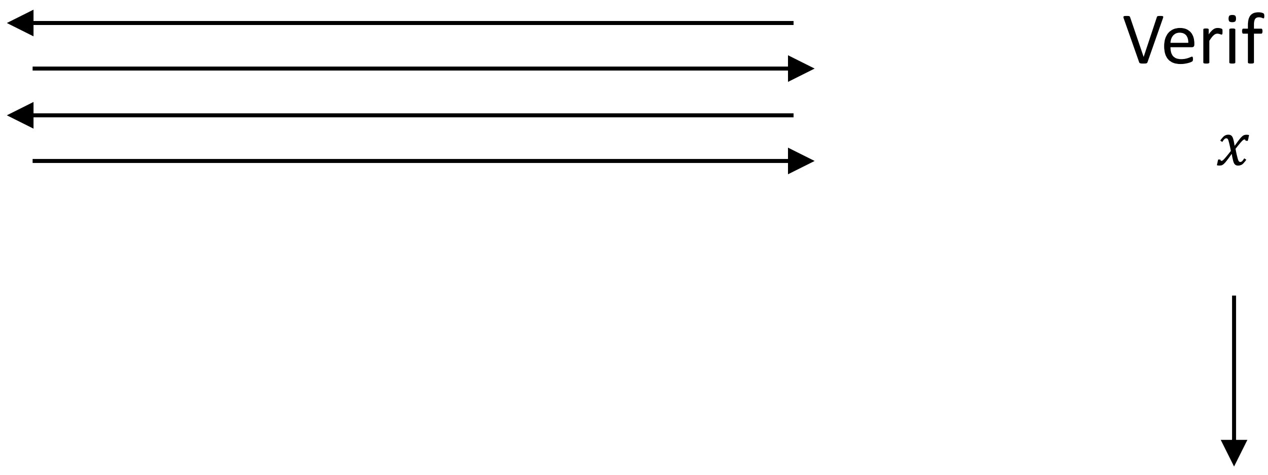
Non-interactive Universal Arguments

Nir Bitansky, Omer Paneth, **Dana Shamir** and Tomer Solomon

Tel-Aviv University

Succinct Arguments [Kilian92, Micali94]

$L \in NP$



$poly(x)$ Prover

x, w

Verifier $\tilde{O}(x)$

x

accept / reject

- Completeness
- Computational soundness
- Doubly efficient

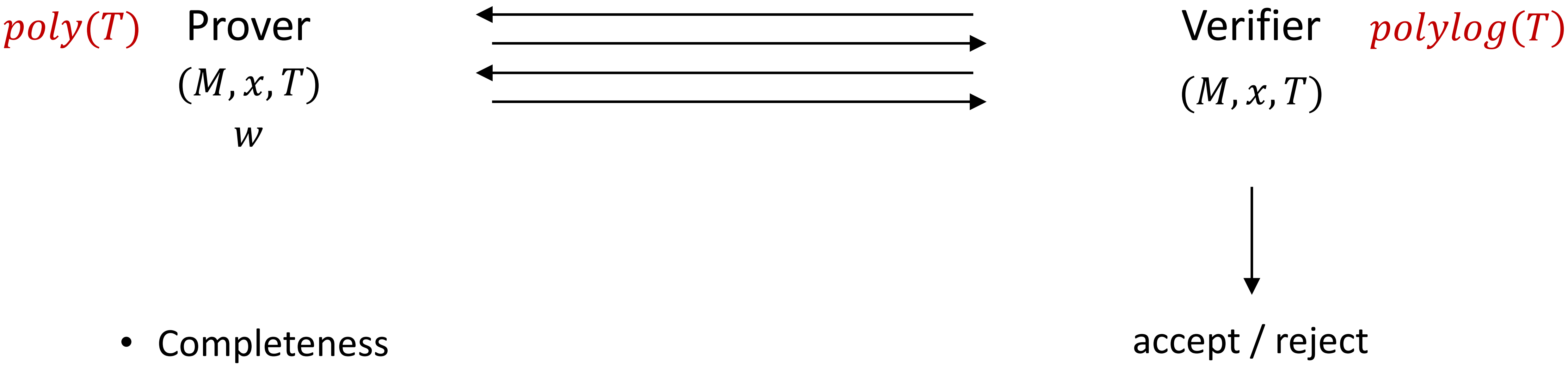
Universal Arguments [Barak-Goldreich08]

- The universal language

$$L_u = \{(M, x, T) \mid M \text{ non-det accepts } x \text{ within } T \text{ steps}\}$$

- $L_u \notin NP$

Universal Arguments [Barak-Goldreich08]



$poly(T)$ Prover

(M, x, T)

w

Verifier $polylog(T)$

(M, x, T)

accept / reject

- Completeness
- Computational soundness against $poly(\lambda)$ adv.
- Doubly efficient

Universal Arguments Motivation

- Succinct argument Fixed poly upper bound on T

- Universal argument One protocol $\forall T$
  - ZK non-black box simulation [Barak 01]
  - Incrementally Verifiable Computation [Valiant 08]

$$\begin{tikzcd}
\boxed{conf_0} \arrow[r, "M"'] & \boxed{conf_1} \arrow[r, "M"'] & \boxed{conf_2} \arrow[r, "M"'] & \cdots \arrow[r, "M"'] & \boxed{conf_T} \\
\pi_0 \arrow[r, "Update"'] & \pi_1 \arrow[r, "Update"'] & \pi_2 \arrow[r, "Update"'] & {} \arrow[r, "Update"'] & \pi_T
\end{tikzcd}$$

Known Results

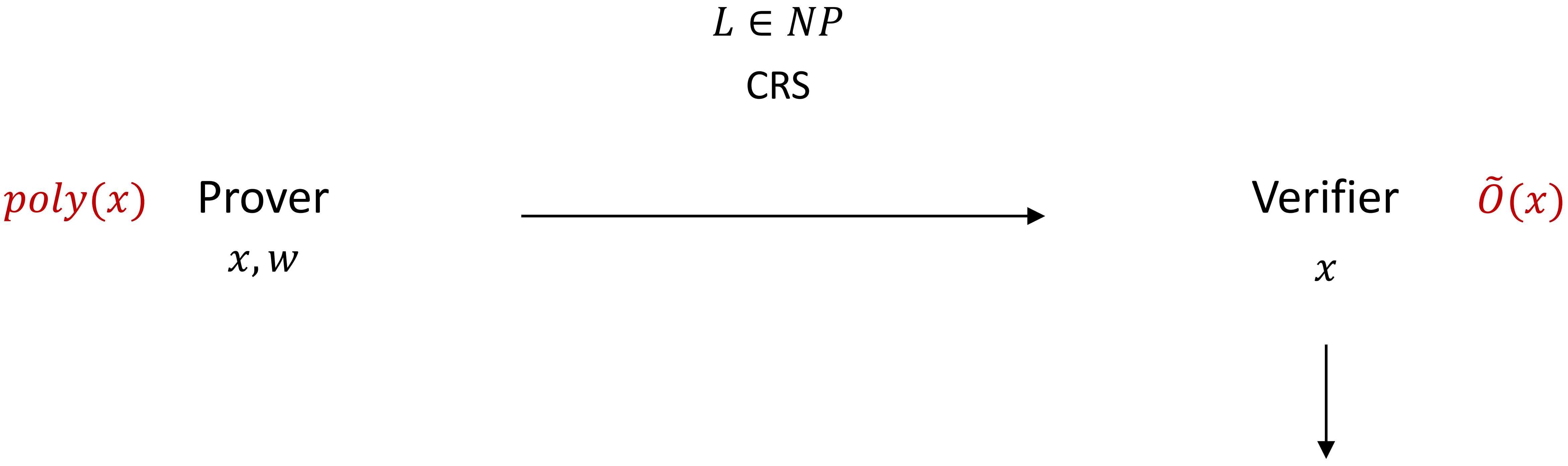
- Kilian92
    - CRH ⇒ succinct arg. for all NP
    - $Poly(\bar{T})$-secure CRH ⇒ universal arg. for $T \leq \bar{T}$

- Barak-Goldreich08
    - $Poly(\lambda)$-secure CRH ⇒ universal arg. for $T \leq 2^{\lambda}$

- The above protocols require 4 messages

Non-interactive Universal Arguments?

Non-interactive Arguments (SNARGS)



$L \in NP$

CRS

$poly(x)$ Prover

x, w

Verifier $\tilde{O}(x)$

x

accept / reject

Publicly verifiable

- Completeness
- Computational soundness
- Doubly efficient

SNARGs for P

- Under polynomial assumptions
  - for $A \in \{LWE, DLIN\}$, $A \Rightarrow$ SNARGs for P

- $Poly(\bar{T})$-secure A

  $\Rightarrow$ universal SNARGs for detereministic computation with $T \leq \bar{T}$

Goal:

$Poly(\lambda)$-secure A

$\Rightarrow$ universal SNARGs for deterministic computation with $T \leq 2^{\lambda}$

Choudhuri-Jain-Jin21, Waters-Wu22, Kalai-Lombardi-Vaikuntanathan-Wichs22, Kalai-Paneth-Yang19, Paneth-Pass22, Devadas-Goyal-Kalai-Vaikuntanathan22, Choudhuri-Jain-Zhengzhong21, Jawale-Kalai-Khurana-Zhang21, Kalai-Lombardi-Vaikuntanathan-Wichs22, Choudhuri-Garg-Jain-Jin-Zhang22

Main Result

Non-interactive universal arguments assuming:

- LWE/DLIN
- FHE
- mild worst case complexity assumption

Results (cont.)

Thm 1 Non-interactive universal argument with uniform soundness assuming LWE/DLIN + FHE

Thm 2 Non-interactive universal argument assuming:

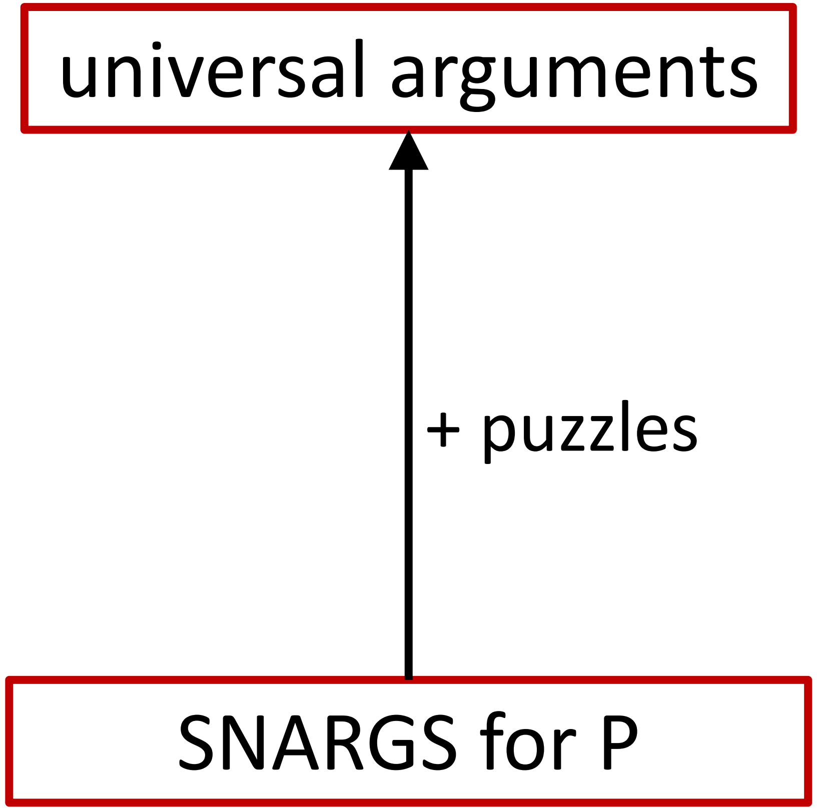
- LWE/DLIN + FHE
- Circuits of fixed poly size can't decide all P ($\forall c \in \mathbb{N}, P \not\subset ioSIZE(n^c)$)

Thm 3 Universal Incrementally Verifiable Computation assuming:

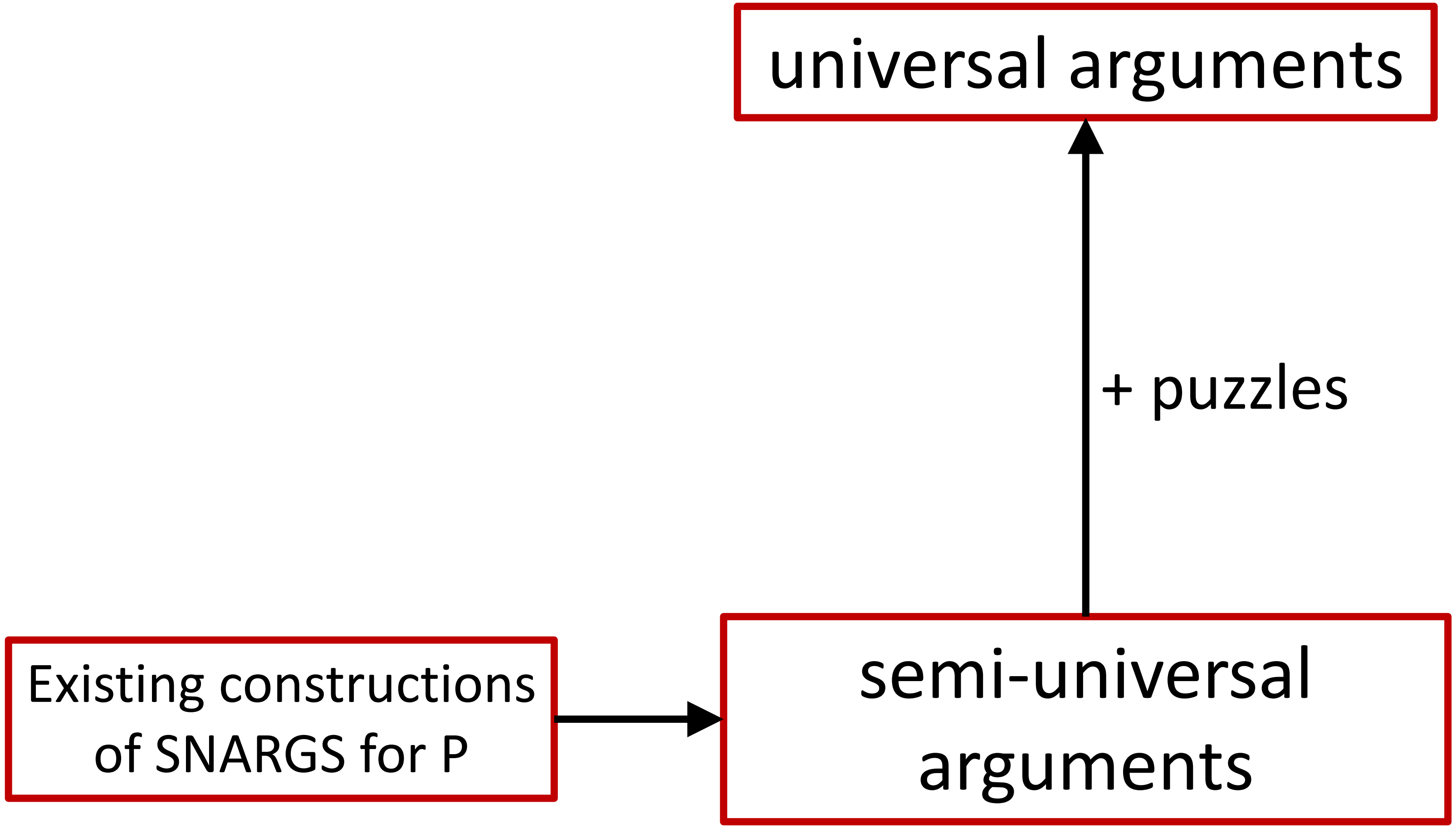
- LWE/DLIN + FHE
- $\exists d, \forall c, P \cap DSPACE\left(n^d\right) \not\subset ioSIZE\left(n^c\right)$

Non-uniform ETH

Lifting Theorem



Lifting Theorem



universal arguments

+ puzzles

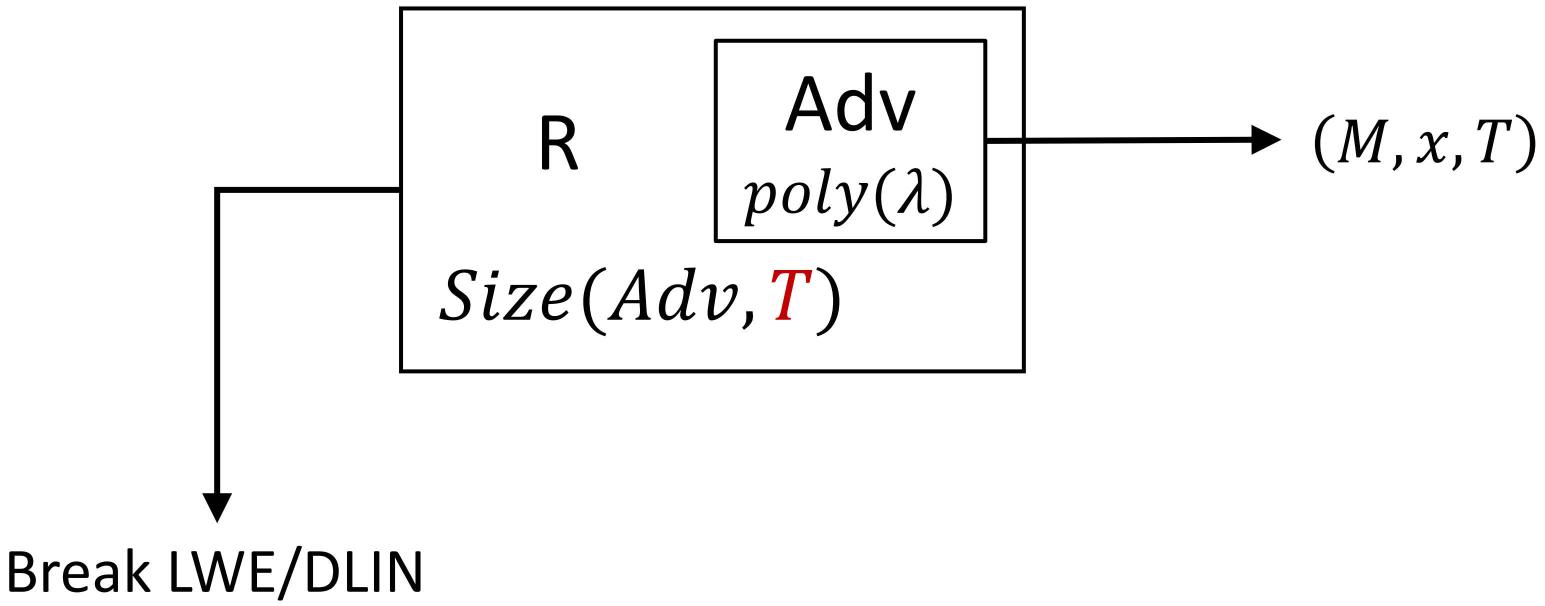
semi-universal arguments

Existing constructions of SNARGS for P

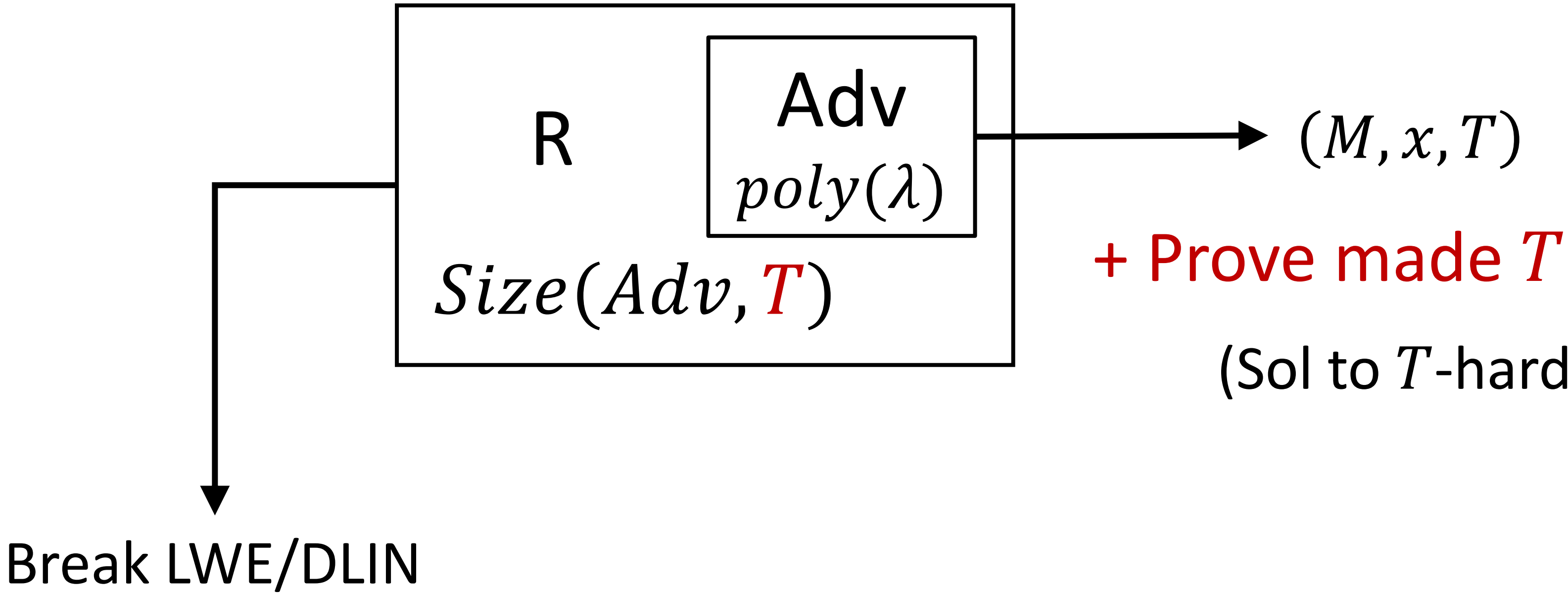
Soundness guaranteed $\forall\, T \leq 2^{\lambda}$

Soundness guaranteed when $T \leq poly(\lambda)$

Existing Constructions Aren’t Universal



Main Idea



R

Adv

$poly(\lambda)$

$Size(Adv, T)$

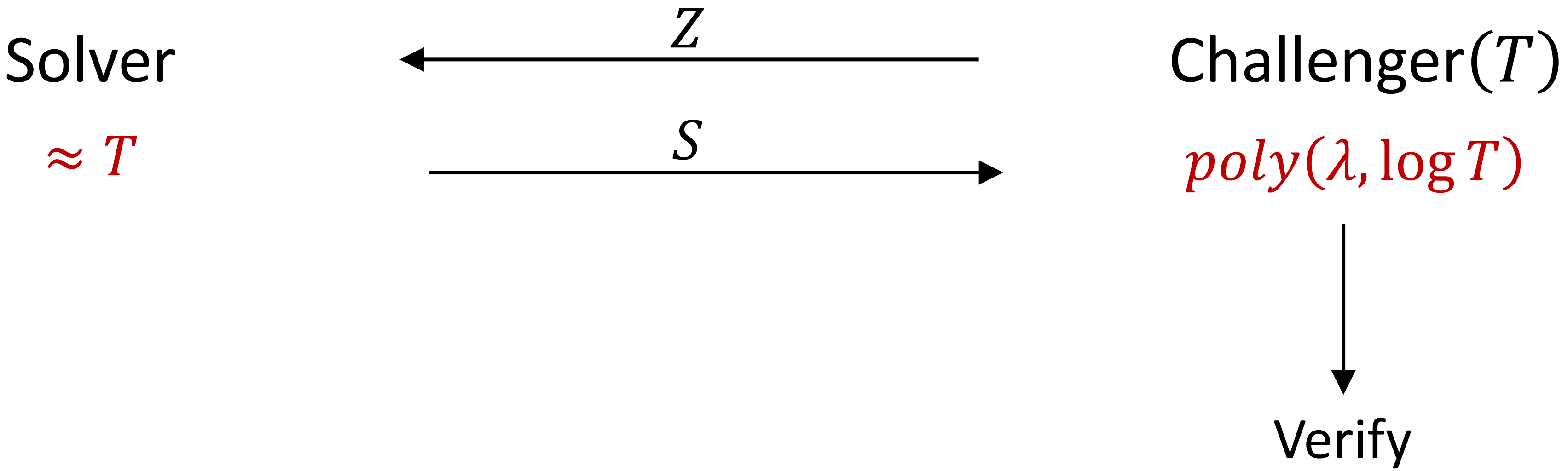
(M, x, T)

Break LWE/DLIN

+ Prove made T-long computation

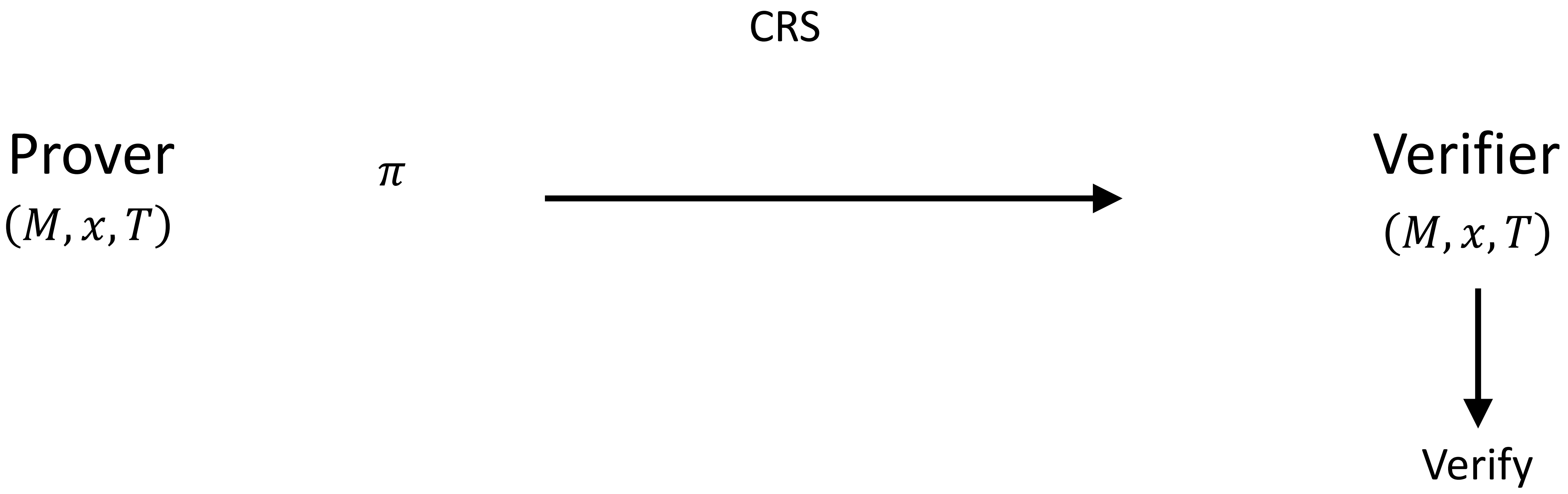
(Sol to T-hard puzzle)

Cryptographic Puzzles



- Completeness
- Fast sampling and verification
- Soundness: can’t solve in time T^{ϵ}

Universal Argument Construction



CRS

Prover

(M, x, T)

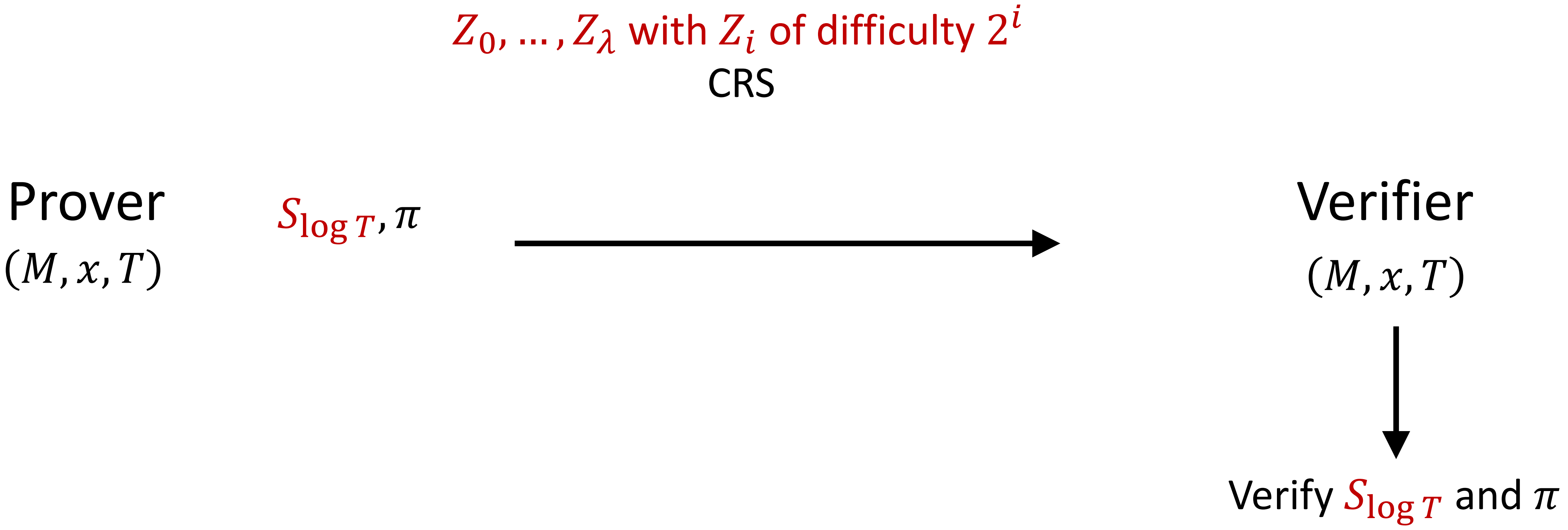
π

Verifier

(M, x, T)

Verify

Universal Argument Construction



$Z_0, \ldots, Z_\lambda$ with Z_i of difficulty 2^i

CRS

Prover

(M, x, T)

$S_{\log T}, \pi$

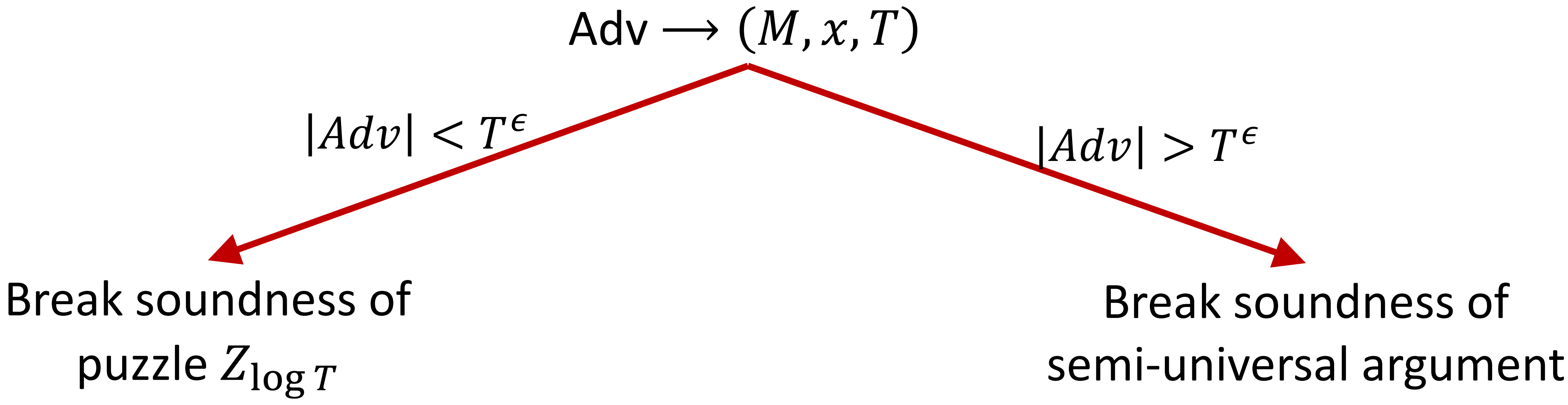
Verifier

(M, x, T)

Verify $S_{\log T}$ and π

Proof Idea

$|Adv| = poly(\lambda)$



Adv $\longrightarrow (M, x, T)$

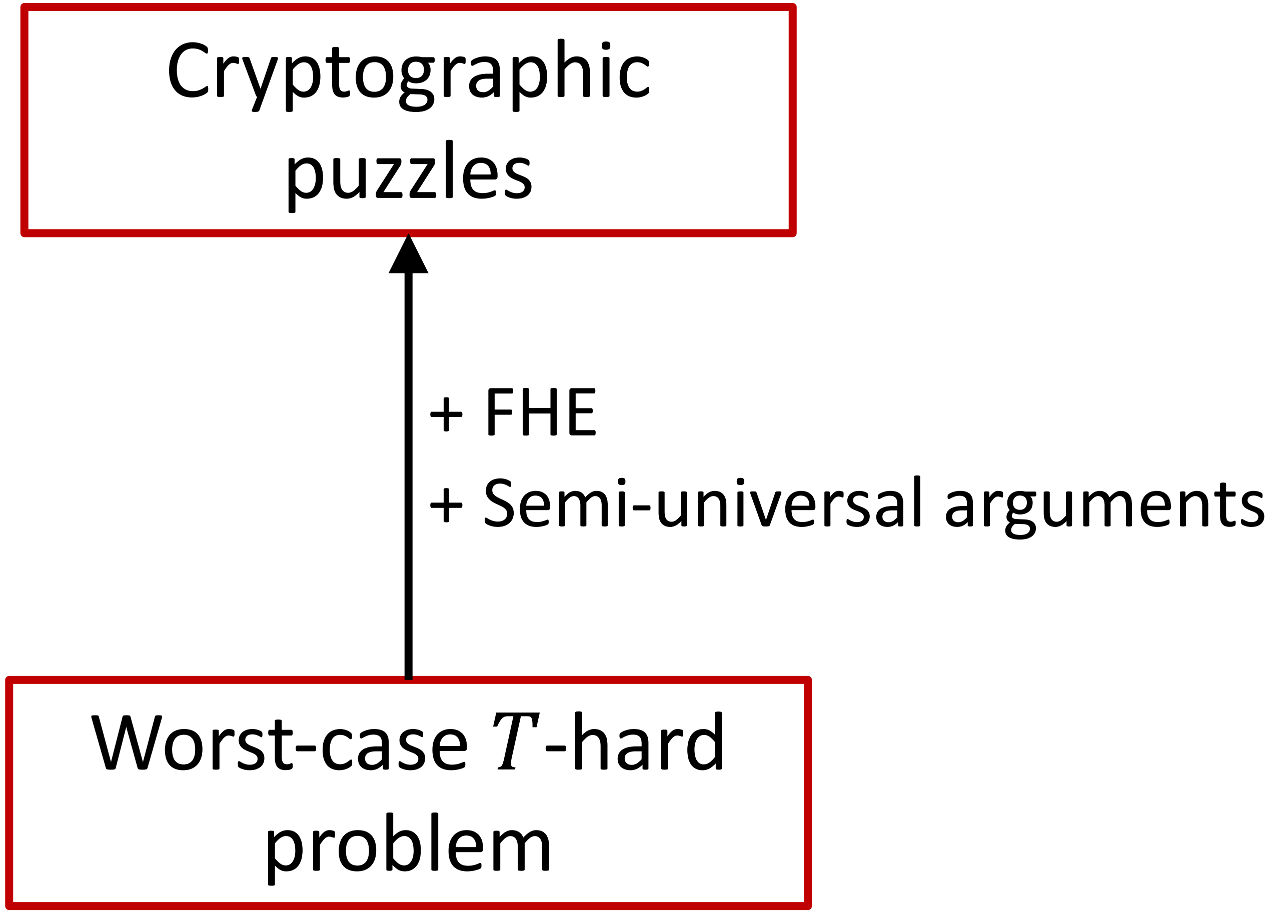
$|Adv| < T^{\epsilon}$

$|Adv| > T^{\epsilon}$

Break soundness of puzzle $Z_{\log T}$

Break soundness of semi-universal argument

Constructing Puzzles



Cryptographic puzzles

+ FHE

+ Semi-universal arguments

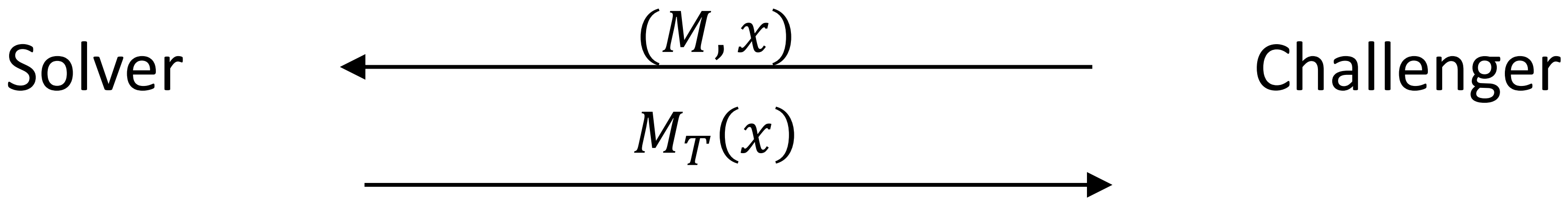
Worst-case T-hard problem

Worst Case Hard Problem

- Language L, decided by M in time T
- $\forall$ solver $< T^{\epsilon}$ fails on some x

- Uniform: time hierarchy
- Non-uniform: complexity assumption
  - $\forall c \in \mathbb{N}, P \not\subset ioSIZE(n^{c})$

The Puzzle



Solver

(M, x)

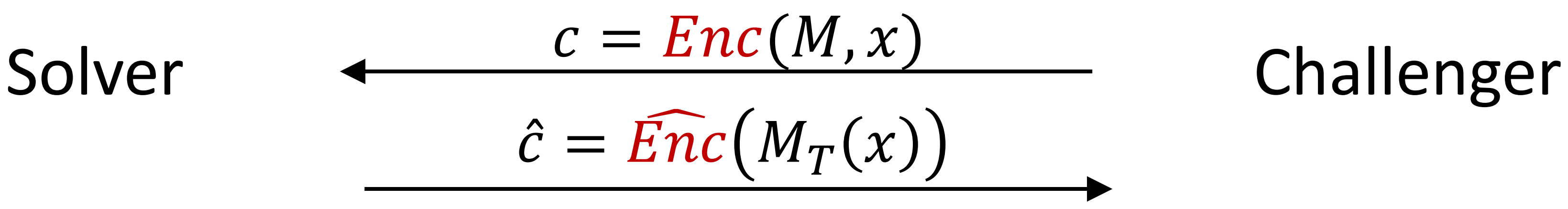
$M_T(x)$

Challenger

Problem 1: Every solver fails on different M, x

Solution [Chung-Kalai-Vadhan10]: Worst → Avg using FHE

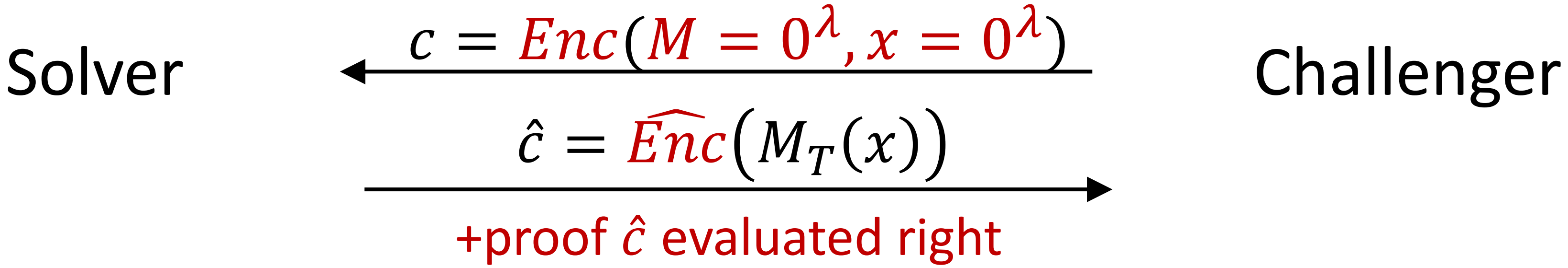
The Puzzle



Problem 1: Every solver fails on different M, x

Solution [Chung-Kalai-Vadhan10]: Worst → Avg using FHE

The Puzzle



Solver

$c = Enc(M = 0^\lambda, x = 0^\lambda)$

$\hat{c} = \widehat{Enc}\big(M_T(x)\big)$

+proof $\hat{c}$ evaluated right

Challenger

Problem 1: Every solver fails on different M, x

Solution [Chung-Kalai-Vadhan10]: Worst → Avg using FHE

Problem 2: Verification

Solution: Semi-universal argument

A Technical Challenge

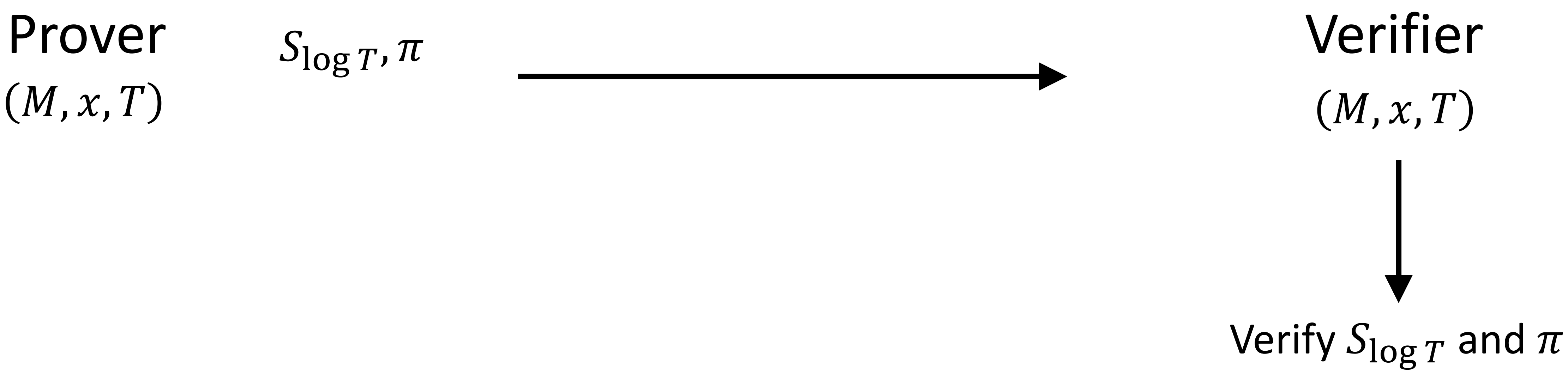
- Semi-universal arguments ⇒ ”semi-universal” puzzles

- Soundness holds for $T = poly(\lambda)$

Universal Argument Construction

$Z_0, \dots, Z_\lambda$ with Z_i of difficulty 2^i

CRS



Prover

(M, x, T)

$S_{\log T}, \pi$

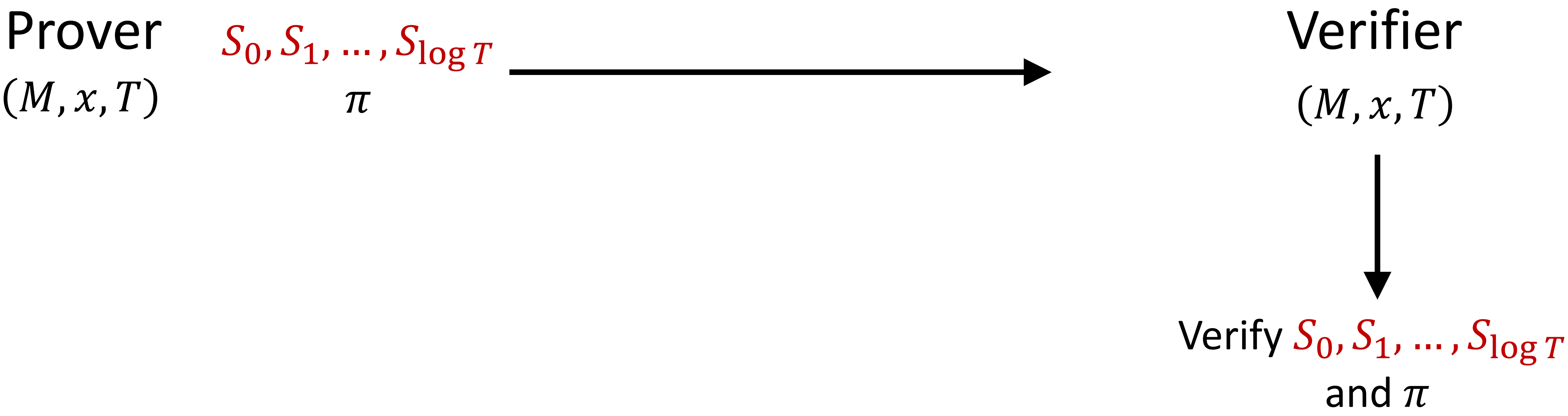
Verifier

(M, x, T)

Verify $S_{\log T}$ and π

Universal Argument Construction

$Z_0, \ldots, Z_\lambda$ with Z_i of difficulty 2^i
CRS



Prover
(M, x, T)

$S_0, S_1, \ldots, S_{\log T}$
π

Verifier
(M, x, T)

Verify $S_0, S_1, \ldots, S_{\log T}$
and π

Future Directions

- Use puzzles to reduce super-poly assumptions to poly assumptions?
  - Example: Bitnasky-Solomon23

- Thank you!