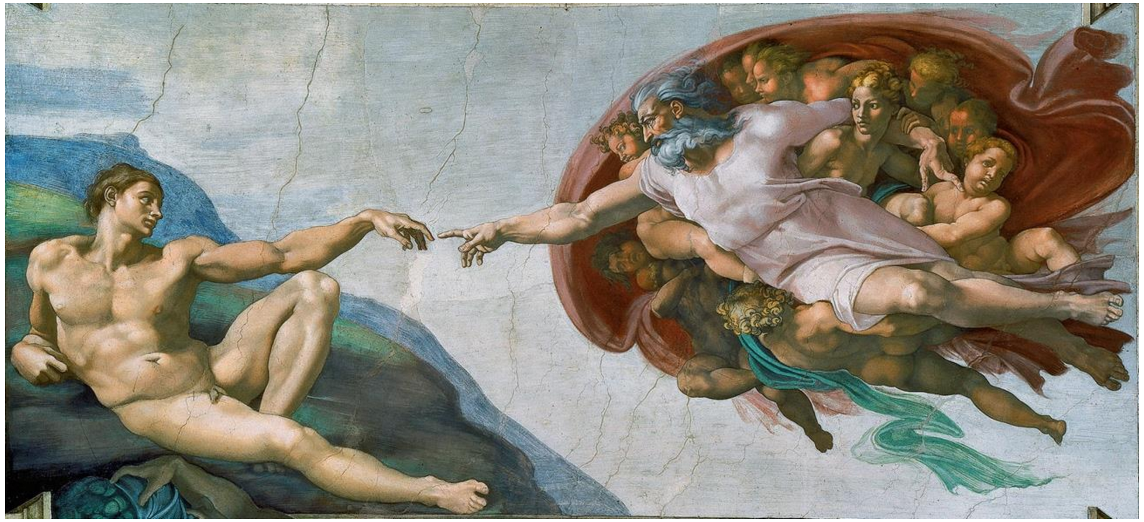
Instance-hiding Interactive Proofs

Changrui Mu, Prashant Nalini Vasudevan

National University of Singapore



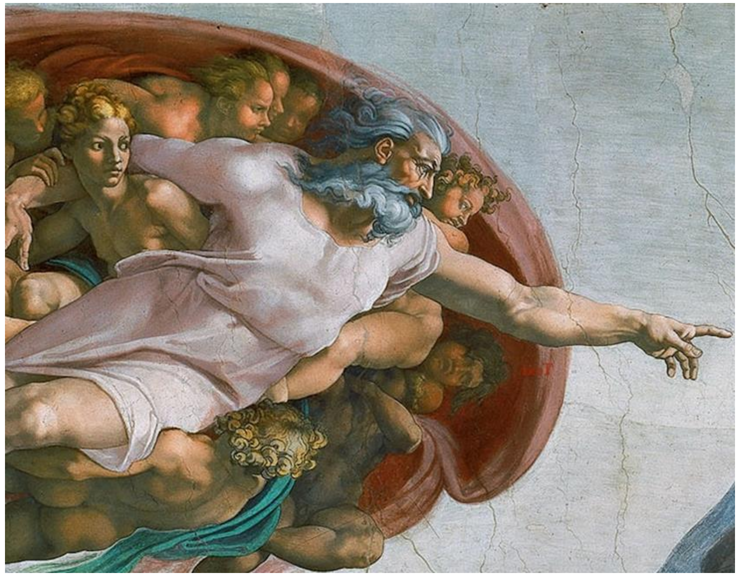
Founded by National Research Foundation, Singapore

Interactive Proofs

Prover P

Verifier V

P interacts with V convincing him that a proposition is true



Interactive Proofs

Prover P

Verifier V

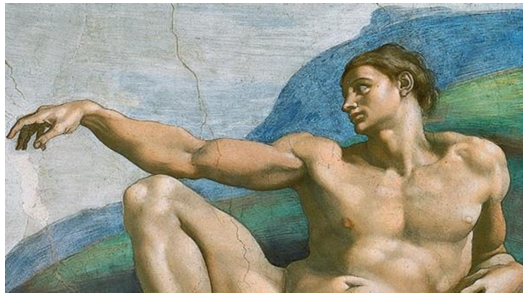
P interacts with V convincing him that a proposition is true

P and V may hold secret that they do not want the other to learn

Secrets in Interactive Proof

Prover P

Verifier V



P interacts with V convincing him that a proposition is true

Zero-knowledge:

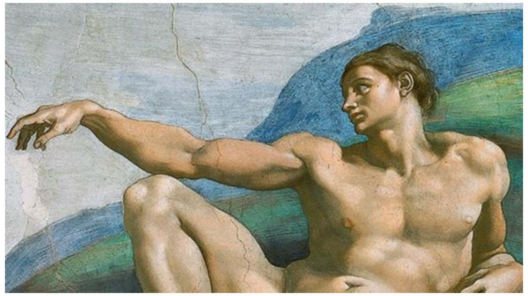
protect prover's *private info*

- NP Witness
- Secret Keys

Secrets in Interactive Proof

Prover P

Verifier V



P interacts with V convincing him that a proposition is true

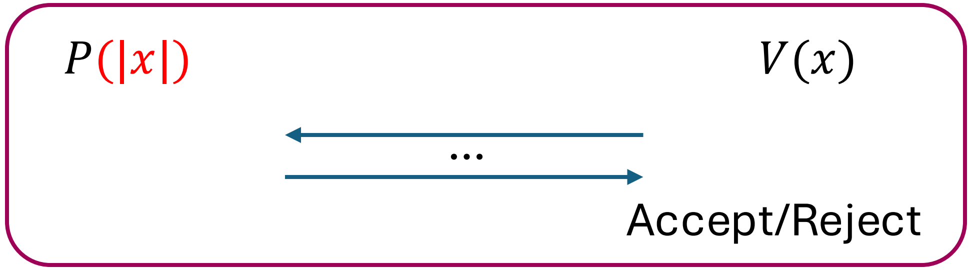
Zero-knowledge:
protect prover's *private info*

- NP Witness
- Secret Keys

Instance-hiding:
protect verifier's *private info*

- Input Instance
- Result of the protocol

Instance-hiding Interactive Proofs [Beavor-Feigenbaum-Shoup90]



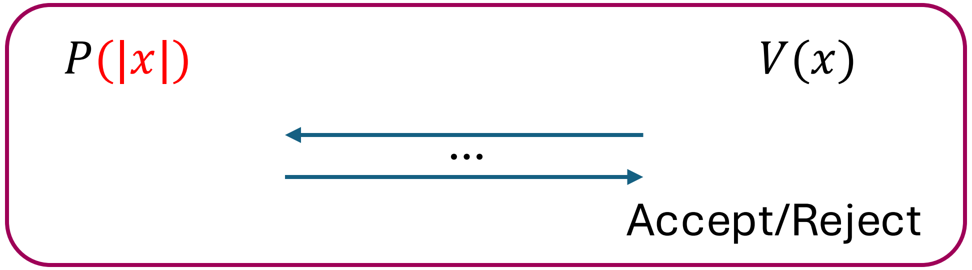
$P(|x|)$

$V(x)$

…

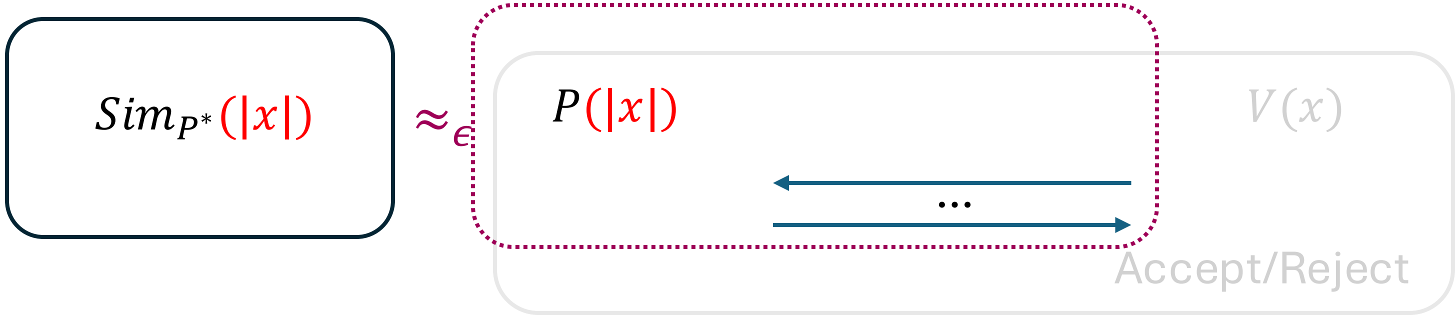
Accept/Reject

Instance-hiding Interactive Proofs [Beavor-Feigenbaum-Shoup90]



- **Completeness/Soundness**:
  - $x \in L$, P makes V accept w.h.p
  - $x \notin L$, **NO** $\boldsymbol{P^*}$ makes V accept w.h.p

Instance-hiding Interactive Proofs [Beavor-Feigenbaum-Shoup90]



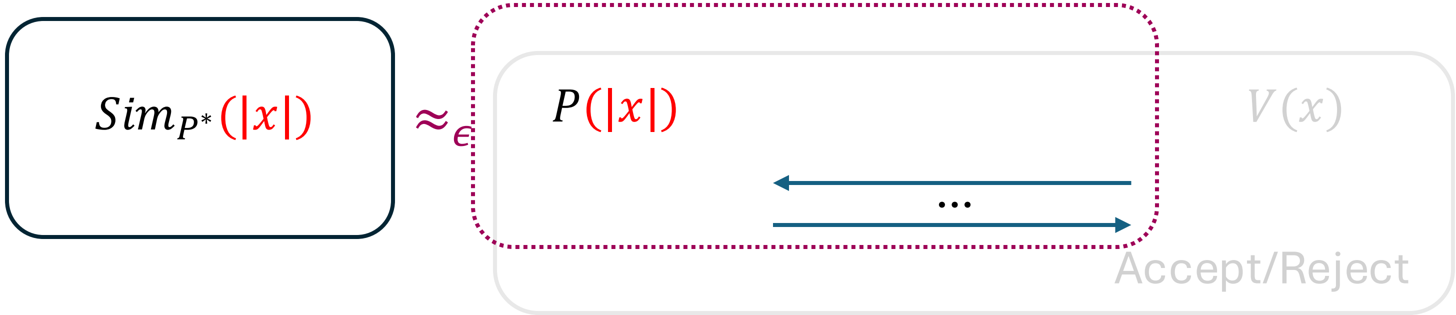
- **Completeness/Soundness:**
  - $x \in L$, P makes V accept w.h.p
  - $x \notin L$, **NO** $\boldsymbol{P^*}$ makes V accept w.h.p

- **Instance-Hiding [BFS90]:**

For any P^*, $\exists\, Sim_{P^*}, for\ any\ x$:

$$Sim_{P^*}(|x|) \approx_\epsilon View_{p^*}(P^*, V(x))$$

Instance-hiding Interactive Proofs [Beavor-Feigenbaum-Shoup90]



- **Completeness/Soundness:**
  - $x \in L$, P makes V accept w.h.p
  - $x \notin L$, **NO** $\boldsymbol{P^*}$ makes V accept w.h.p

- **Instance-Hiding [BFS90]:**

For any P^*, $\exists\ Sim_{P^*}, for\ any\ x$:

$$Sim_{P^*}(|x|) \approx_\epsilon View_{p^*}(P^*, V(x))$$

- $\boldsymbol{\epsilon}$-IHIP$= \{L \mid L\ has\ \boldsymbol{\epsilon}-$instance$-$hiding IP$\}$

Instance-hiding Interactive Proofs [BFS90]

Prover P

Verifier V

P interacts with V convincing him that a proposition is true

Make the proof without knowing the exact statement you are proving

Instance x

IHIP Example

Consider a cyclic group $(\mathrm{g}, \mathbb{G})$, define the language L of group element with most significant bit of the discrete logarithm equal to 1:

$$L = \{x \in \mathbb{G} \mid msb\left(DL_g(x)\right) = 1\}$$

IHIP Example

Consider a cyclic group $(\mathrm{g}, \mathbb{G})$, define the language L of group element with most significant bit of the discrete logarithm equal to 1:

$$L = \{x \in \mathbb{G} \mid msb\left(DL_g(x)\right) = 1\}$$

Instance-Hiding Interactive Proofs for L

P

V(x)

$r \leftarrow \mathbb{Z}_{|\mathbb{G}|}$

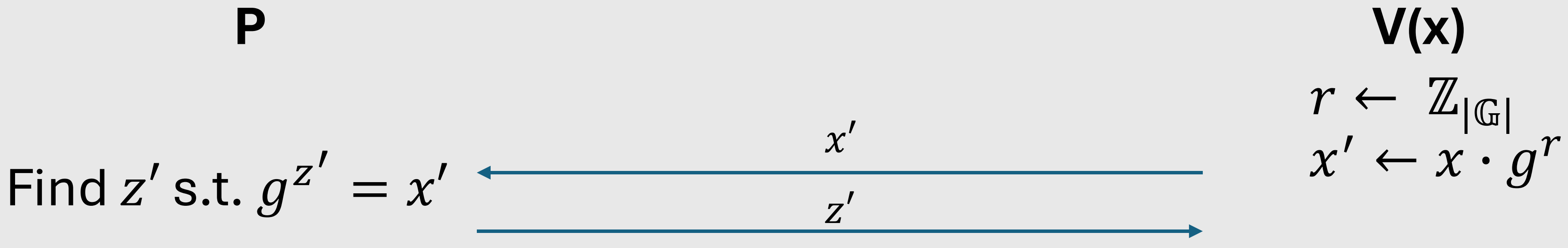
$x' \leftarrow x \cdot g^r$

IHIP Example

Consider a cyclic group $(\mathrm{g}, \mathbb{G})$, define the language L of group element with most significant bit of the discrete logarithm equal to 1:

$$L = \{x \in \mathbb{G} \mid msb\left(DL_g(x)\right) = 1\}$$

Instance-Hiding Interactive Proofs for L



P

V(x)

$r \leftarrow \mathbb{Z}_{|\mathbb{G}|}$

$x' \leftarrow x \cdot g^r$

x'

Find z' s.t. $g^{z'} = x'$

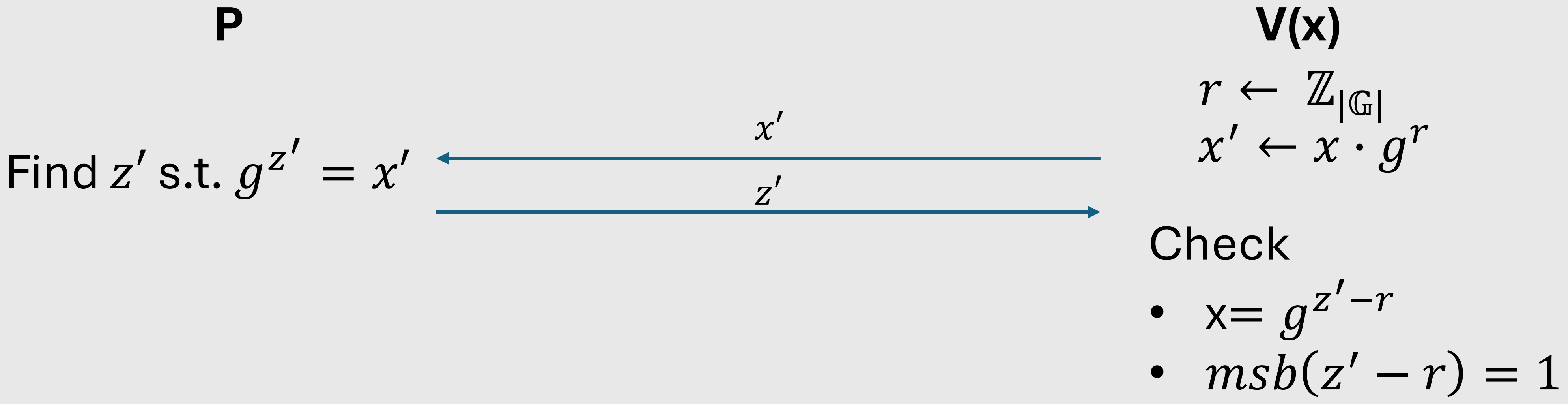
z'

IHIP Example

Consider a cyclic group $(\mathrm{g}, \mathbb{G})$, define the language L of group element with most significant bit of the discrete logarithm equal to 1:

$$L = \{x \in \mathbb{G} \mid msb\big(DL_g(x)\big) = 1\}$$

Instance-Hiding Interactive Proofs for L



P

V(x)

$r \leftarrow \mathbb{Z}_{|\mathbb{G}|}$

$x' \leftarrow x \cdot g^r$

x'

Find z' s.t. $g^{z'} = x'$

z'

Check

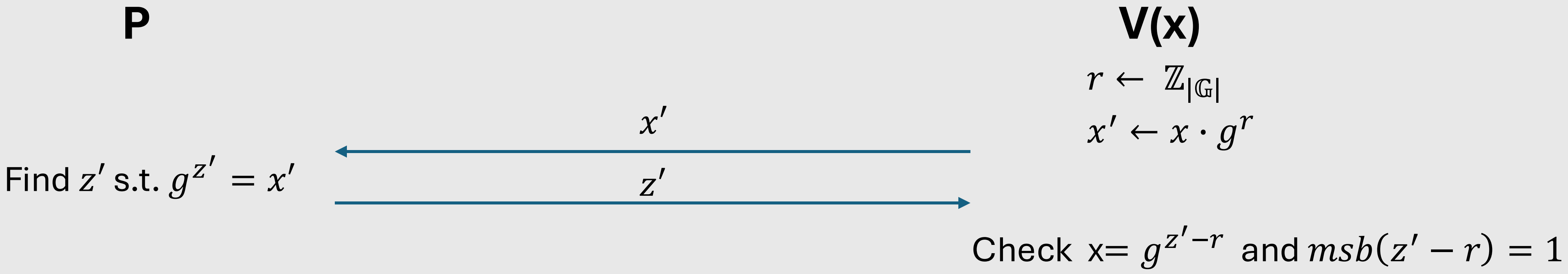
- x= $g^{z'-r}$
- $msb(z' - r) = 1$

IHIP Example

Consider a cyclic group $(\mathrm{g}, \mathbb{G})$, define the language L of group element with most significant bit of the discrete logarithm equal to 1:

$$L = \{x \in \mathbb{G} \mid msb\big(DL_g(x)\big) = 1\}$$

Instance-Hiding Interactive Proofs for L



P

V(x)

$r \leftarrow \mathbb{Z}_{|\mathbb{G}|}$

$x' \leftarrow x \cdot g^r$

Find z' s.t. $g^{z'} = x'$

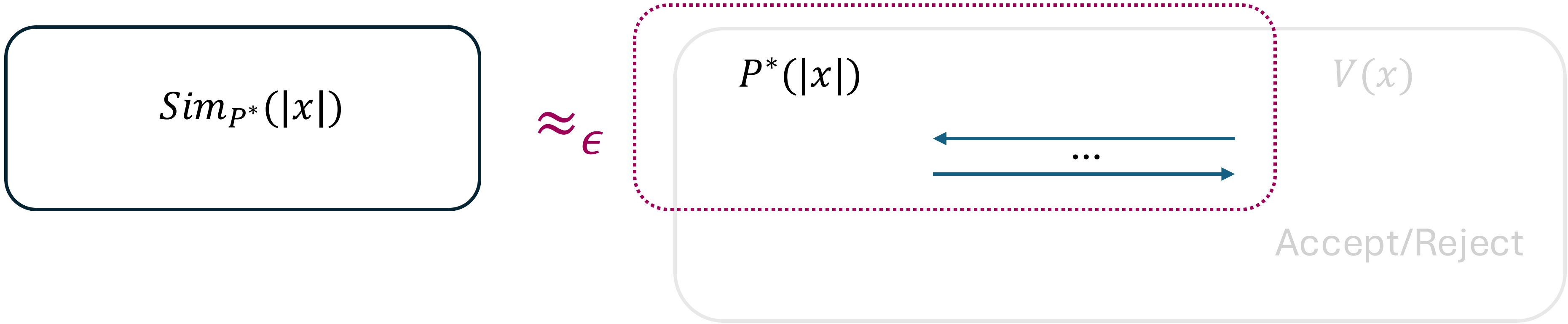
Check x= $g^{z'-r}$ and $msb(z'-r) = 1$

Completeness and Soundness: $(z'-r)$ is NP witness for x

Instance-hiding: x' follows uniform distribution over $\mathbb{G}$, independent of x

Instance-hiding Interactive Proofs:

Definition [BFS90] $\langle P, V\rangle$ is instance-hiding IP for L:



$Sim_{P^*}(|x|)$

$\approx_\epsilon$

$P^*(|x|)$

$V(x)$

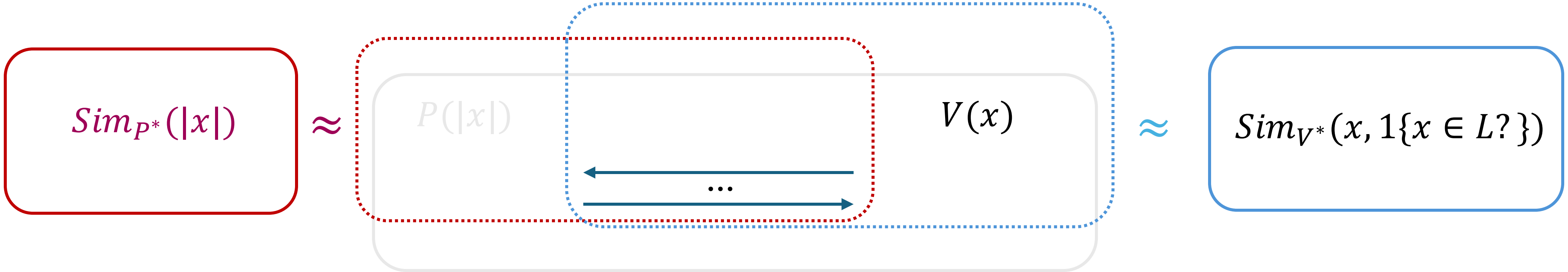
$\ldots$

Accept/Reject

- **Completeness/Soundness:**
  - $x \in L$, P makes V accept w.h.p
  - $x \notin L$, **NO** $\boldsymbol{P^*}$ makes V accept w.h.p
- **ϵ-Instance-Hiding**: for any P^*, $\exists\ Sim_{P^*}$
- ϵ-IHIP$=\{L \mid L\ has\ \epsilon{-}$instance$-$hiding IP$\}$

- Sim_{P} is efficient: simulatable IHIP.

Zero-Knowledge Proofs [GMR85]



Instance-Hiding [BFS90]:

$\forall P^*, \exists\, Sim_{P^*}, \quad \forall x$:

$$Sim_{P^*}(|x|) \approx View_{p^*}(P, V(x))$$

Zero-Knowledge [GMR85]:

$\forall V^*, \exists$ PPT $Sim_{V^*}, \forall x$:

$$Sim_{V^*}(x, 1\{x \in L?\}) \approx View_{V^*}(P, V(x))$$

SZK and IHIP class

	SZK
1980-2000	[GMR85], [For87], [AH91], [BFS90], [GK90] [BGG++88], [GO94], [Ost91], [GK96], [Gol96], [Oka96], [VS97], [GSV98], [GV98], [Vad99], [GSV99]…
2000-2010	[Lip01], [DSDCPY08], [Mal08], [OV06], [GOS05], [Gol02]…
2010-2020	[GOVW11], [MX12], [GT14], [AR16], [HRV18], [BCHTV16], [LZ17], [KRRSV20], [LV15]…
2020-Present	[KRV21], [GIKKLS23], [MNRV24], [KRV24]…

SZK and IHIP class

	SZK	IHIP
1980-2000	[GMR85], [For87], [AH91], [BFS90], [GK90] [BGG++88], [GO94], [Ost91], [GK96], [Gol96], [Oka96], [VS97], [GSV98], [GV98], [Vad99], [GSV99]…	[AFK90], [BF90], [BFOS93], [BFS90], [FO91]
2000-2010	[Lip01], [DSDCPY08], [Mal08], [OV06], [GOS05], [Gol02]…	
2010-2020	[GOVW11], [MX12], [GT14], [AR16], [HRV18], [BCHTV16], [LZ17], [KRRSV20], [LV15]…	
2020-Present	[KRV21], [GIKKLS23], [MNRV24], [KRV24]…	[This Work]

Natural Questions

- The Power of IHIP
  - Can NP-complete problem have IHIP?

Natural Questions

- The Power of IHIP
    - Can NP-complete problem have IHIP?
- Relationship between IHIP and cryptography primitives?

Natural Questions

- The Power of IHIP
  - Can NP-complete problem have IHIP?
- Relationship between IHIP and cryptography primitives?
- Relationship between IHIP and SZK?

Natural Questions

- The Power of IHIP
  - Can NP-complete problem have IHIP?
- Relationship between IHIP and cryptography primitives?
- Relationship between IHIP and SZK?
- Closure properties of IHIP

Natural Questions

- The Power of IHIP
  - Can NP-complete problem have IHIP?
- Relationship between IHIP and cryptography primitives?
- Relationship between IHIP and SZK?
- Closure properties of IHIP
- Complete Problems

Upperbound

Theorem [Abadi-Feigenbaum-Kilian90]

Perfect-instance-hiding IHIP ⊆ NP/Poly ∩ coNP/Poly

Upperbound

Theorem [Abadi-Feigenbaum-Kilian90]

Perfect-instance-hiding IHIP $\subseteq$ NP/Poly $\cap$ coNP/Poly

Theorem [This Work]

ε-IHIP $\subseteq$ NP/Poly $\cap$ coNP/Poly $\quad \varepsilon < \frac{1}{32}$

Upperbound

Theorem [Abadi-Feigenbaum-Kilian90]

Perfect-instance-hiding IHIP ⊆ NP/Poly ∩ coNP/Poly

Theorem [This Work]

ε-IHIP ⊆ NP/Poly ∩ coNP/Poly $\qquad \varepsilon < \frac{1}{32}$

Theorem [This Work]

ε-simulatable IHIP ⊆ AM ∩ coAM $\qquad$ negligible $\mathcal{E}$

Upperbound

Theorem [Abadi-Feigenbaum-Kilian90]

Perfect-instance-hiding IHIP ⊆ NP/Poly ∩ coNP/Poly

Theorem [This Work]

ε-IHIP ⊆ NP/Poly ∩ coNP/Poly $\varepsilon < \frac{1}{32}$

Theorem [This Work]

ε-simulatable IHIP ⊆ AM ∩ coAM negligible $\mathcal{E}$

Theorem [Fortnow87]

SZK ⊆ AM ∩ coAM

Bridge Heuristica, Pessiland and Minicrypt

Theorem [This Work]
If ∃ L that is **average-case hard**, and has *constant-round* **IHIP** protocol, then there exist *infinitely-often non-uniform* **one-way functions** (OWF*).

Bridge Heuristica, Pessiland and Minicrypt

Theorem [This Work]
If ∃ L that is **average-case hard**, and has *constant-round* **IHIP** protocol, then there *exist infinitely-often non-uniform* **one-way functions** (OWF*).

Theorem [This Work]
If ∃ L that is **worst-case hard**, and has **Simulatable-IHIP** protocol, then there exist **one-way functions** (OWF).

IHIP/SZK/SRE

IHIP/Simulatable-IHIP	SZK/SRE
Avg-Hard + constant-round IHIP ⇒ io-OWF	[Ostrovsky91]: Avg-Hard + SZK ⇒ io-OWF
Worst-Hard + Simulatable-IHIP ⇒ OWF	[Applebaum-Raykov16]: Worst-Hard + SRE ⇒ io-OWF
Simulatable-IHIP ⊆ IHIP	[Applebaum14]: SRE⊆ SZK
Simulatable-IHIP ⊆ AM∩ coAM IHIP ⊆ AM/Poly∩ coAM/Poly	[Fortnow87]: SZK ⊆ AM∩ coAM

SRE = Statistical Randomized Encodings [Ishai-Kushilevitz00], [Applebaum-Ishai-Kushilevitz04]

IHIP is also connected to **interactive version** of **randomized encoding** [Applebaum-Ishai-Kushilevitz10]

Oracle Separation

Given The Similarity between SZK and IHIP:

What’s the relationship between SZK and IHIP?

Oracle Separation

Given The Similarity between SZK and IHIP:

What's the relationship between SZK and IHIP?

Oracle Separation of IHIP from SZK:

Theorem [This work]

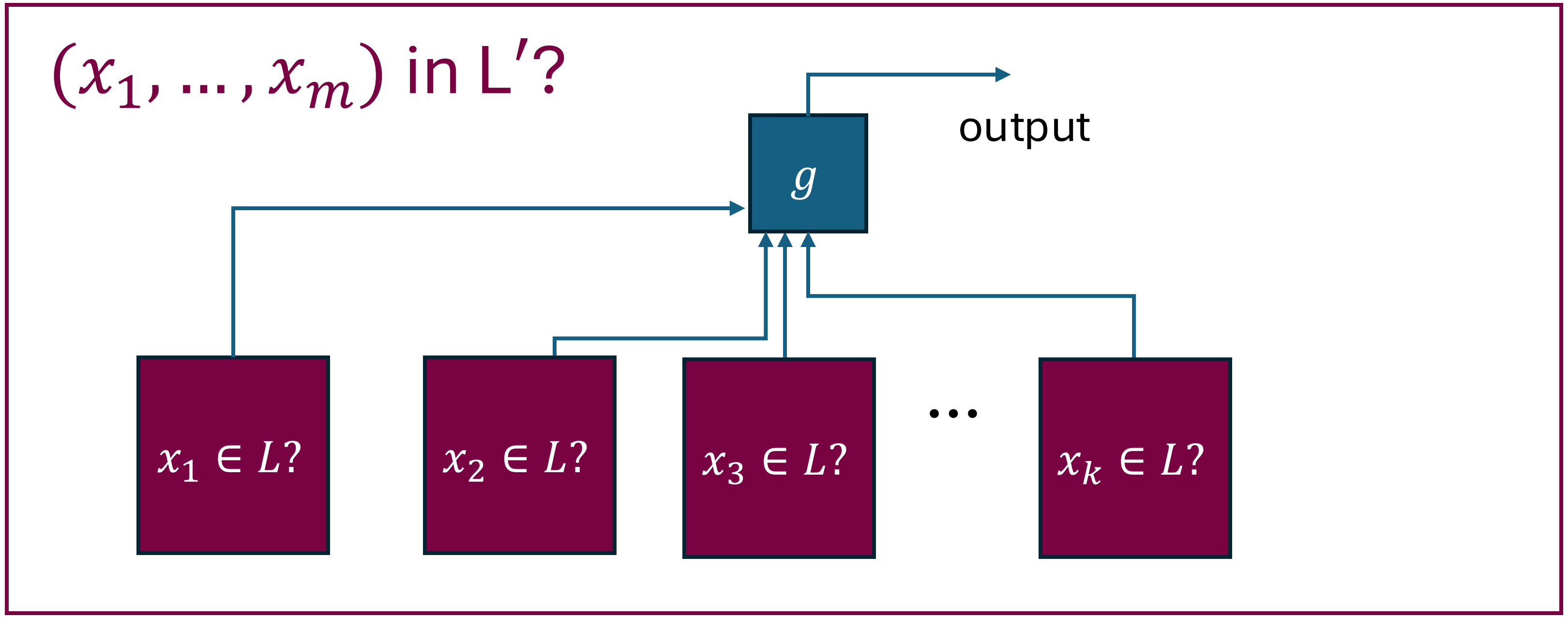
There exists an oracle $\mathcal{O}$ with respect to which there exists a language that has a IHIP but not a SZK. In short:

$$IHIP^{\mathcal{O}} \not\subseteq SZK^{\mathcal{O}}$$

Closure Property

Theorem [This work]:
L has IHIP, and $g\colon \{0,1\}^k \to \{0,1\}$ is a poly-size circuit, then $L' = g \circ L^{\otimes k}$ also has IHIP.

$(x_1, \dots, x_m)$ in L′?



Closure Property

Theorem [This work]:
L has IHIP, and $g: \{0,1\}^k \to \{0,1\}$ is a poly-size circuit, then $L' = g \circ L^{\otimes k}$ also has IHIP.

Theorem [Sahai-Vadhan97]:
L has SZK, and $g: \{0,1\}^k \to \{0,1\}$ is a poly-size formula, then $L' = g \circ L^{\otimes k}$ also has SZK.

Main Results Overview

Upper Bound

- IHIP ⊆ NP/Poly ∩ coNP/Poly
- simulatable IHIP ⊆ AM ∩ coAM

Hardness Implication

- Avg-Hard + constant-round IHIP ⇒ io-OWF
- Worst-Hard + Simulatable-IHIP ⇒ OWF

Oracle Separation

- $\exists \mathcal{O},\ IHIP^{\mathcal{O}} \not\subseteq\ SZK^{\mathcal{O}}$

Closure Property

- IHIP is closed under polynomial circuit

Proof in the talk

Upper Bound

- IHIP ⊆ NP/Poly ∩ coNP/Poly
- simulatable IHIP ⊆ AM ∩ coAM

Hardness Implication

- Avg-Hard + constant-round IHIP ⇒ io-OWF
- Worst-Hard + Simulatable-IHIP ⇒ OWF

Oracle Separation

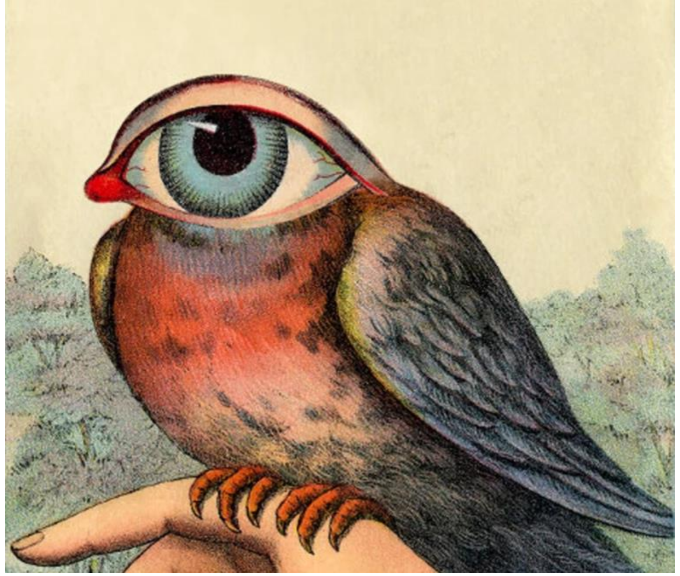
- $\exists \mathcal{O},\ IHIP^{\mathcal{O}} \not\subseteq\ SZK^{\mathcal{O}}$

Closure Property

- IHIP is closed under polynomial circuit

Bird's Eyes' View

- Avg-Hard + 1-round Simulatable-IHIP ⇒ distributionally OWF



Avg-Hard 1-round Simulatable IHIP ⇒ OWF

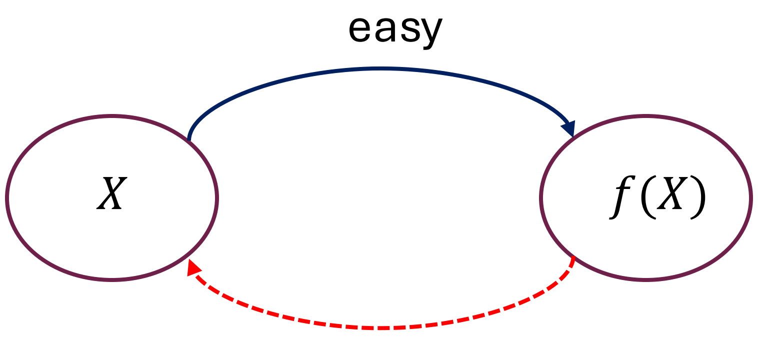
Def (Hardness on average)

Uniform for this talk

L is Avg-hard if there exists an efficiently sampleable distribution X such that for any PPT A, ∃ $negl$:

$$Pr_{x \leftarrow X}[A(x) = L(x)] \leq \frac{1}{2} + negl(|x|)$$

Def (Distributionally One-Way Function [Impagliazzo-Luby89])

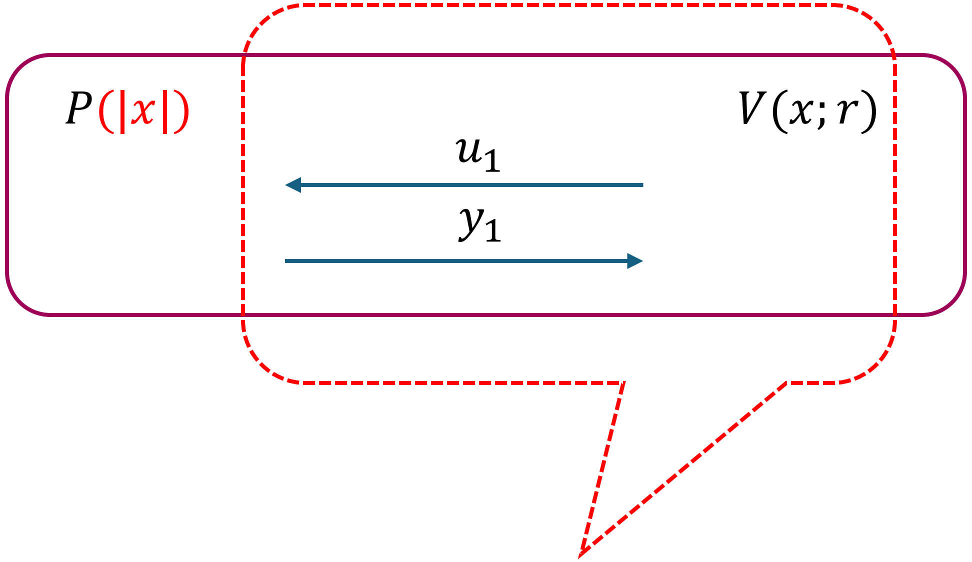


HARD to **invert uniformly**

Avg-Hard 1-round Simulatable IHIP ⇒ Distributionally OWF

P V Sim_P

Simulatable IHIP for L



$P(|x|)$

$V(x;r)$

u_1

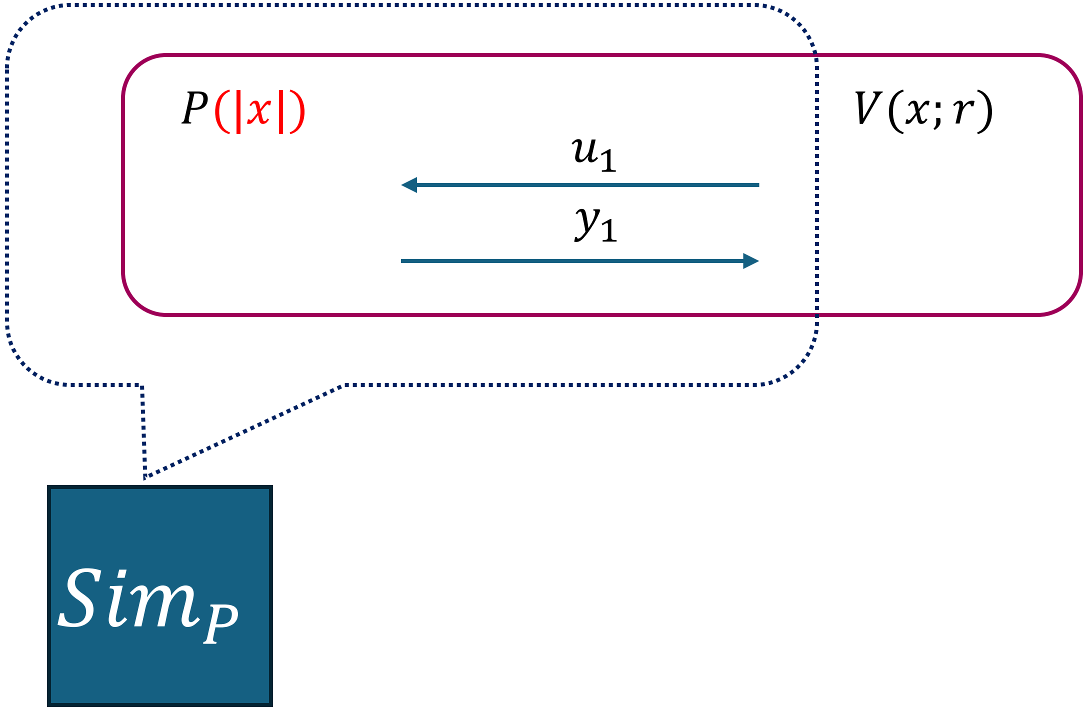
y_1

V's View: (x, r, u_1, y_1)

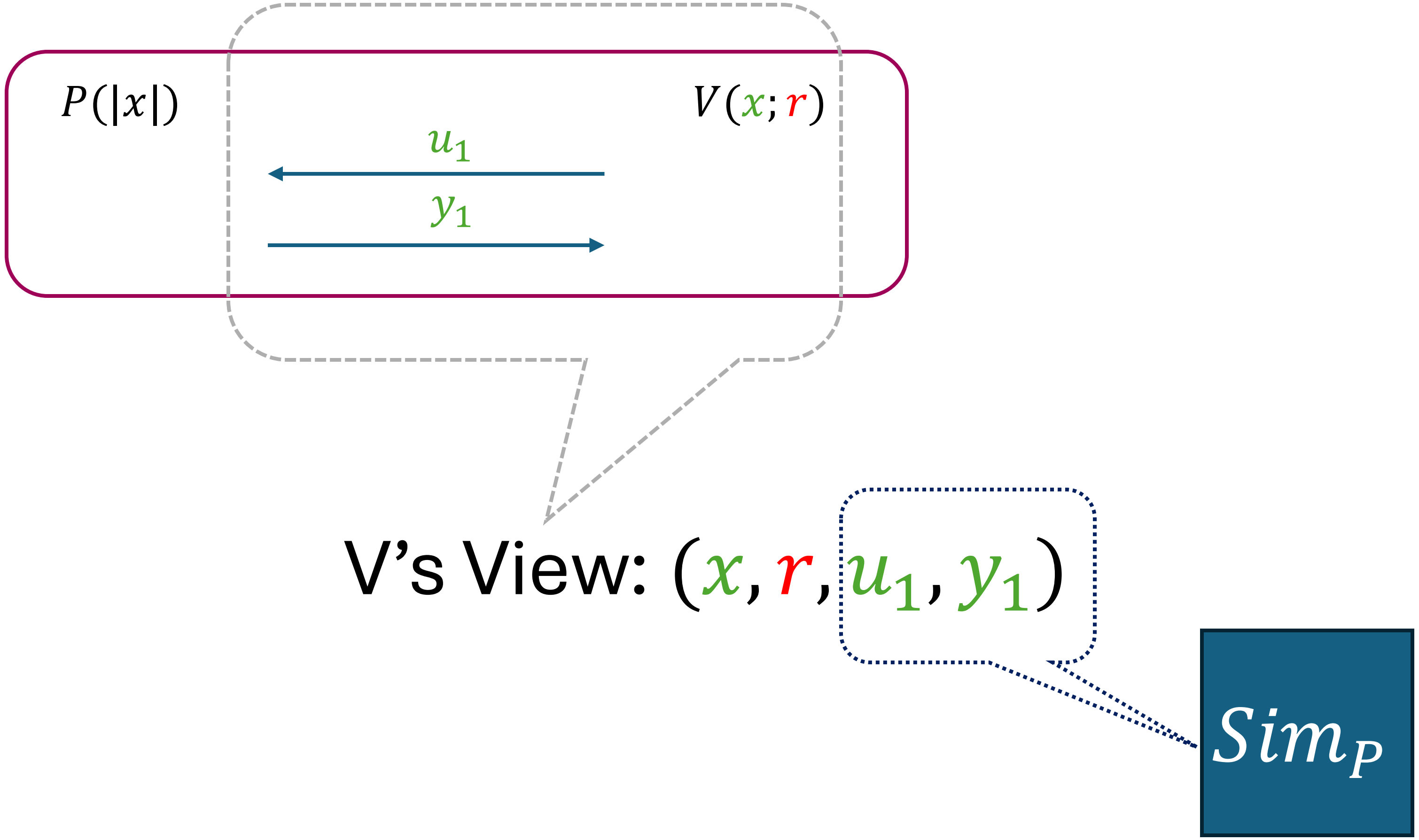
Avg-Hard 1-round Simulatable IHIP ⇒ Distributionally OWF

P V Sim_P

Simulatable IHIP for L



Avg-Hard 1-round Simulatable IHIP ⇒ Distributionally OWF

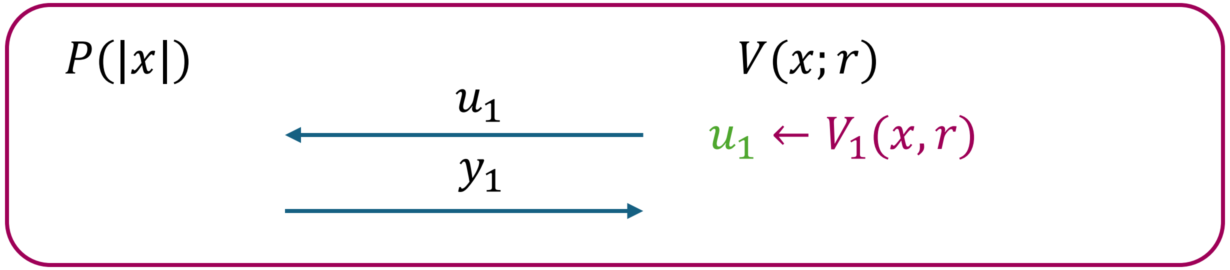


V's View: (x, r, u_1, y_1)

Avg-Hard 1-round Simulatable IHIP ⇒ Distributionally OWF

Distributional OWF Candidate:

$$F_1(x, r) = (x, V_1(x, r))$$



$P(|x|)$

$V(x; r)$

u_1

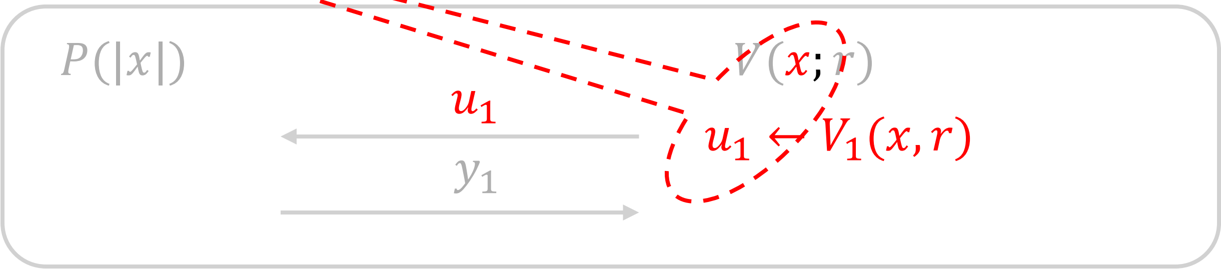
$u_1 \leftarrow V_1(x, r)$

y_1

Avg-Hard 1-round Simulatable IHIP ⇒ Distributionally OWF

Distributional OWF Candidate:

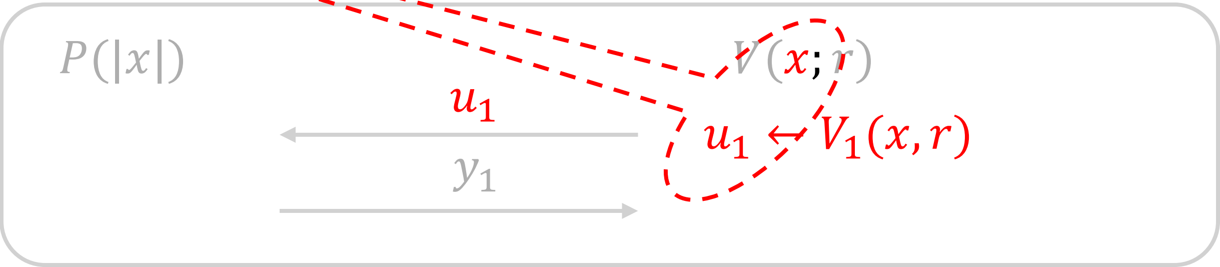
$$F_1(x,r) = (x, \underbrace{V_1(x,r)}_{u_1})$$



Avg-Hard 1-round Simulatable IHIP ⇒ Distributionally OWF

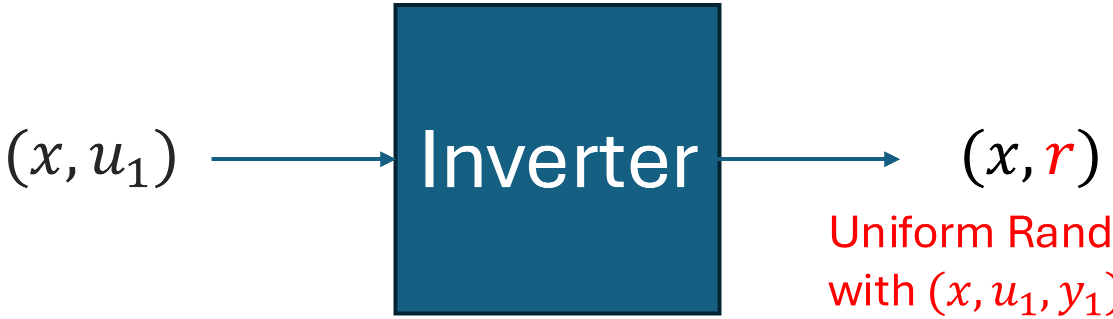
Distributional OWF Candidate:

$$F_1(x,r) = (x, \underbrace{V_1(x,r)}_{u_1})$$



Suppose F_1 is not distributionally one-way

∃ PPT Inverter:

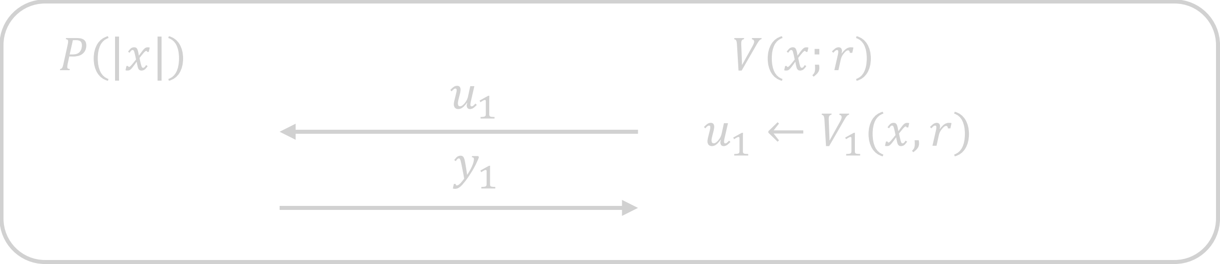


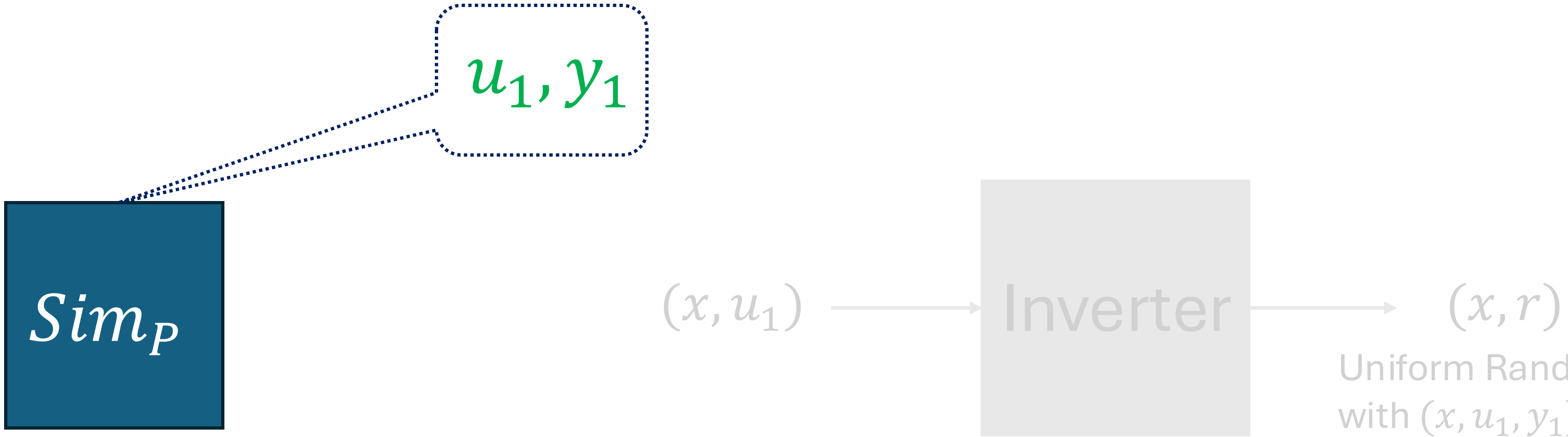
Uniform Random seed consistent with (x, u_1, y_1)

Avg-Hard 1-round Simulatable IHIP ⇒ Distributionally OWF

Distributional OWF Candidate:

$$F_1(x,r) = (x, \underbrace{V_1(x,r)}_{u_1})$$



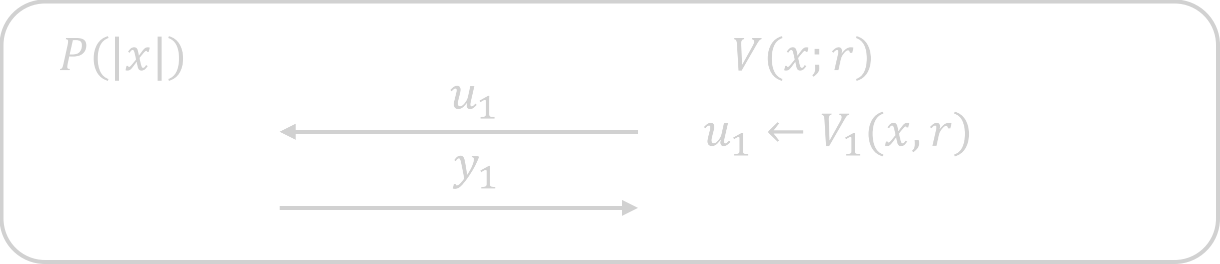


Uniform Random seed consistent with (x, u_1, y_1)

Avg-Hard 1-round Simulatable IHIP ⇒ Distributionally OWF

Distributional OWF Candidate:

$$F_1(x,r) = (x, \underbrace{V_1(x,r)}_{u_1})$$



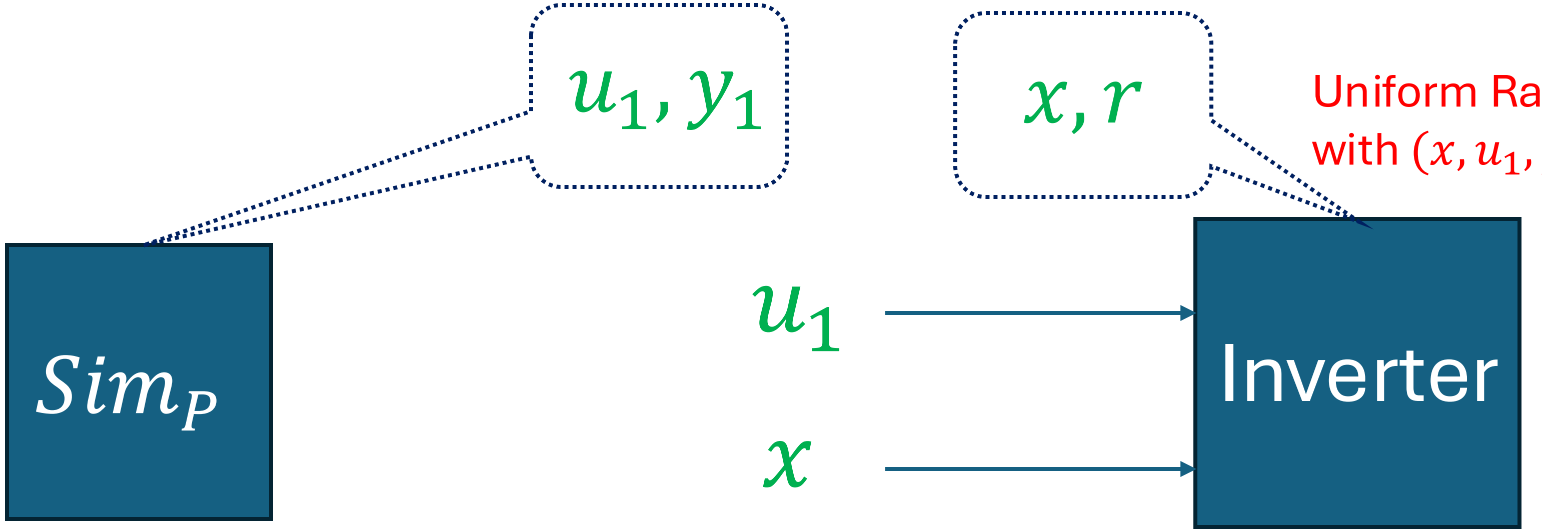
$P(|x|)$

$V(x;r)$

$u_1 \leftarrow V_1(x,r)$

$\xleftarrow{u_1}$

$\xrightarrow{y_1}$



u_1, y_1

x, r

Sim_P

u_1

x

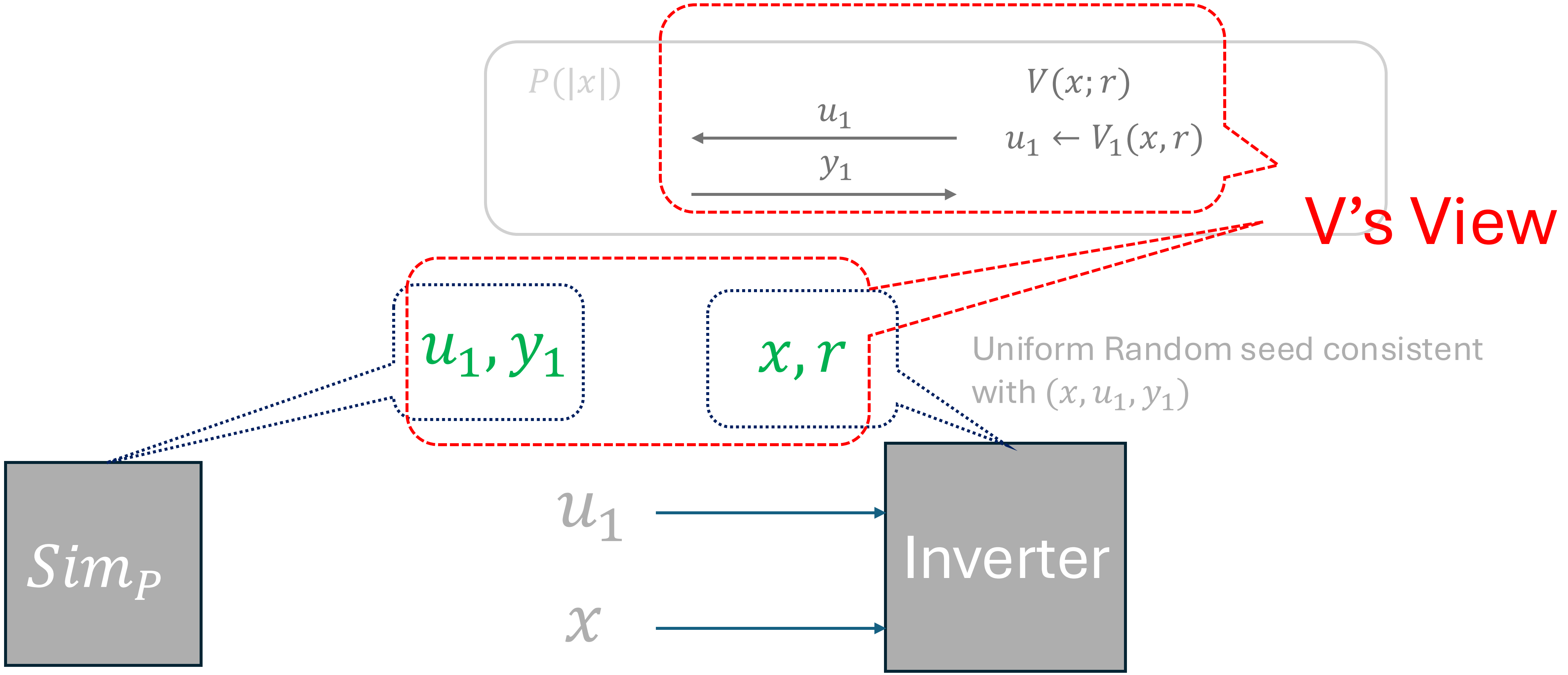
Inverter

Uniform Random seed consistent with (x, u_1, y_1)

Avg-Hard 1-round Simulatable IHIP ⇒ Distributionally OWF

Distributional OWF Candidate:

$$F_1(x,r) = (x, \underbrace{V_1(x,r)}_{u_1})$$

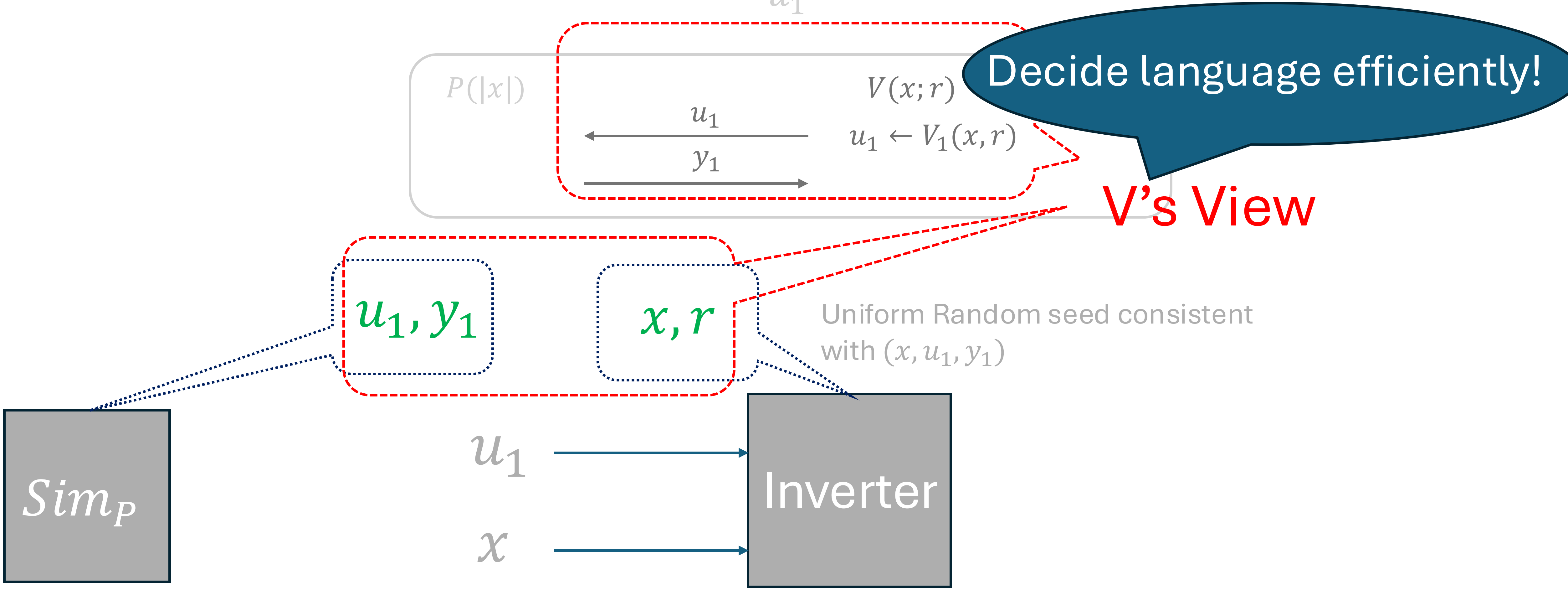


Uniform Random seed consistent with (x, u_1, y_1)

Avg-Hard 1-round Simulatable IHIP ⇒ Distributionally OWF

Distributional OWF Candidate:

$$F_1(x,r) = (x, \underbrace{V_1(x,r)}_{u_1})$$



$P(|x|)$
$V(x;r)$
u_1
$u_1 \leftarrow V_1(x,r)$
y_1
Decide language efficiently!
V's View
u_1, y_1
x, r
Uniform Random seed consistent with (x, u_1, y_1)
Sim_P
u_1
x
Inverter

Avg-Hard 1-round Simulatable IHIP ⇒ Distributionally OWF

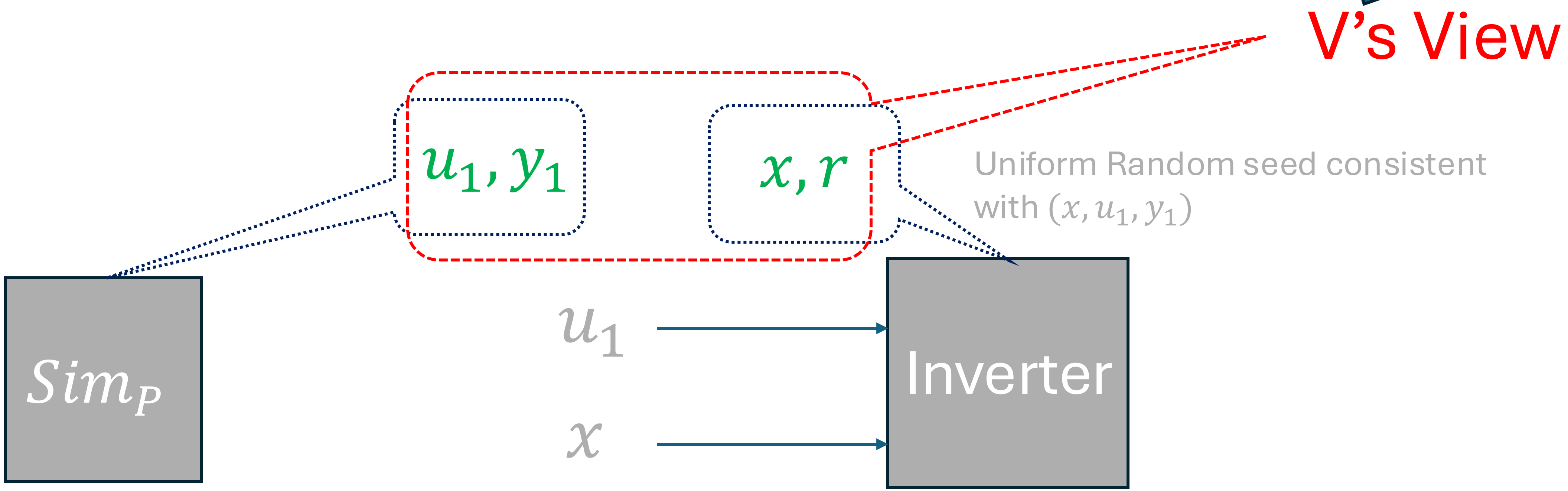
Distributional OWF Candidate:

$$F_1(x,r) = (x, V_1(x,r))$$

Contradict Assumption that L is hard on average

Decide language efficiently!

Suppose F_1 is not distributionally one-way

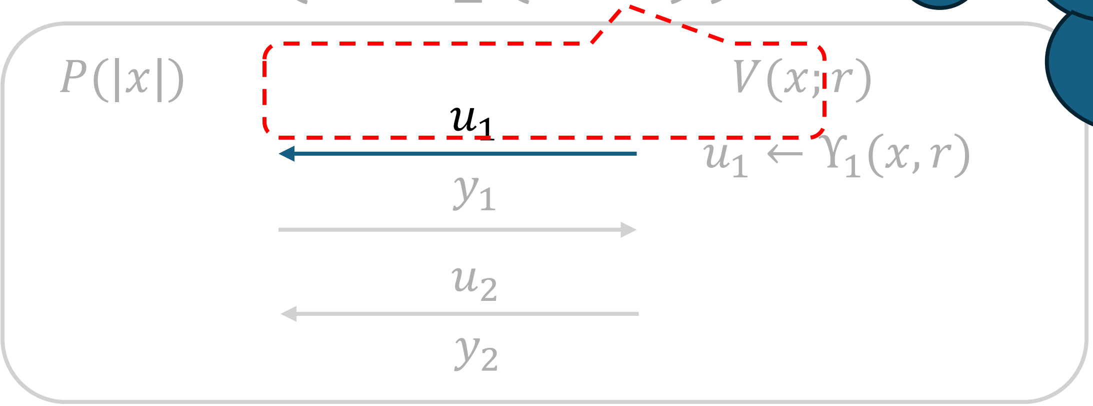


Avg-Hard 2-round Simulatable IHIP ⇒ Distributionally OWF

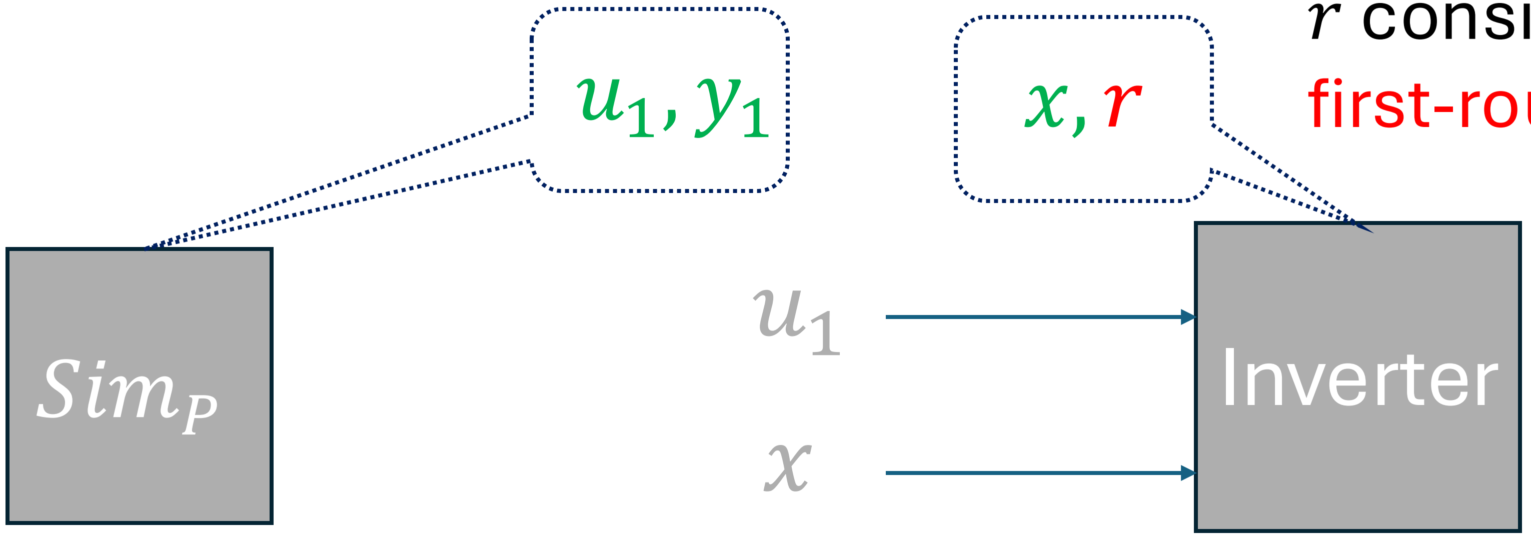
Distributional OWF Candidate:

$$F_1(x,r) = (x, \Upsilon_1(x,r))$$

First-round message



r consistent with only the first-round interaction

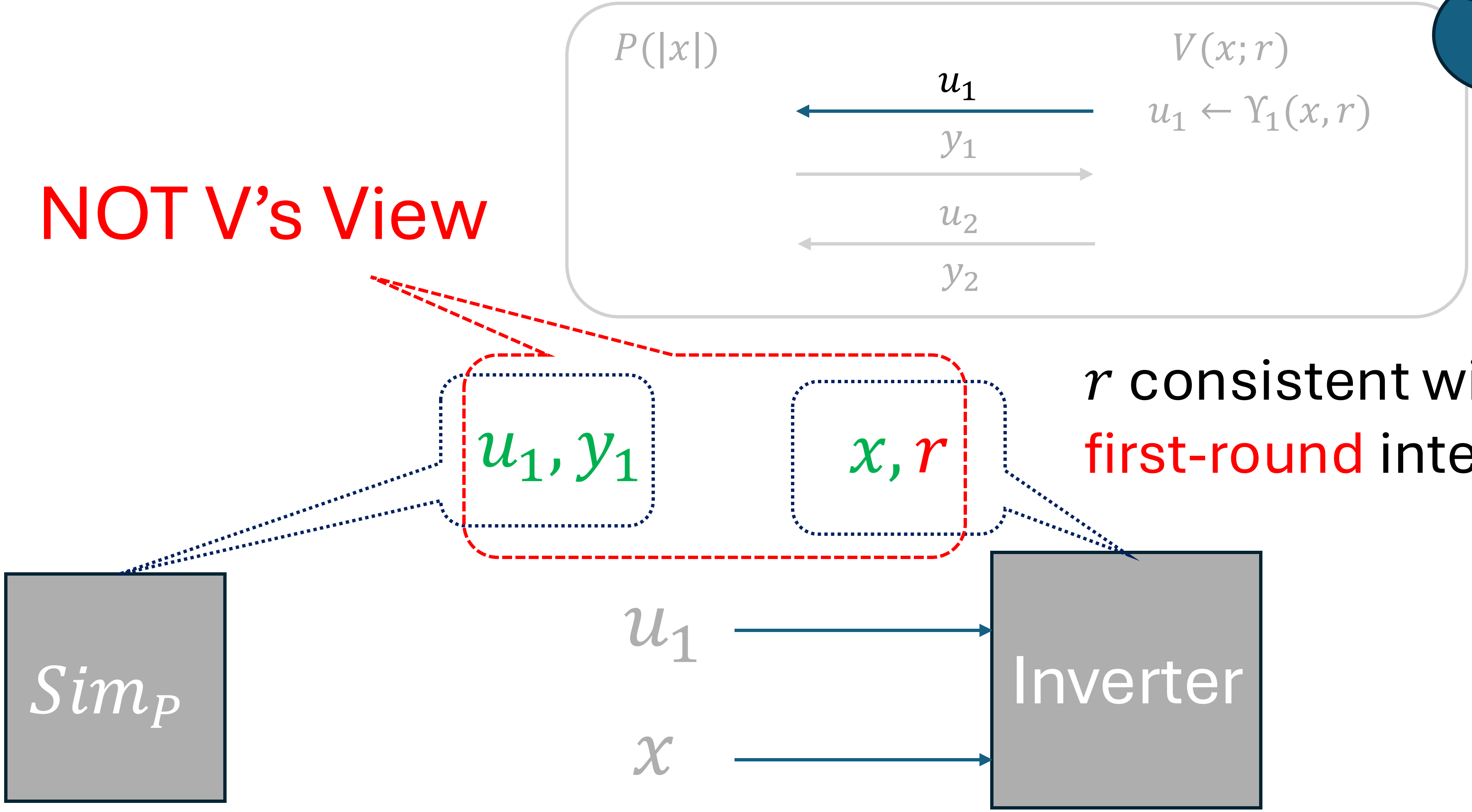


Avg-Hard 2-round Simulatable IHIP ⇒ Distributionally OWF

Distributional OWF Candidate:

$$F_1(x,r) = (x, \Upsilon_1(x,r))$$

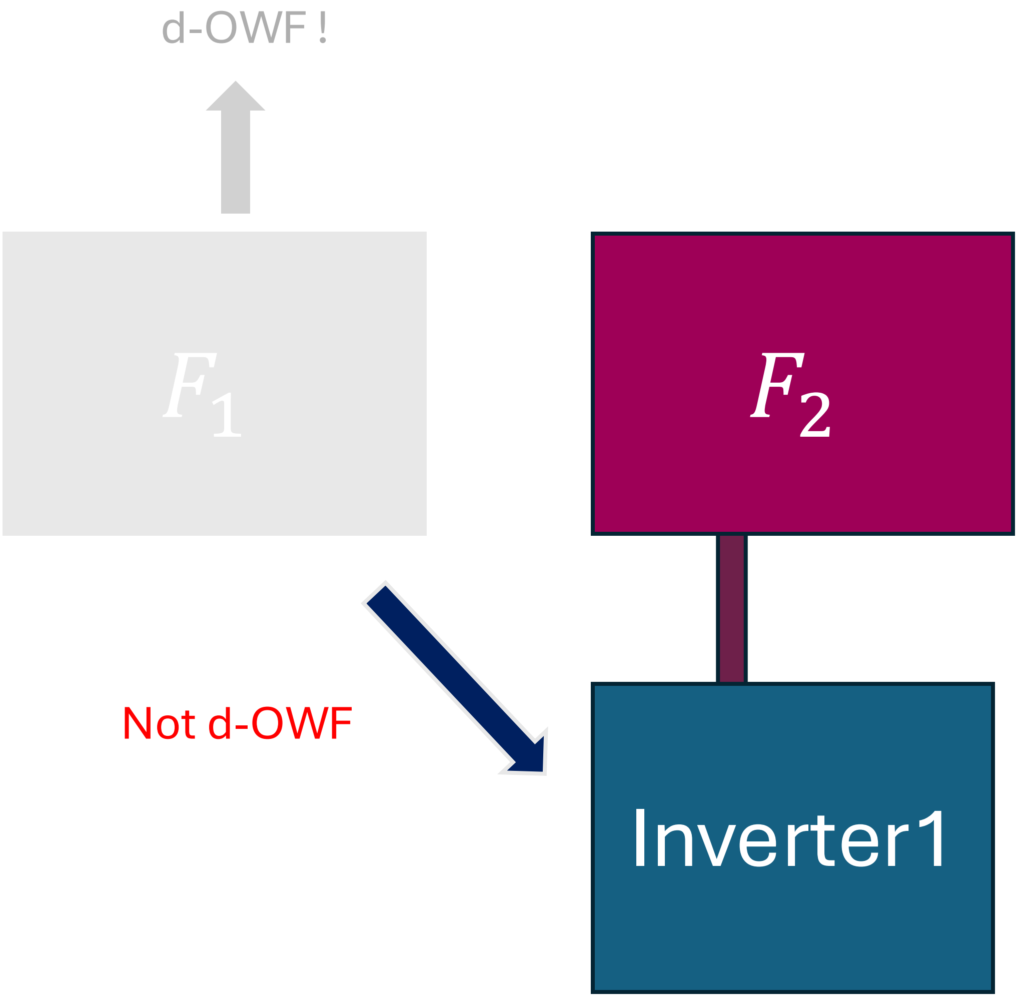
First-round message



r consistent with only the first-round interaction

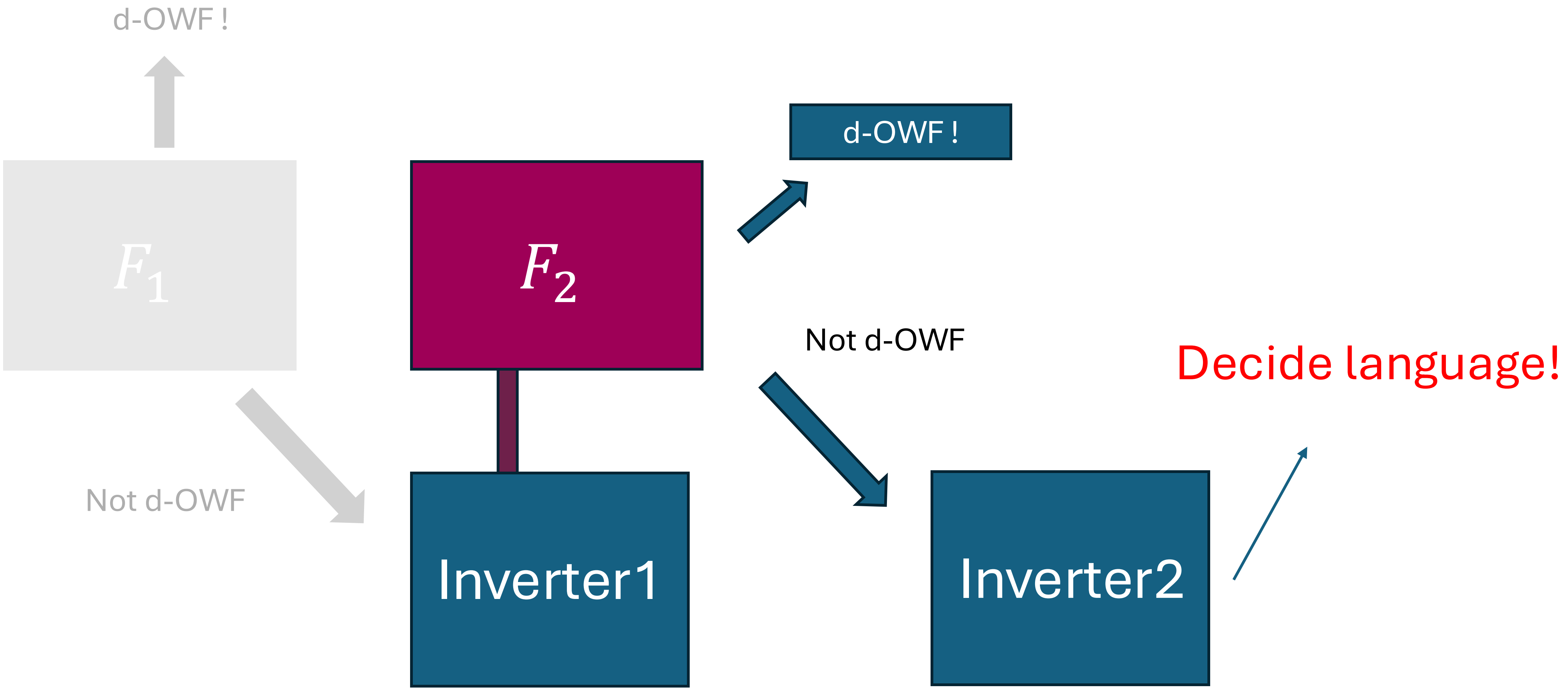
Avg-Hard 2-round Simulatable IHIP ⇒ Distributionally OWF

Use adversary for construction [Komargodski-Yogev18, Rothblum-Vasudevan22]



Avg-Hard 2-round Simulatable IHIP ⇒ Distributionally OWF

Use adversary for construction [Komargodski-Yogev18, Rothblum-Vasudevan22]



Main Results

Upper Bound

- ε-IHIP $\subseteq$ NP/Poly $\cap$ coNP/Poly
- ε-simulatable IHIP $\subseteq$ AM $\cap$ coAM

Hardness Implication

- Avg-Hard + constant-round IHIP ⇒ OWF*
- Worst-Hard + Simulatable-IHIP ⇒ OWF

Oracle Separation

- $\exists \mathcal{O},\ IHIP^{\mathcal{O}} \nsubseteq\ SZK^{\mathcal{O}}$

Closure Property

- IHIP is closed under polynomial circuit

Open Problems

- Are there natural complete problems for the class of languages that have instance-hiding proofs?

- Are there other cryptographic consequences of the existence of hard problems in this class, beyond one-way functions?

- What is power of computational instance-hiding interactive proof?
  - What is the correct definition?