Delegating Computation: A New Perspective

Yael Tauman Kalai
Microsoft Research

The Power of Proofs

Interactive proofs [GMR85]

↓

multi-prover interactive proofs [BGKW88]

All powerful provers!

↓

Probabilistically checkable proofs [FRS88,FGLSS91, BFLS91,AS92,ALMSS92]

Doubly Efficient Proofs

[GKR08]

Proofs for **poly-time computations**:

Prover runtime ≈ computation runtime

Verifier runtime ≈ |input|

Doubly Efficient Proofs

[GKR08]

[GKR08]

Doubly efficient Interactive proofs
for bounded depth

$O(depth)$
rounds

Summary of Delegation Under **Standard Assumpti**

Doubly efficient interactive proof or argument

[GKR08]

Doubly efficient Interactive proofs for bounded depth

[KR09] →

2-message for bounded depth (under PIR)

PCP/MIP

[Ki92, Mi94] →

[IKO07, BC12,...]

4-message for NP (under CRH)

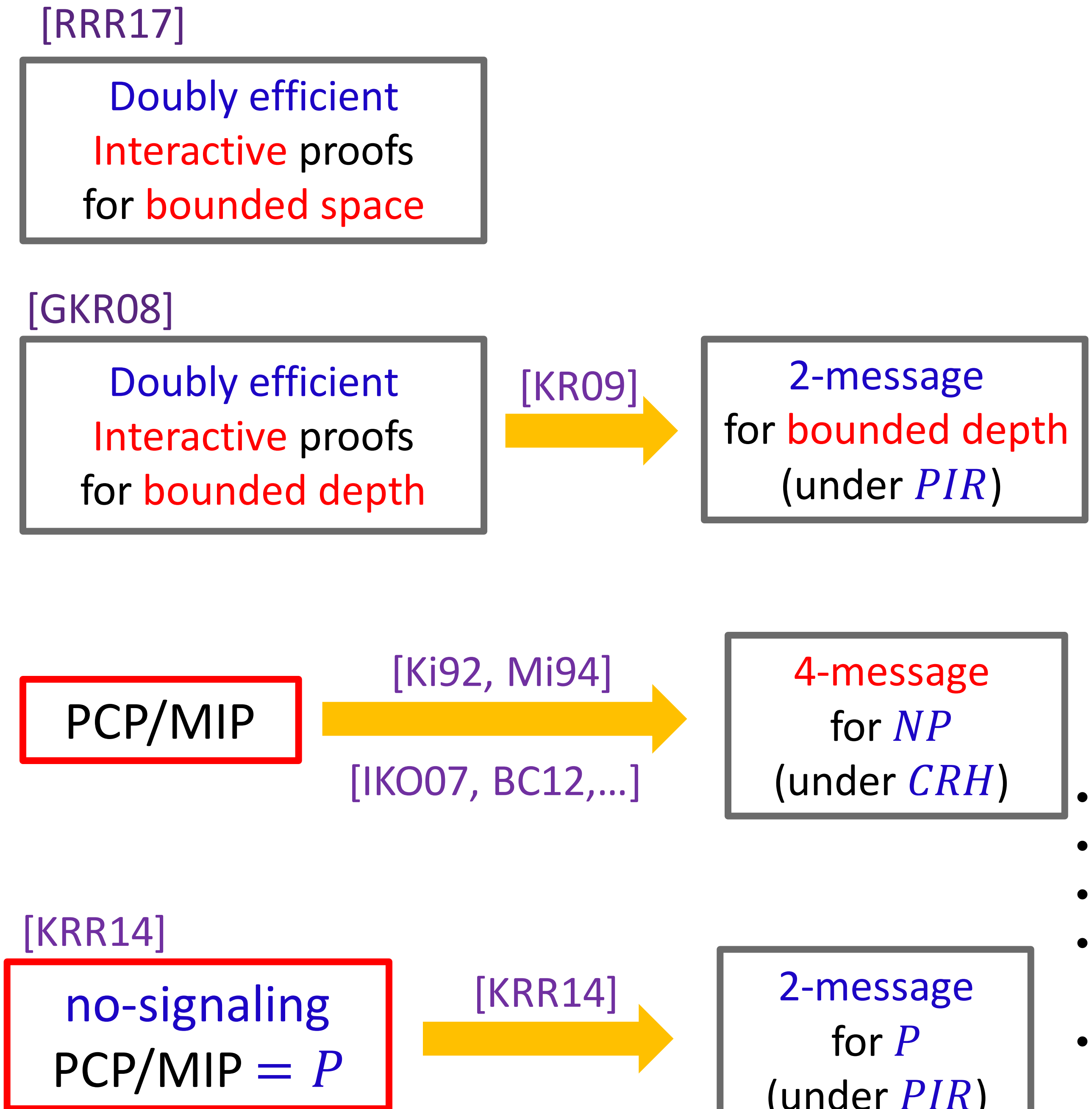
- **RAM** [KP15]
- **Poly PIR** [DNR16, BHK17]
- **Adaptive security** [BHK17]
- **Amortized NP delegation** [BHK17]
- **Quasi-linear runtime, and additive space overhead** [HR17]

[KRR14]

no-signaling PCP/MIP $= P$

[KRR14] →

2-message for P (under PIR)



- **RAM** [KP15]
- **Poly PIR** [DNR16, BHK17]
- **Adaptive security** [BHK17]
- **Amortized NP delegation** [BHK17]
- **Quasi-linear runtime, and additive space overhead** [HR17]

We Will NOT Talk About:

2-message for NP
(non-falsifiable assumptions)

[Micali94, Groth10, Goldwasser-Lin-Rubinstein11, Damgard-Faust -Hazay11, Lipma12, Gennaro-Gentry-Parno-Raykova12, Bitansky-Canetti-Chiesa-Tromer12a, Bitansky-Canetti-Chiesa-Tromer12b, Bitansky-Chiesa-Ishai-Ostrovsky-Paneth13 …]

2-message for P
($i\mathcal{O}$)

[Paneth-Rothblum14, Bitansky-Sanjam-Lin-Pass-Telang14, Canetti-Holmgren-Jain-Vaikuntanathan14, Koppula-Lewko-Waters14, Canetti-Holmgren16, Chen-Chow-Chung-Lai16]

Delegation in the Preprocessing Model

[Gennaro-Gentry-Parno2010 , Chung-K-Vadhan2010, Applebaum-Ishai-Kushilevitz2010, Parno-Raykova-Vaikuntanathan2011,…]

Theoretical Results → Implementations

[GKR08] →

Implementations

[CMT12, TRMP12, Thaler2013, VSBW13, WHGSW16, WJBSTWW17, ZGKPP17]

Pepper
[SMBW12]

Ginger
[SVPBBW12]

Pinocchio/libsnark
[PHGR13, BCGTV13]

Zaatar
[SBVBPW13]

Pantry
[BFRSBW13]

Buffet
[WSRBW15]

Proof Carrying Data
[BCTV14, CTV15]

Scalable Zero Knowledge
[BCTZ14]

Theoretical Results → Implementations

[GKR08] →

Implementations

[CMT12, TRMP12, Thaler2013, VSBW13, WHGSW16, WJBSTWW17, ZGKPP17]

[GKR08] blue-print proved itself useful!

Main drawback: Only useful for low depth

Today: Use GKR Blueprint **Beyond** Bounded Depth Delegation

Obtain previous theoretical results using GKR blueprint

Hope:

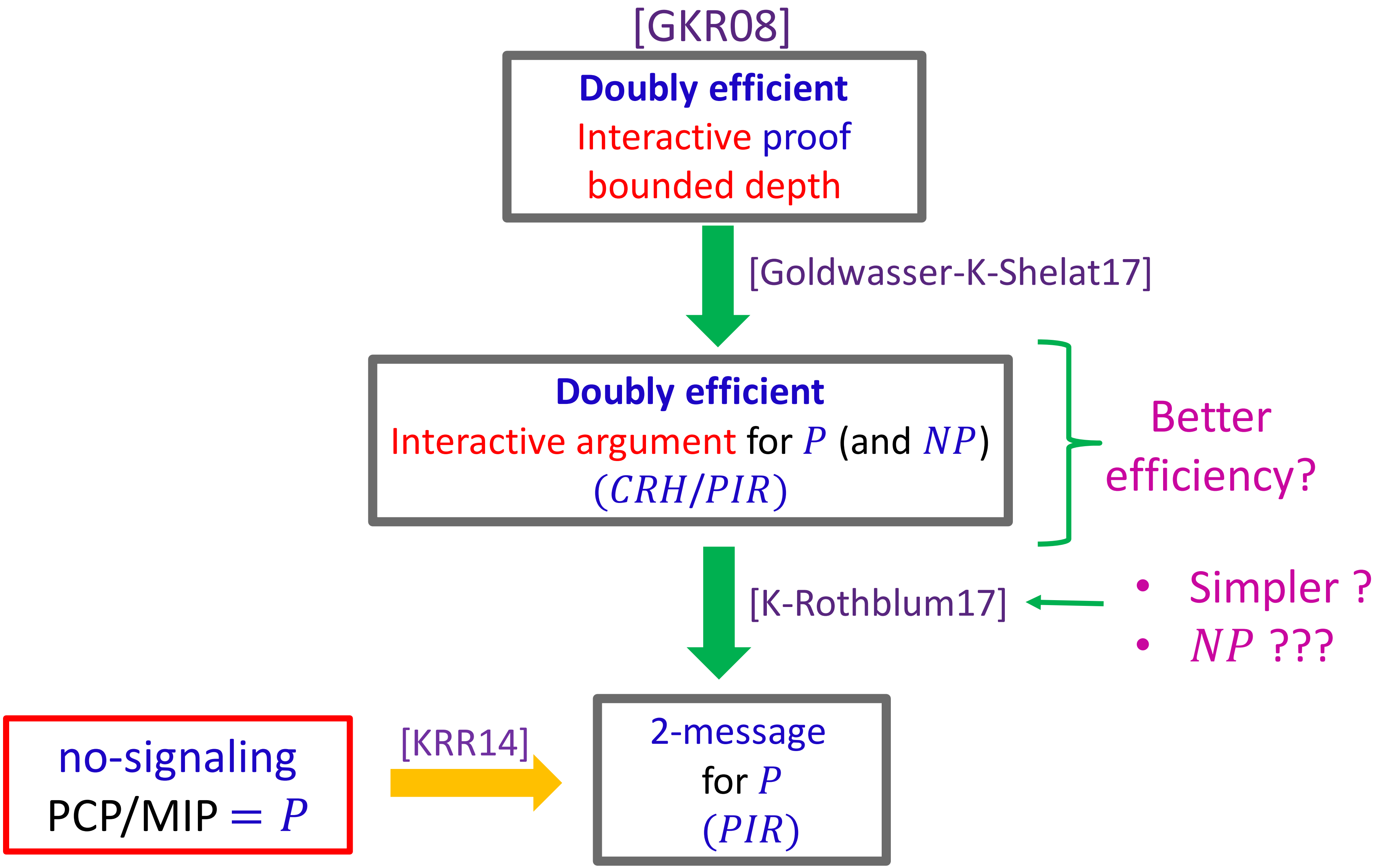
1. Lead to practical improvements

   Practical delegation for P (and NP)

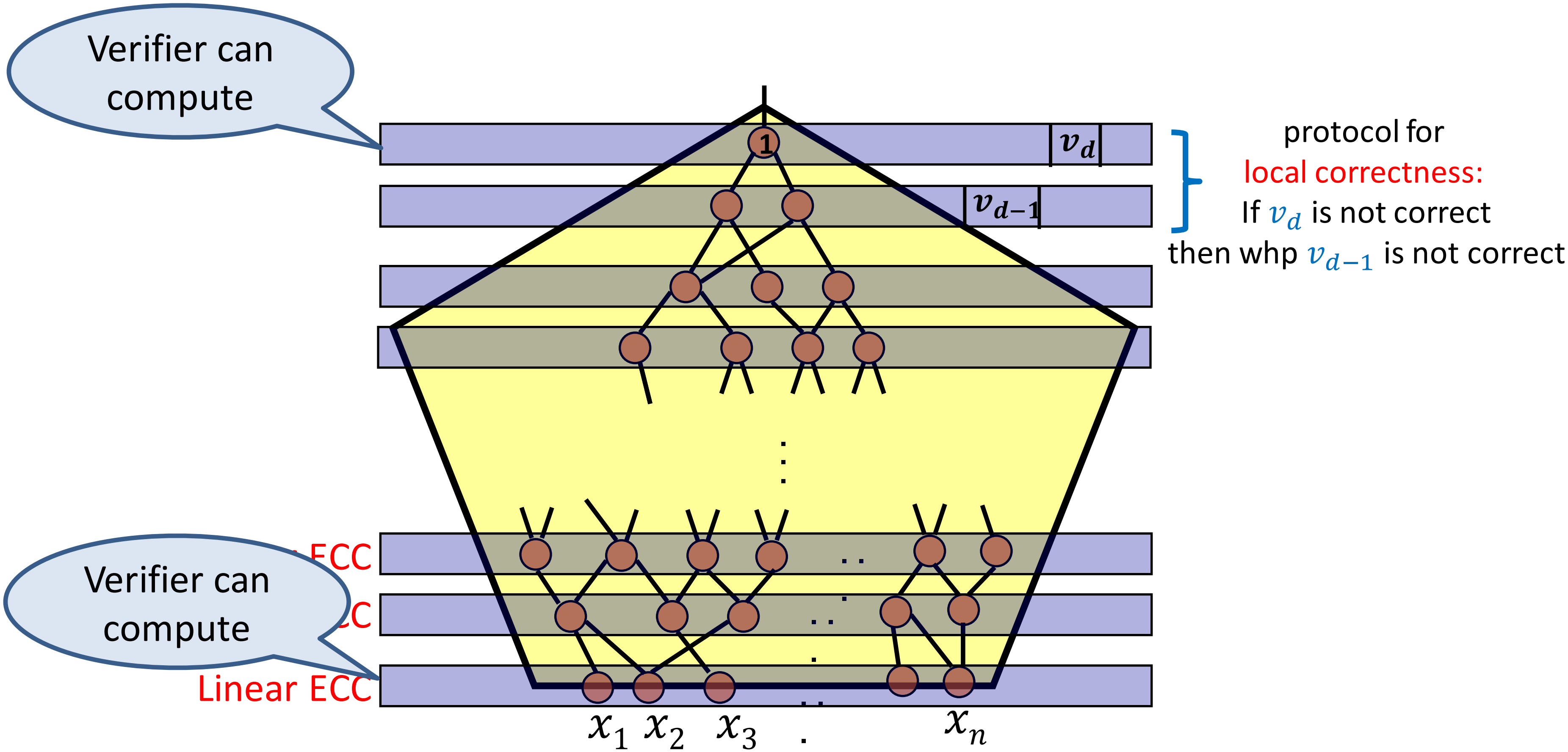
2. Shed light towards theoretical improvements

   2-message delegation for NP?

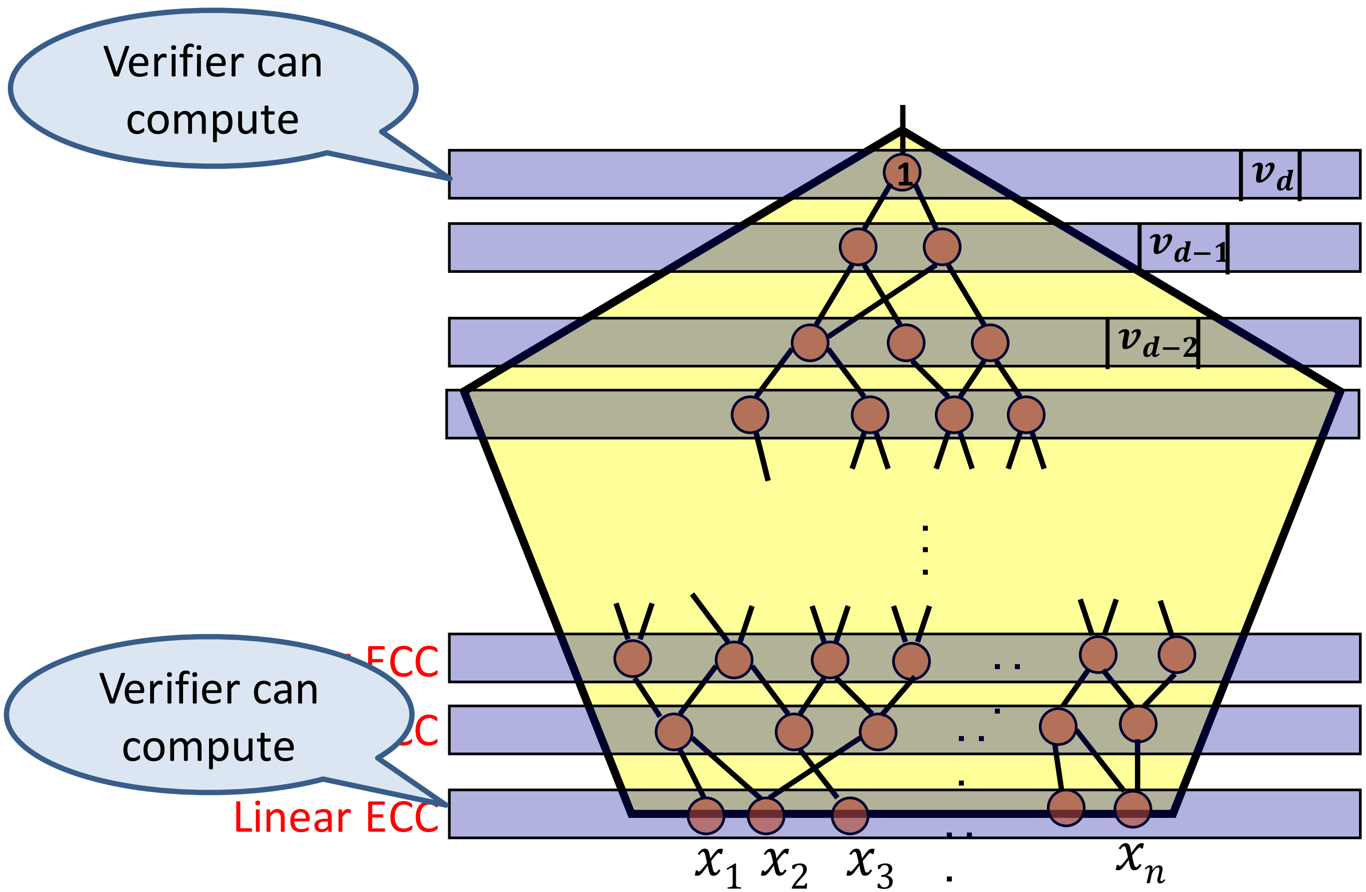
Today


[GKR08]
Doubly efficient
Interactive proof
bounded depth
[Goldwasser-K-Shelat17]
Doubly efficient
Interactive argument for P (and NP)
(CRH/PIR)
Better
efficiency?
[K-Rothblum17]
• Simpler ?
• NP ???
no-signaling
PCP/MIP $= P$
[KRR14]
2-message
for P
(PIR)

[GKR08] Blue Print

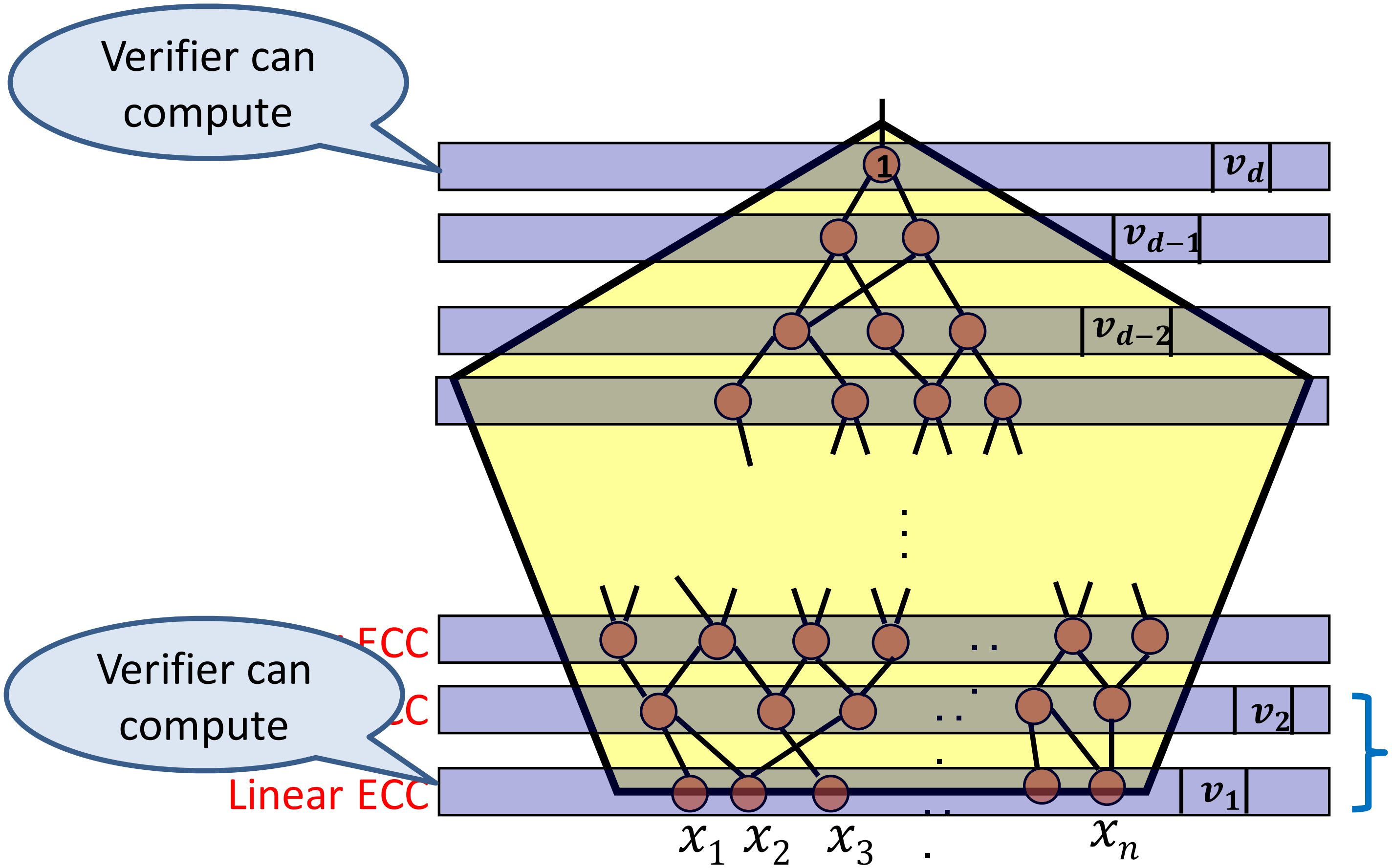


[GKR08] Blue Print



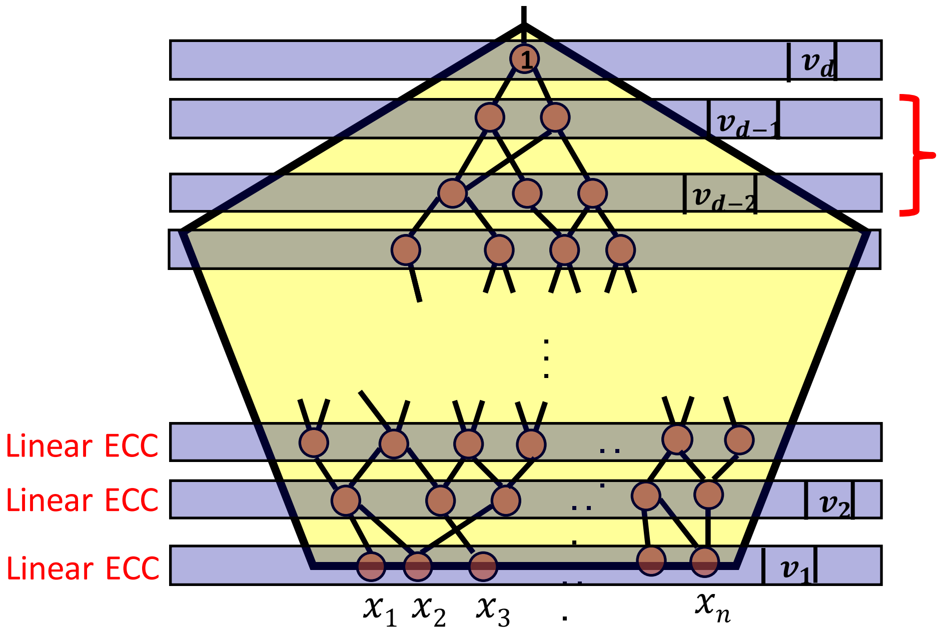
protocol for
local correctness:
If v_{d-1} is not correct
then whp v_{d-2} is not correct

[GKR08] Blue Print



protocol for
local correctness:
If v_2 is not correct
then whp v_1 is not correct

[GKR08] Blue Print



protocol for local correctness:

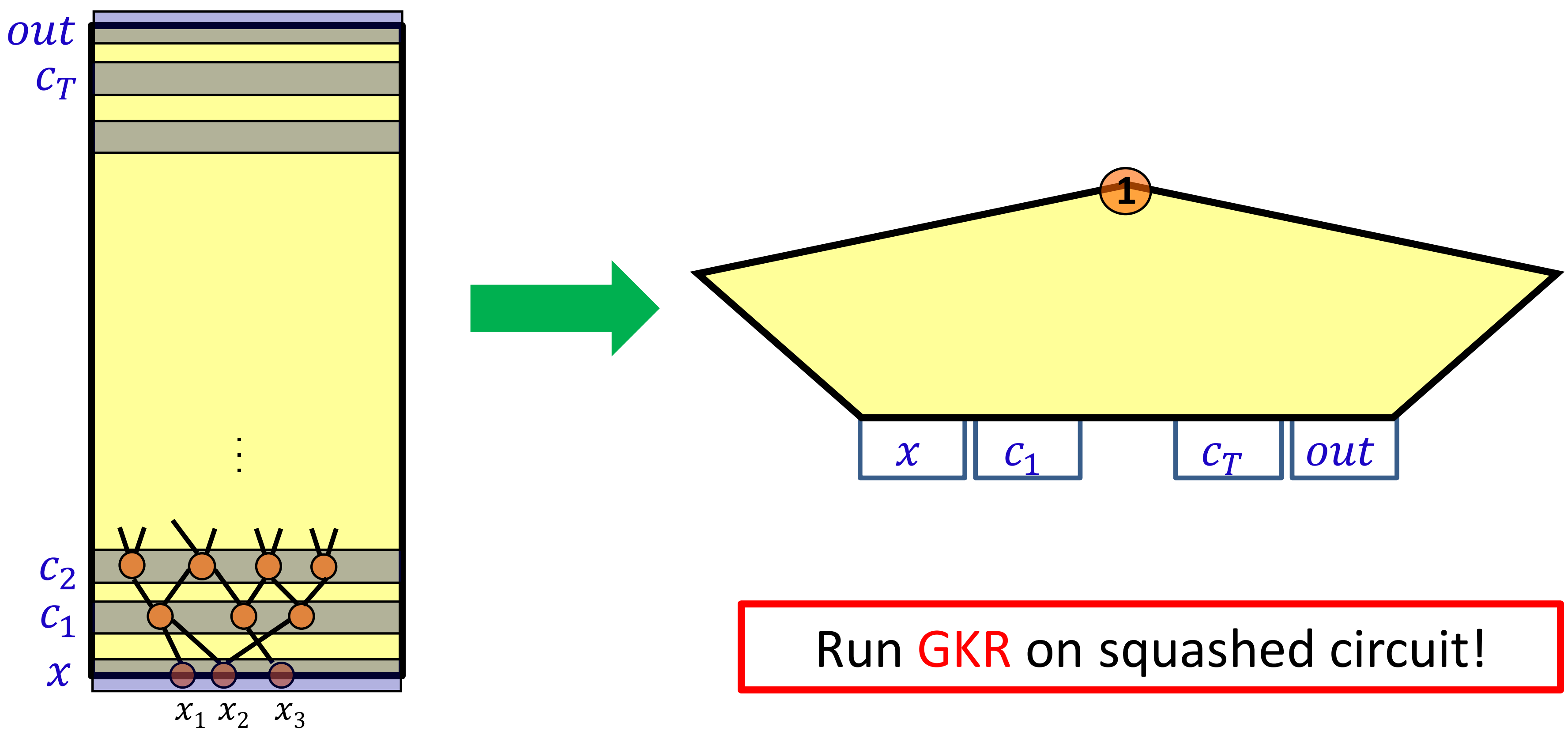
Sum-check

- Verifier runtime $polylog(S)$
- Number of rounds $polylog(S)$
- Prover runtime $poly(S)$

Verifier runtime and communication grows with the depth

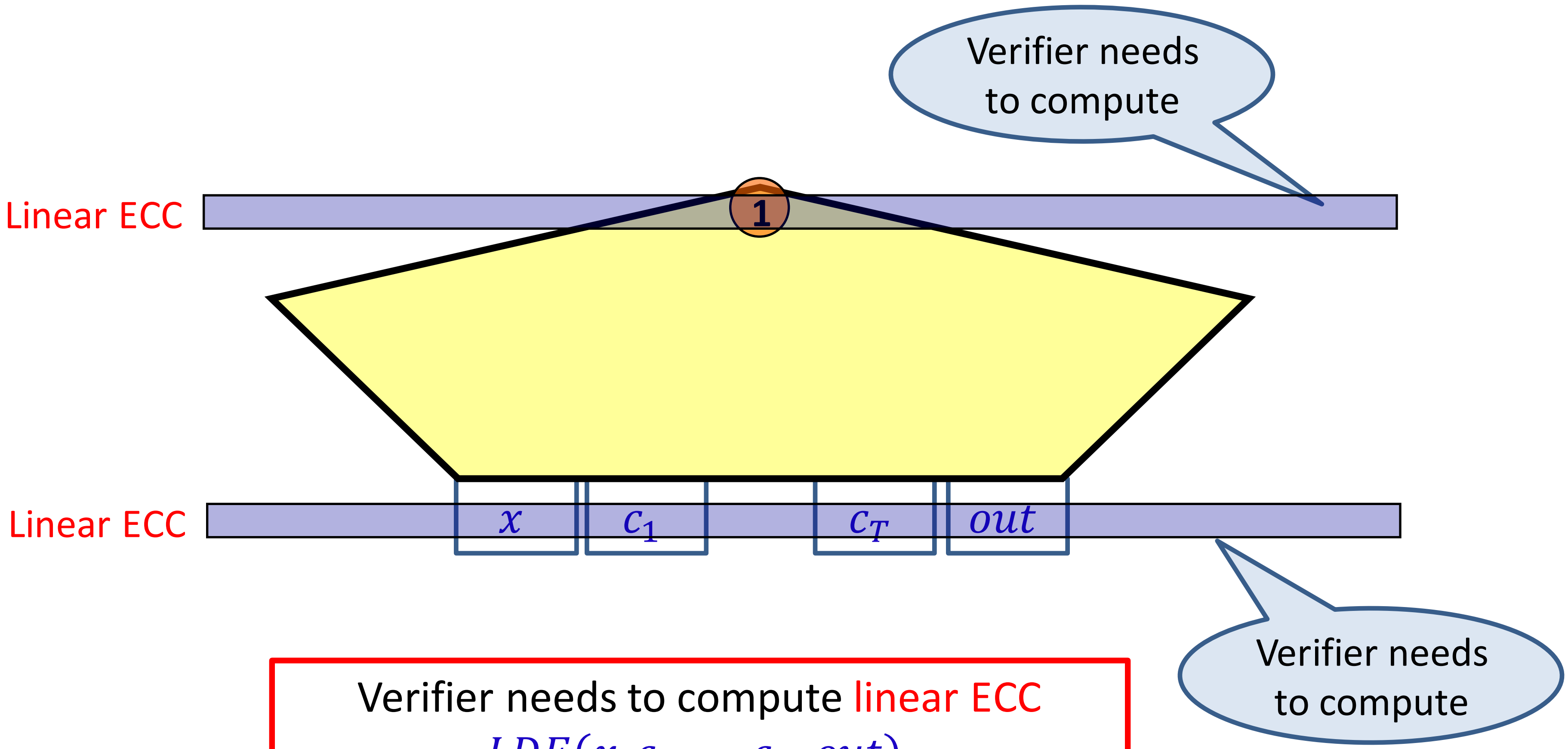
Eliminate Depth Restriction in GKR

Idea: Convert computation to low-depth circuit!



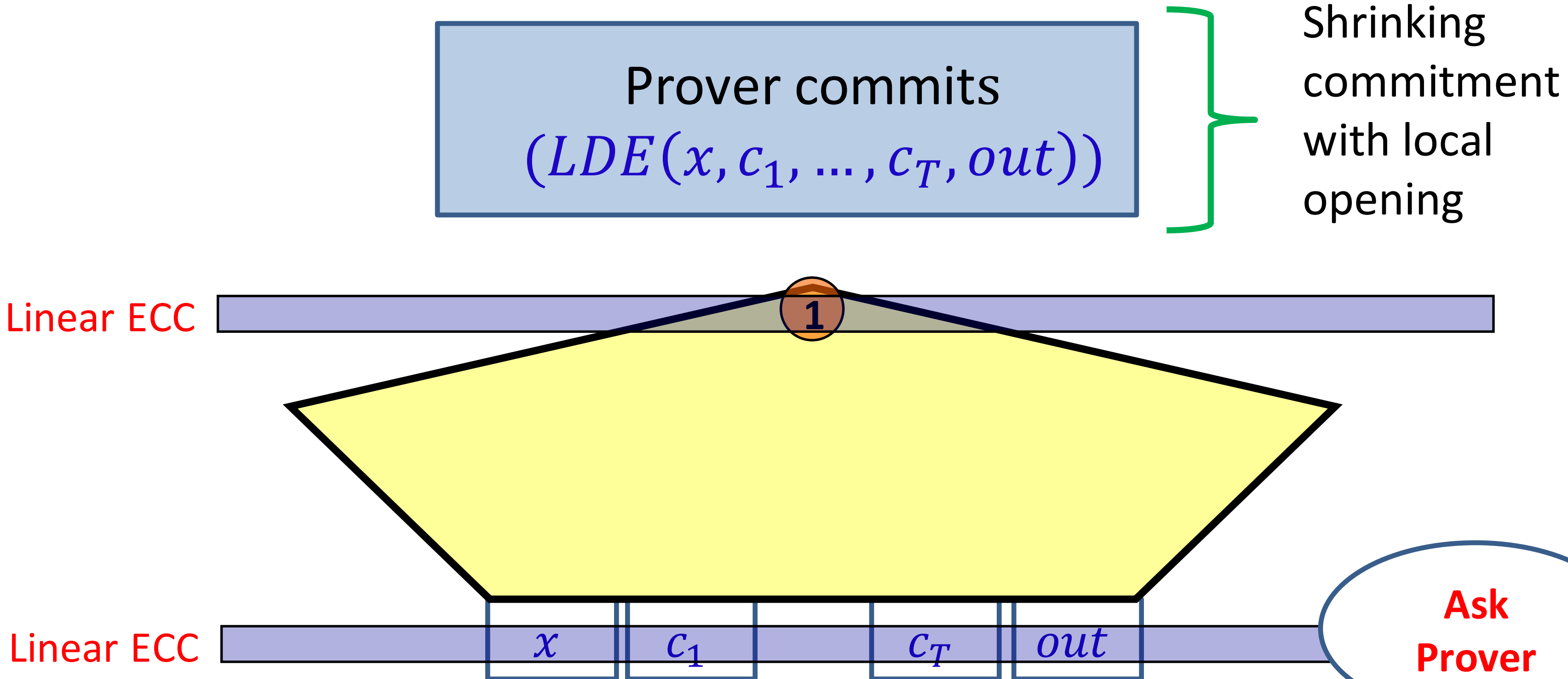
Run GKR on squashed circuit!

Squashed GKR



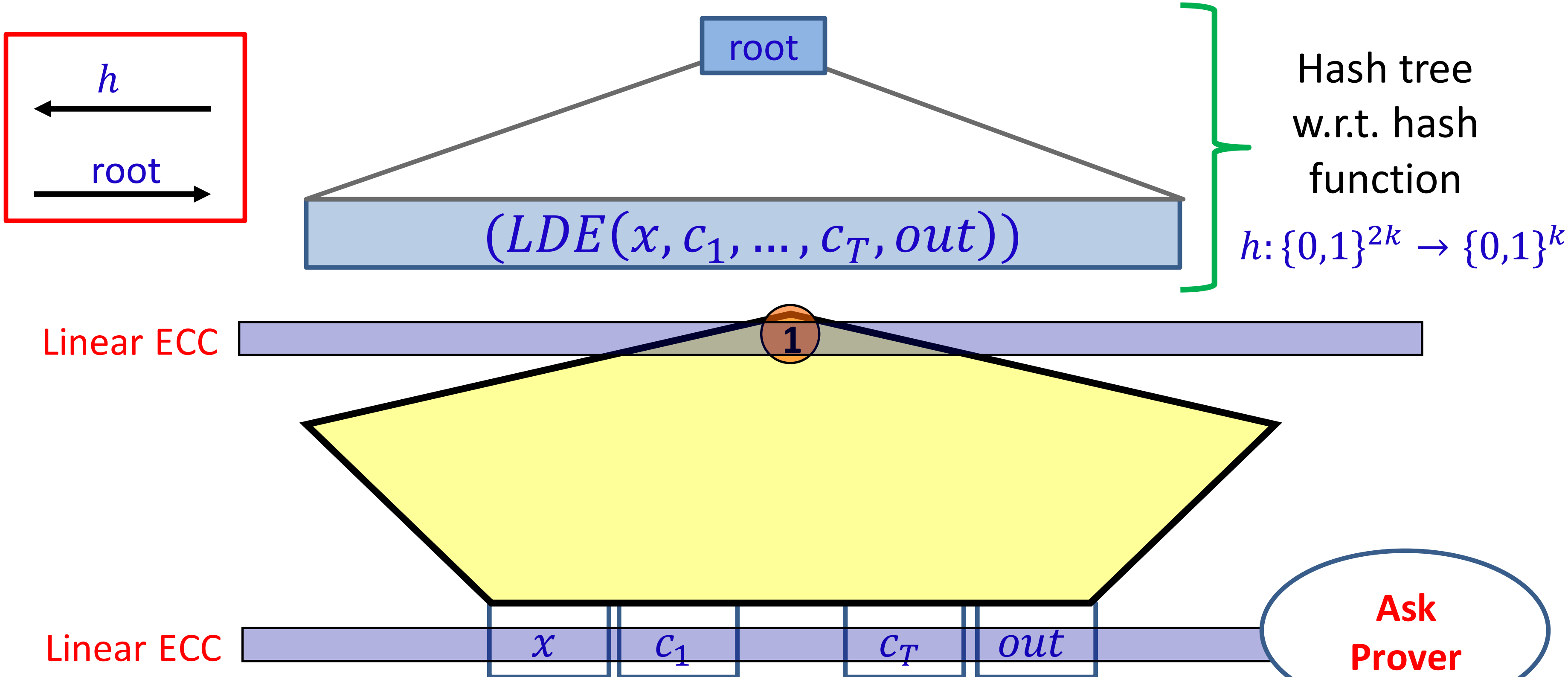
Verifier needs to compute linear ECC
$LDE(x, c_1, \ldots, c_T, out)$
on a single point of his choice!

Squashed GKR



Verifier needs to compute linear ECC
$LDE(x, c_1, \dots, c_T, out)$
on a single point of his choice!

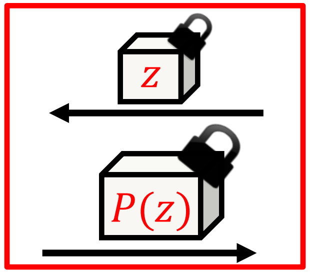
Squashed GKR

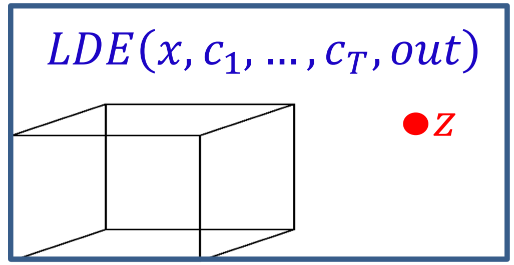


Verifier needs to compute linear ECC
$LDE(x, c_1, \ldots, c_T, out)$
on a single point of his choice!

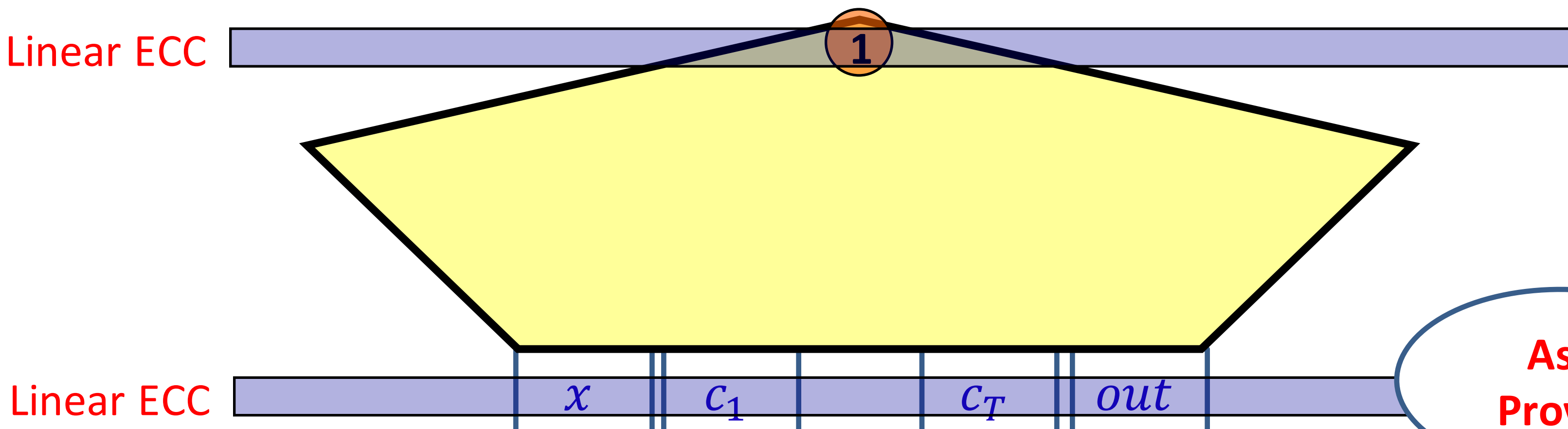
Squashed GKR

[Chunk-K-Liu-Raz11]





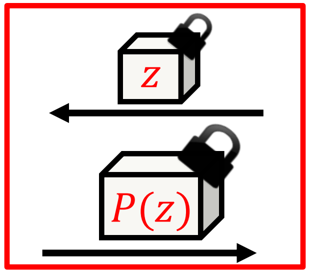
Shrinking commitment using Enc

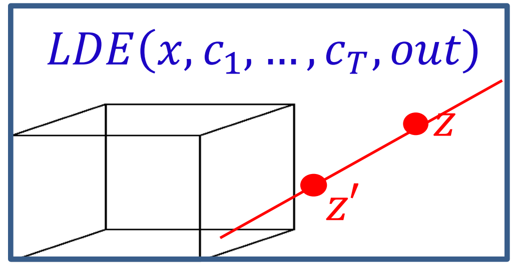


Verifier needs to compute linear ECC
$LDE(x, c_1, \dots, c_T, out)$
on a single point of his choice!

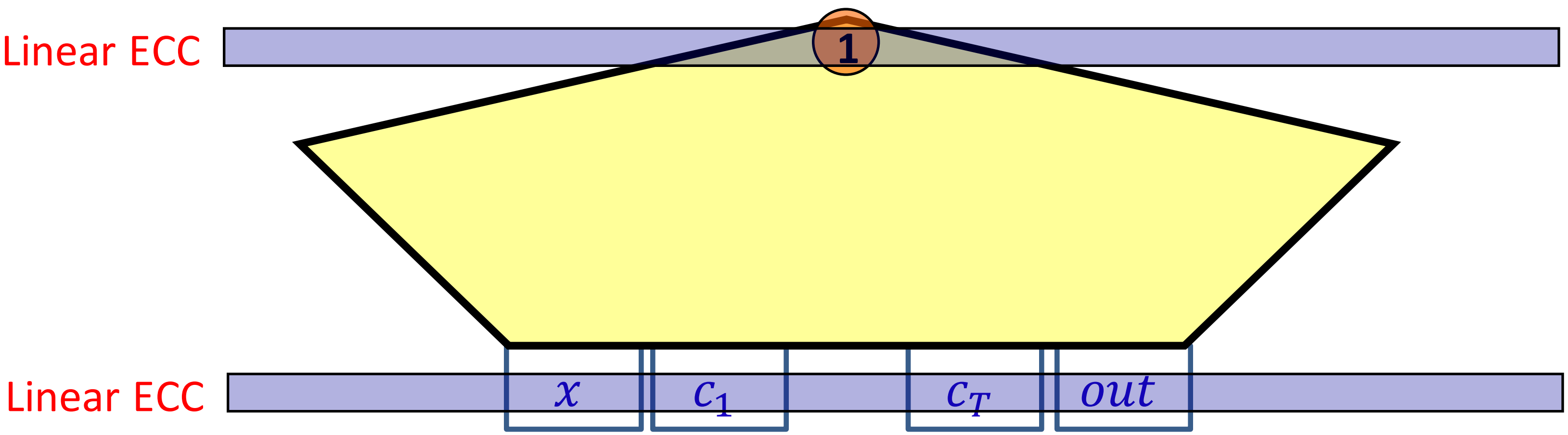
Squashed GKR

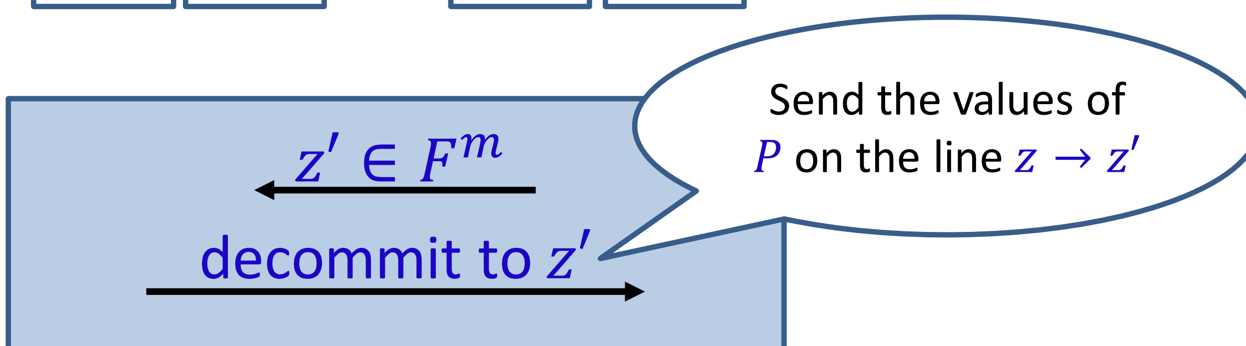
[Chunk-K-Liu-Raz11]





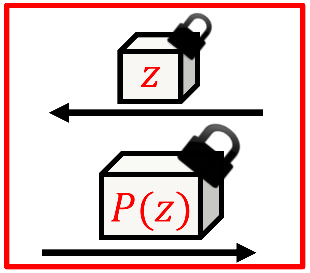
Shrinking commitment using Enc





Squashed GKR

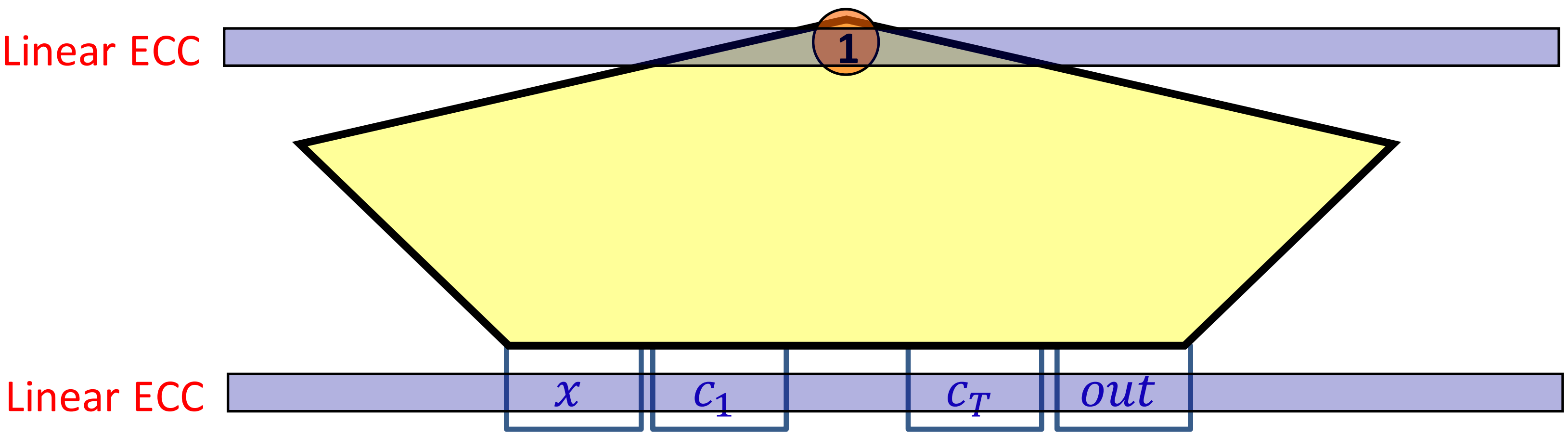
[Chunk-K-Liu-Raz11]



Commit$\left(LDE(x, c_1, \ldots, c_T, out)\right)$

+

Low degree test

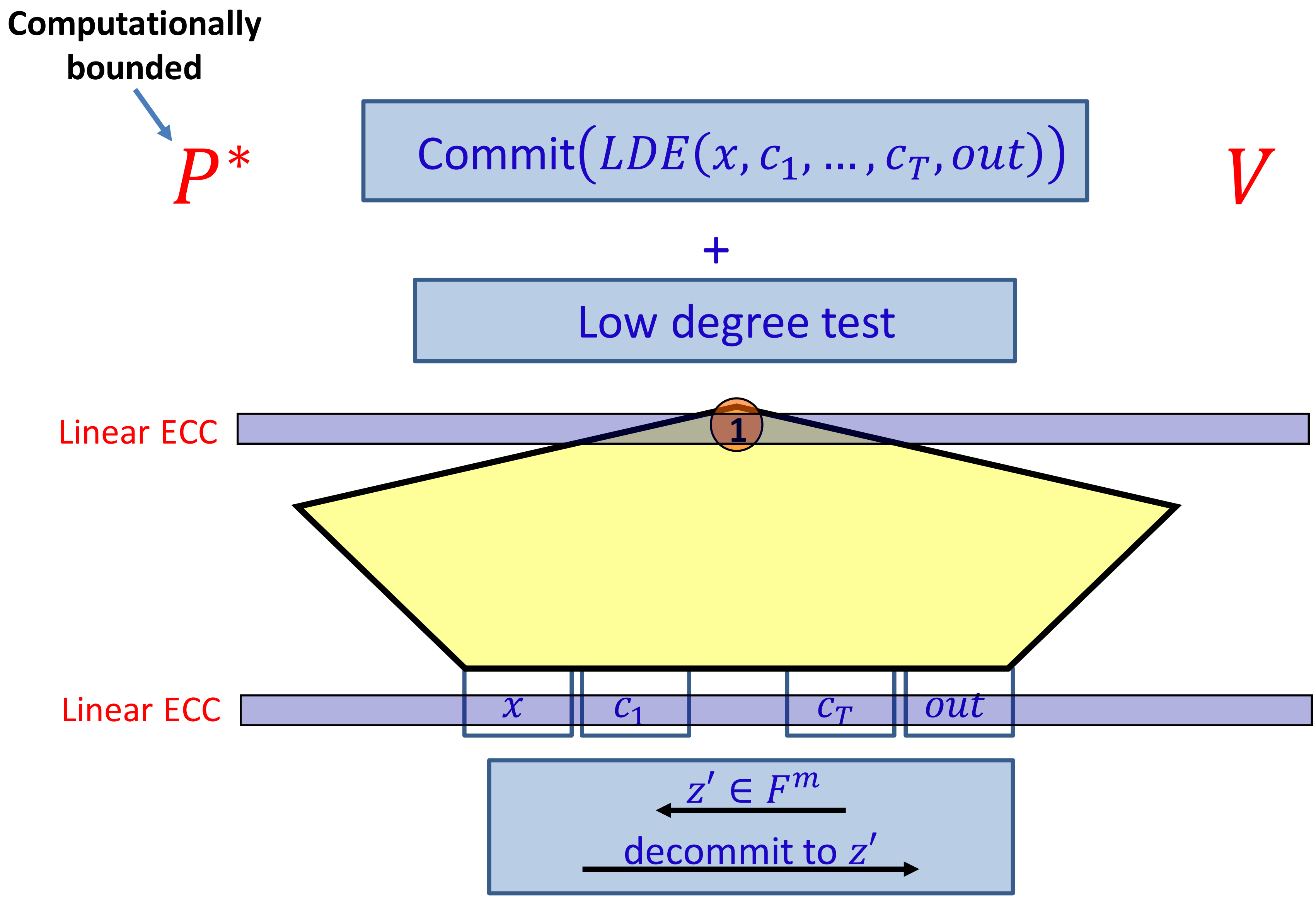


$z' \in F^m$

decommit to z'

Send the values of P on the line $z \to z'$

Soundness of Squashed GKR

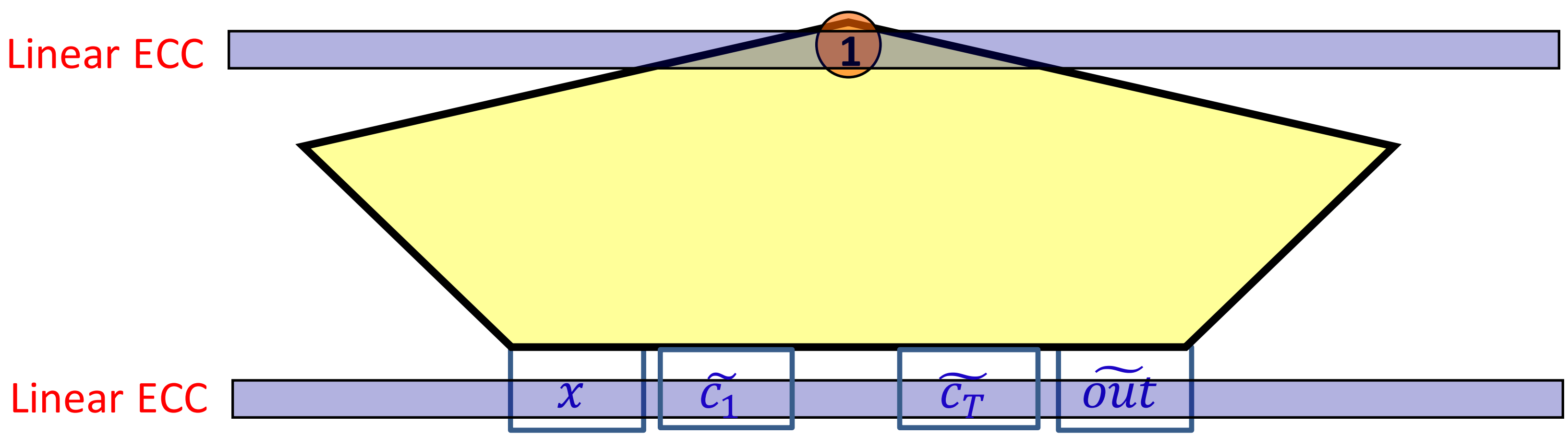


Soundness of Squashed GKR

P^*

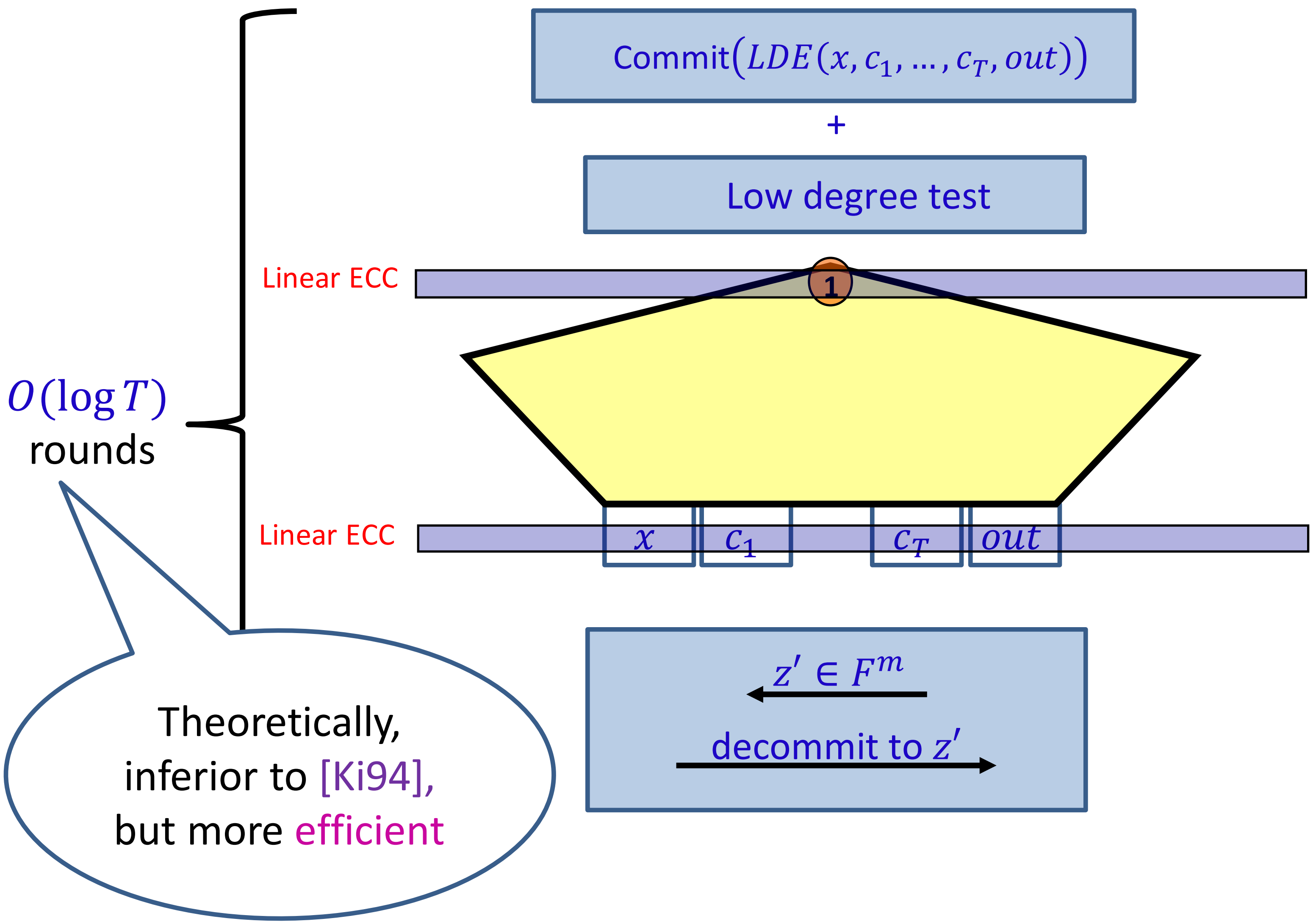
$$LDE(x, \tilde{c}_1, \ldots, \widetilde{c_T}, \widetilde{out})$$

V

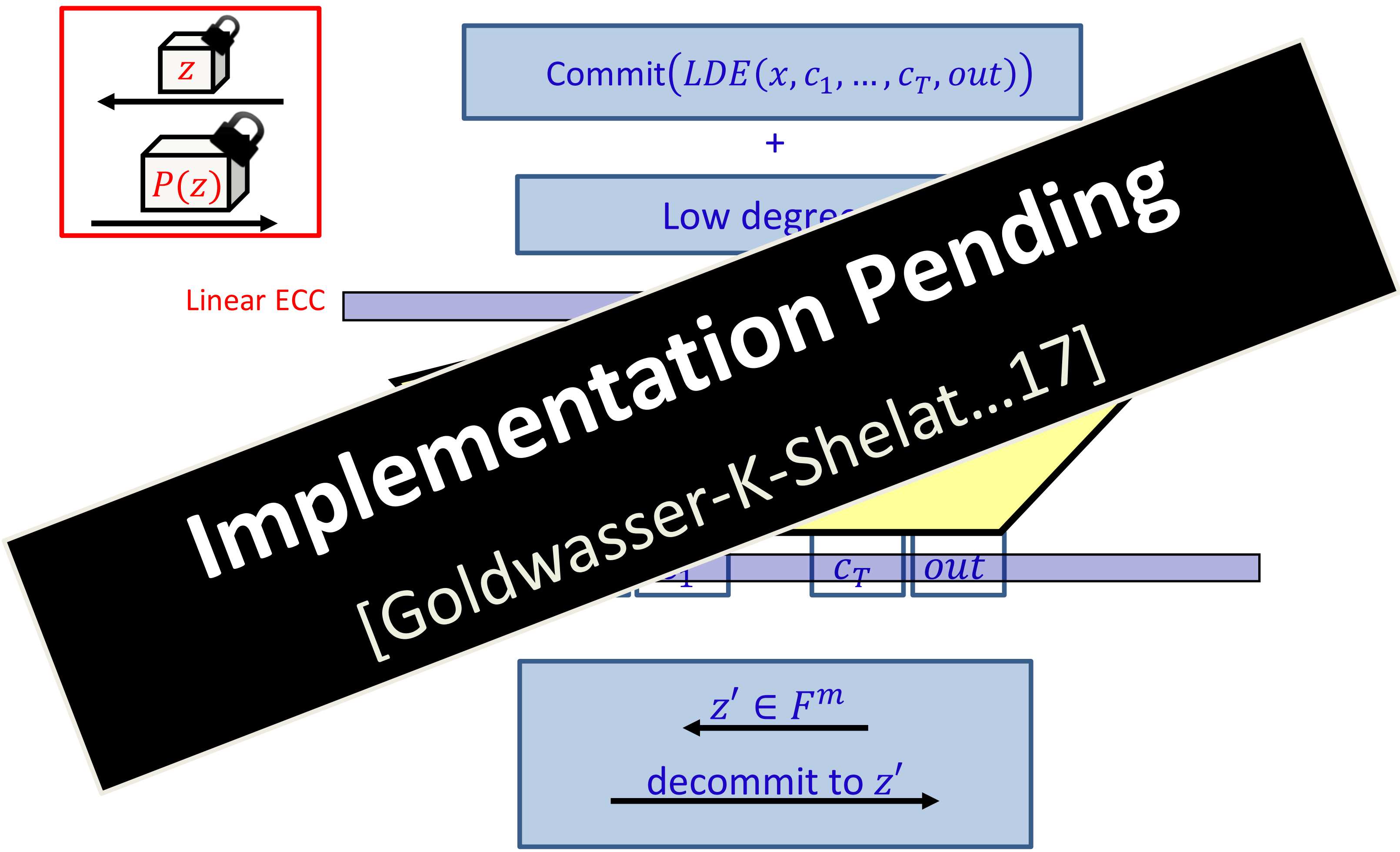


Soundness is implied by soundness of GKR

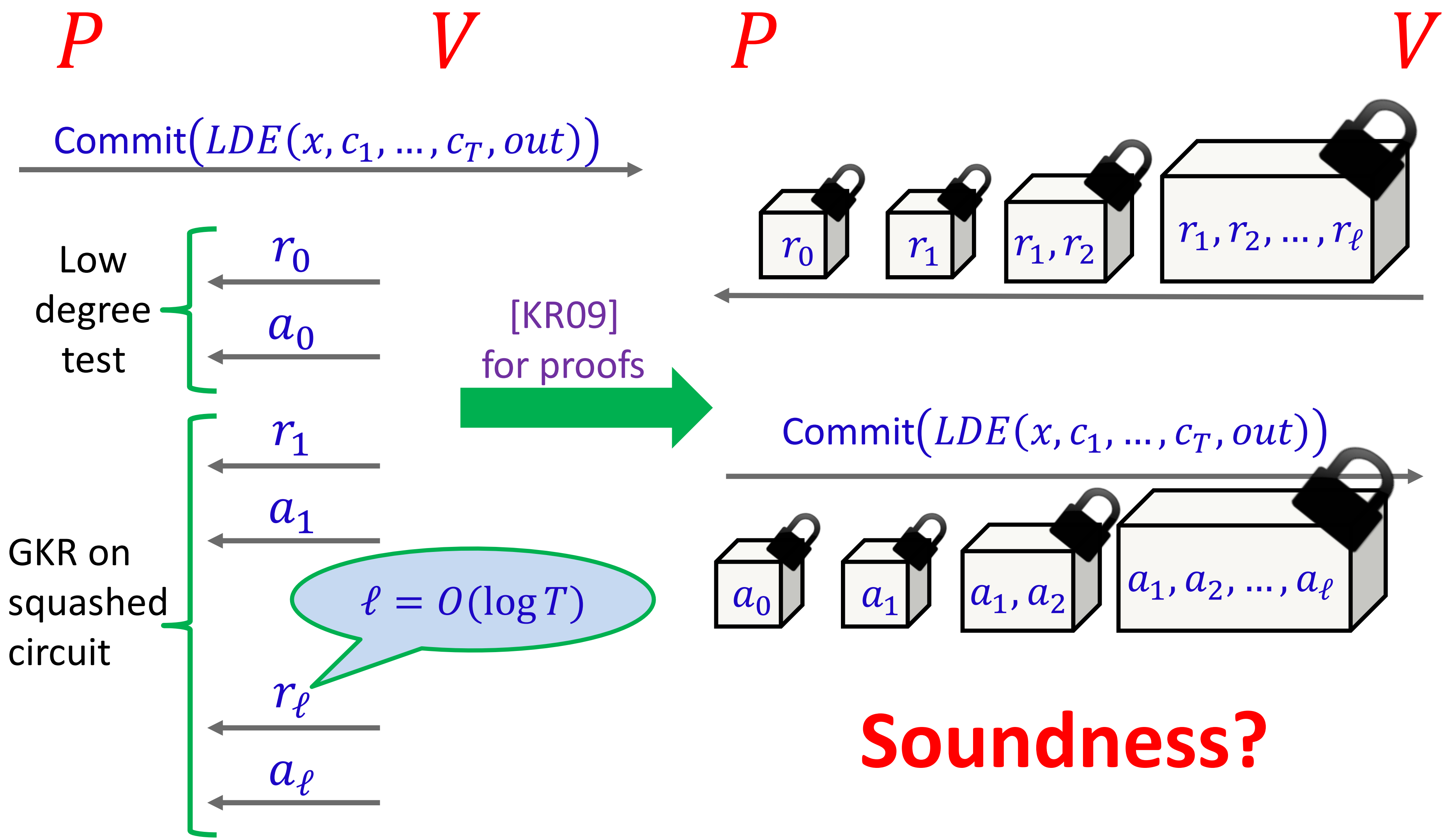
Squashed GKR

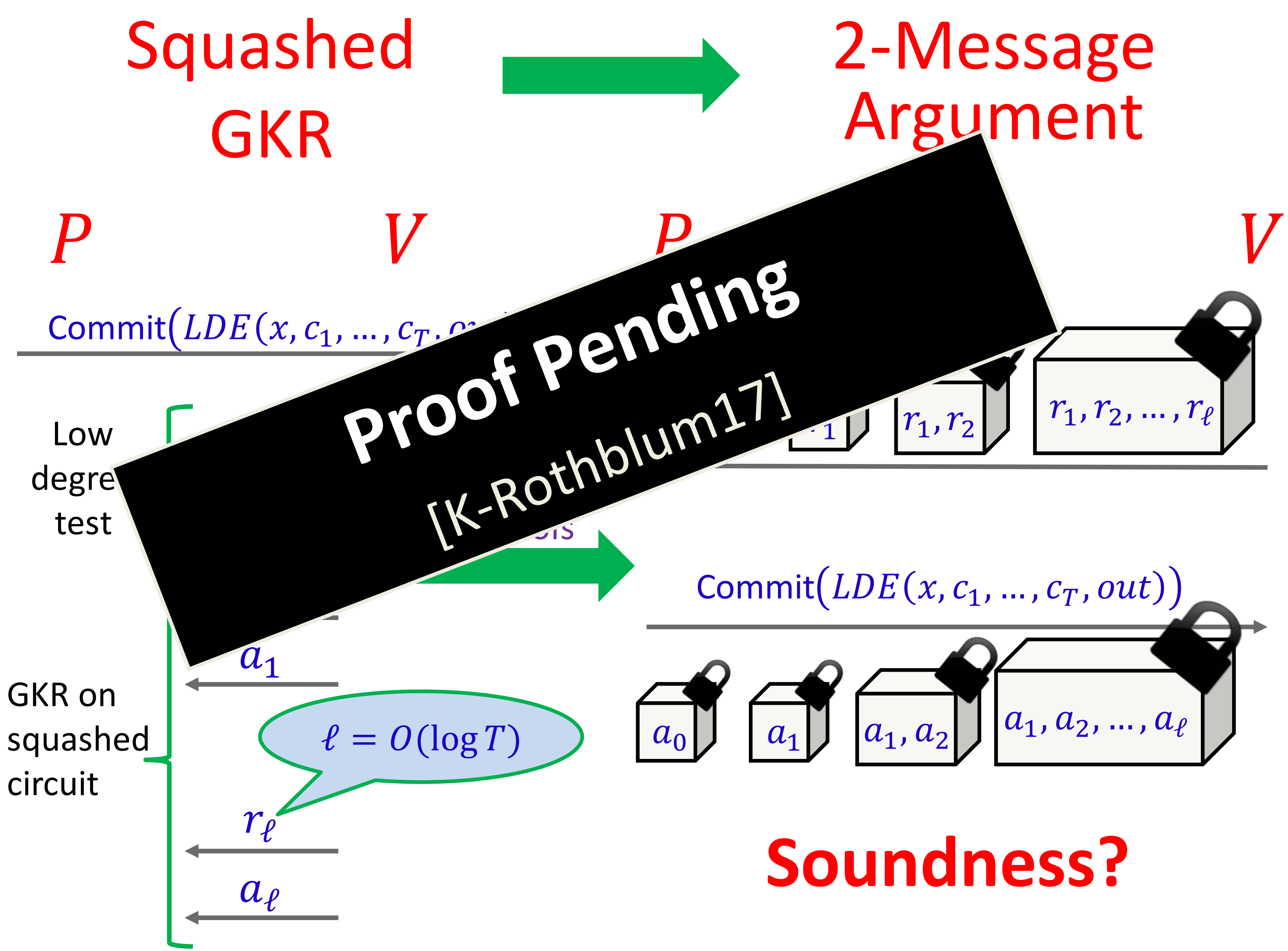


Squashed GKR



Squashed GKR → 2-Message Argument




Squashed GKR
2-Message Argument
P
V
P
V
Commit(LDE(x, c_1, …, c_T, o
Low
degre
test
Proof Pending
[K-Rothblum17]
r_1, r_2
r_1, r_2, …, r_ℓ
Commit(LDE(x, c_1, …, c_T, out))
a_1
ℓ = O(log T)
r_ℓ
a_ℓ
GKR on
squashed
circuit
a_0
a_1
a_1, a_2
a_1, a_2, …, a_ℓ
Soundness?

Squashed GKR → 2-Message Argument

Interactive argument with **no-signaling** soundness → [KR09, KRR13] → **Sound**

Soundness

Interactive proof → [KR09] → 2-message delegation

No-signaling PCP/MIP → [KRR14] → 2-message delegation

$NP???$

No-signaling interactive argument → [KR09, KRR13] → 2-message delegation

Summary

[GKR08]

Doubly efficient
Interactive proof
bounded depth

[Goldwasser-K-Shelat17]

Interactive argument
for P with **no-signaling** soundness
(CRH/PIR)

[K-Rothblum17]

2-message
for P
(PIR)

- More efficient?
- Simpler?
- $NP???$


THANK
YOU