

# Concurrent Zero Knowledge: Simplifications and Generalizations

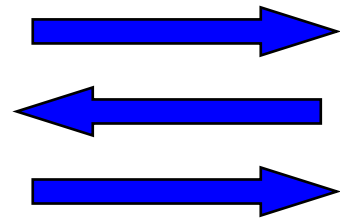
Rafael Pass      Dustin Tseng

Muthuramakrishnan Venkatasubramanian

**CORNELL UNIVERSITY**



**Alice**

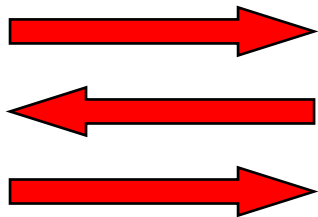
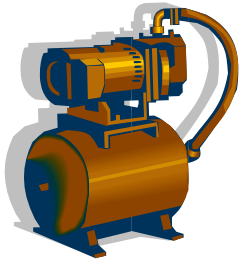


**Bob**

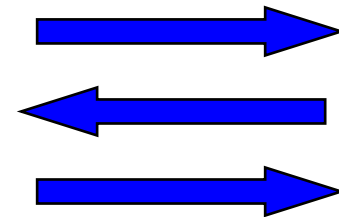
# What is Zero Knowledge?

$\forall$  PPT verifier  $V^*$ ,  $\exists$  PPT simulator  $S$  such that

Simulator  $S$



Prover



Verifier  $V^*$



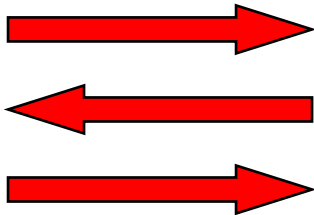
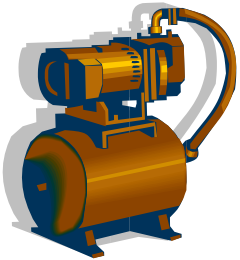
Simulated View

View in real interaction

# What is Zero Knowledge?

$\forall$  PPT verifier  $V^*$ ,  $\exists$  PPT simulator  $S$  such that

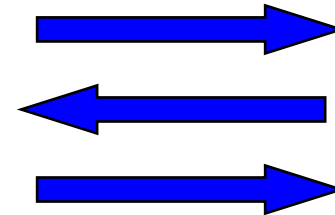
Simulator  $S$



Simulated View



Prover



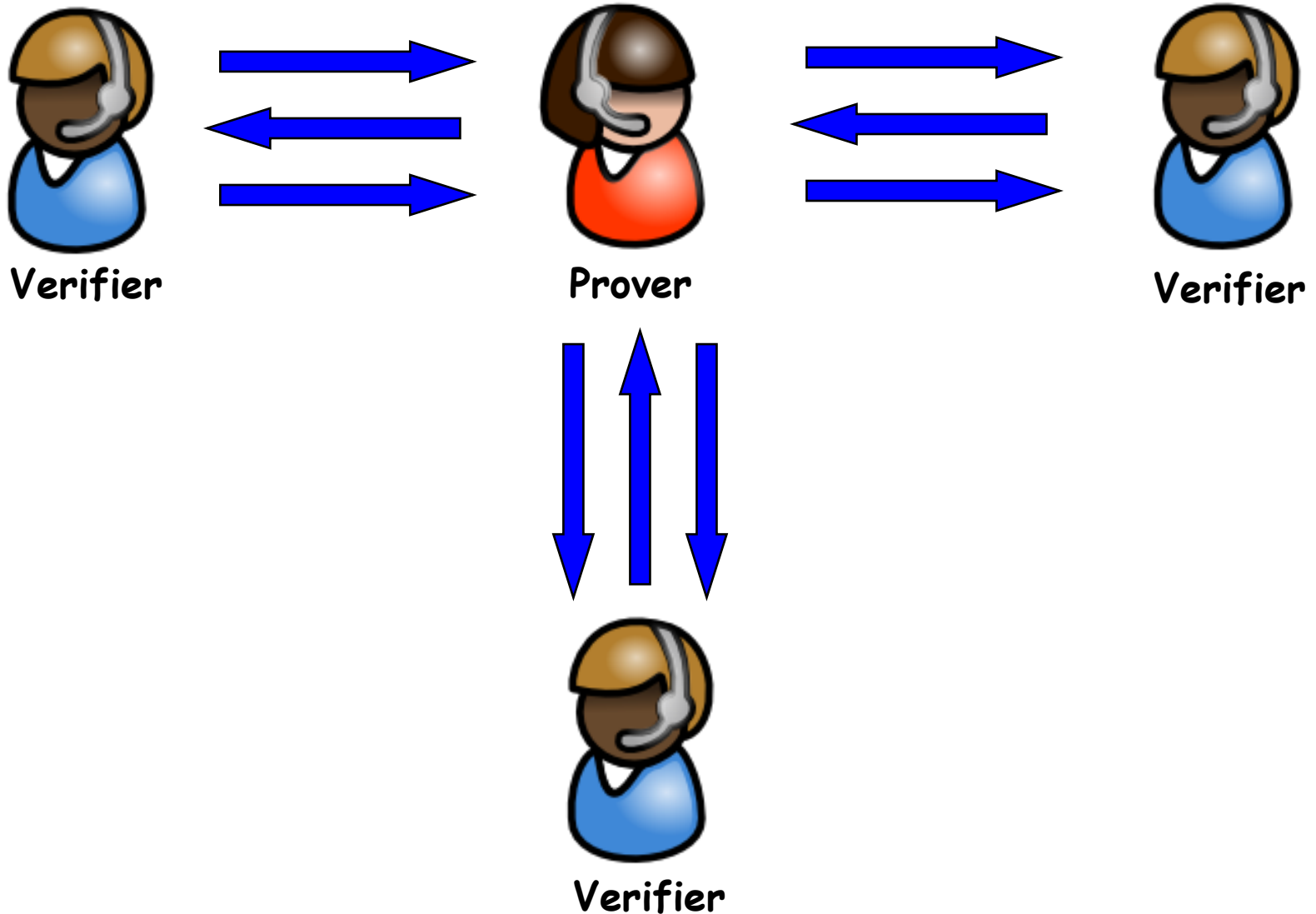
View in real interaction

Verifier  $V^*$



# Concurrent Zero-Knowledge

[DNS, DDN, RK, CKPR, KP, PRS, ...]



# What is known?

[RK, KP, PRS] For all languages in  $\text{P}$ , there exists  $\tilde{O}(\log n)$  round black-box non-interactive ZK proof.

[KP] a simulator

**More tomorrow!**

generator

– Not on a

– Dep

***Precise Concurrent Zero Knowledge*** changed

# Our Simplification

**Bad Random tape:** Simulator **fails**

**Good Random tape:** Simulator **succeeds**

**Idea:** Map **1 bad** to (distinct)  **$2^k$  good**

**Previous Approach:** **Complicated mapping**

**Our Idea - Composable proof**

Map **1 bad unit** to **2 good**

Compose  **$k$**  times  $\Rightarrow$  failure probability  **$1/2^k$**

We need  **$\tilde{O}(\log n)$**  rounds

# Our Generalization

**First concurrent ZK protocol** that works for multi-round commitments.

Result by Ong and Vadhan:

- Instance based commitments
- Unconditional constructions of commitments for languages in Statistical ZK Proof



# ZK $\Rightarrow$ Concurrent ZK (unconditional)

If L has

1. **Stat. ZK Proof**  $\Rightarrow$   $\tilde{O}(\log n)$  round **Concurrent Stat. ZK Proof**

If  $L \in \text{NP}$  and has

2. **Stat. ZK Arg.**  $\Rightarrow$   $\tilde{O}(\log n)$  round **Concurrent Stat. ZK Arg.**

3. **Comp. ZK Proof**  $\Rightarrow$   $O(t(n)) + \tilde{O}(\log n)$  **Concurrent Comp. ZK Proof**

4. **Comp. ZK Arg.**  $\Rightarrow$   $O(t(n)) + \tilde{O}(\log n)$  **Concurrent Comp. ZK Arg.**

Thank You!