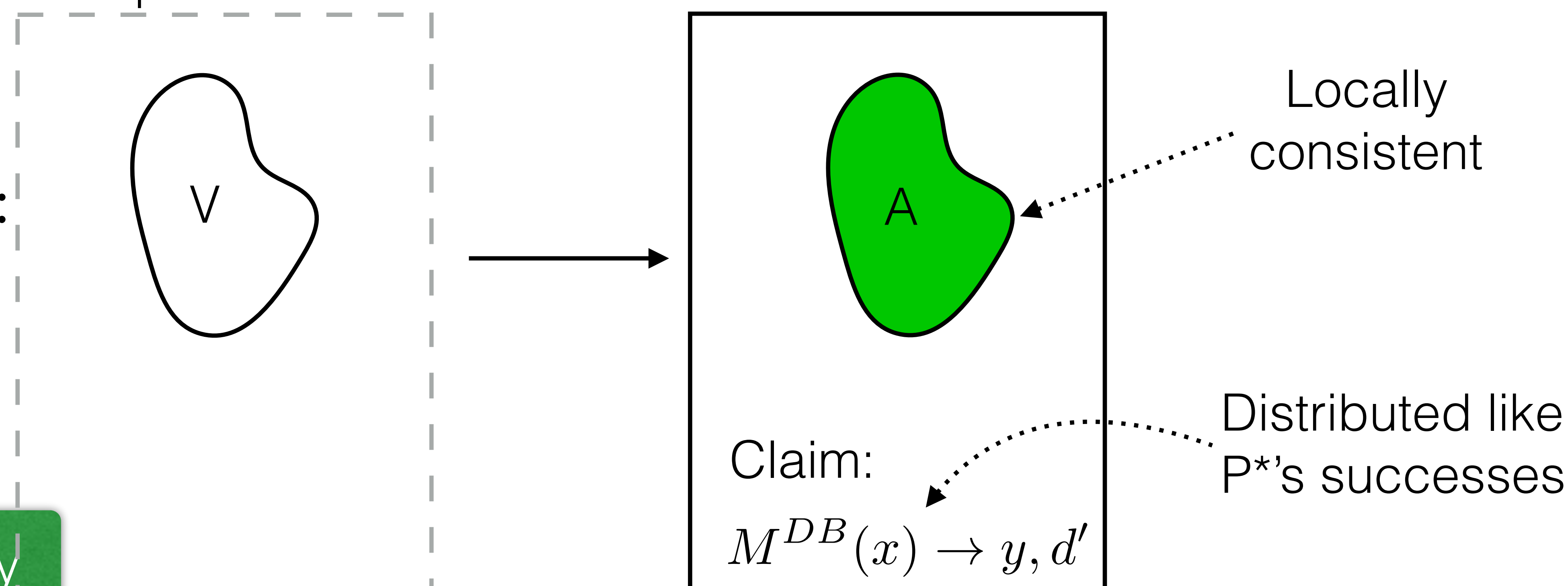
we can construct algorithm

Assign$^{P^*}$:

Any V

$|V| \leq k$

T-step tableau

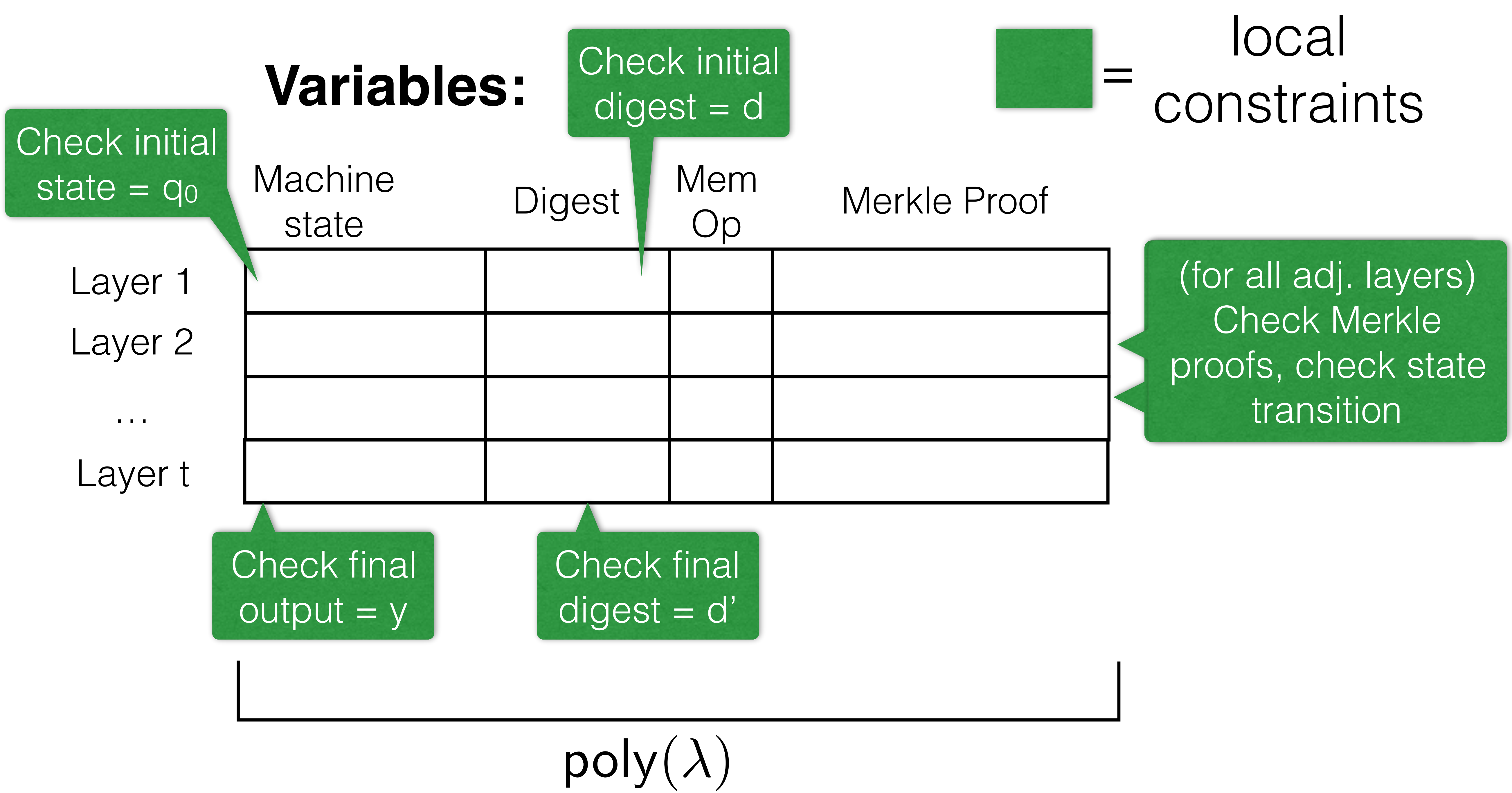


Our focus today

2. Lemma: local soundness implies soundness.

Tableau for RAMs

Kalai-Paneth 15



Local to global

Claim

Assign$^{P^*}$ → $M^{DB}(x) \to y, d'$

With probability ϵ

$M^{DB}(x) \not\to y, d'$

■ = queries to Assign$^{P^*}$

Variables

	Machine state	Merkle root	Mem Op	Merkle Proof
Layer 1	$M.q_0$	d		
Layer 2				
…				
Layer t	y	d'		

By hybrid argument,
For some i…

Local to global

Claim

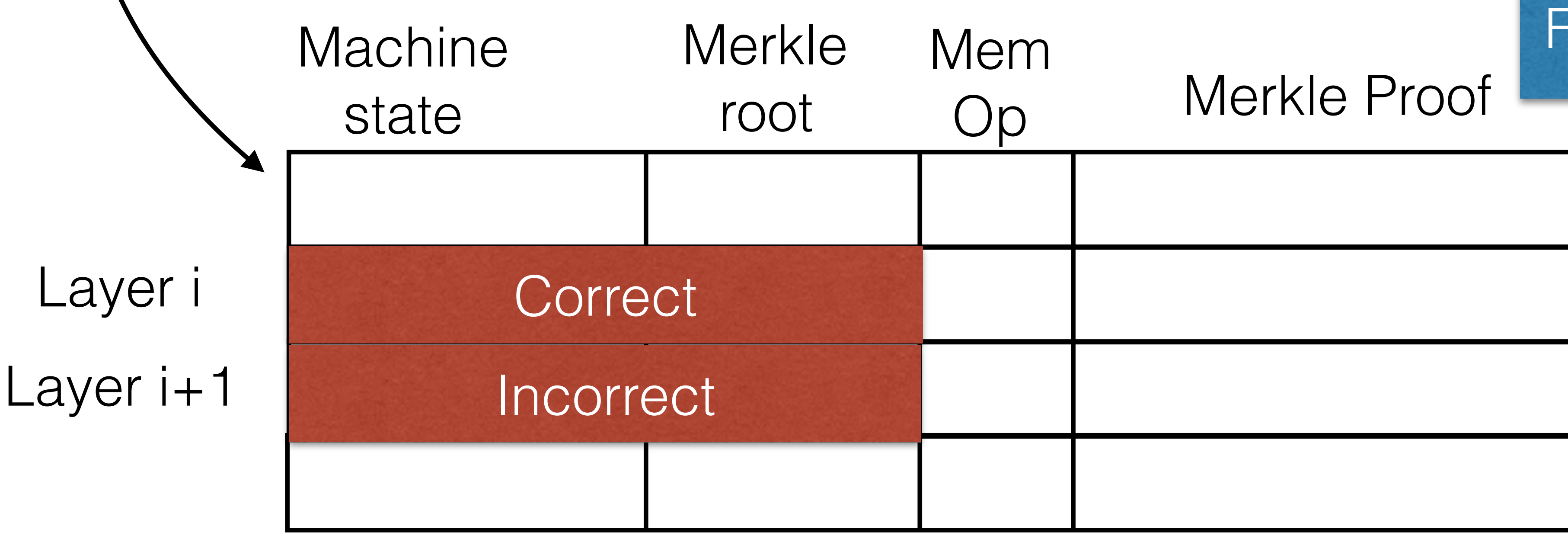
$\text{Assign}^{P^*} \longrightarrow M^{DB}(x) \to y, d'$

With probability ϵ
$M^{DB}(x) \not\to y, d'$

■ = queries to Assign^{P^*}

Variables

By hybrid argument,
For some i…



with prob ϵ/t

Local to global

Claim

$\text{Assign}^{P^*} \longrightarrow M^{DB}(x) \rightarrow y, d'$

With probability ϵ

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

= queries to Assign^{P^*}

Variables

By hybrid argument,
For some i…

	Machine state	Merkle root	Mem Op	Merkle Proof
Layer i	Correct		Locally	
Layer i+1	Incorrect		Consistent	

with prob ϵ/t

Hash
Collision!

Application:
NP Delegation

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

running time
|x| + |w|

Prover

Verifier

$vk \leftarrow \mathsf{Gen}(1^\lambda)$

x,w

With modifications,

Can prove many x's
"for the price of one"

For deterministic
computations

$R_{\mathcal{L}}(x, w) = 1$

Optimal
communication*
[Gentry-Wichs]

deterministic
computation

Soundness follows
from deterministic
adaptive soundness

* from falsifiable assumptions

Thanks