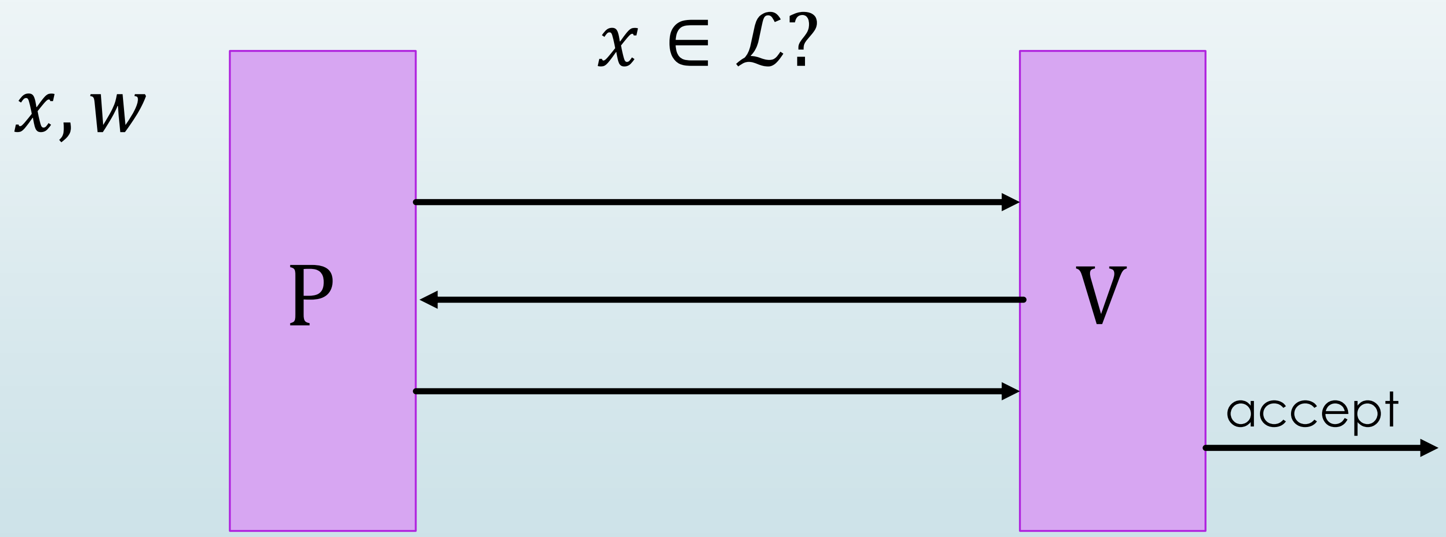
Distinguisher-Dependent Simulation

Dakshita Khurana

Joint work with Abhishek Jain, Yael Kalai and Ron Rothblum

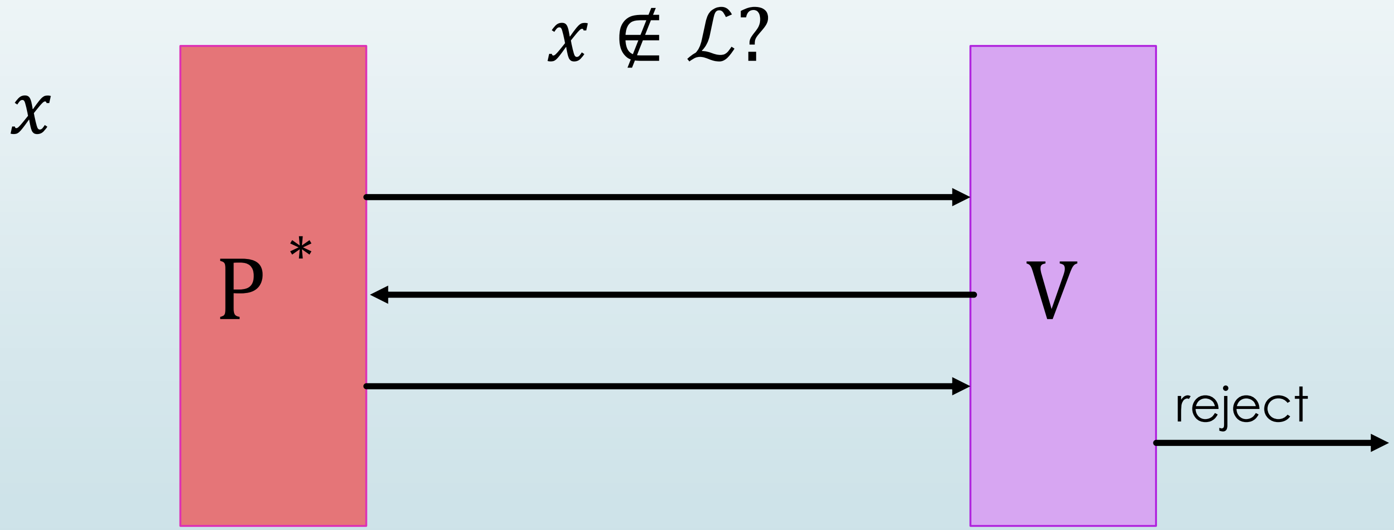
Interactive Proofs for NP

Interactive Proof (GMR85, Babai85)



Security Against Malicious Provers

Soundness



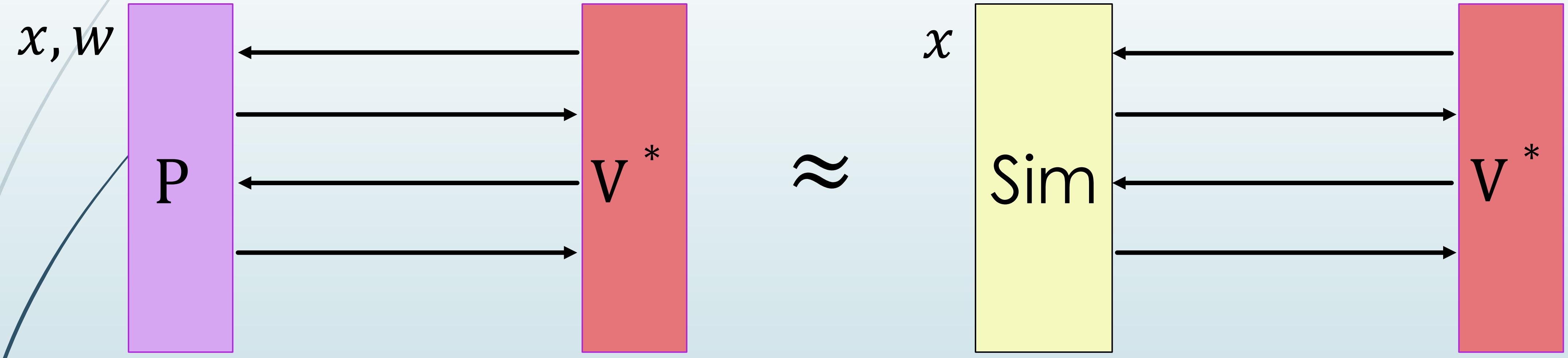
Security Against Malicious Verifiers

Shouldn't learn witness w

- Zero-Knowledge (GMR85)
- Distributional Zero-Knowledge (Goldreich93)
- Weak Zero-Knowledge (DNRS99)
- Witness Hiding (FS90)
- Witness Indistinguishability (FS90)
- Strong Witness Indistinguishability (Goldreich93)

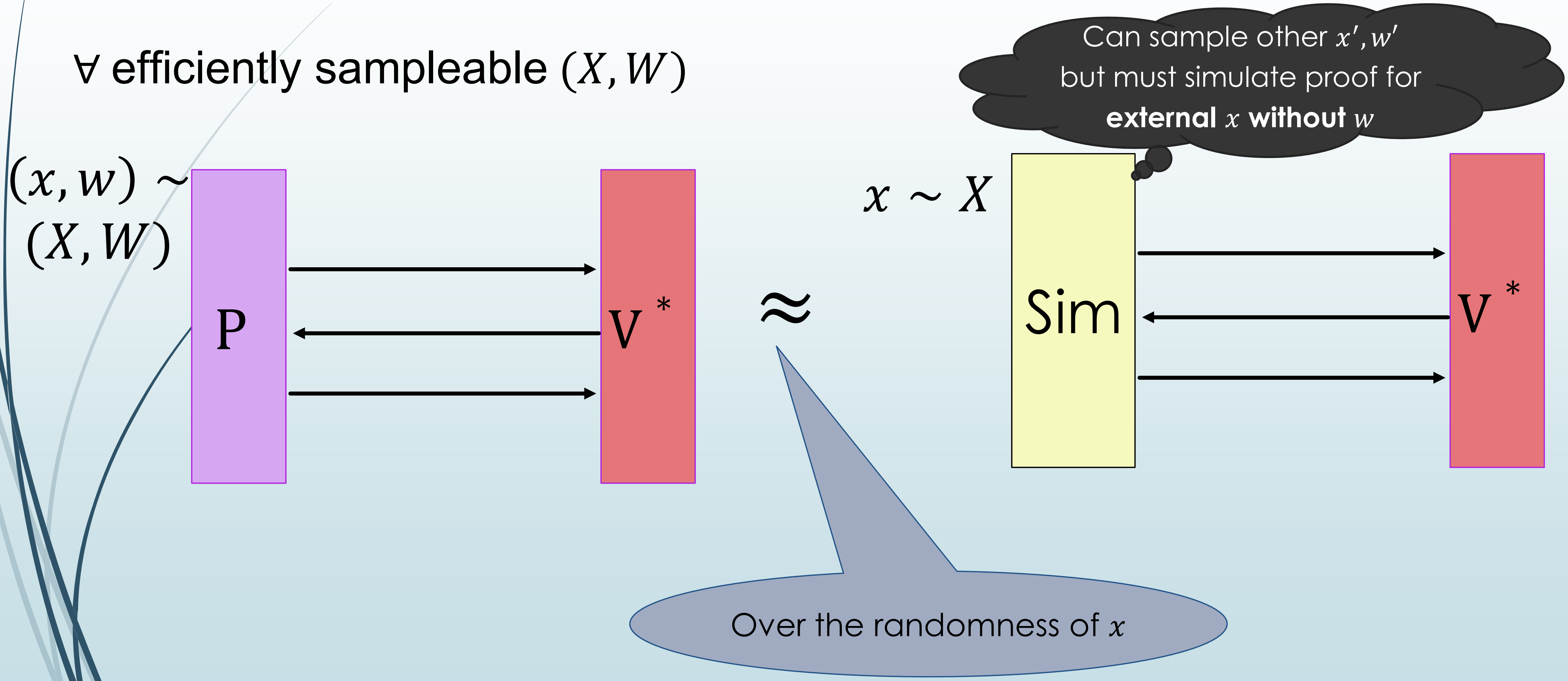
Zero-Knowledge

$\forall\, x,$

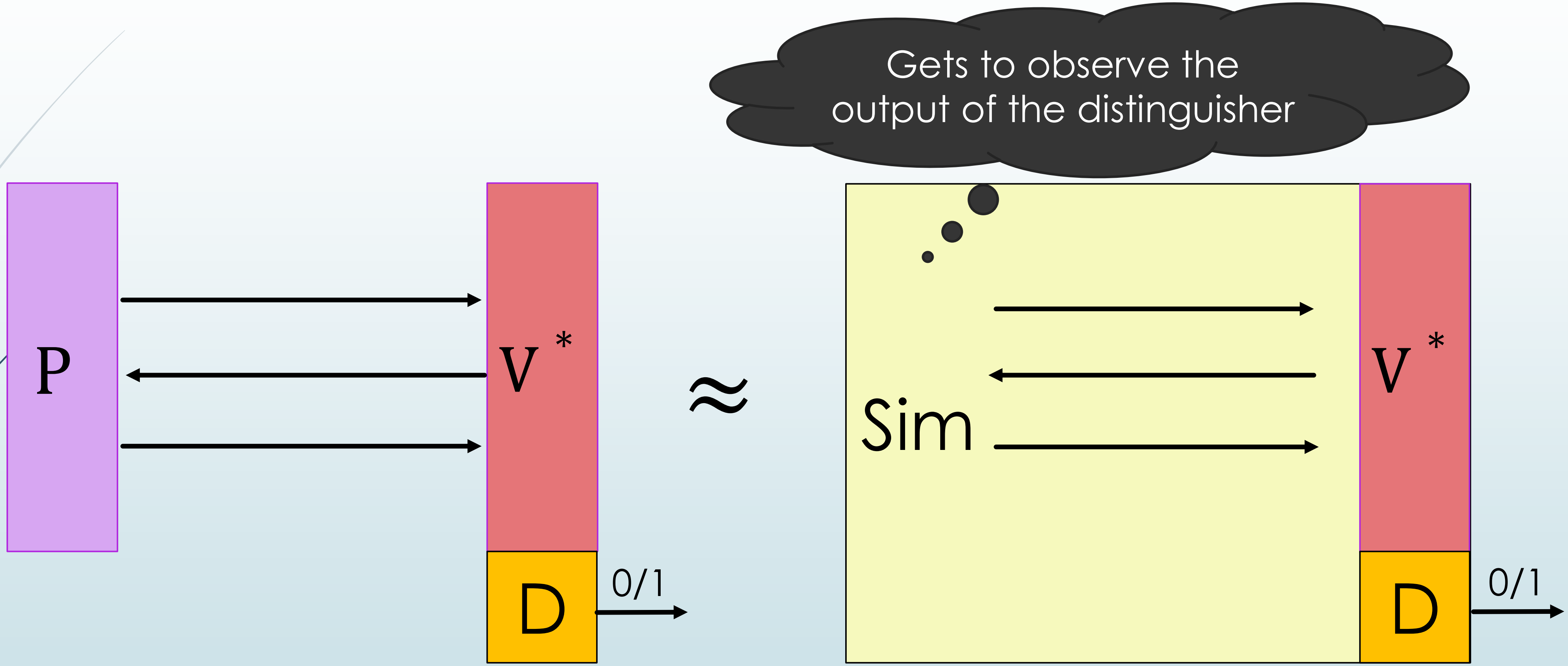


Distributional Zero-Knowledge

$\forall$ efficiently sampleable (X, W)



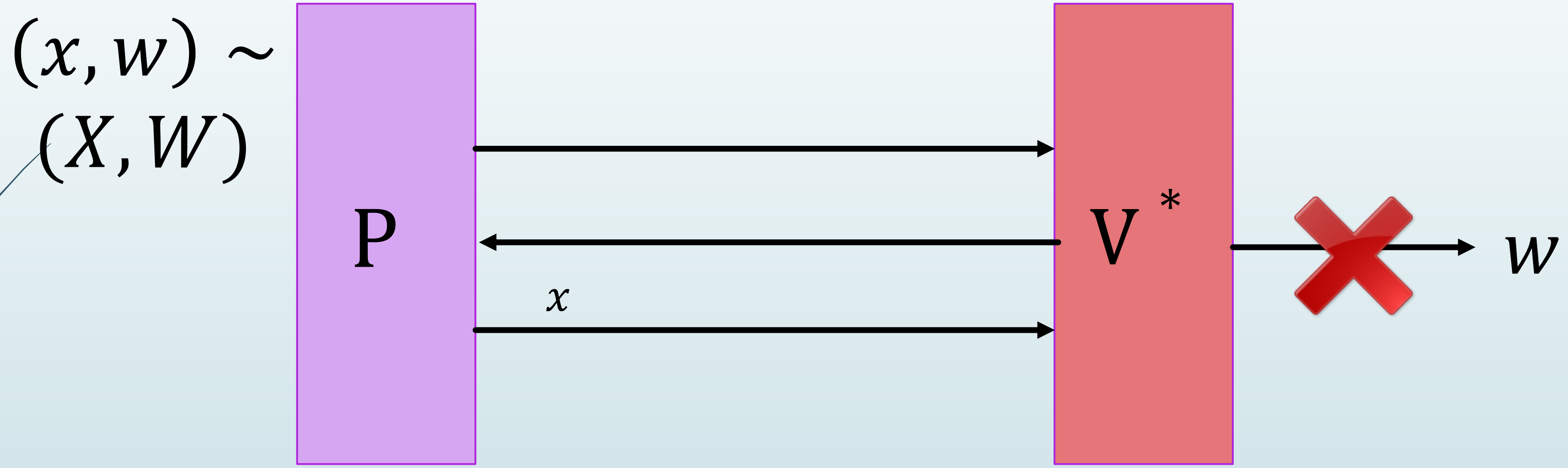
Weak Zero-Knowledge



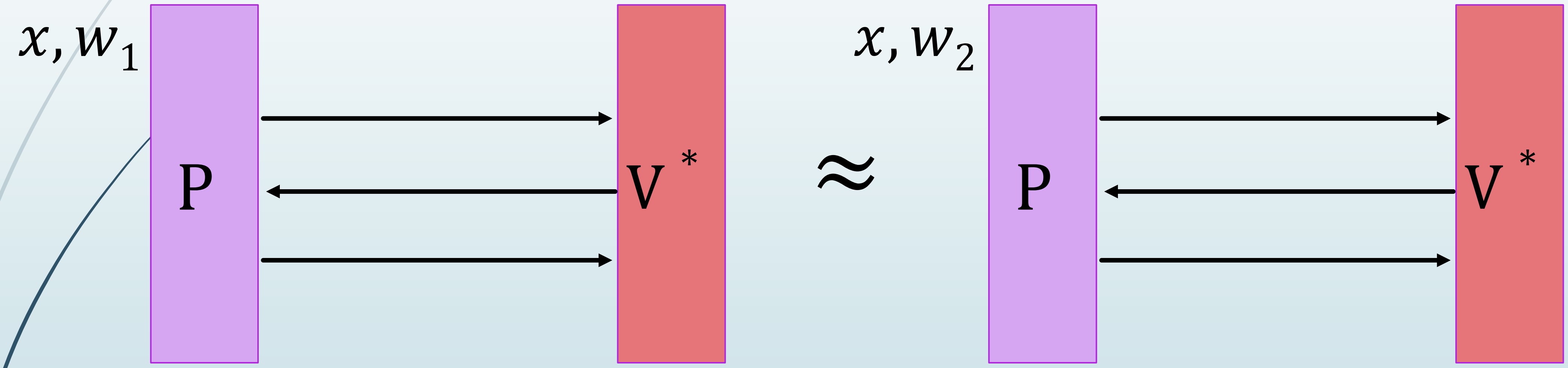
$$Pr[D = 1|real] \; - \; \Pr[D = 1|Sim] \leq negl$$

Witness Hiding

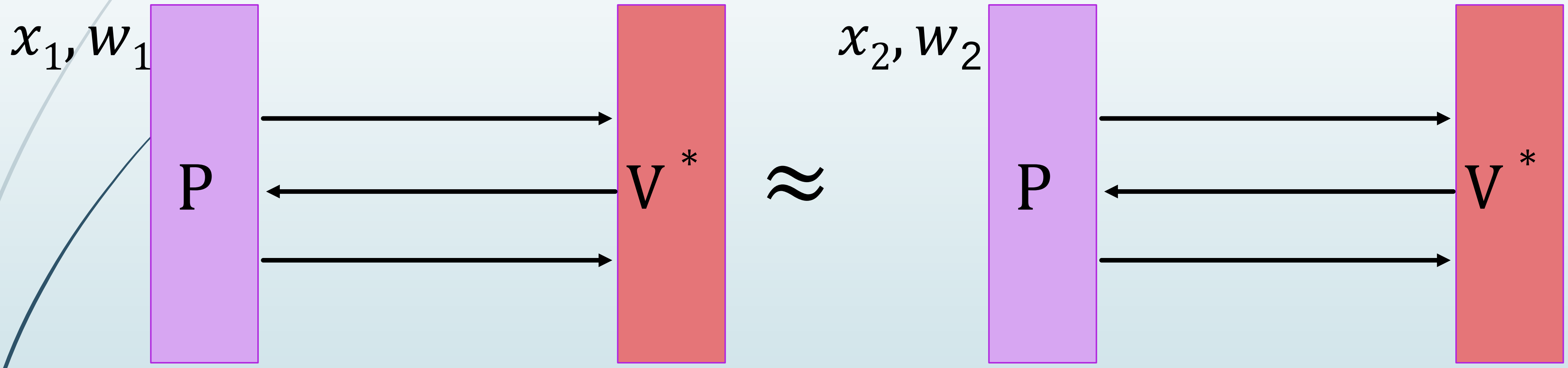
∀ efficiently sampleable (X, W) with hard to find witnesses,



Witness Indistinguishability

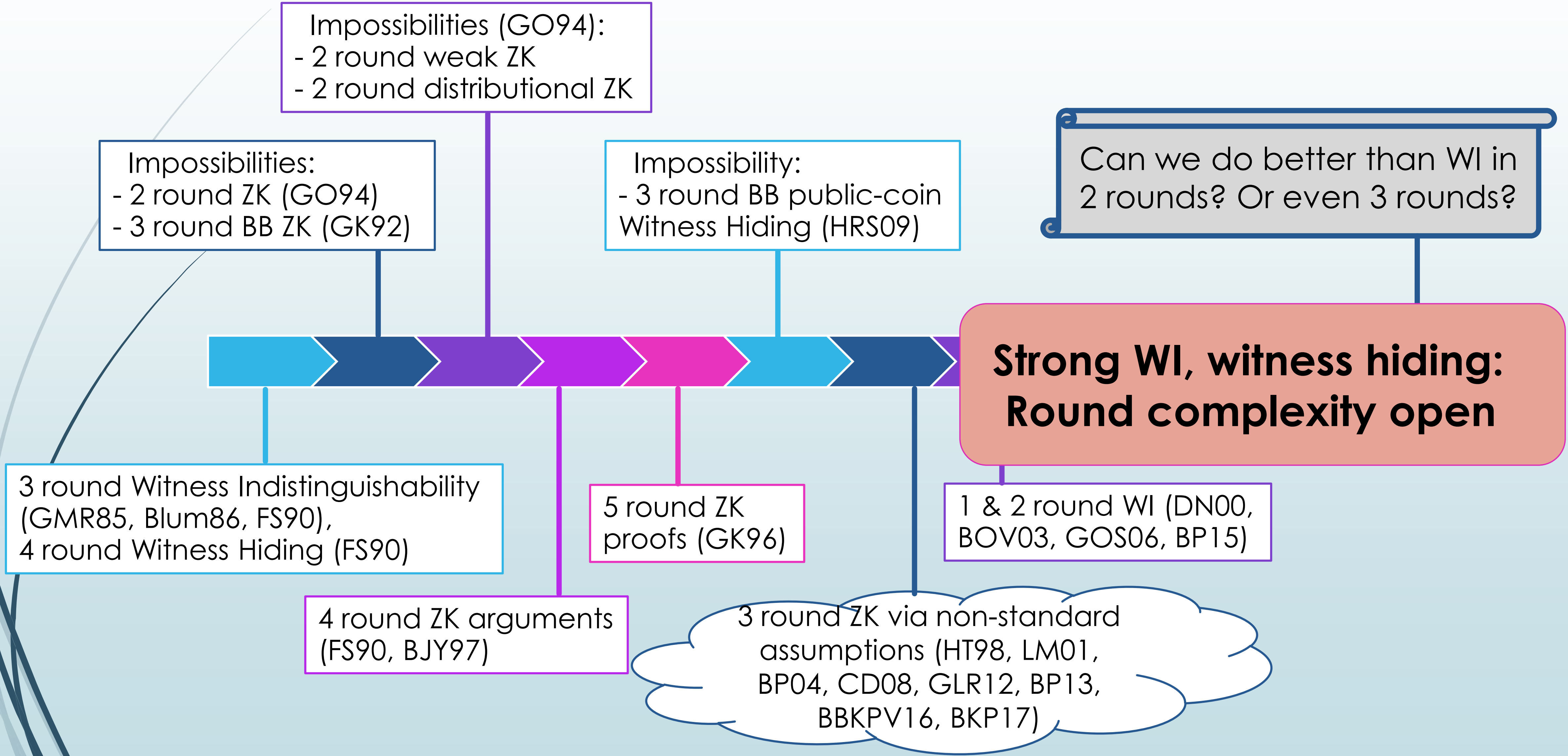


Strong Witness Indistinguishability



when $x_1 \approx x_2$

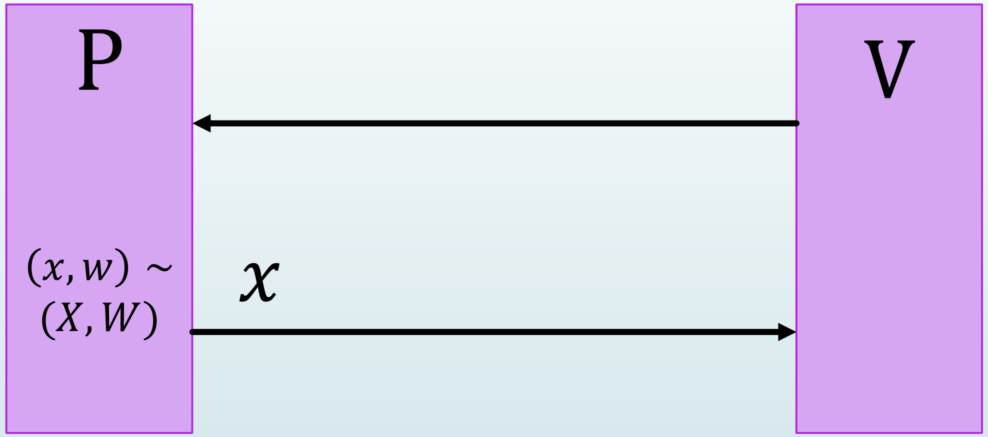
Round Complexity Timeline



Overcoming Barriers

Distributional Protocols

- Prover samples instance x from some distribution

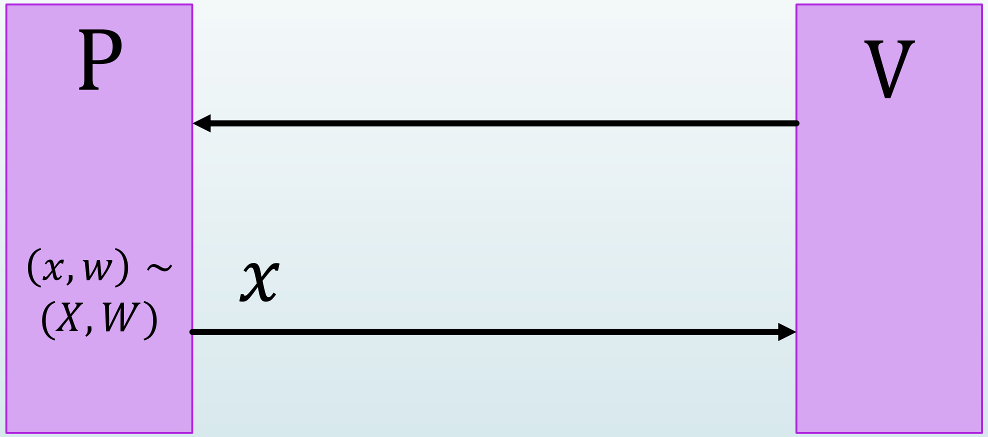


Why should we care?

- ZK proofs used to prove correctness of cryptographic computation
- Almost always, instances are chosen from some distribution
- Strong WI, WH by definition are distributional notions

Distributional Protocols

- Prover samples instance x from some distribution

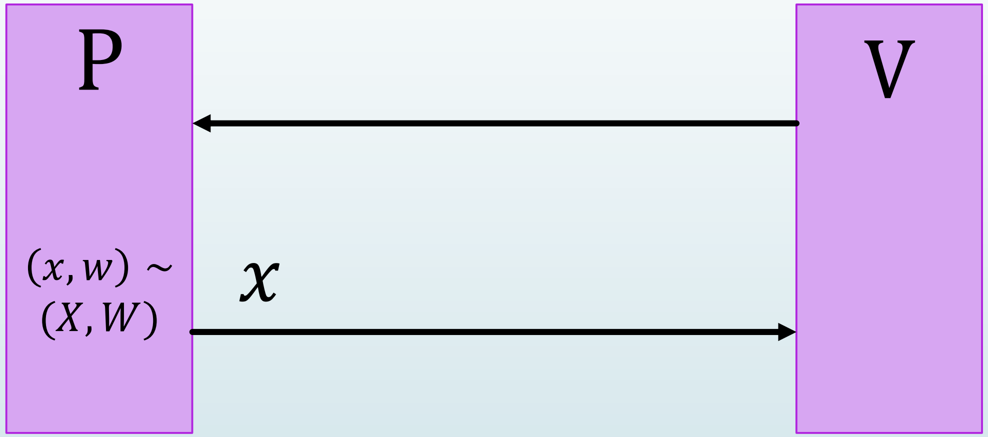


- Useful in secure computation: [KO05, GLOV14, COSV16]
- Our paper: extractable commitments, 3 round 2pc
- Specific 2 & 3 round protocols: [KS17, K17, ACJ17]

- In 2 round protocols, P sends x together with proof
- Adaptive soundness: P* samples x after V's message
- We will restrict to: **delayed-input** protocols
- Cheating verifier cannot choose first message depending on x

Distributional Protocols, Delayed-Input

- Prover samples instance x from some distribution



- Simulate the view of malicious V*, when V* is committed to 1st message, before P reveals instance x?
- **Distributional privacy for delayed-input statements.**
- Get around negative results!

Our Results

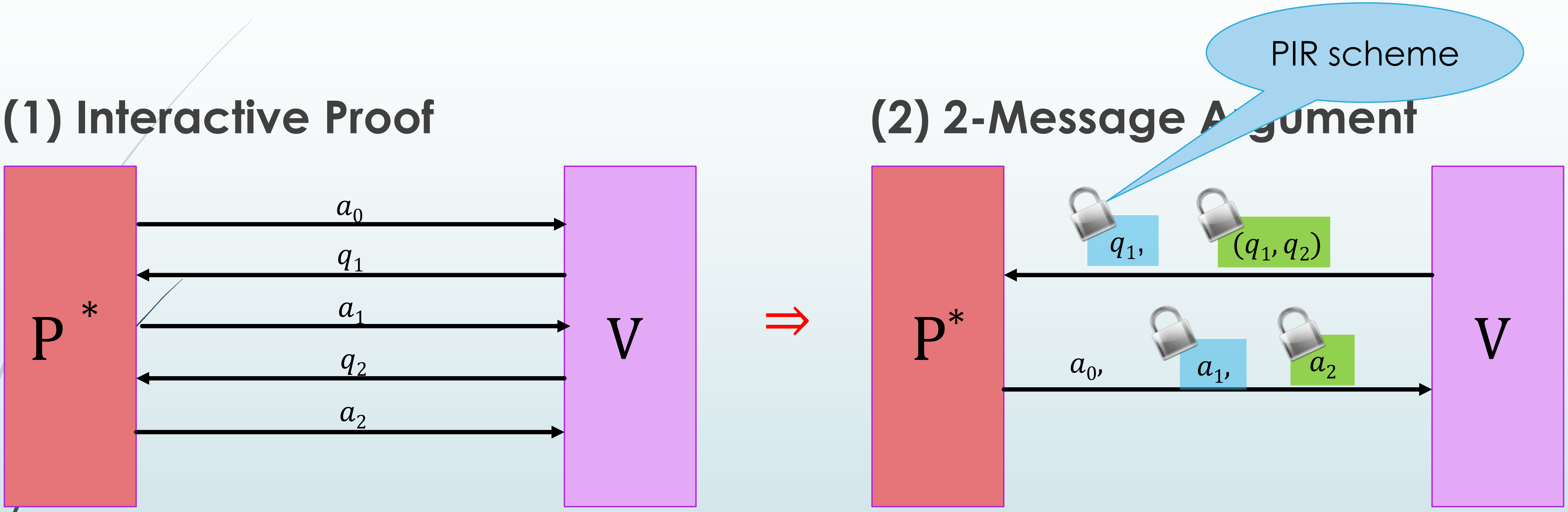
Assuming quasi-polynomial DDH, QR or N^{th} residuosity, we get

- **2 Round arguments in the delayed-input setting**
  - **Distributional weak ZK**
  - **Witness Hiding**
  - **Strong Witness Indistinguishability**
- **2 Round WI arguments** [concurrent work: BGISW17]
  - Previously, trapdoor perm (DN00), b-maps (GOS06), or iO (BP15)
- 3 Round protocols from polynomial hardness + applications

Sim depends on distinguisher

New Technique:
Black-box Simulation in 2 Rounds

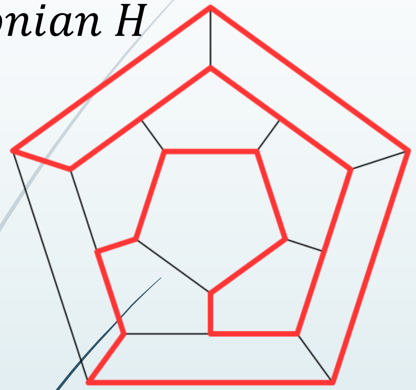
Kalai-Raz (KR09) Transform

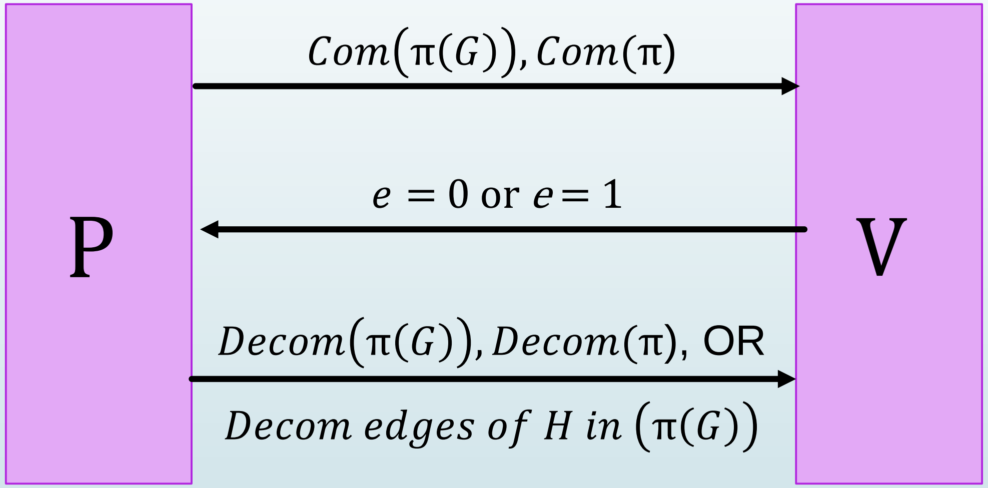


- KR09: Assuming quasi-polynomially secure PIR, (2) is sound against adaptive PPT P*.
- Our goal: 2 message arguments for NP with privacy.
- Apply KR09 transform to three round proof of Blum86.

Blum Protocol for Graph Hamiltonicity

Graph G,
Hamiltonian H

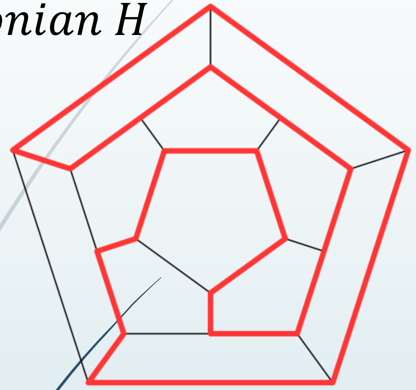


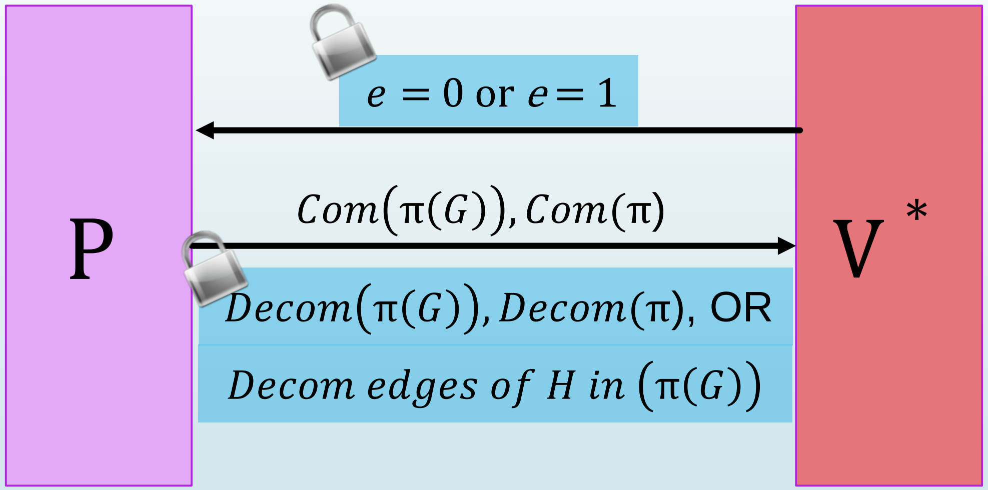


- Honest verifier zero-knowledge: Sim that knows e can simulate.
- Repeat in parallel to amplify soundness. Preserves honest verifier ZK.

KR09 transform on Blum

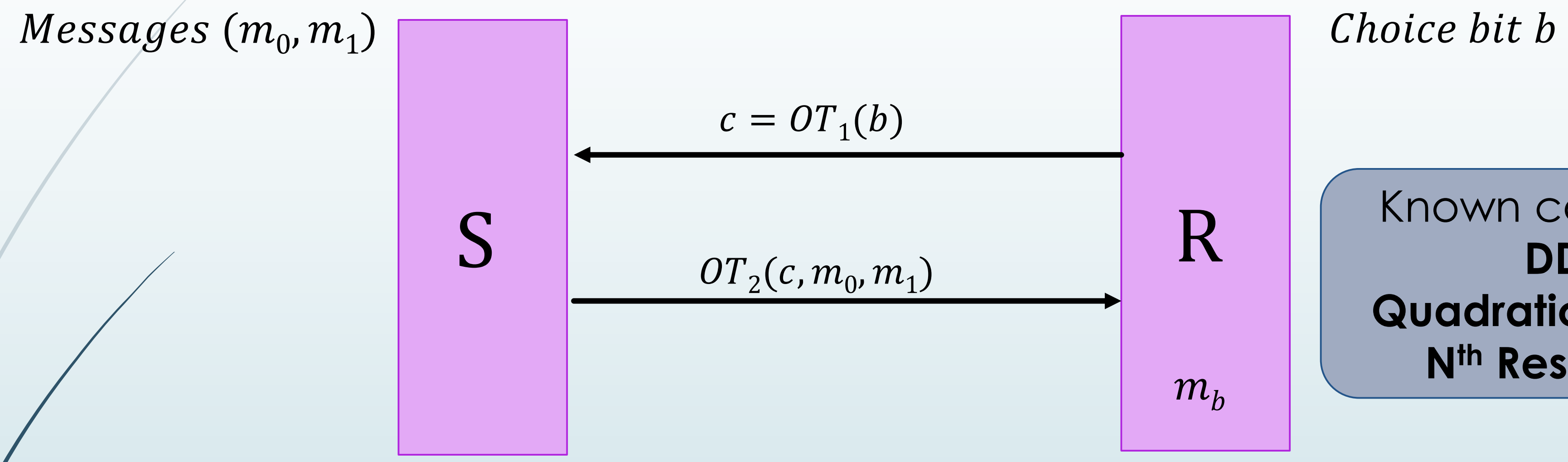
Graph G,
Hamiltonian H





- Remains honest verifier zero-knowledge.
- What if malicious V* sends malformed query that doesn't encode any bit?
- Prevent this by using a special PIR scheme.

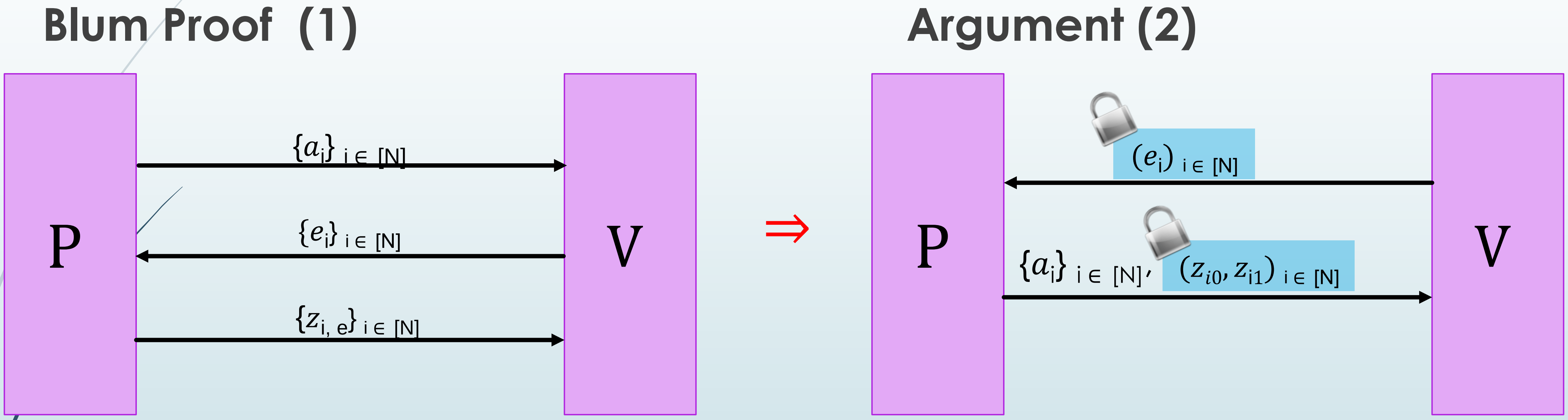
2-Message Oblivious Transfer



Known constructions from **DDH** (NP01), **Quadratic Residuosity** and **N^th Residuosity** (HK05)

- S cannot guess b
- R cannot distinguish $\mathrm{OT}_2(m_0, m_1)$ from :
  - $\mathrm{OT}_2(m_0, m_0)$ when $b = 0$, OR
  - $\mathrm{OT}_2(m_1, m_1)$ when $b = 1$.
- Every string c corresponds to $OT_1(b)$ for some bit b

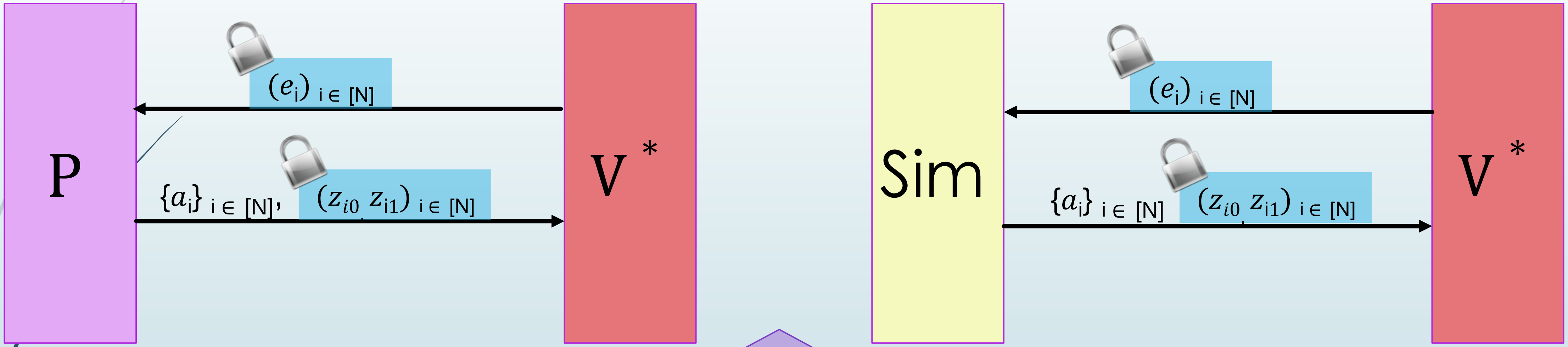
Kalai-Raz Transform on Blum using OT



- KR09: (2) remains sound against PPT provers, even if they choose x adaptively
- What about privacy?

Kalai-Raz Transform on Blum

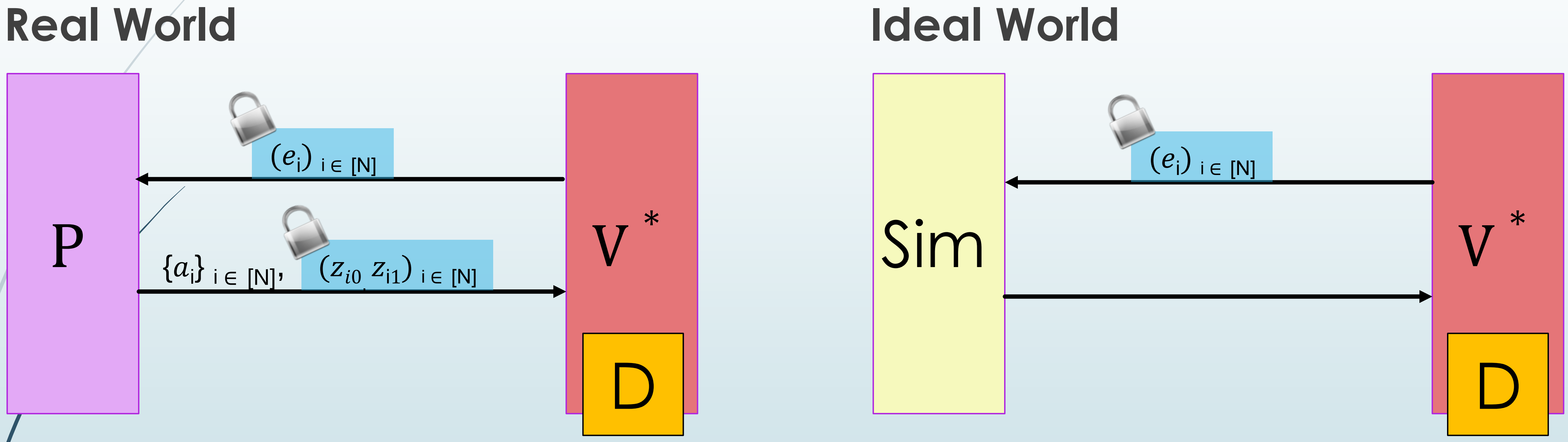
Real World



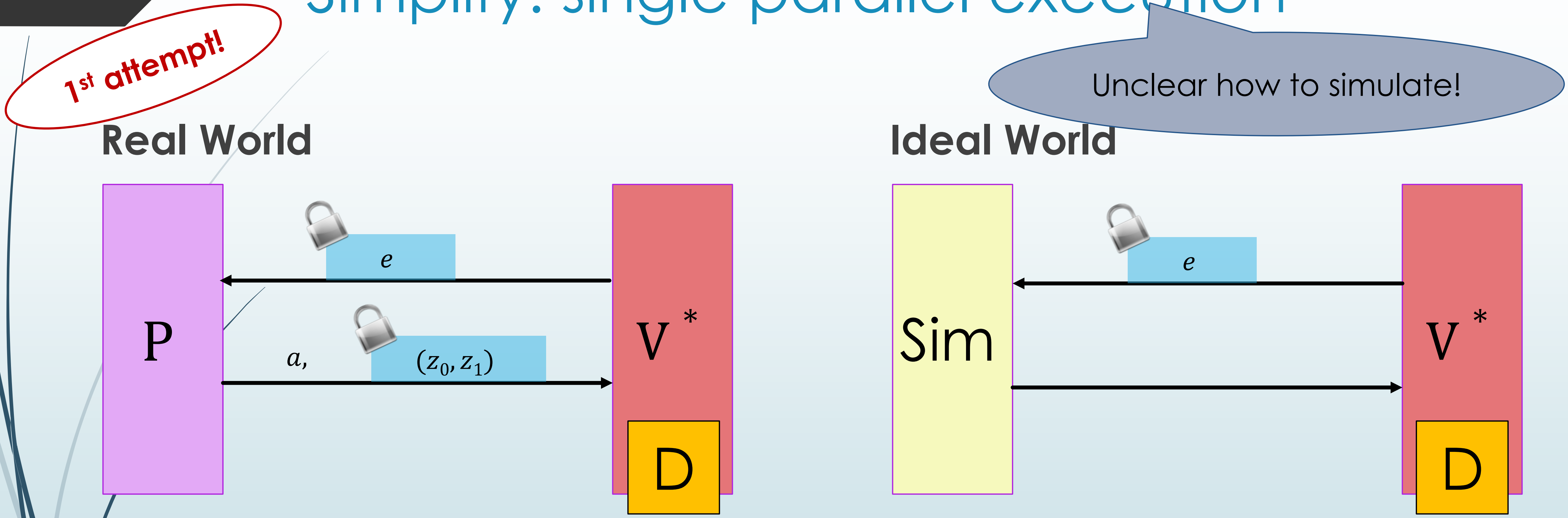
- Every message sent by ... cryption of some $\{e_i\}_{i \in [N]}$
- If Sim knew $\{e_i\}_{i \in [N]}$, the ... ZK).
- Privacy via super-poly sim ... encryption to find e_i [BGISW17]

Polynomial Simulation??

Rely on the Distinguisher to find e



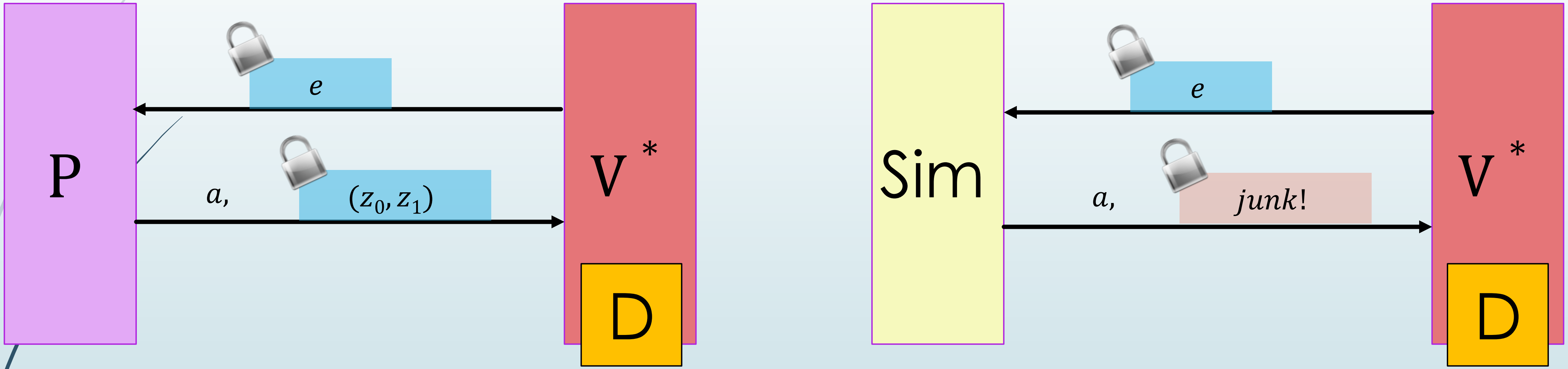
Simplify: single parallel execution



Simplify: single parallel execution

1st attempt!

Real World **Ideal World**

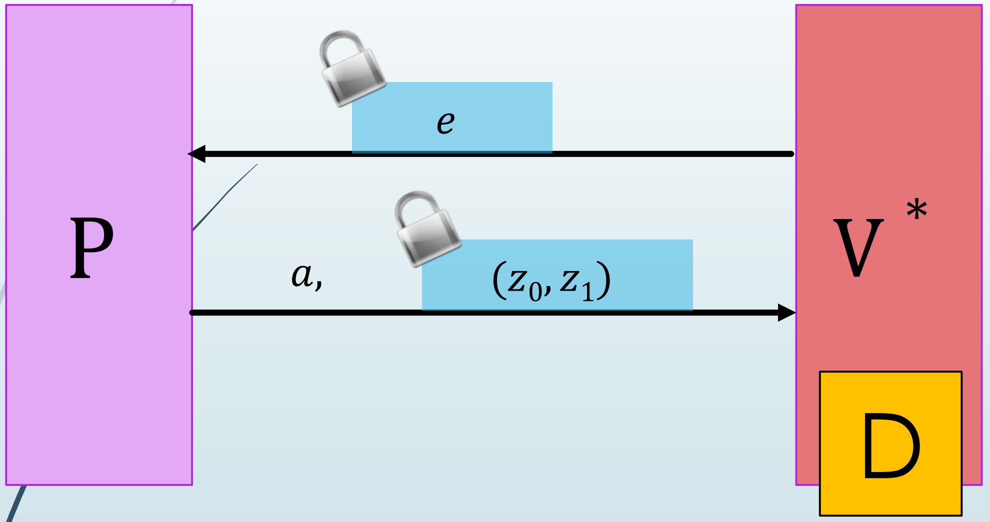


Can D tell the difference?

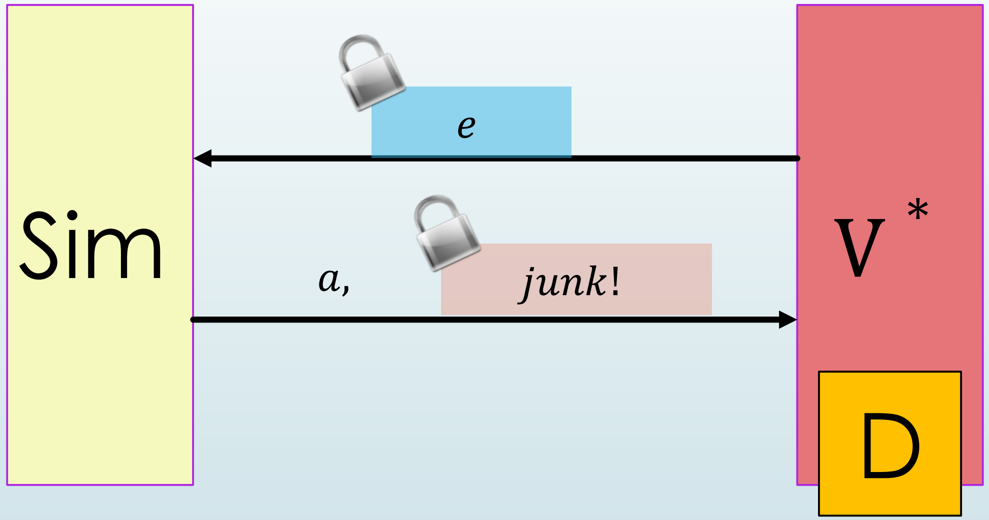
- Suppose **NOT**: eg, D doesn't know randomness for e
- a is already computationally hiding, Sim can easily sample $a,$ $junk!$

Simplify: Single parallel execution

Real World



Ideal World

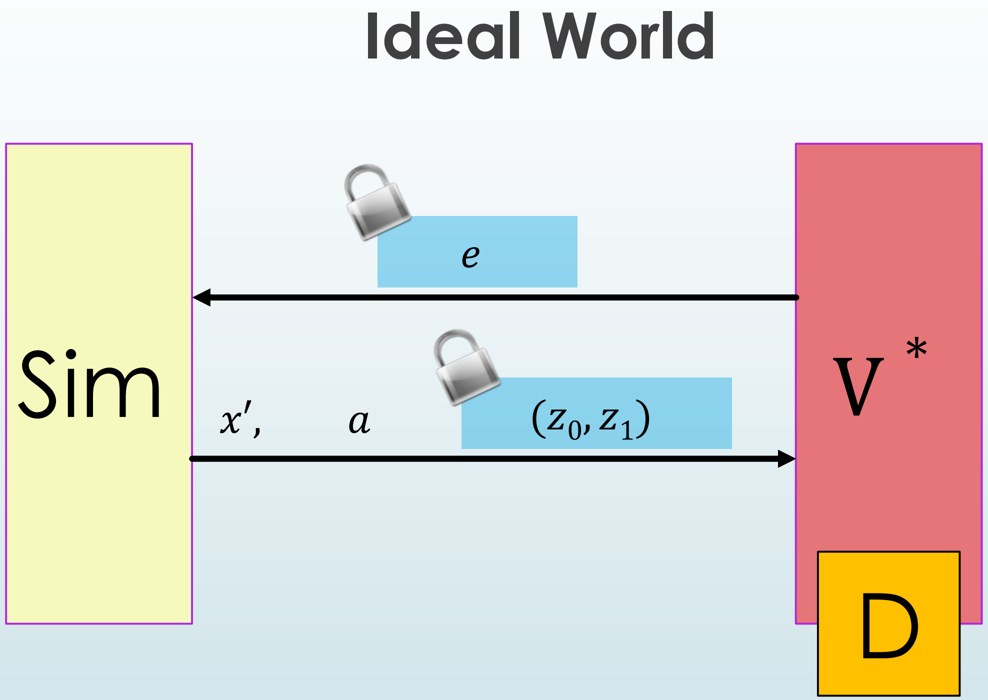


Can D tell the difference?

- Suppose **YES**: eg, D knows randomness for e
- Sim can't just sample $a,$ $junk!$: will be distinguishable!

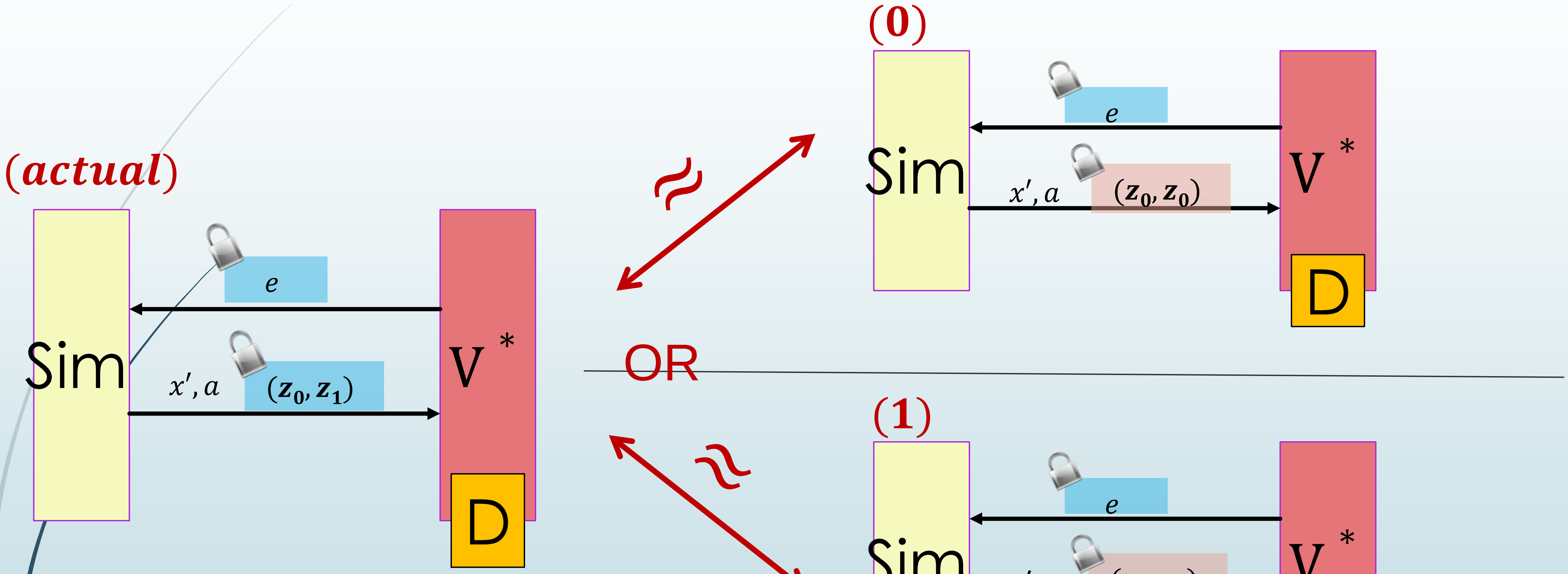
Sim will use D to extract *e* !

Recall: Distributional Simulation



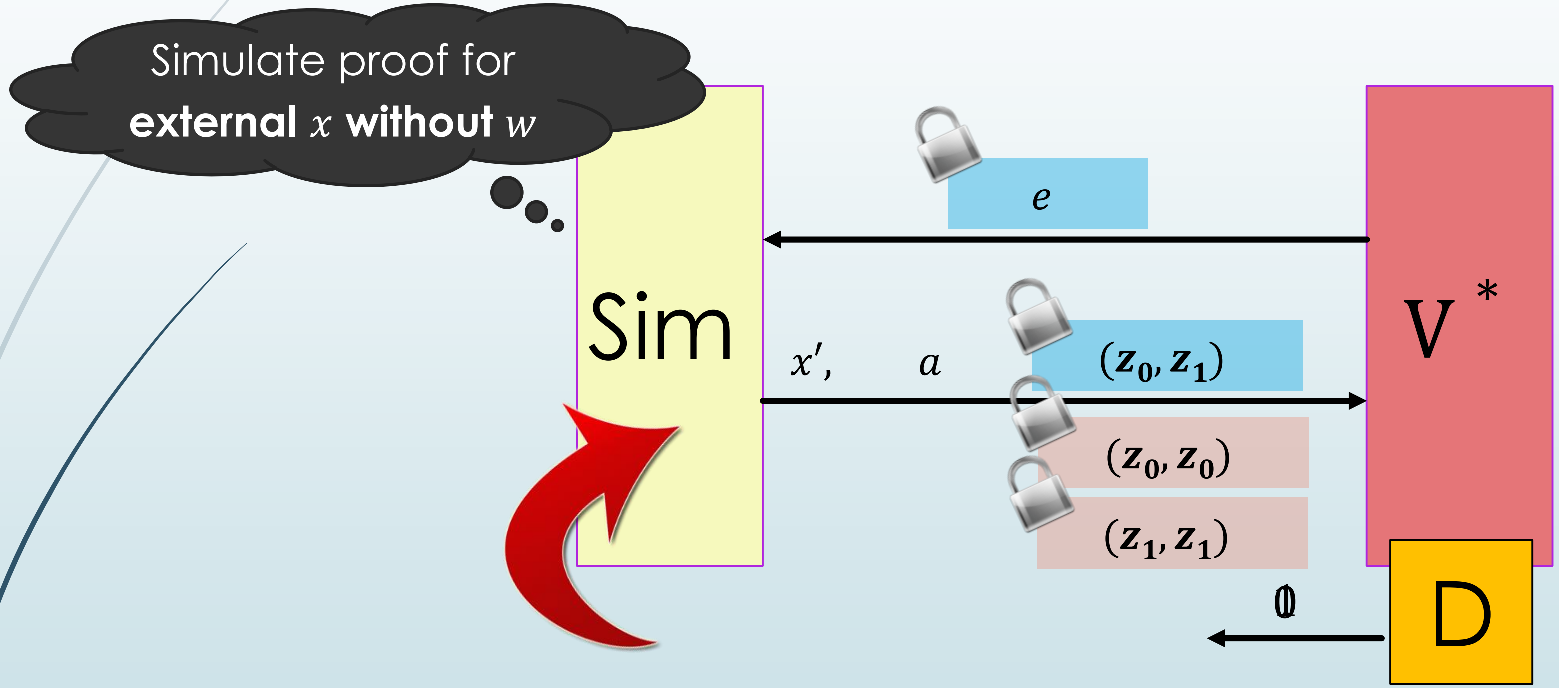
- Recall: want a simulator for $x \sim X$, which generates a proof without witness.
- However, Sim can sample other $(x', w') \sim (X, W)$ from the same distribution.
- Sim can also sample proofs for these other $(x', w') \sim (X, W)$.

Main Simulation Technique



Checks if $(actual) \approx (0)$
Or, if $(actual) \approx (1)$
Use this to extract e.

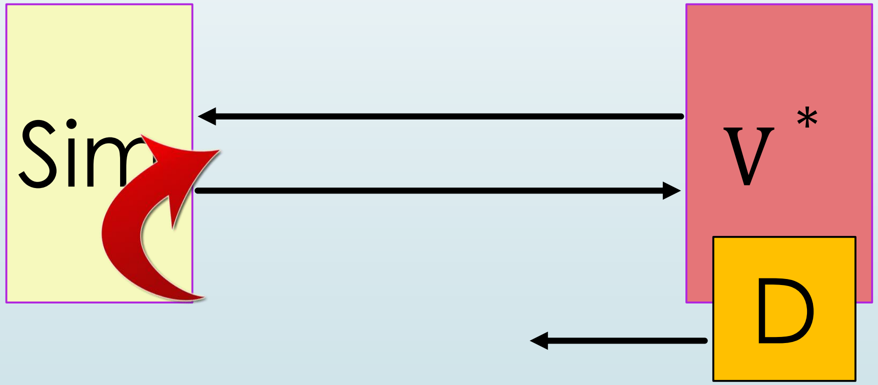
Polynomial Simulation



- Simulator *rewinds the distinguisher* to learn the OT challenge e.
- Technique extends to extracting $\{e_i\}_{i \in [N]}$ from parallel repetition.

Perspective: Extraction in Cryptography

- Black-box polynomial simulation strategy that requires only 2 messages.
- Previously, rewinding took more rounds



- Towards resolving open problems on round complexity of WH, strong WI.
- Applications to multiple 2-round, 3-round protocols, beyond proofs.

Conclusion & Open Problems

Round Complexity Timeline

3 round Witness Indistinguishability (FS90),
4 round Witness Hiding (FS90)

Impossibilities:
- 2 round ZK (GO94)
- 3 round BB ZK (GK92)

Impossibilities (GO94):
- 2 round weak ZK
- 2 round distributional ZK

4 round ZK arguments (FS90, BJY97)

5 round ZK proofs (GK96)

Impossibility:
- 3 round Witness Hiding (HRS09)

3 round ZK from non-std assumptions (HT98, LM01, BP04, CD08, GLR12, BP13, BBKPV16, BKP17)

1 & 2 round WI From TDPs / iO (DN00, BOV03, BP15)

Delayed-input setting:
- **Distributional weak ZK**
- **Witness Hiding, Strong WI**

2 rounds from quasi-poly &,
3 rounds from poly assumptions

2 round WI from quasi-poly DDH, QR, N^{th} residuosity

Open Questions

- 2 round protocols from *polynomial hardness*?
- Low round *public-coin* protocols with strong privacy?
- New applications of distinguisher-dependent simulation
- Other black-box/non-black-box techniques for 2 round protocols
  - A 2-round rewinding technique from superpoly DDH in [KS17, BKS17]

Thank you!