Fiat–Shamir Bulletproofs are Non-Malleable (in AGM)

[1] Chaya Ganesh, [2] Claudio Orlandi, [2] **Mahak Pancholi**, [2] Akira Takahashi, and [3] Daniel Tschudi

1 INDIAN INSTITUTE OF SCIENCE भारतीय विज्ञान संस्थान

2 AARHUS UNIVERSITET

3 CONCORDIUM

This Work

- Concrete modular security analysis of simulation-extractability (SIM-EXT) for multi-round Fiat-Shamir NIZK ==> **non-malleability**
- First to show **Fiat-Shamir Bulletproofs** satisfy **SIM-EXT** in the AGM.

Zero-Knowledge Proofs

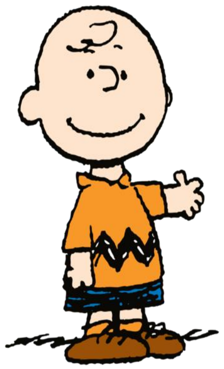
Claim: $(x, w) \in R$

Message: m_1 →

← Challenge c_1

↔

Message: m_r →



Prover

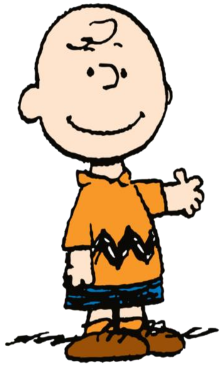
(x,w)

Verifier

x

Zero-Knowledge Proofs

Claim: $(x, w) \in R$



Message: m_1 →

← Challenge c_1

↔

Message: m_r →

Prover

(x,w)

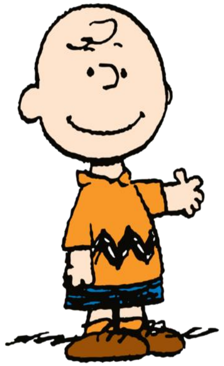
Verifier

x

- **Complete.**

Zero-Knowledge Proofs

Claim: $(x, w) \in R$



Message: m_1 →

Challenge c_1 ←

↔

Message: m_r →

Prover

(x,w)

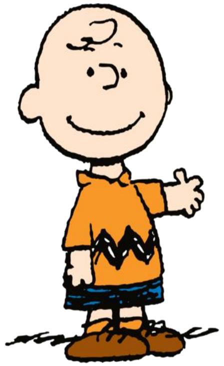
Verifier

x

- **Complete.**
- **Proof of knowledge**: There exists an extractor that can extract a witness.

Zero-Knowledge Proofs

Claim: $(x, w) \in R$



Message: m_1 →

Challenge c_1 ←

↔

Message: m_r →

Prover

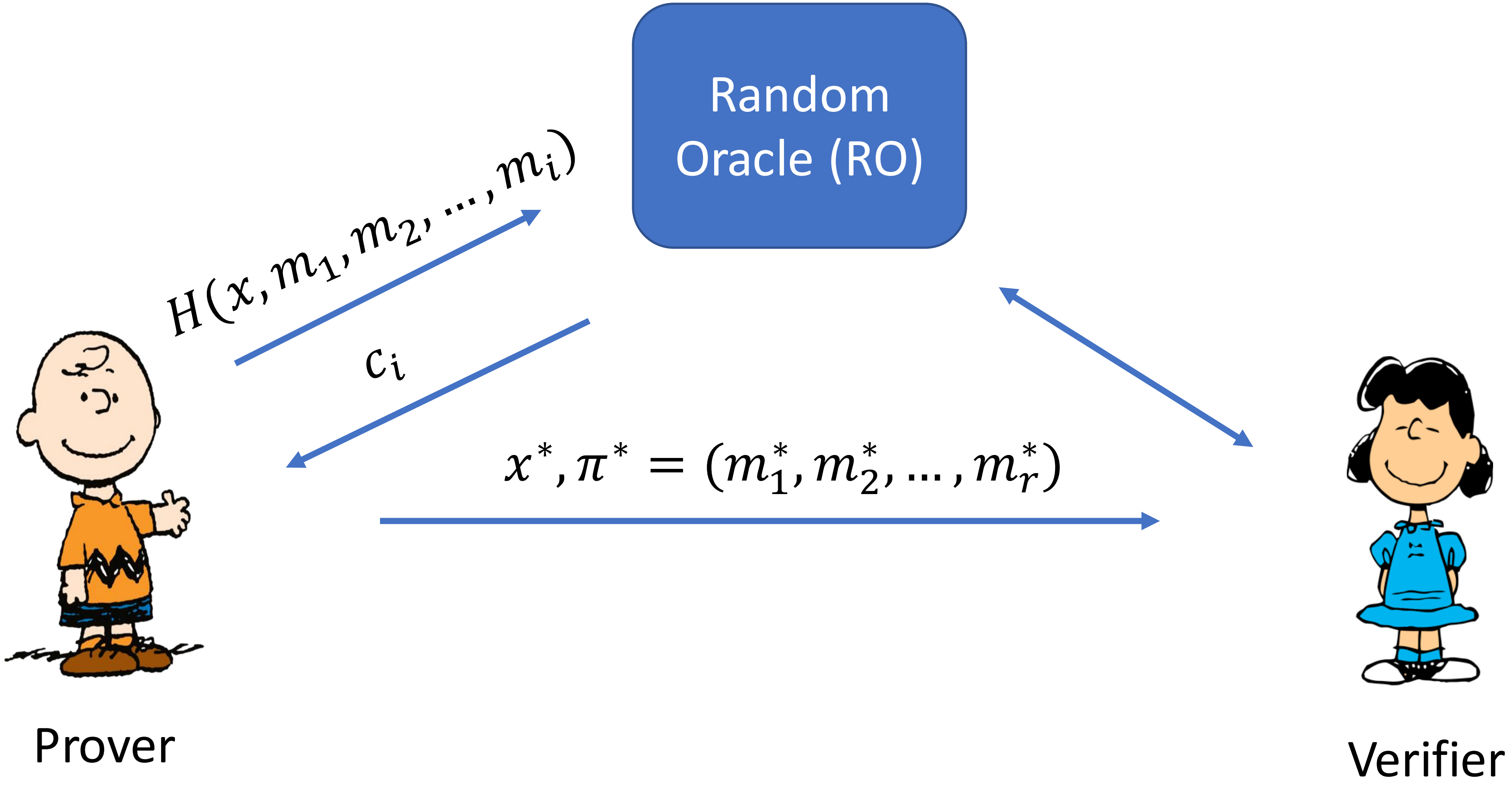
(x,w)

Verifier

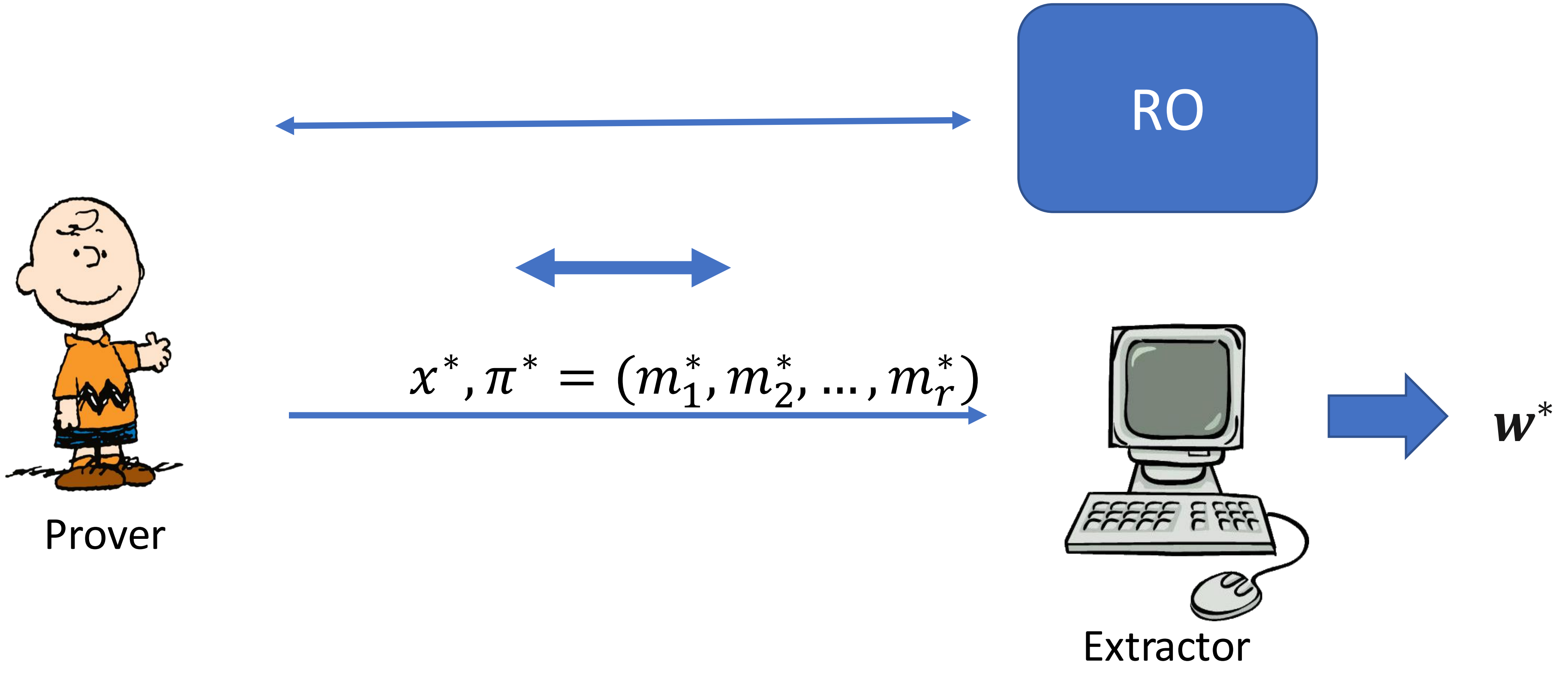
x

- **Complete.**
- **Proof of knowledge**: There exists an extractor that can extract a witness.
- **Zero-Knowledge**: There exists a simulator that can simulate corrupt Verifier's view.

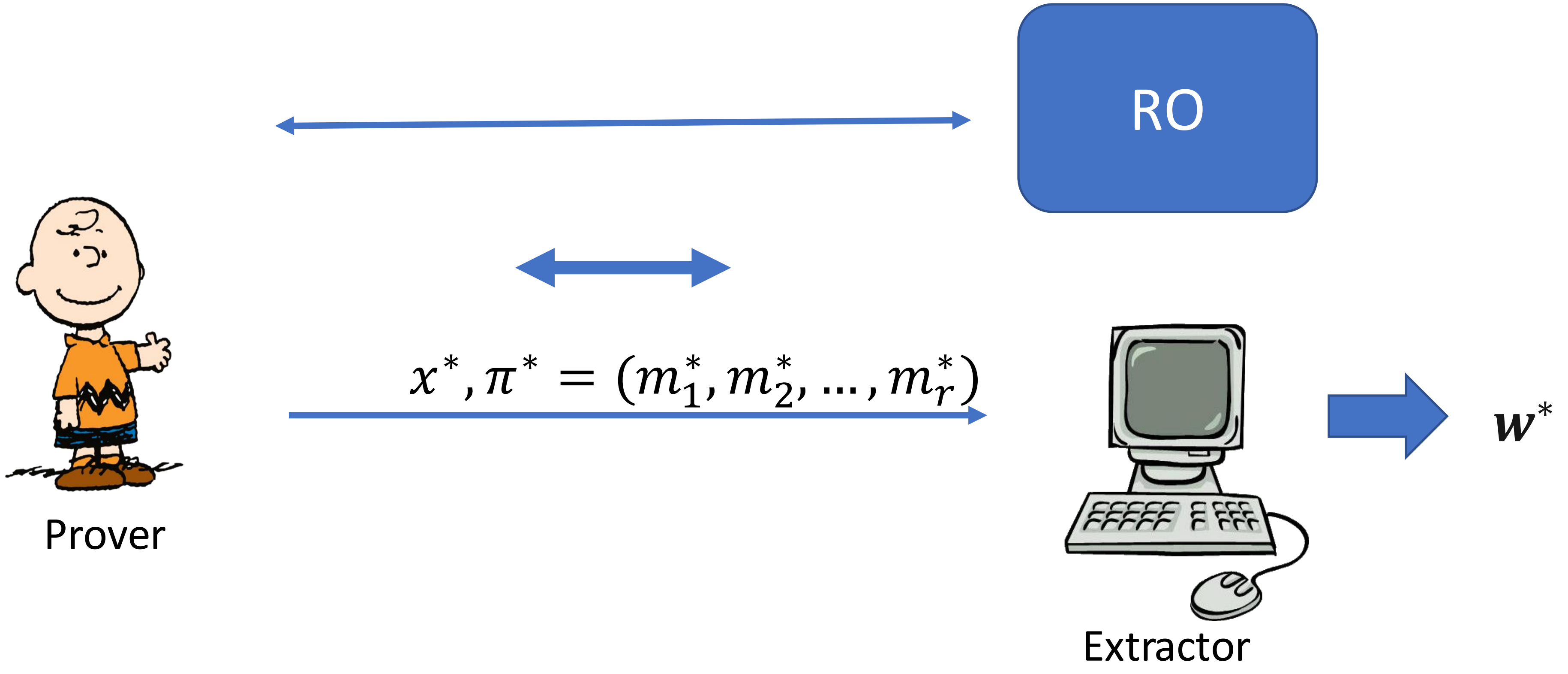
NIZK via Fiat-Shamir Transform



Proof of Knowledge (FS-EXT)



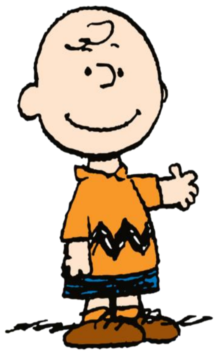
Proof of Knowledge (FS-EXT)



$$((x^*, \pi^*)\ verifies\ ) \implies (x^*, w^*) \in R$$

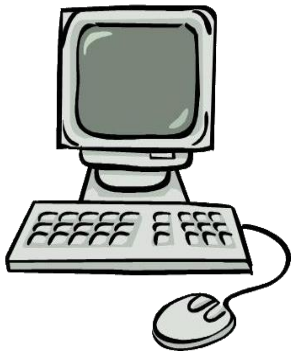
Proof of Knowledge (FS-EXT)

RO



Prover

$x^*, \pi^* = (m_1^*, m_2^*, \dots, m_r^*)$



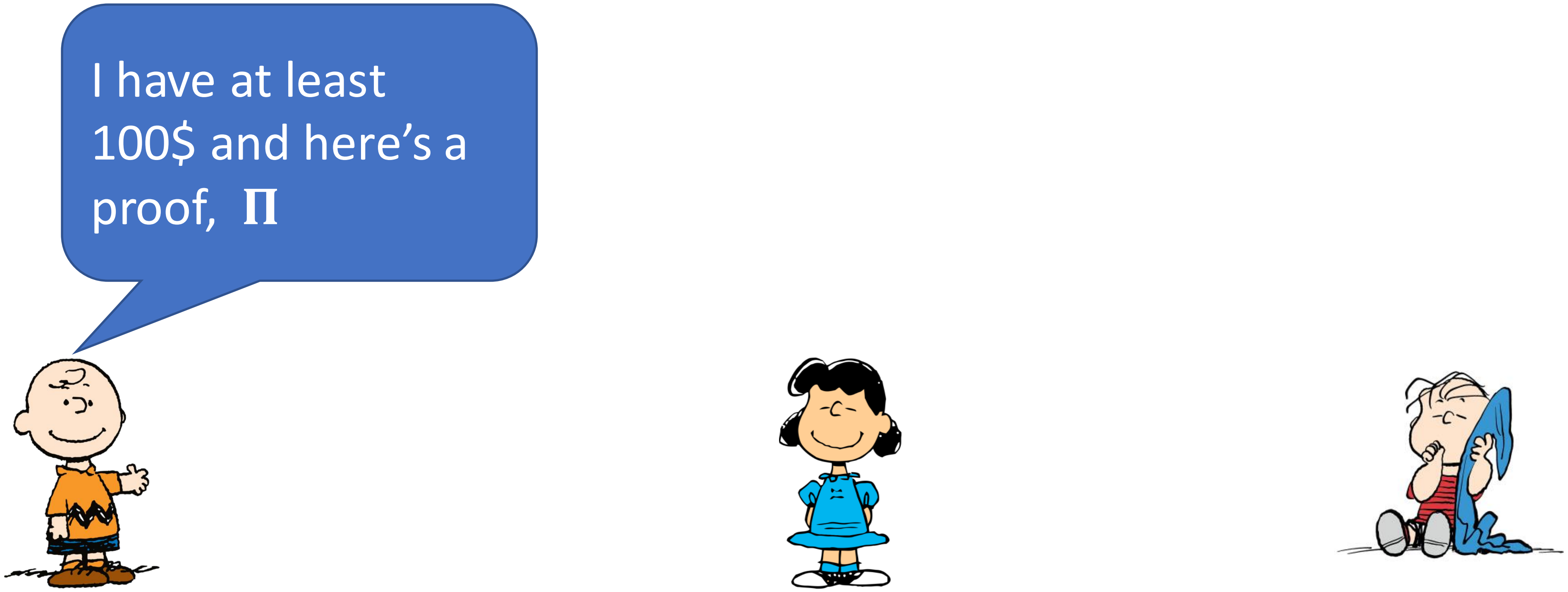
Extractor

$\boldsymbol{w^*}$

$$\boldsymbol{((x^*, \pi^*)\ verifies\ ) \implies (x^*, w^*) \in R}$$

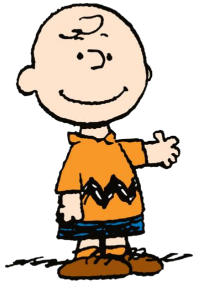
Is extraction enough?

Why is Extraction not enough?



Why is Extraction not enough?

I have at least 100$ and here's a proof, $\boldsymbol{\Pi}$

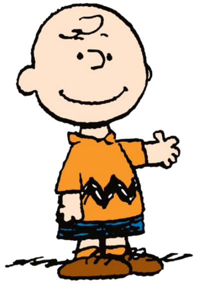


I also have at least 100$ and here's a proof, $\boldsymbol{\Pi}^*$

$\Pi^* \leftarrow \mathrm{Maul}(\Pi)$

Why is Extraction not enough?

I have at least 100$ and here's a proof, $\boldsymbol{\Pi}$

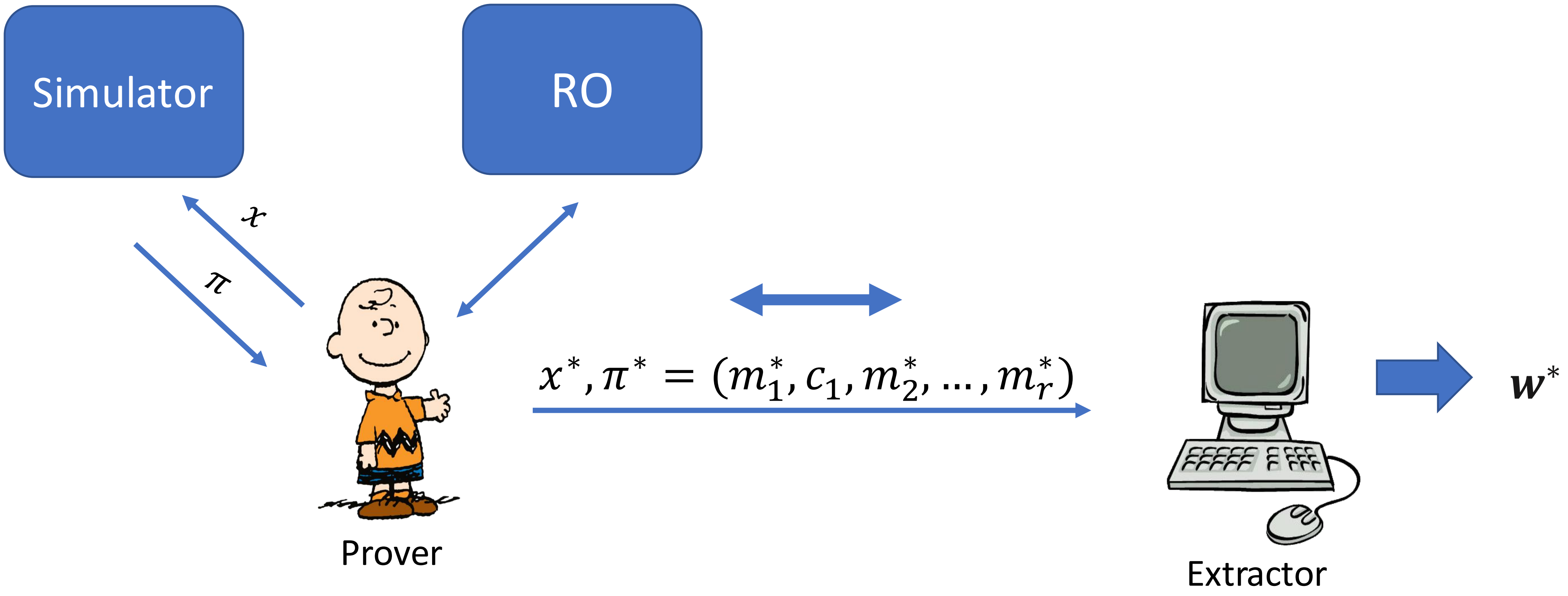


I also have at least 100$ and here's a proof, $\boldsymbol{\Pi}^*$

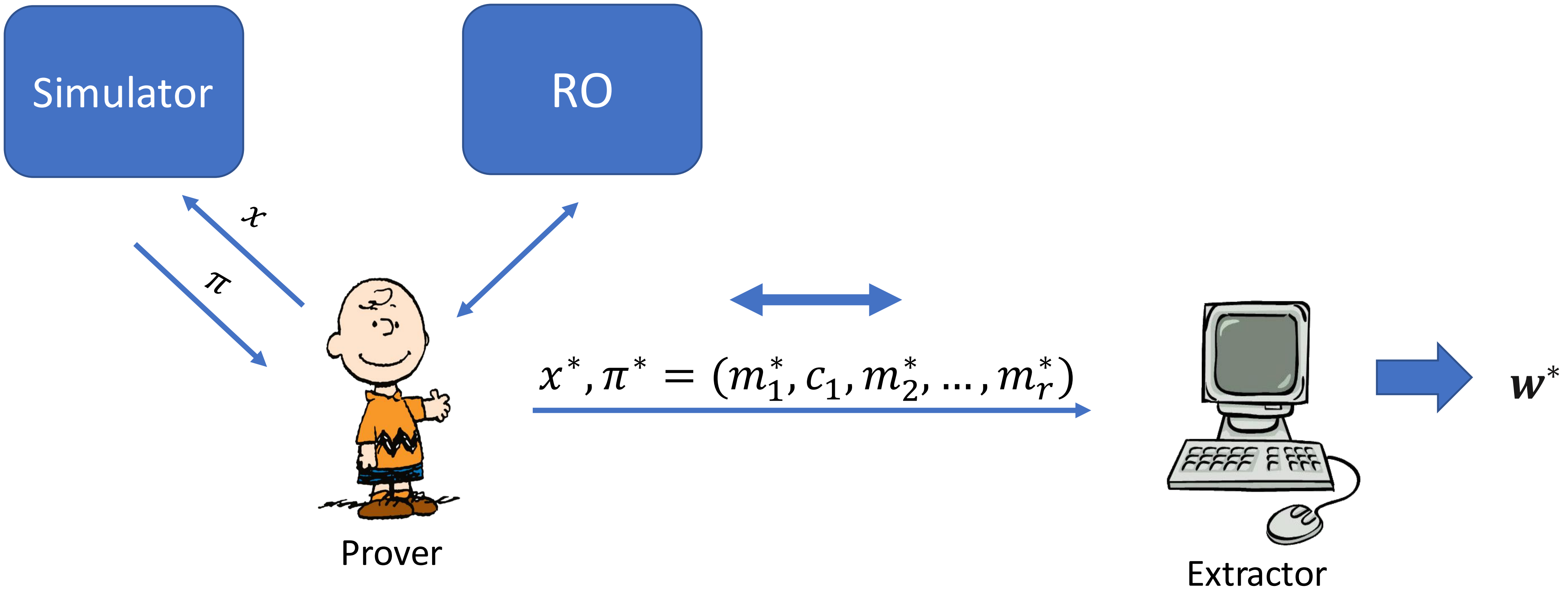
$$\Pi^* \leftarrow \mathrm{Maul}(\Pi)$$

I trust Lucy

Simulation Extractability (FS-SIMEXT)



Simulation Extractability (FS-SIMEXT)



$$((\boldsymbol{x}^*, \boldsymbol{\pi}^*)\ \boldsymbol{verifies} \wedge (\boldsymbol{x}^*, \boldsymbol{\pi}^*) \notin \boldsymbol{Q_s}) \implies (\boldsymbol{x}^*, \boldsymbol{w}^*) \in \boldsymbol{R}$$

Why Bulletproofs (BP)?

[BBB+17]

- Public-coin, transparent setup
- Extremely efficient
- Real world applications (Monero, MobileCoin…)

Why Bulletproofs (BP)?

[BBB+17]

- Public-coin, transparent setup
- Extremely efficient
- Real world applications (Monero, MobileCoin…)
- Challenge: Non-constant rounds

FS-SIMEXT for BP

- Challenge: Non-constant rounds
- Ghoshal and Tessaro [GT21]:
  - Online extraction for FS(BP).
  - In the Algebraic Group Model (AGM) and **just extraction**.

Online Extraction

- A stronger variant.

Online Extraction

- A stronger variant.
- Extractor runs with the adversary. No need for rewinding.

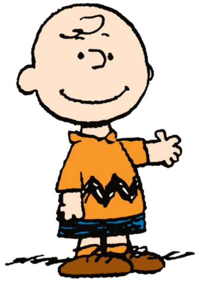
Online Extraction

- A stronger variant.
- Extractor runs with the adversary. No need for rewinding.
- In this work, we assume AGM:

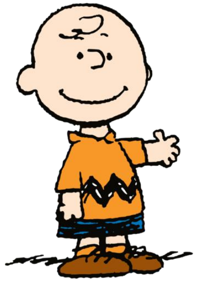
$(y, e_1, e_2, \dots, e_n) \leftarrow A_{alg}(g_1, g_2, \dots, g_n)$ such that $y = \mathrm{g}_1^{e_1} \times \cdots \times \mathrm{g}_\mathrm{n}^{e_n}$

Online Extraction (FS-EXT)

Real

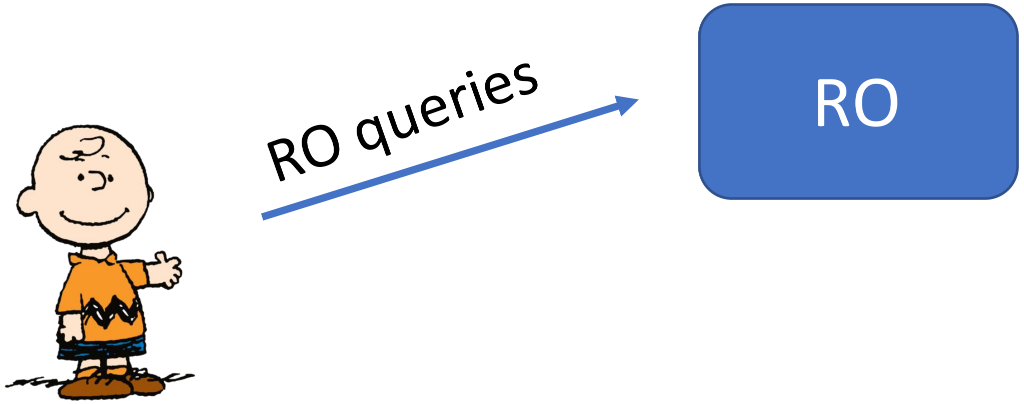


Ideal

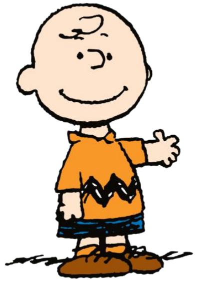


Online Extraction (FS-EXT)

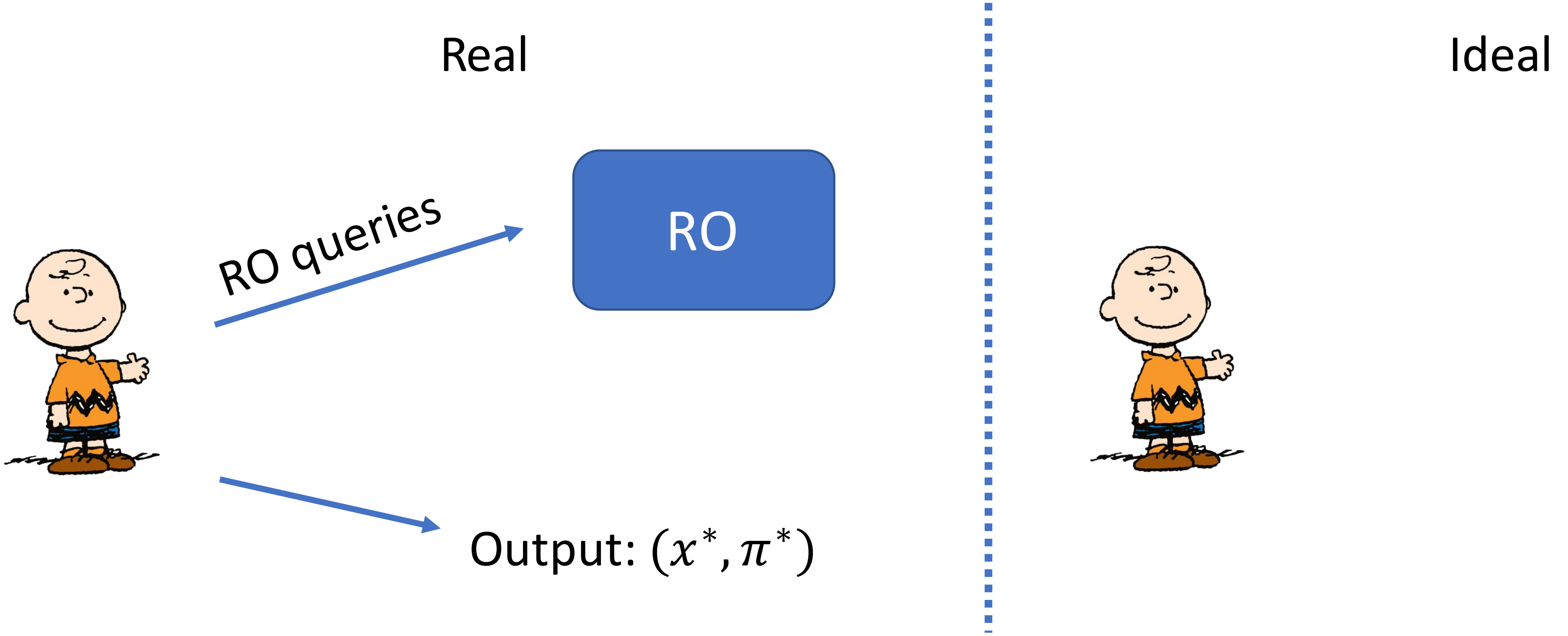
Real



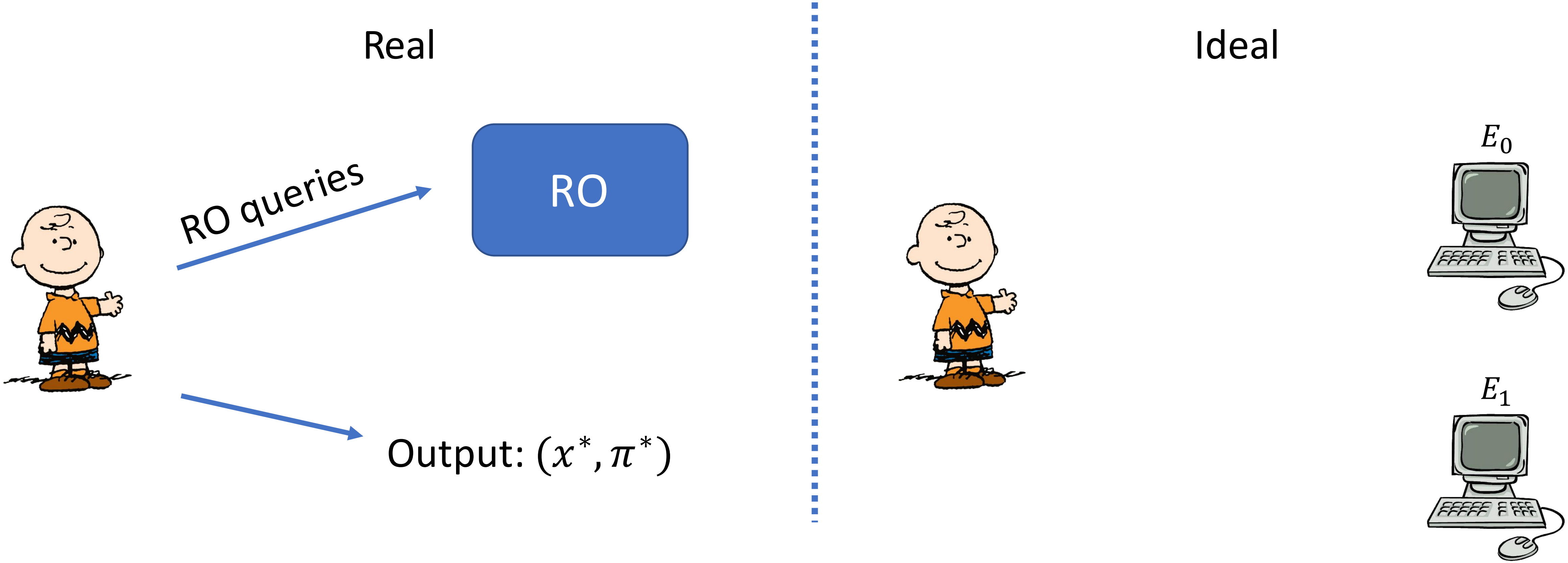
Ideal



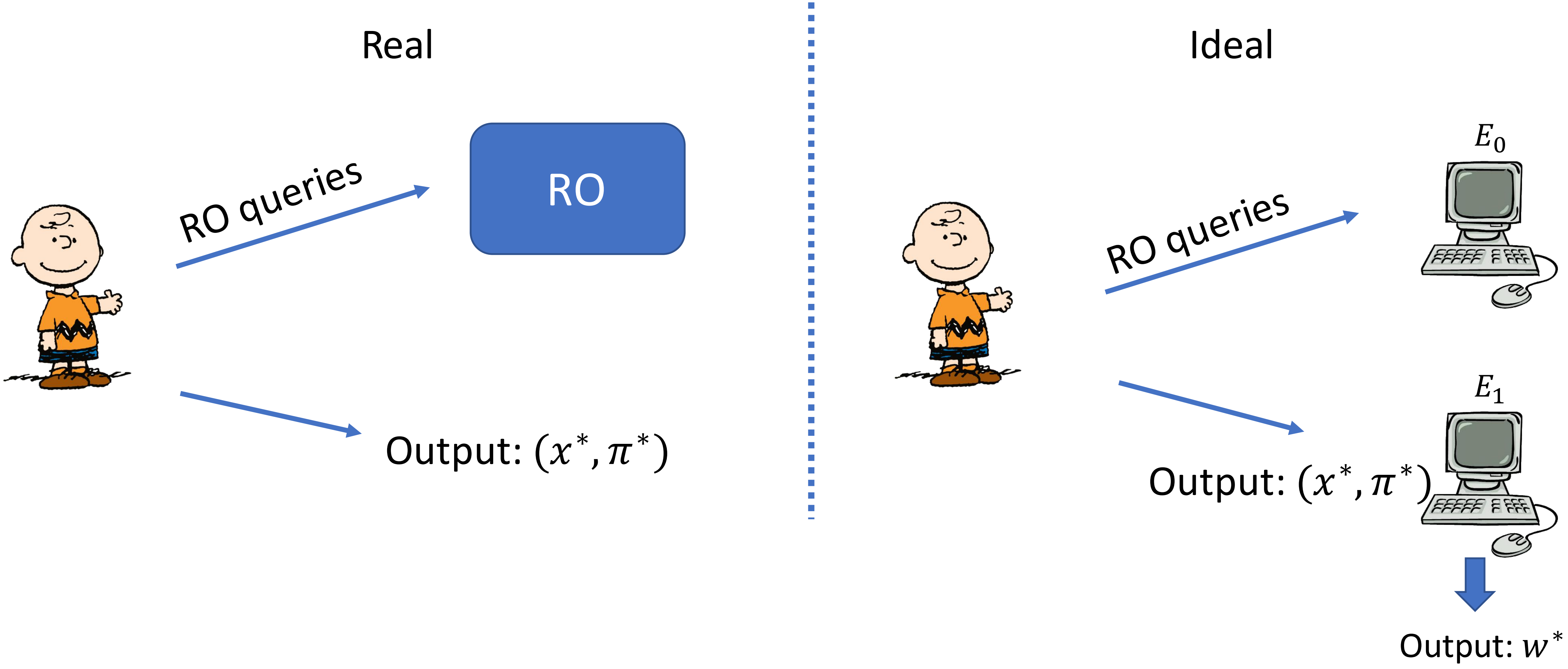
Online Extraction (FS-EXT)



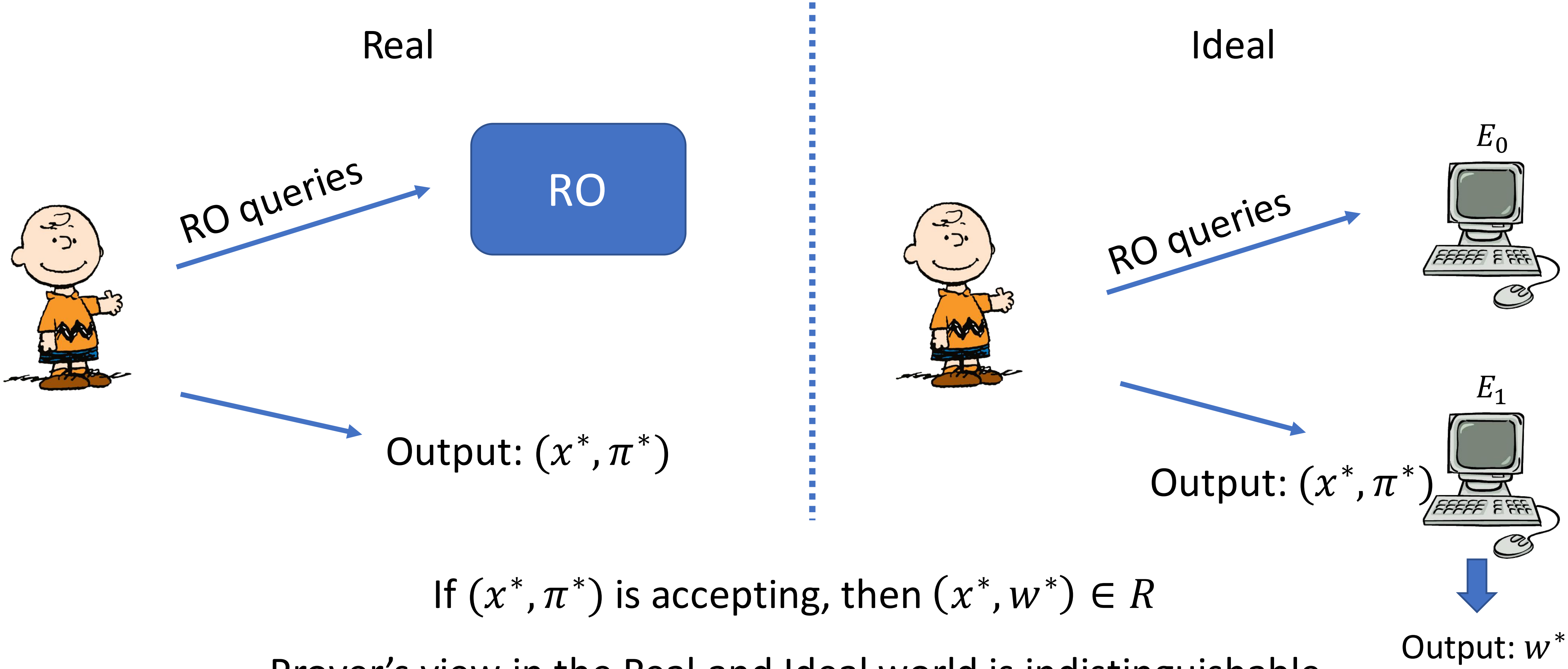
Online Extraction (FS-EXT)



Online Extraction (FS-EXT)



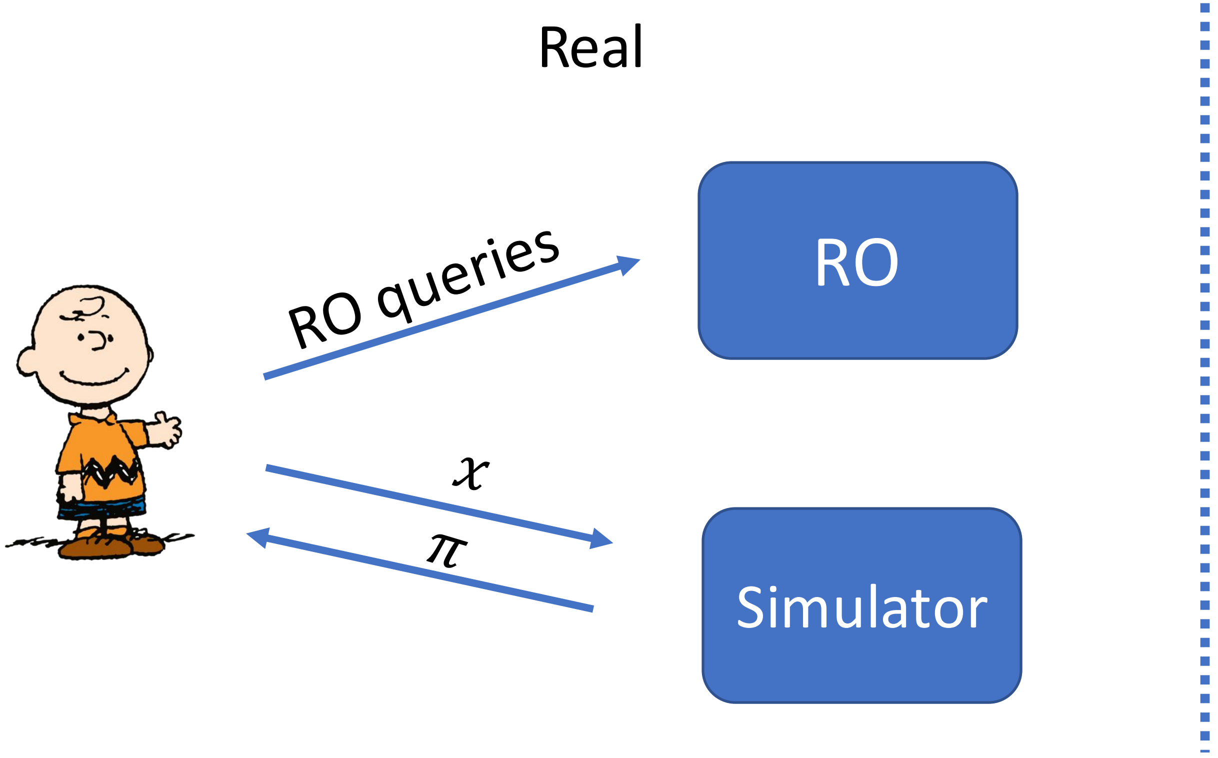
Online Extraction (FS-EXT)



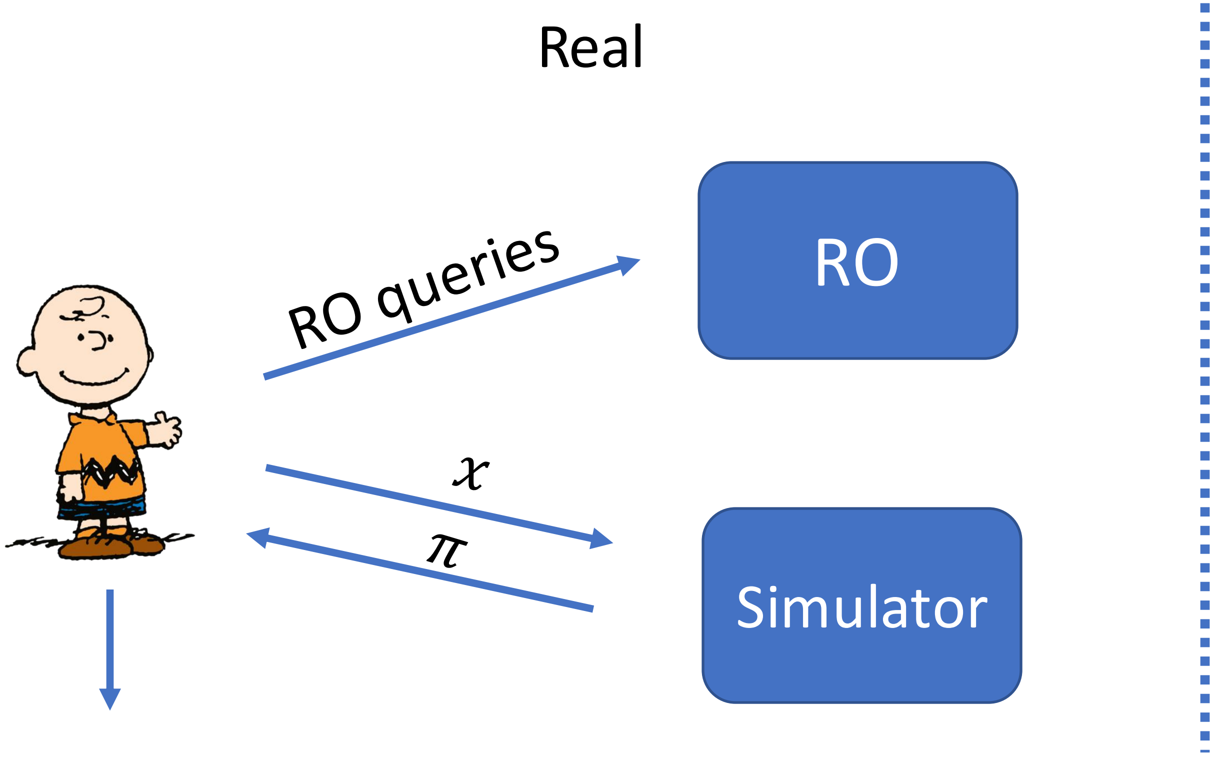
If (x^*, π^*) is accepting, then $(x^*, w^*) \in R$

Prover's view in the Real and Ideal world is indistinguishable

Online FS-SIMEXT

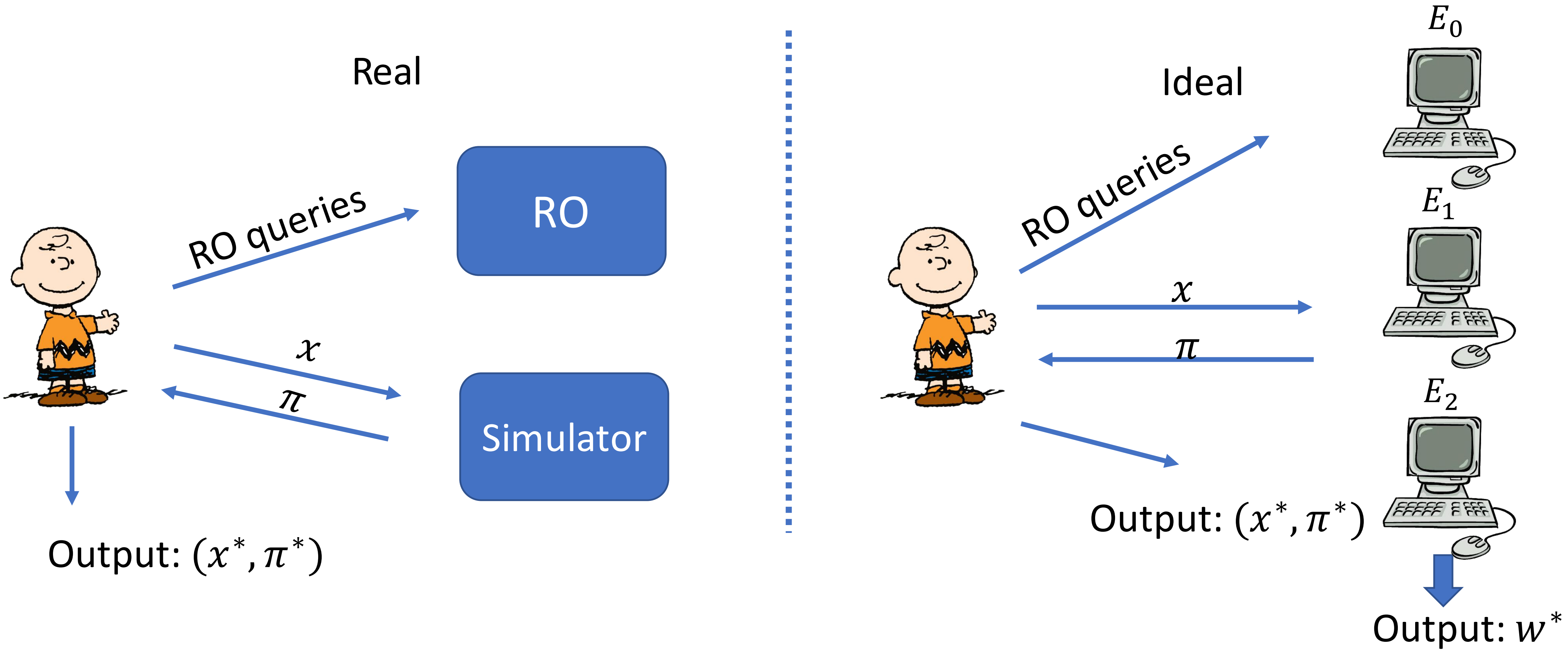


Online FS-SIMEXT

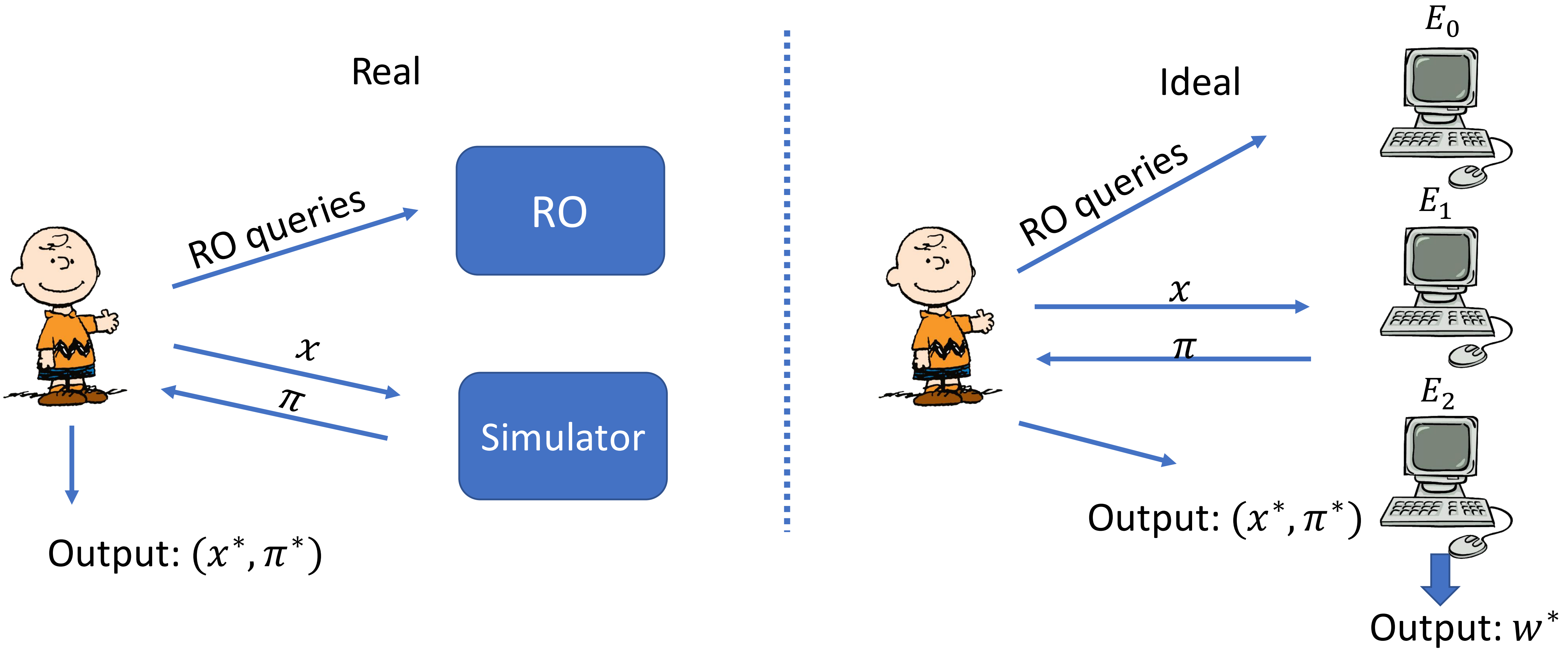


Output: (x^*, π^*)

Online FS-SIMEXT



Online FS-SIMEXT



If (x^*, π^*) is accepting **and** $(\boldsymbol{x}^*, \boldsymbol{\pi}^*)$ **was not queried**, then $(x^*, w^*) \in R$

Prover's view in the Real and Ideal world is indistinguishable

General Recipe

[FKMV12,GKK+21]

- Simulator gives **no extra power** to the adversary.

General Recipe

[FKMV12,GKK+21]

- Simulator gives **no extra power** to the adversary.

- Rely on **extractability** of FS(Π).

General Recipe

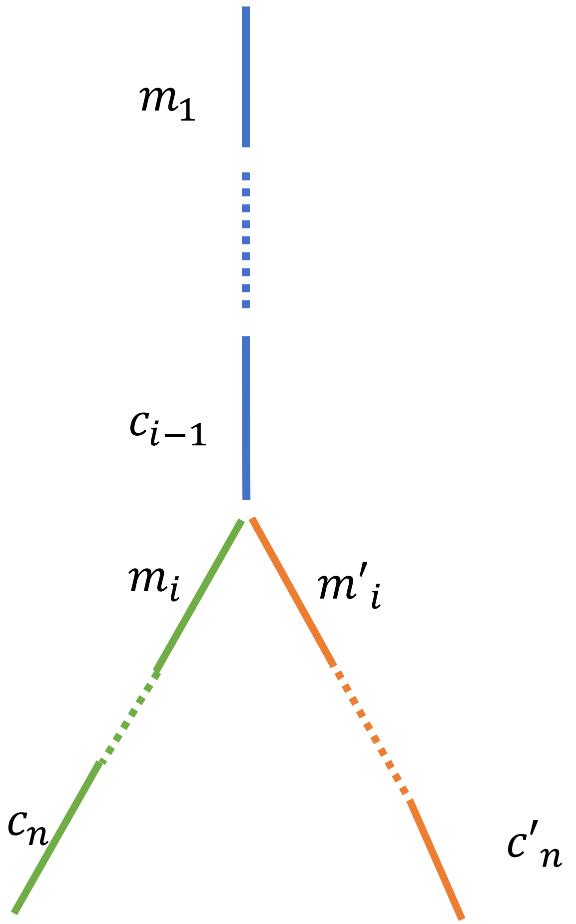
[FKMV12,GKK+21]

- Simulator gives **no extra power** to the adversary.
- Rely on **extractability** of FS(Π).
- Use **unique response** for FS(Π).

General Recipe

[FKMV12,GKK+21]

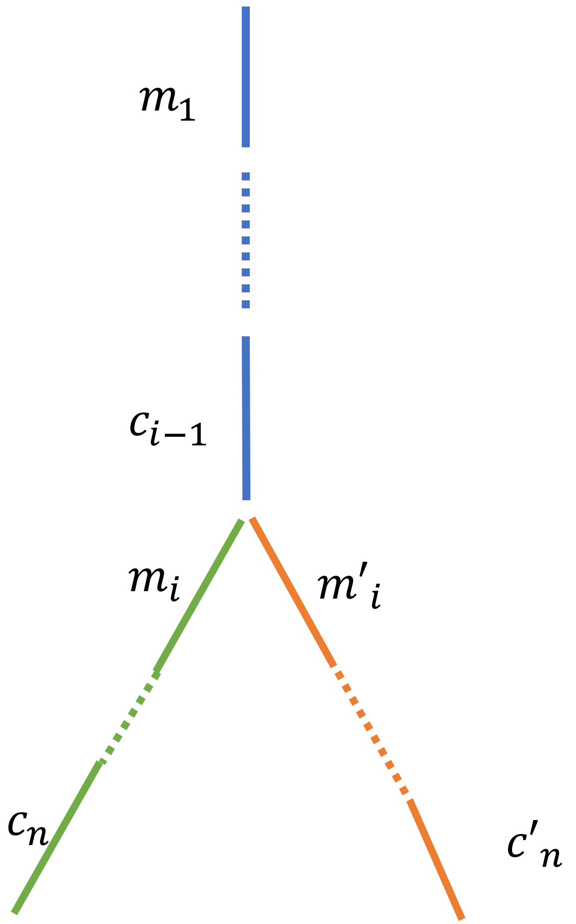
- Simulator gives **no extra power** to the adversary.
- Rely on **extractability** of FS(Π).
- Use **unique response** for FS(Π).



General Recipe

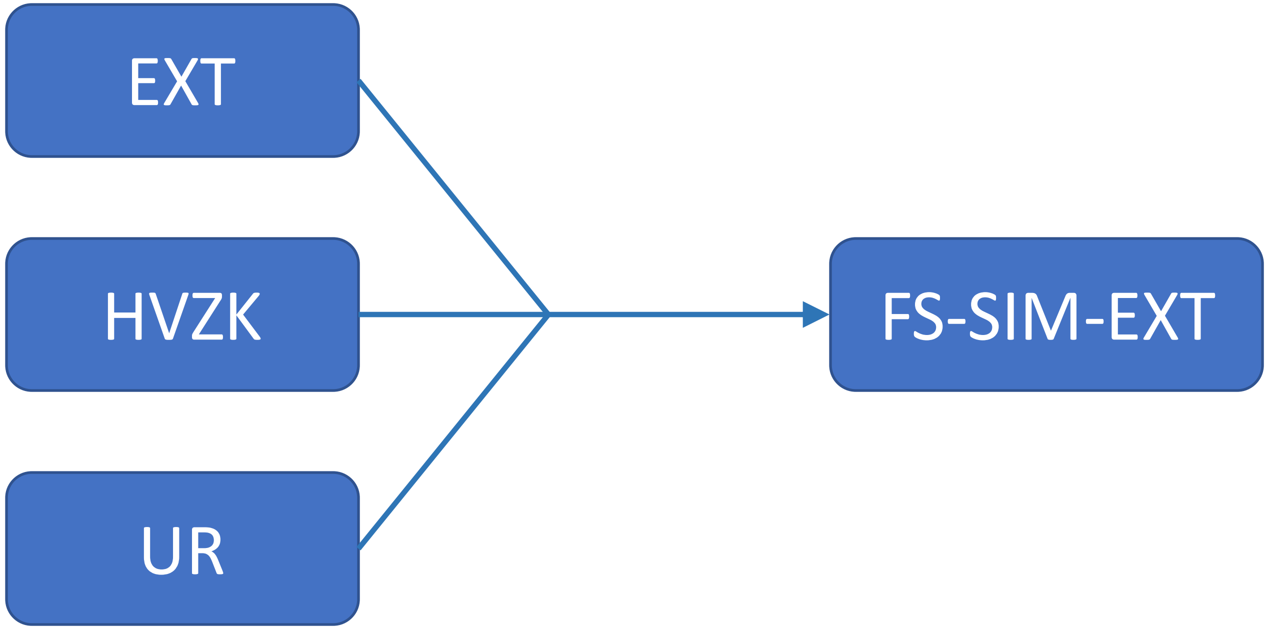
[FKMV12,GKK+21]

- Simulator gives **no extra power** to the adversary.
- Rely on **extractability** of FS(Π).
- Use **unique response** for FS(Π).
- → Adversary cannot reuse simulated transcript.



General Recipe

[FKMV12,GKK+21]



Proof: If the forged proof shares a prefix with one of the simulated transcripts, reduce it to UR property. Else, use the Extractor.

Missing Pieces

Is Non-interactive Bulletproofs:

- **Online Extractable**?
- **Unique Response**?

Is Non-interactive Bulletproofs Extractable?

Tight State-Restoration Soundness in the Algebraic Group Model*

Ashrujit Ghoshal and Stefano Tessaro

Paul G. Allen School of Computer Science & Engineering
University of Washington, Seattle, USA
{ashrujit,tessaro}@cs.washington.edu

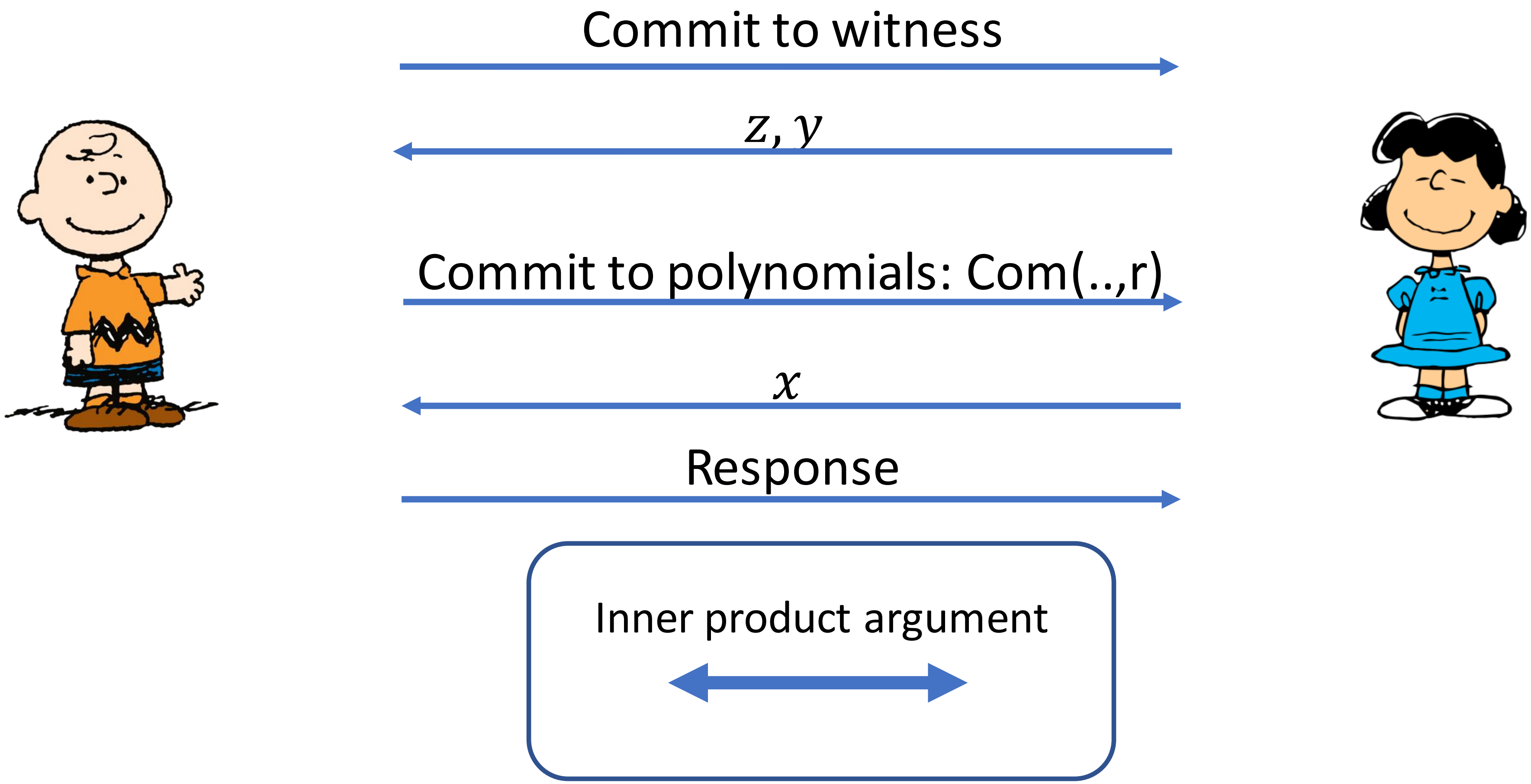
Result: FS(BP) is online extractable in the AGM.

Missing Pieces

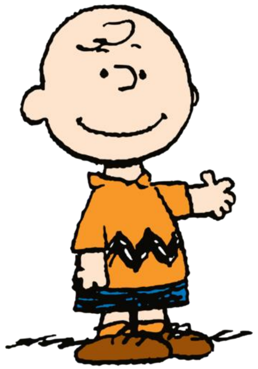
Is Non-interactive Bulletproofs:

- Online Extractable?
- **Unique Response**?

Bulletproofs.RngPf



Bulletproofs.RngPf



Commit to witness

z, y

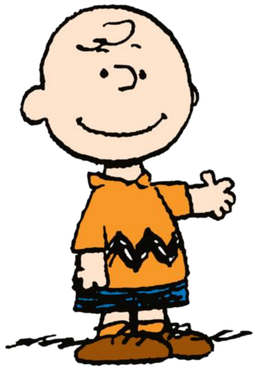
Commit to polynomials: Com(..,r)

x

Response

Inner product argument

Bulletproofs.RngPf



Commit to witness

z, y

Commit to polynomials: Com(..,r)

x

Response

Inner product argument

Any protocol with an **intermediate randomized round** cannot have unique responses.

Defining Weak UR (SR-UR)

- We want: Adversary should **not reuse a simulated transcript**.

Defining Weak UR (SR-UR)

- We want: Adversary should **not reuse a simulated transcript**.
- Existing UR definitions are too strong.

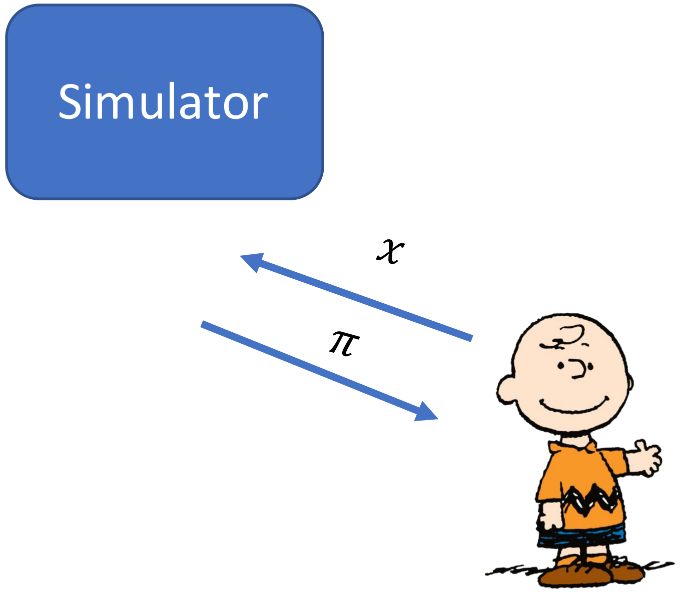
Defining Weak UR (SR-UR)

- We want: Adversary should **not reuse a simulated transcript**.
- Existing UR definitions are too strong.
- One of the transcripts can be fixed!
  - Given honest $\pi = (m_1, c_{1,} \ldots, m_i, c_i, \ldots)$, it is hard to come up with $\pi' = (m_1 \ , c_{1,} \ldots,$ $m_i', c_i', \ldots)$.

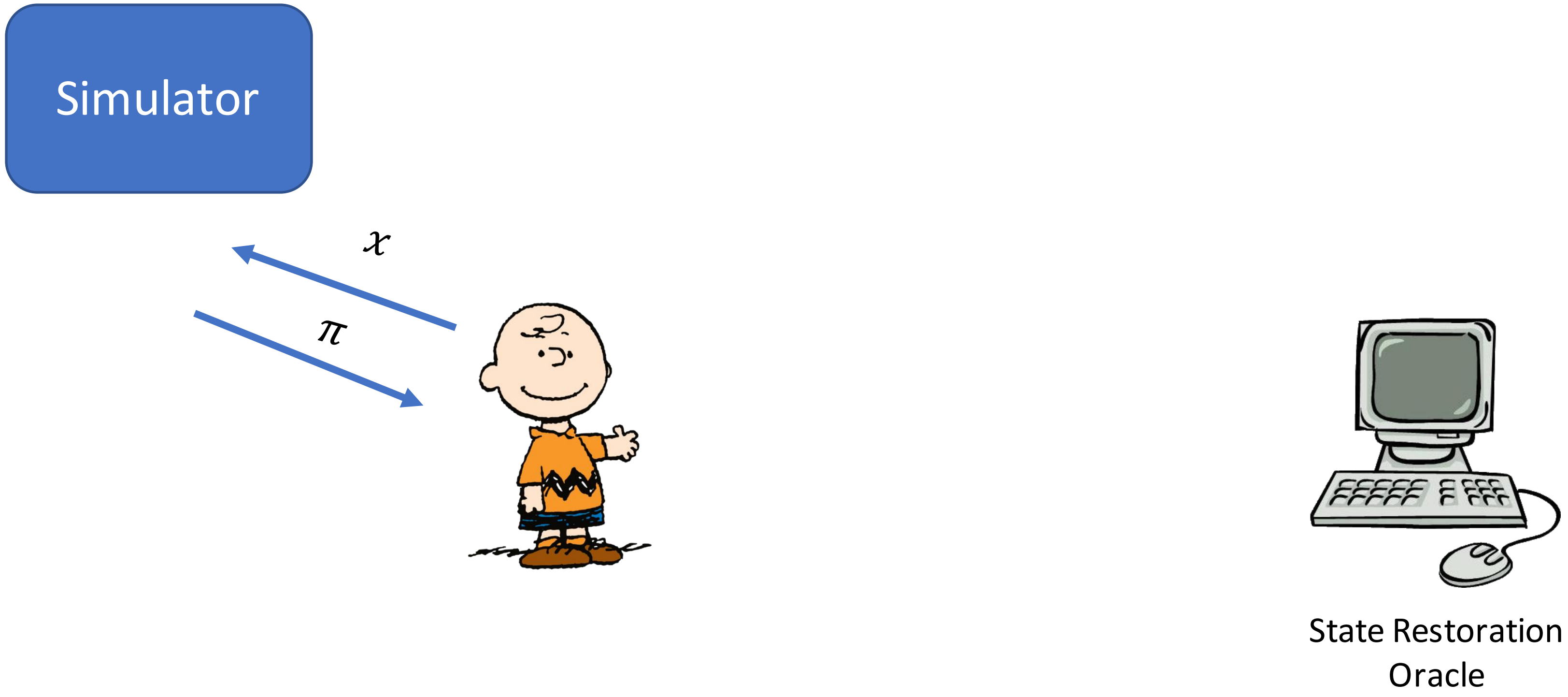
Defining Weak UR (SR-UR)

- We want: Adversary should **not reuse a simulated transcript**.
- Existing UR definitions are too strong.
- One of the transcripts can be fixed!
  - Given honest $\pi = (m_1, c_{1,} \ldots, m_i, c_i, \ldots)$, it is hard to come up with $\pi' = (m_1\ , c_{1,}\ \ldots, m_i',$ $c_i', \ldots)$.
- Interactive version is inspired from State restoration soundness definition [BCS16].

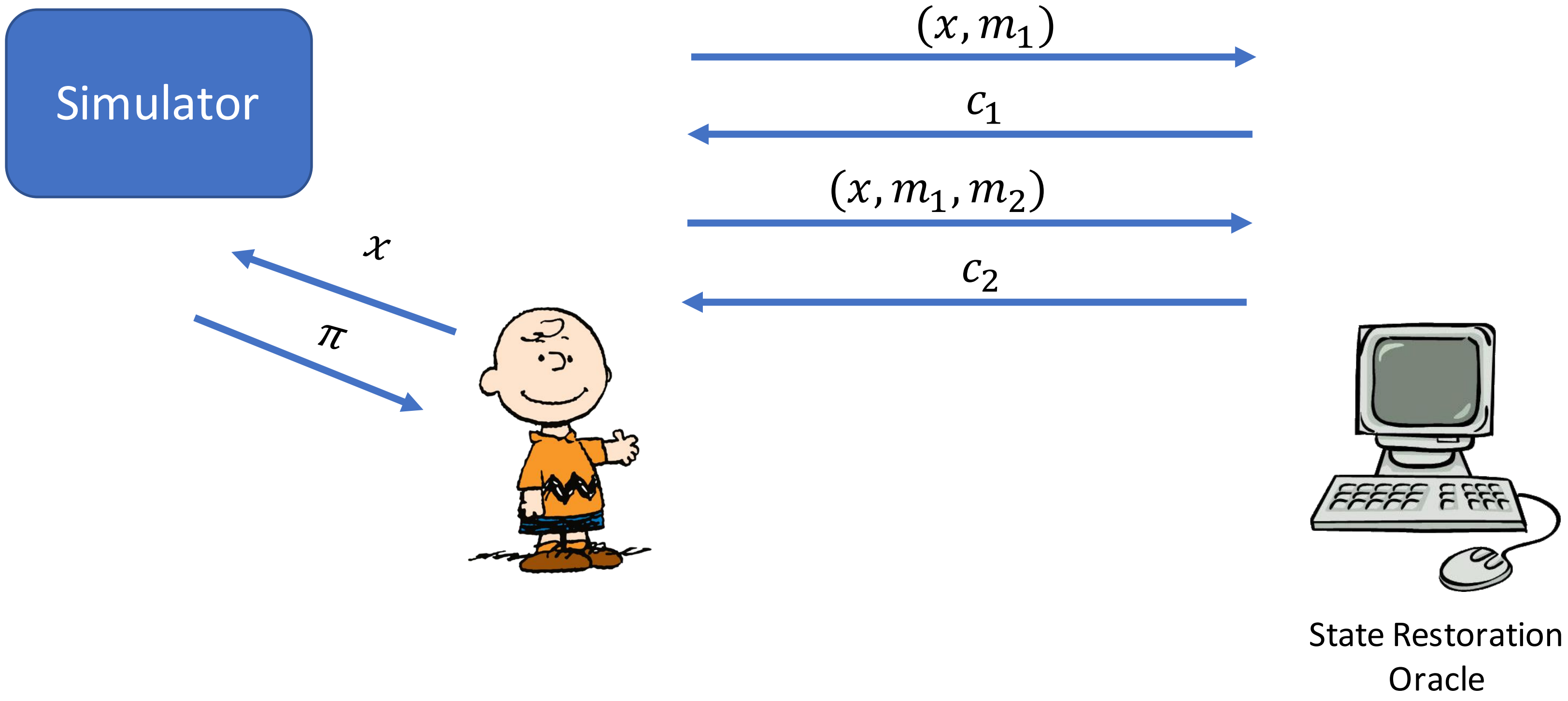
Defining Weak UR (SR-UR)



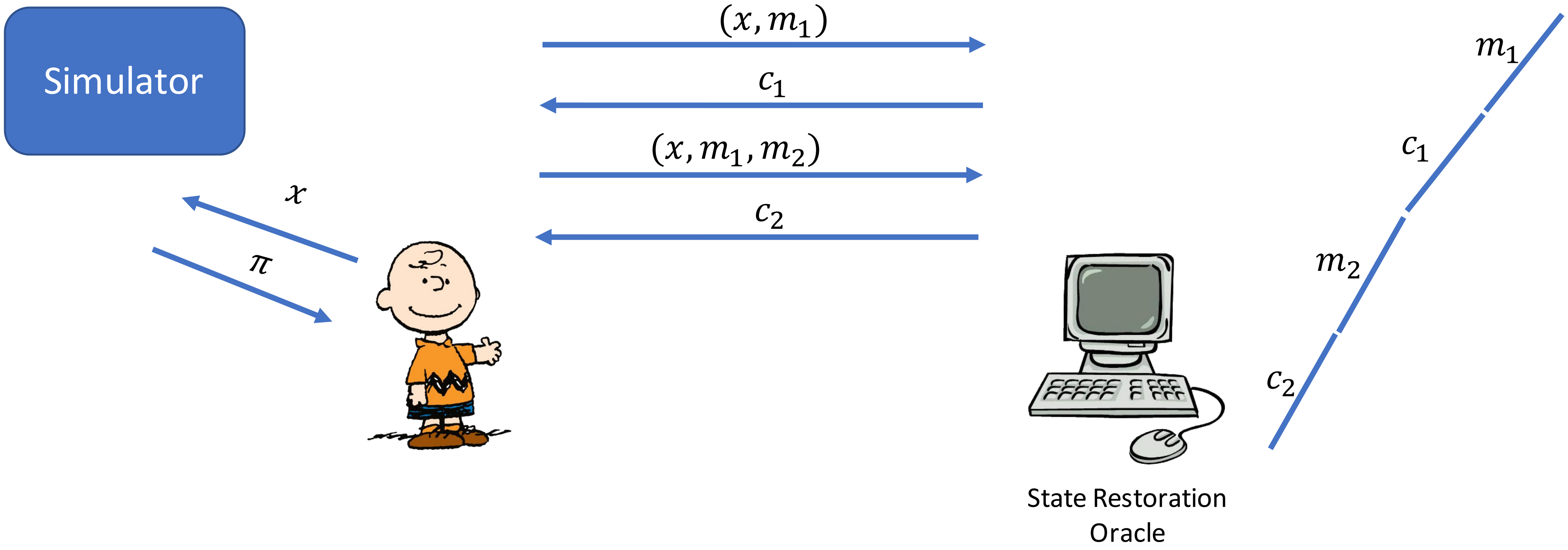
Defining Weak UR (SR-UR)



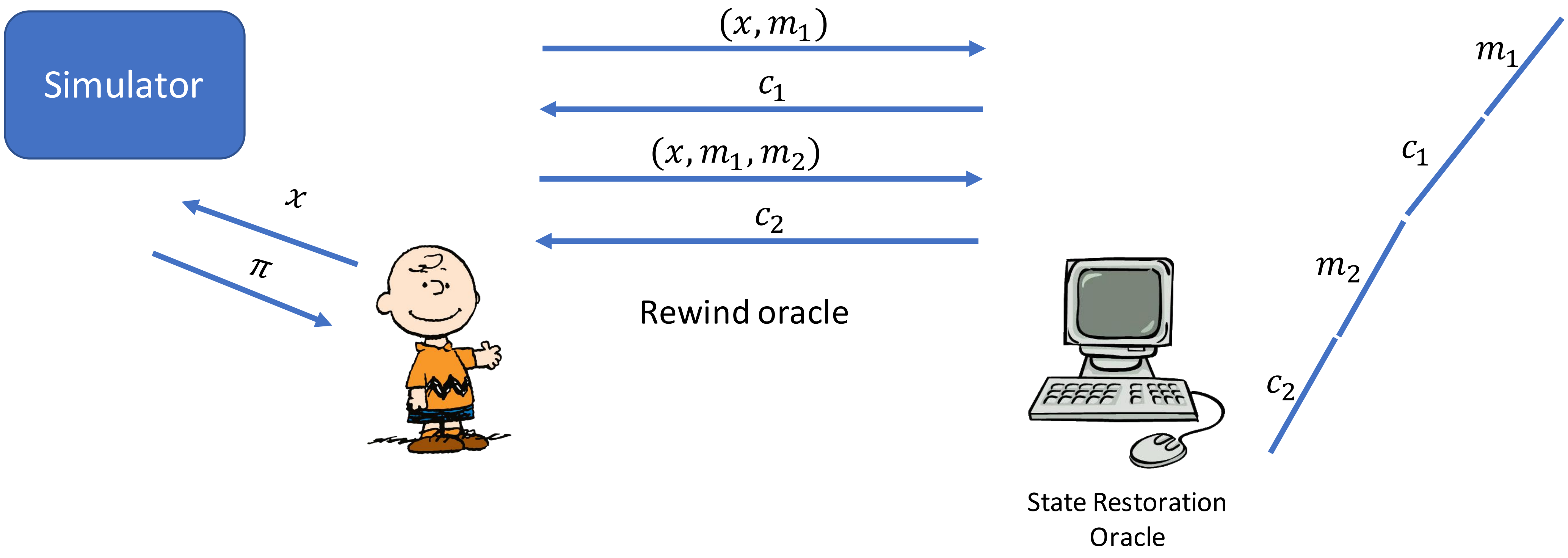
Defining Weak UR (SR-UR)



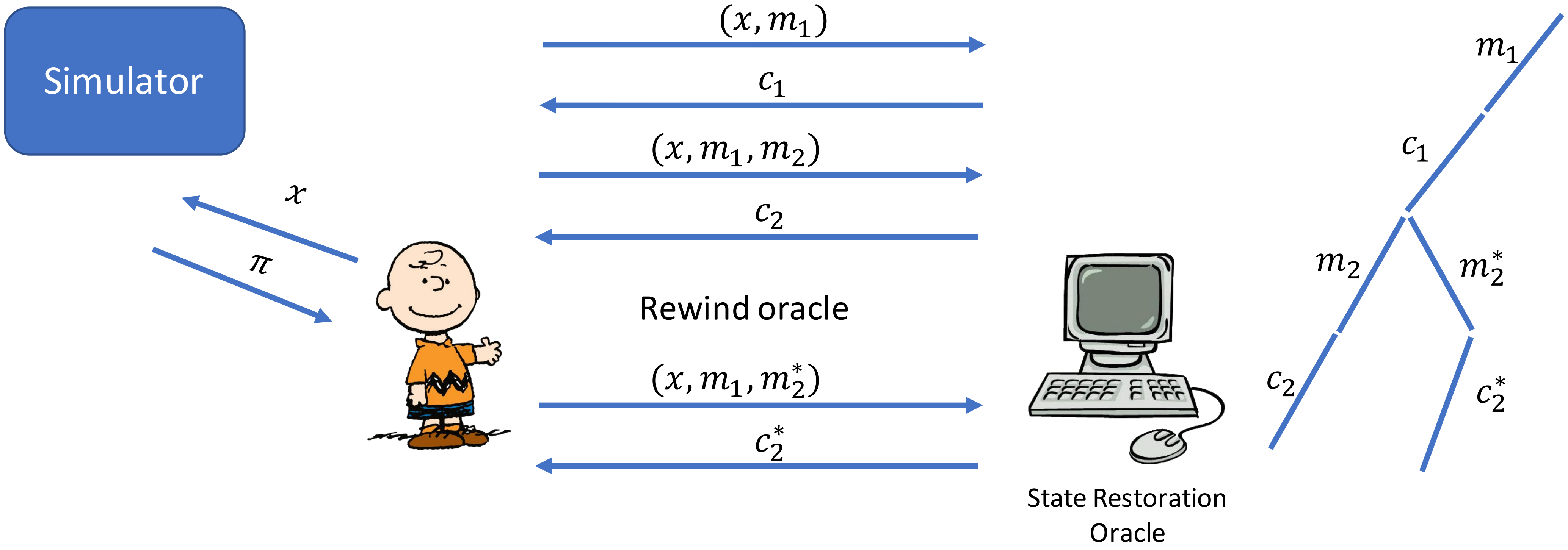
Defining Weak UR (SR-UR)



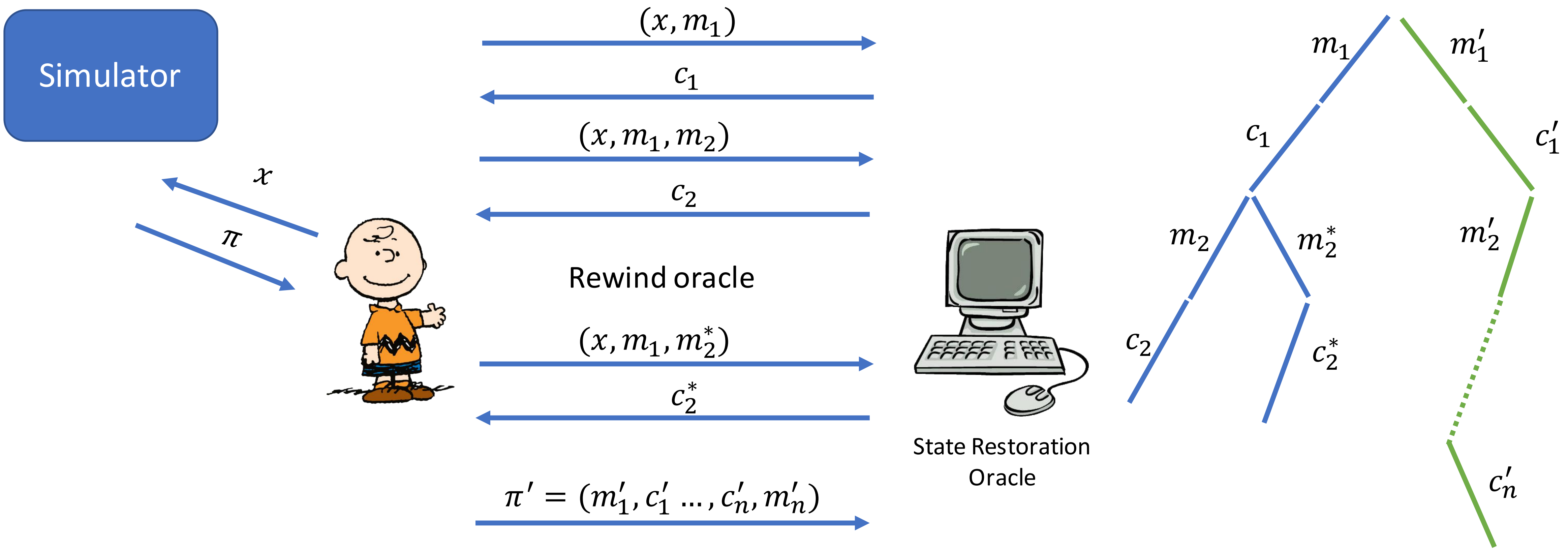
Defining Weak UR (SR-UR)



Defining Weak UR (SR-UR)

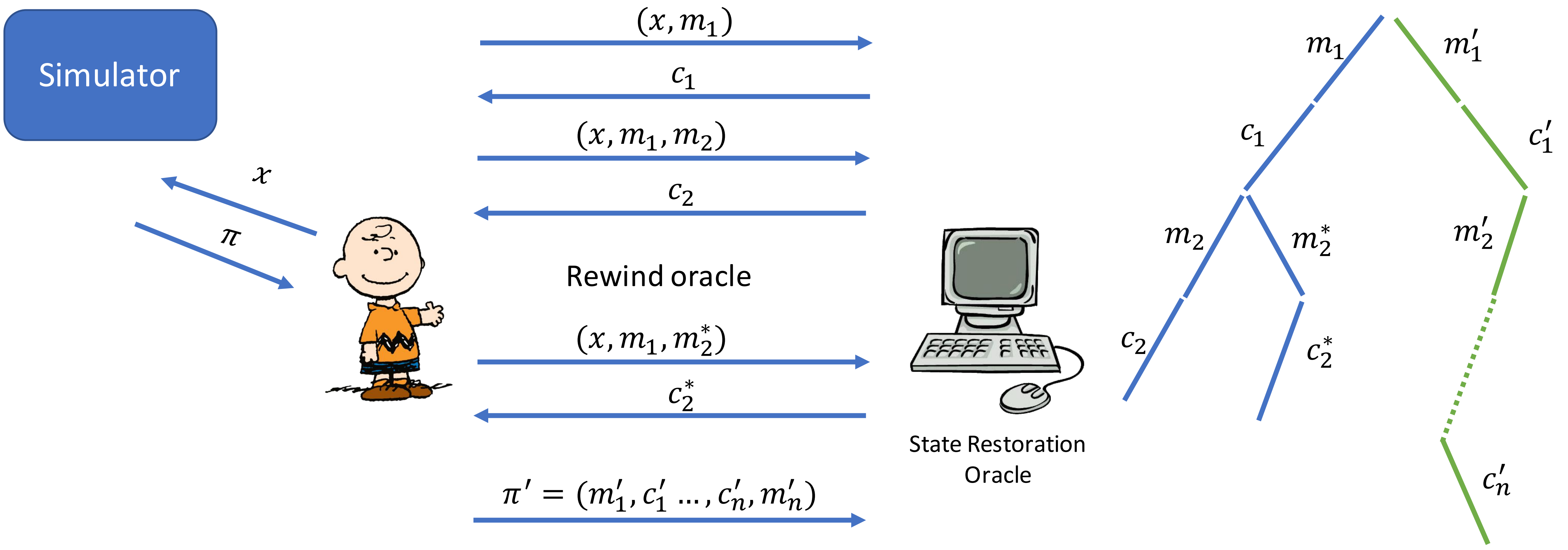


Defining Weak UR (SR-UR)



Winning condition: A different (π') such that $(m_1, \dots, m_i) = (m_1', \dots, m_i')$ but $m_{i+1} \neq m_{i+1}'$

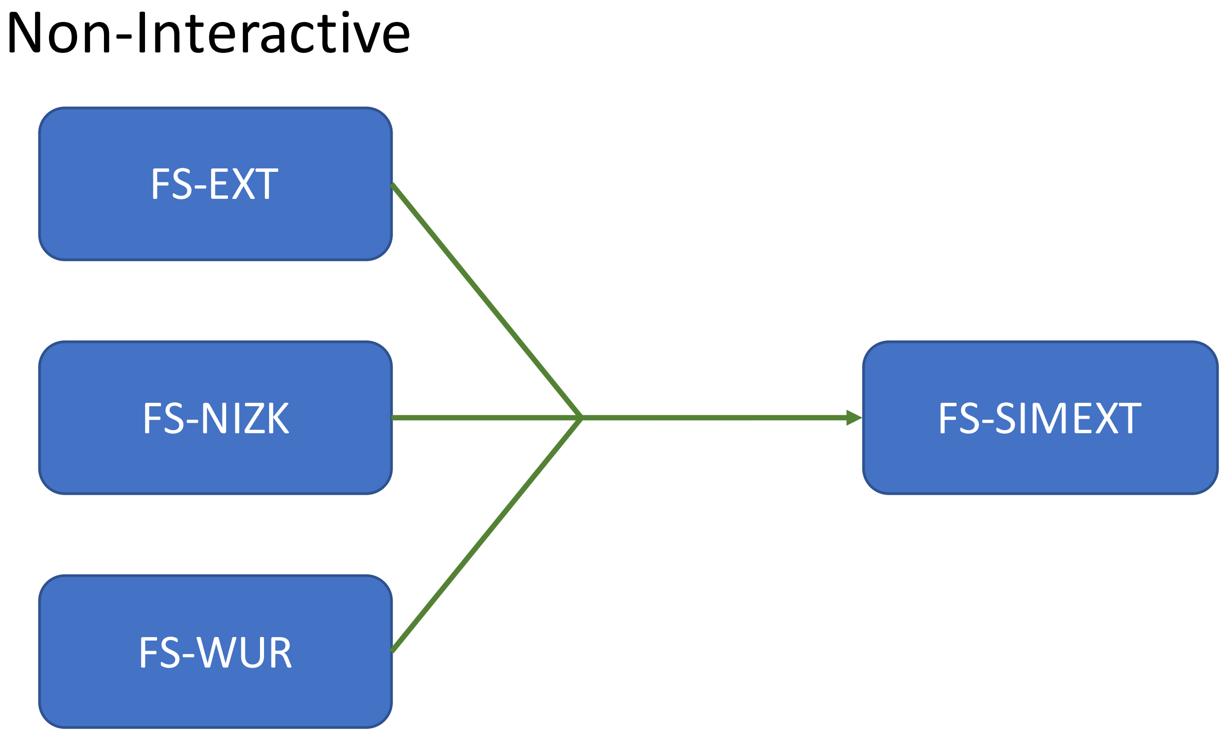
Defining Weak UR (SR-UR)



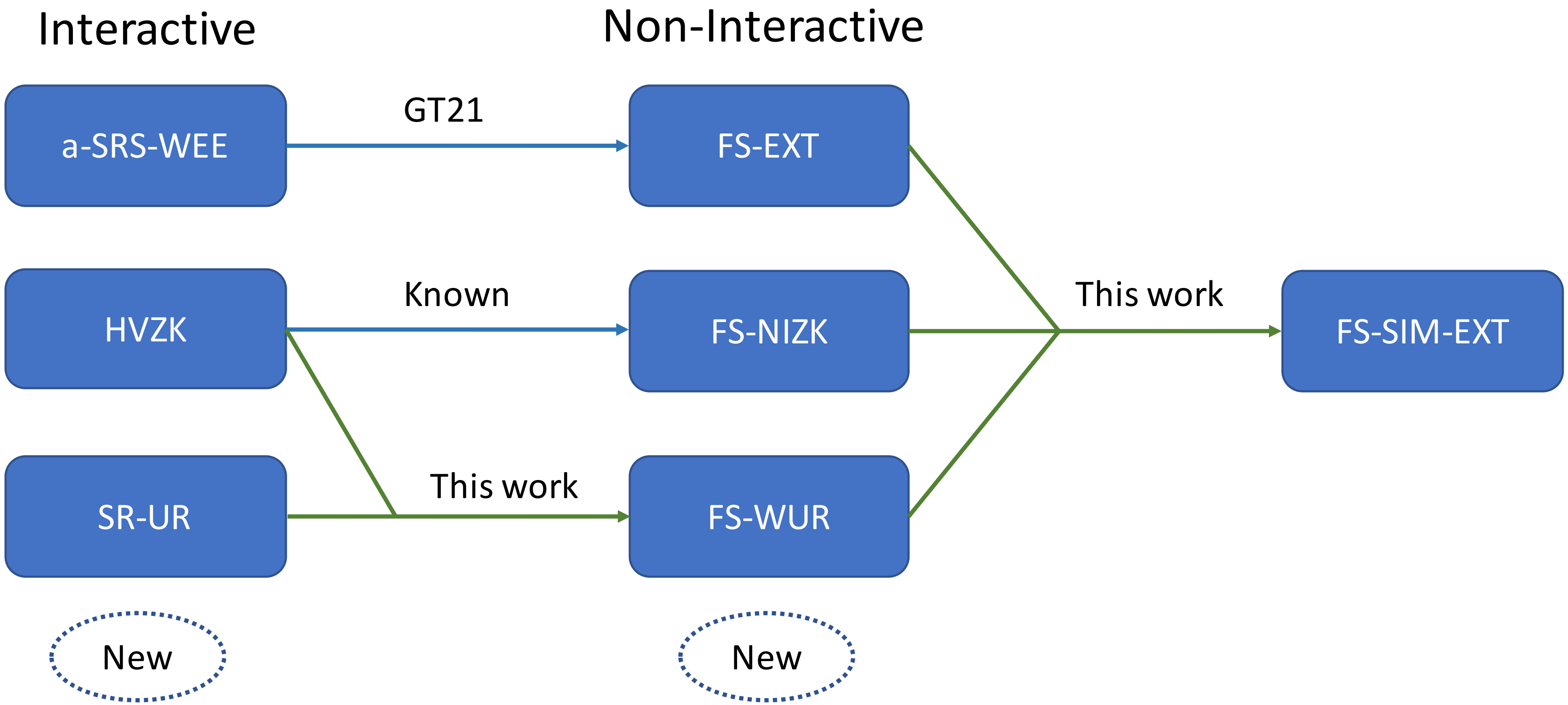
Winning condition: A different (π') such that $(m_1, \dots, m_i) = (m_1', \dots, m_i')$ but $m_{i+1} \neq m_{i+1}'$

If Π has weak UR $\Rightarrow$ FS(Π) has weak UR

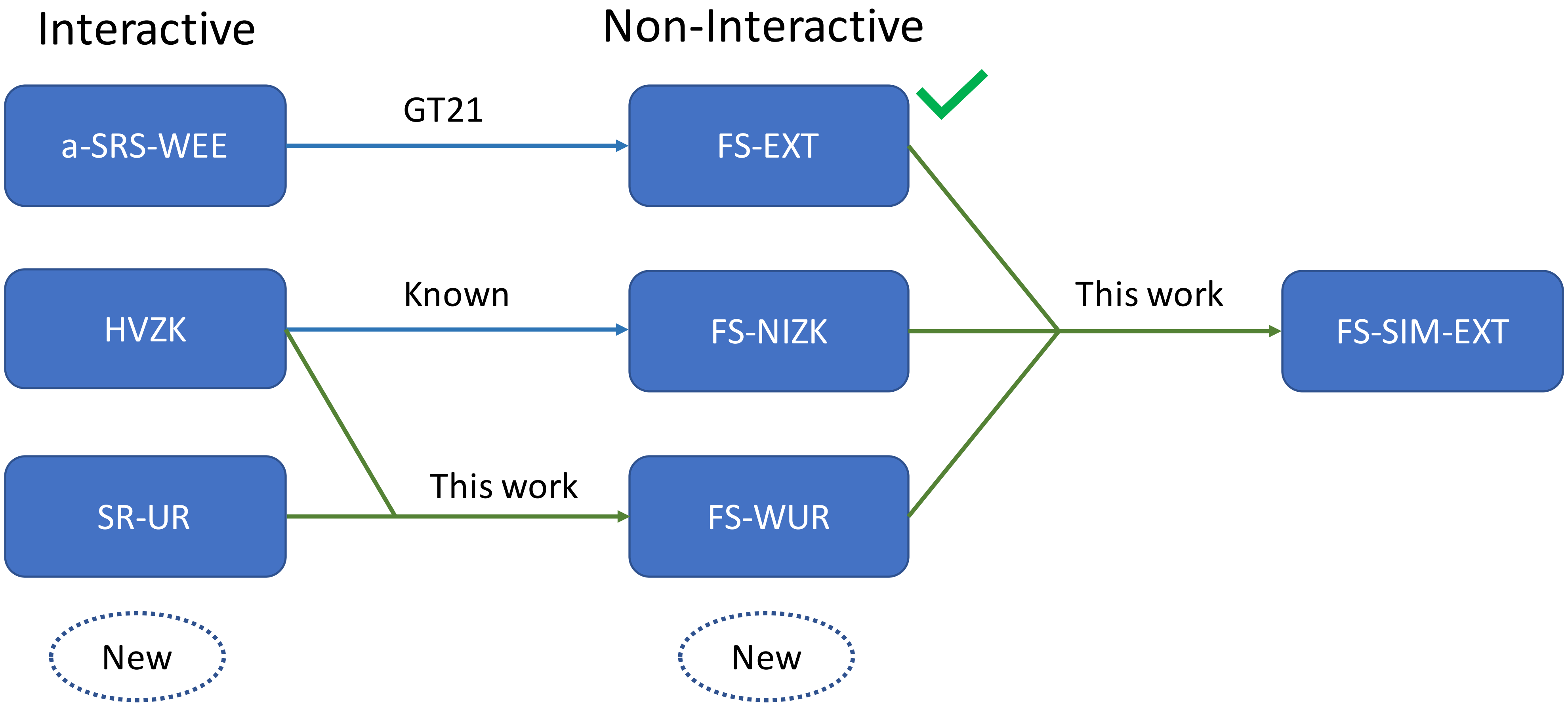
Roadmap



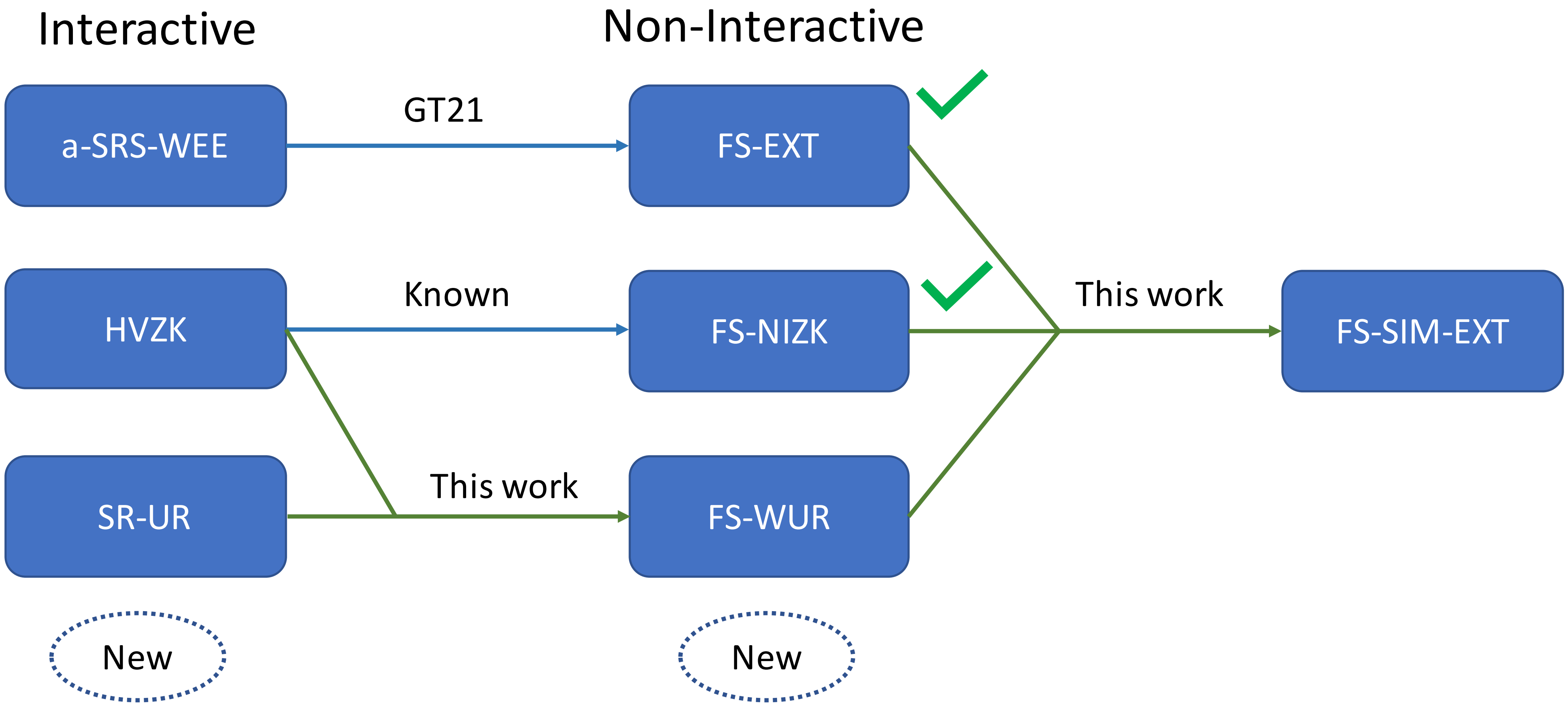
Roadmap


Interactive
Non-Interactive
a-SRS-WEE
GT21
FS-EXT
HVZK
Known
FS-NIZK
This work
FS-SIM-EXT
SR-UR
This work
FS-WUR
New
New

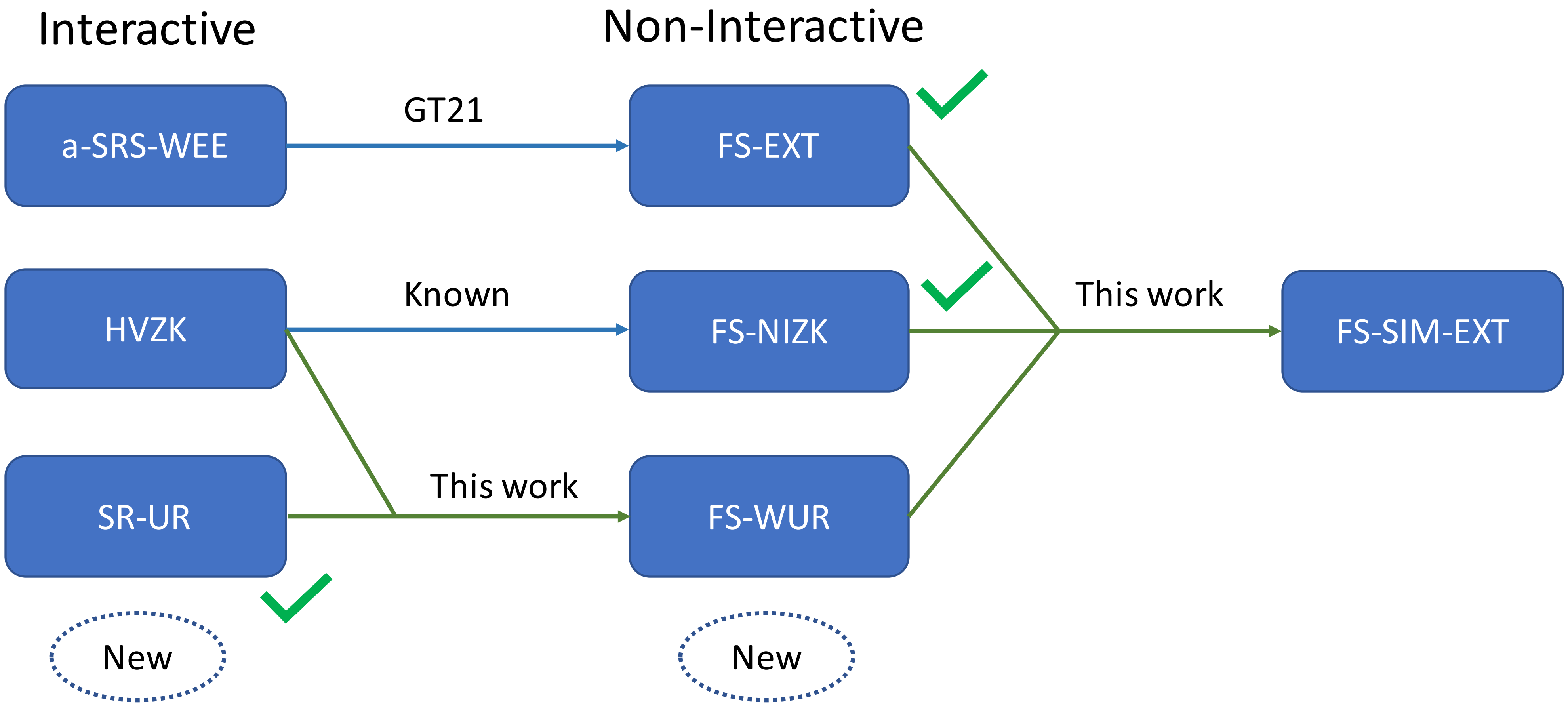
Roadmap


Interactive
Non-Interactive
a-SRS-WEE
GT21
FS-EXT
HVZK
Known
FS-NIZK
This work
FS-SIM-EXT
SR-UR
This work
FS-WUR
New
New

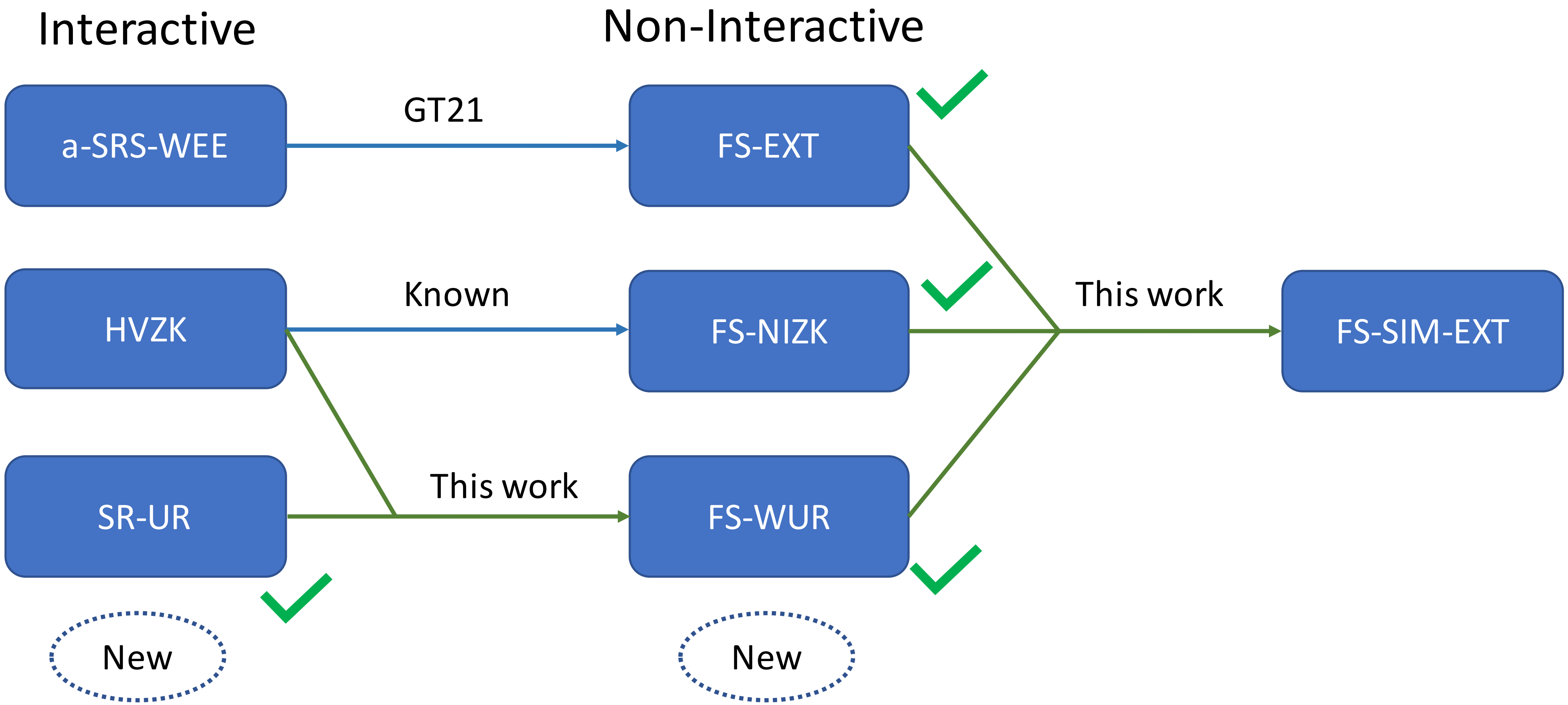
Roadmap


Interactive
Non-Interactive
a-SRS-WEE
GT21
FS-EXT
HVZK
Known
FS-NIZK
This work
FS-SIM-EXT
SR-UR
This work
FS-WUR
New
New

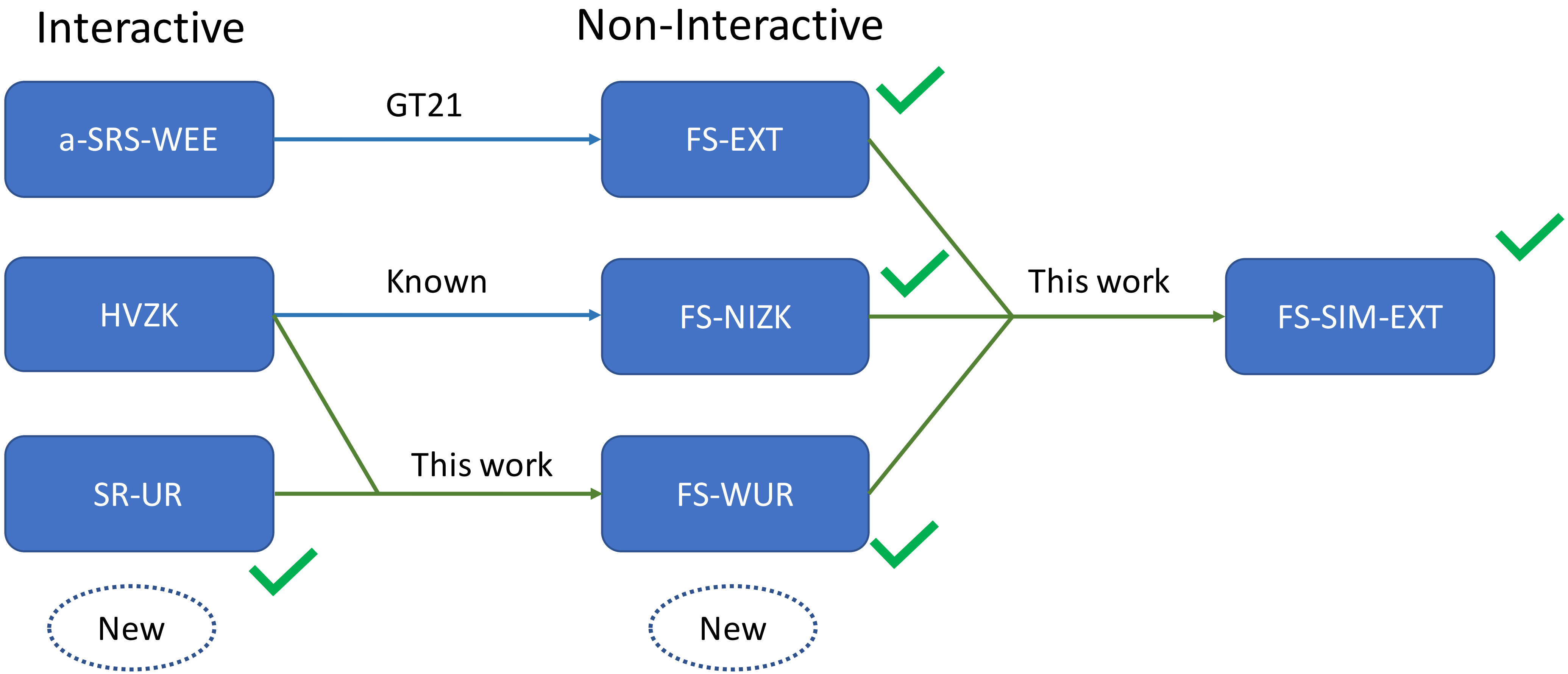
Roadmap


Interactive
Non-Interactive
a-SRS-WEE
GT21
FS-EXT
HVZK
Known
FS-NIZK
This work
FS-SIM-EXT
SR-UR
This work
FS-WUR
New
New

Roadmap


Interactive
Non-Interactive
a-SRS-WEE
GT21
FS-EXT
HVZK
Known
FS-NIZK
This work
FS-SIM-EXT
SR-UR
This work
FS-WUR
New
New

Roadmap



Interactive
Non-Interactive
a-SRS-WEE
GT21
FS-EXT
HVZK
Known
FS-NIZK
This work
FS-SIM-EXT
SR-UR
This work
FS-WUR
New
New

Proving SR-UR

- Simulated: $x, \pi = (m_1, c_1, \ldots, m_i, \ldots, m_r) \Rightarrow \left(g^{a_1} h^{b_1}, c_1, \ldots, \boldsymbol{g^{a_i} h^{b_i}, c_i} \ldots\right)$.

Proving SR-UR

- Simulated: $x, \pi = (m_1, c_1, \ldots, m_i, \ldots, m_r) \Rightarrow \left(g^{a_1}h^{b_1}, c_1, \ldots, \boldsymbol{g^{a_i}h^{b_i}, c_i} \ldots\right)$.
- Adversarial: $x', \pi' = (m_{1,} c_1 \ldots, m'_i, \ldots, m'_n) \Rightarrow \ (g^{a_1}h^{b_1}, c_1, \ldots, \boldsymbol{g^{x_i}h^{y_i} \ \ , c'_i} \ldots)$.

Proving SR-UR

Algebraic Simulator

- Simulated: $x, \pi = (m_1, c_1, \ldots, m_i, \ldots, m_r) \Rightarrow (g^{a_1}h^{b_1}, c_1, \ldots, \boldsymbol{g^{a_i}h^{b_i}, c_i} \ldots)$.
- Adversarial: $x', \pi' = (m_{1,} c_1 \ldots, m'_i, \ldots, m'_n) \Rightarrow (g^{a_1}h^{b_1}, c_1, \ldots, \boldsymbol{g^{x_i}h^{y_i}\ \ , c'_i} \ldots)$.

Proving SR-UR

- Simulated: $x, \pi = (m_1, c_1, \dots, m_i, \dots, m_r) \Rightarrow (g^{a_1}h^{b_1}, c_1, \dots, \boldsymbol{g^{a_i}h^{b_i}, c_i} \dots)$.
- Adversarial: $x', \pi' = (m_1, c_1 \dots, m'_i, \dots, m'_n) \Rightarrow (g^{a_1}h^{b_1}, c_1, \dots, \boldsymbol{g^{x_i}h^{y_i}, c'_i} \dots)$.

Algebraic Simulator

Algebraic Adversary

Proving SR-UR

Algebraic Simulator

- Simulated: $x, \pi = (m_1, c_1, \dots, m_i, \dots, m_r) \Rightarrow \left(g^{a_1}h^{b_1}, c_1, \dots, \boldsymbol{g^{a_i}h^{b_i}, c_i} \dots\right).$
- Adversarial: $x', \pi' = (m_{1,} c_1 \dots, m'_i, \dots, m'_n) \Rightarrow (g^{a_1}h^{b_1}, c_1, \dots, \boldsymbol{g^{x_i}h^{y_i}\ , c'_i} \dots).$
- Break Dlog using Schwartz-Zippel lemma.

Algebraic Adversary

Proving SR-UR

Simulated: $\left(x, g^{a_1}h^{b_1}, c_1, \dots, \boldsymbol{g^{a_i}h^{b_i}}, c_i, \dots\right)$

Adversarial: $(x, g^{a_1}h^{b_1}, c_1, \dots, \boldsymbol{g^{x_i}h^{y_i}}, \boldsymbol{c'_i} \dots)$

Proving SR-UR

Simulated: $\left(x, g^{a_1}h^{b_1}, c_1, \ldots, \boldsymbol{g^{a_i}h^{b_i}}, c_i, \ldots\right)$

Adversarial: $\left(x, g^{a_1}h^{b_1}, c_1, \ldots, \boldsymbol{g^{x_i}h^{y_i}, c'_i} \ldots\right)$

π verifies

$$\boldsymbol{m_1 \times g^{a_i}h^{b_i} = R}$$

$$\boldsymbol{m_1 \times g^{x_i}h^{y_i} = R}$$

π' verifies

Proving SR-UR

Simulated: $\left(x, g^{a_1}h^{b_1}, c_1, \ldots, \boldsymbol{g^{a_i}h^{b_i}}, c_i, \ldots\right)$

Adversarial: $\left(x, g^{a_1}h^{b_1}, c_1, \ldots, \boldsymbol{g^{x_i}h^{y_i}}, \boldsymbol{c'_i} \ldots\right)$

π verifies

$$\boldsymbol{m_1 \times g^{a_i}h^{b_i} = R}$$

$$\boldsymbol{m_1 \times g^{x_i}h^{y_i} = R}$$

π' verifies

(Using Schwartz-Zippel)

π' verifies

$$\boldsymbol{a_1}\widetilde{c_i}c_i + \boldsymbol{a_1 c_i^2} = \boldsymbol{0}$$

$$\boldsymbol{a_1}\widetilde{c_i}\boldsymbol{X} + \boldsymbol{a_1 X^2} = \boldsymbol{0}$$

$$\boldsymbol{a_1 = 0}$$

Result

- Fiat-Shamir BP is simulation extractable in the AGM and RO model.
- Concretely,

Let $\mathcal{E}$ be an FS-EXT extractor for Π_{FS}. $\exists \mathcal{E}^*$ for Π_{FS}: $\forall (\mathcal{P}^*, \mathcal{D}^*)$ against Π_{FS} that makes q_1 RO queries and q_2 simulation queries, $\exists (\mathcal{P}, \mathcal{D})$ against FS-EXT, and $\exists \mathcal{A}$ against FS-WUR:

$$\mathbf{Adv}^{\mathit{FS\text{-}SIM\text{-}EXT}}_{\Pi_{\mathsf{FS}},\mathcal{R}}(\mathcal{S}_{\mathsf{FS}}, \mathcal{E}^*, \mathcal{P}^*, \mathcal{D}^*) \leq \mathbf{Adv}^{\mathit{FS\text{-}EXT}}_{\Pi_{\mathsf{FS}},\mathcal{R}}(\mathsf{H}, \mathcal{E}, \mathcal{P}, \mathcal{D}) + q_2 \cdot \mathbf{Adv}^{\mathit{FS\text{-}WUR}}_{\Pi_{\mathsf{FS}},\mathcal{R}}(\mathcal{A}, \mathcal{S}_{\mathsf{FS}})$$

Conclusion

- New approach to the FS simulation-extractability.
- Concrete analysis for BP/RngPf in the AGM.
- May apply to other FS-NIZK/signatures constructed from multi-round protocols.

Thank You!

ePrint: 2021/1393

Conclusion

- New approach to the FS simulation-extractability.
- Concrete analysis for BP/RngPf in the AGM.
- May apply to other FS-NIZK/signatures constructed from multi-round protocols.

Attema, Fehr and Klooß [ATK21]: Only $O(q)$ multiplicative loss in the knowledge error incurred by multi-round FS **without the AGM**!

Improved result without AGM (WIP)

Thank You!

ePrint: 2021/1393