Robust Non-Interactive Zero-Knowledge Combiners

Michele Ciampi
The University of Edinburgh

Lorenzo Magliocco
Sapienza University of Rome
Personal Capacity

Daniele Venturi
Sapienza University of Rome

Yu Xia
The University of Edinburgh
Hong Kong Polytechnic University

EUROCRYPT 2026

Bird’s eye view

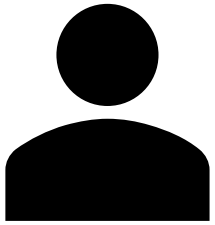
Warm-up: Robust Combiners	Definitions & Impossibility Results
Constructions	Wrapping up

Bird’s eye view

Warm-up: Robust Combiners	Definitions & Impossibility Results
Constructions	Wrapping up

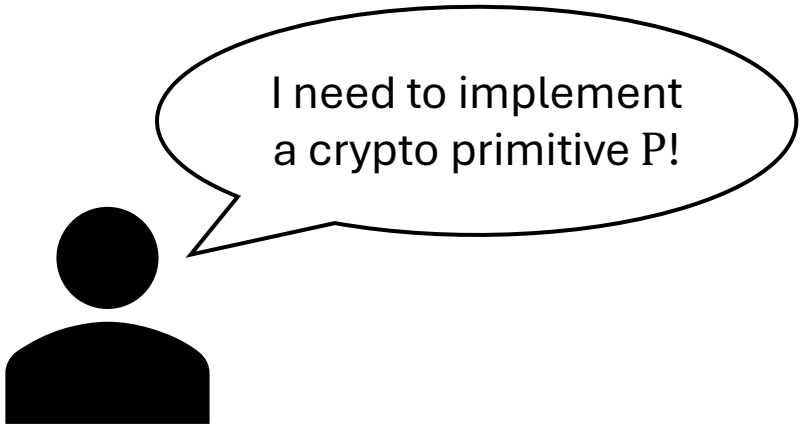
Robust Combiners

Robust Combiners

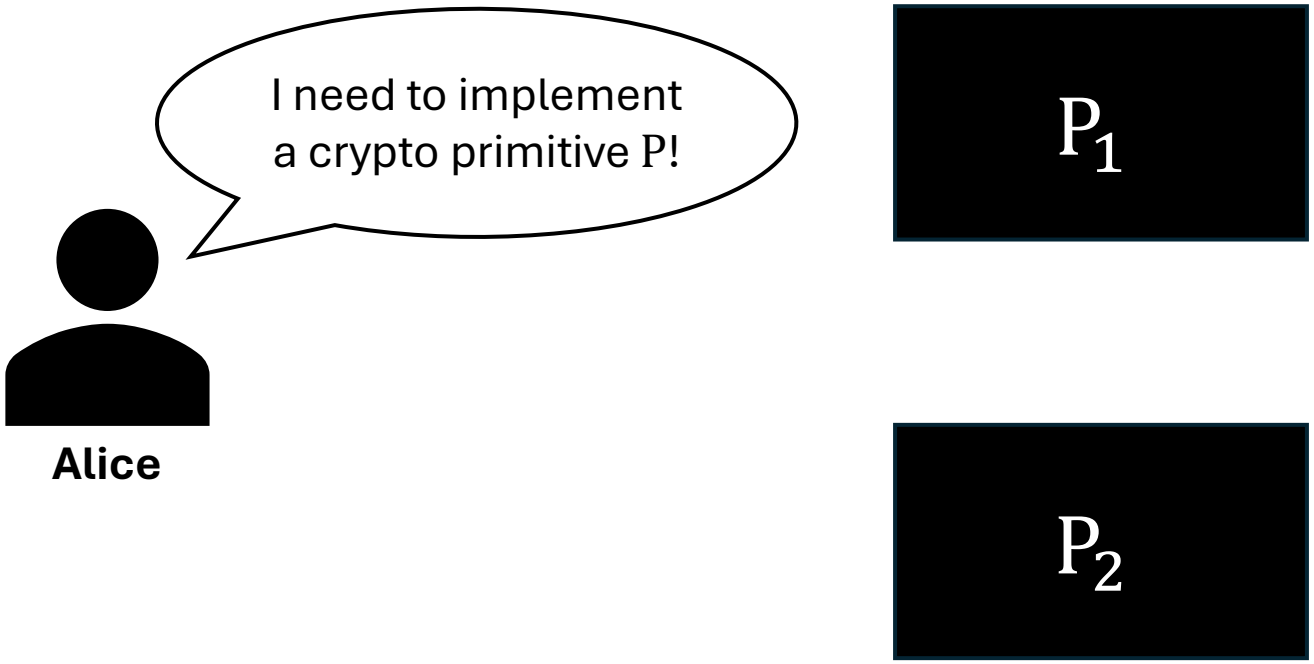


Alice

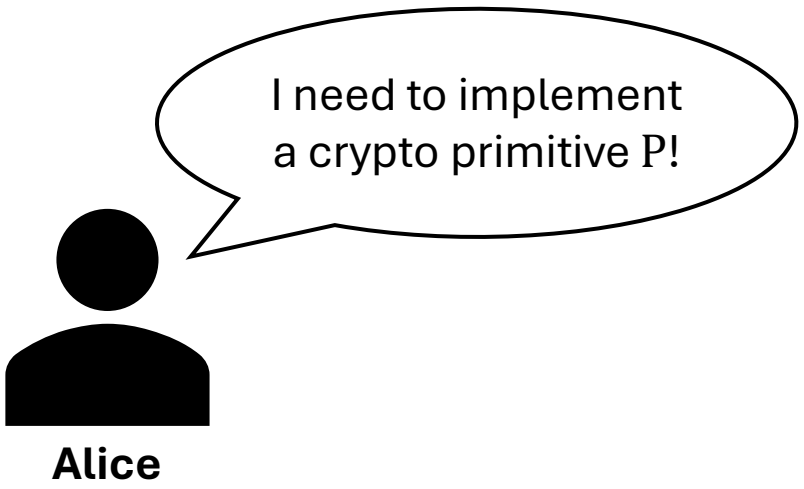
Robust Combiners



Robust Combiners



Robust Combiners

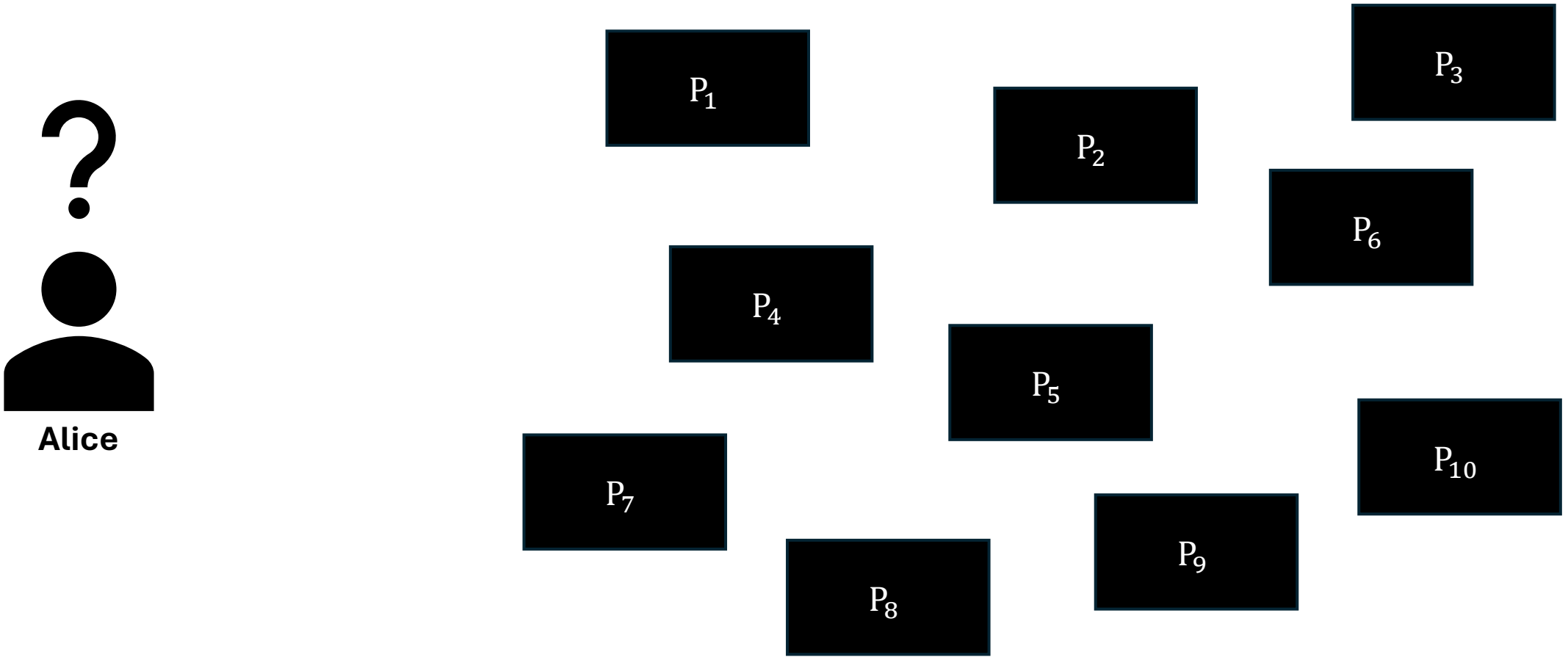


P_1

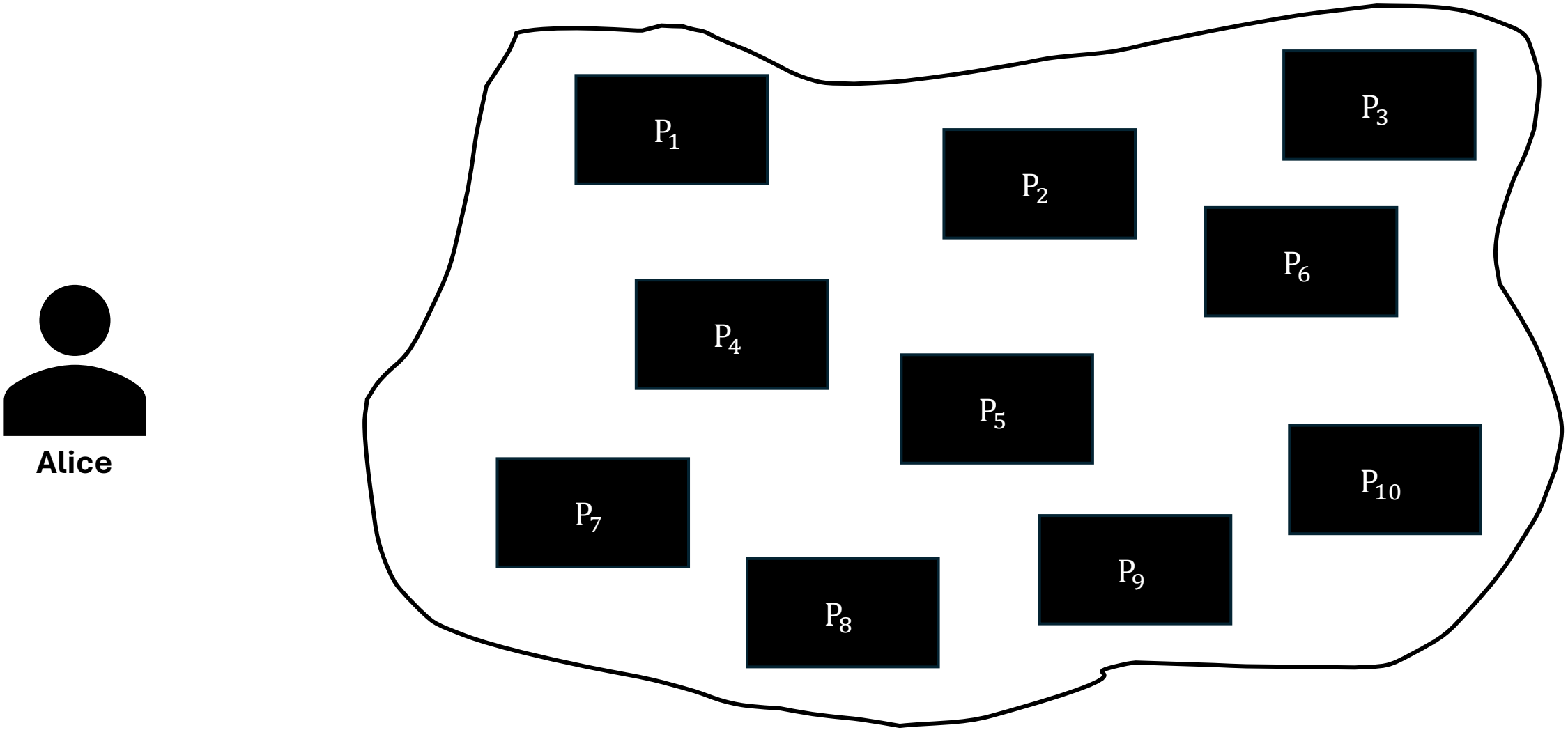
P_2

- Pre-quantum vs post-quantum?
- Setup assumptions?
- Open vs closed source?
- …

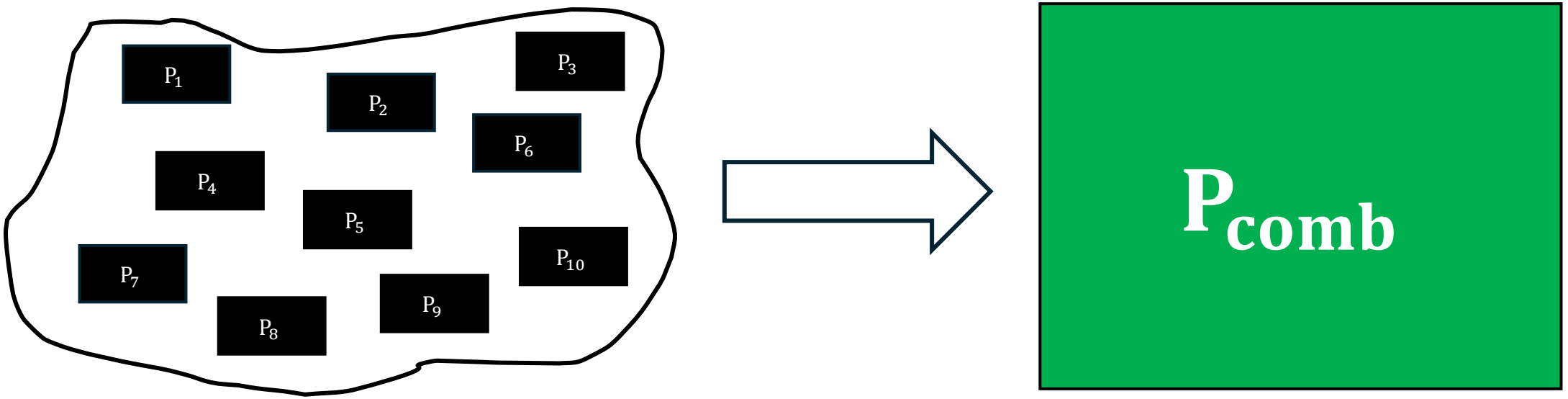
Robust Combiners



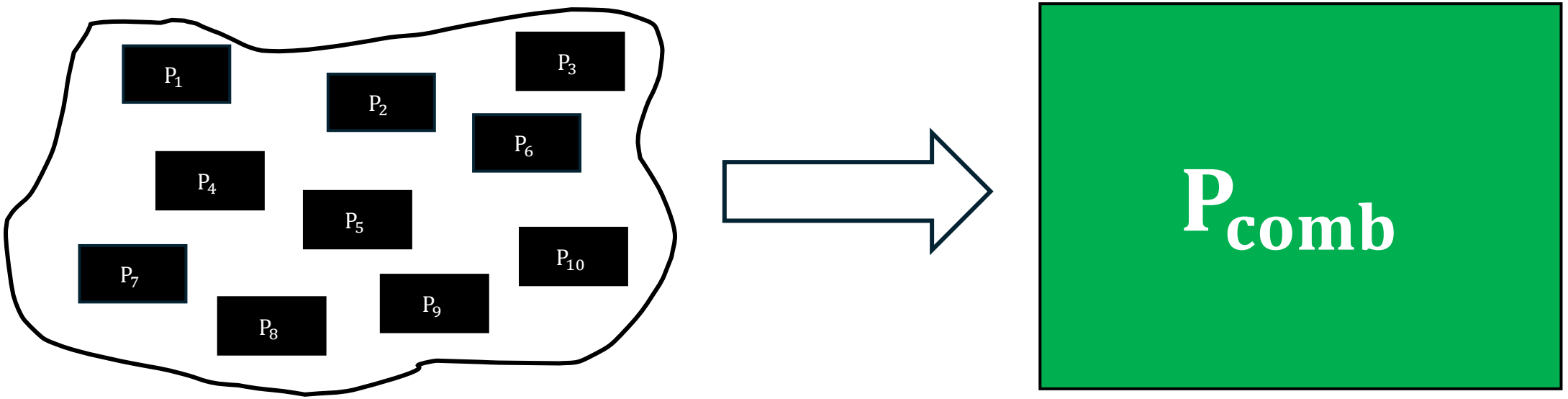
Robust Combiners



Robust Combiners



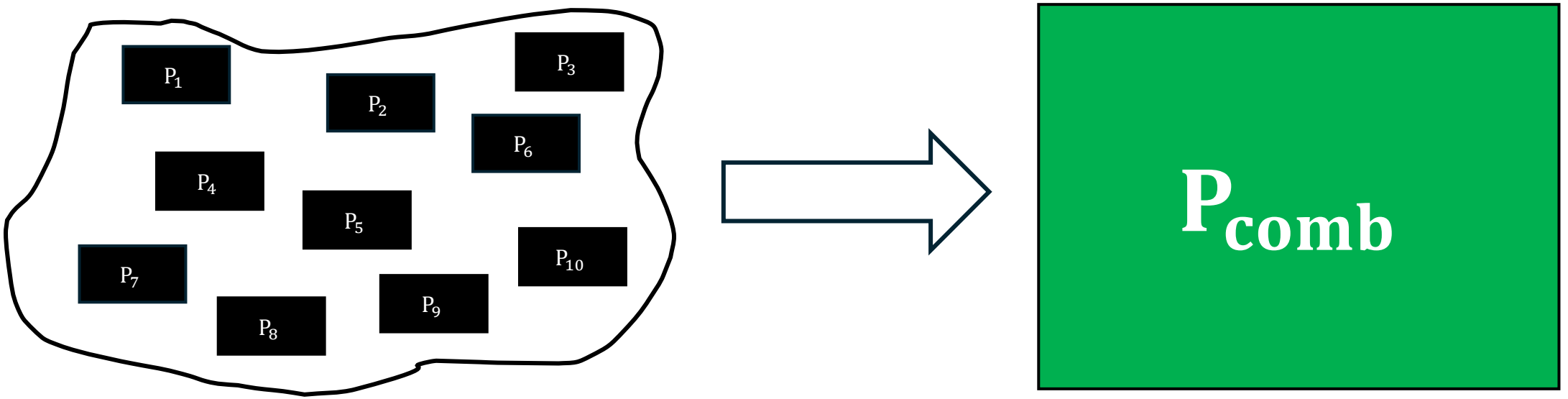
Robust Combiners



- "As long as at least t out of the n candidates are secure (with $t \leq n$), the combiner is also secure".

[HKN+05] D. Harnik, J. Kilian, M. Naor, O. Reingold, and A. Rosen, “On Robust Combiners for Oblivious Transfer and Other Primitives.” EUROCRYPT’05. https://www.iacr.org/archive/eurocrypt2005/34940096/34940096.pdf

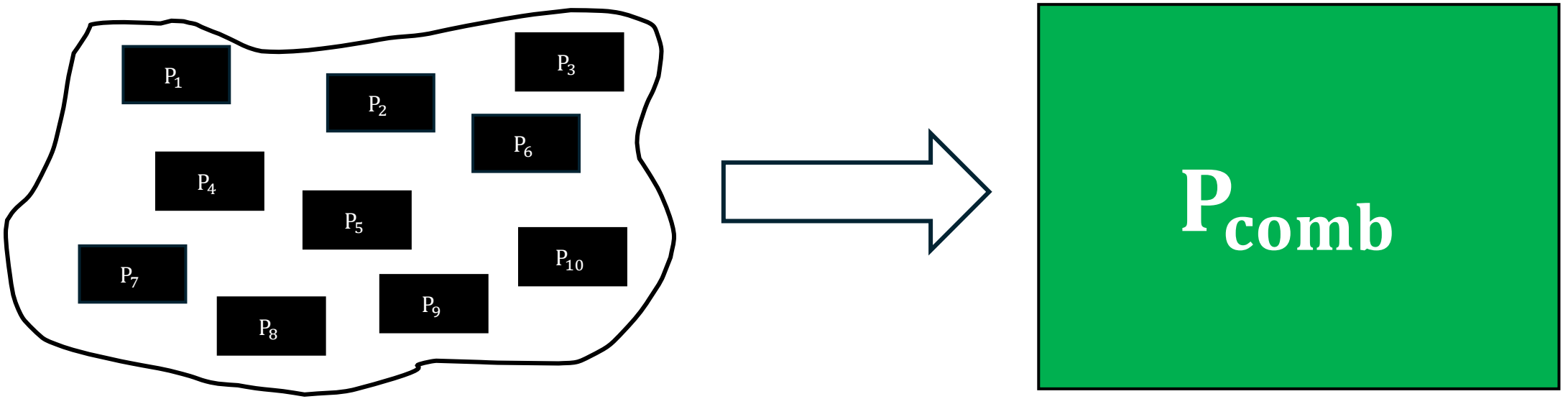
Robust Combiners



- “As long as at least t out of the n candidates are secure (with $t \leq n$), the combiner is also secure”.
  - **Robustness**: the combiner’s security **must** derive from its candidates.

[HKN+05] D. Harnik, J. Kilian, M. Naor, O. Reingold, and A. Rosen, “On Robust Combiners for Oblivious Transfer and Other Primitives.” EUROCRYPT’05. https://www.iacr.org/archive/eurocrypt2005/34940096/34940096.pdf

Robust Combiners



- “As long as at least t out of the n candidates are secure (with $t \leq n$), the combiner is also secure”.
  - **Robustness**: the combiner’s security **must** derive from its candidates.
- **More formally**: if the combiner is broken, we have at least $(n - t) + 1$ reductions to the candidates.

A simple example: CRH!

A simple example: CRH!

$$\mathrm{H}_{\mathrm{comb}}(\mathrm{x}) = \mathrm{H}_1(\mathrm{x}) \,||\, \mathrm{H}_2(\mathrm{x}) \,||\, \mathrm{H}_3(\mathrm{x})$$

A simple example: CRH!

$n = 3$	$t = 1$
$(n - t) + 1 = 3$	

$$\mathrm{H}_{\mathrm{comb}}(\mathrm{x}) = \mathrm{H}_1(\mathrm{x}) \,||\, \mathrm{H}_2(\mathrm{x}) \,||\, \mathrm{H}_3(\mathrm{x})$$



- Optimal security: **one** good candidate suffices.

[BB06] D. Boneh, X. Boyen, “On the Impossibility of Efficiently Combining Collision Resistant Hash Functions.” CRYPTO’06. https://iacr.org/archive/crypto2006/41170565/41170565.pdf

$n = 3$	$t = 1$
$(n - t) + 1 = 3$	

A simple example: CRH!

$$\mathrm{H}_{\mathrm{comb}}(\mathrm{x}) = \mathrm{H}_1(\mathrm{x}) \,||\, \mathrm{H}_2(\mathrm{x}) \,||\, \mathrm{H}_3(\mathrm{x})$$



- Optimal security: **one** good candidate suffices.

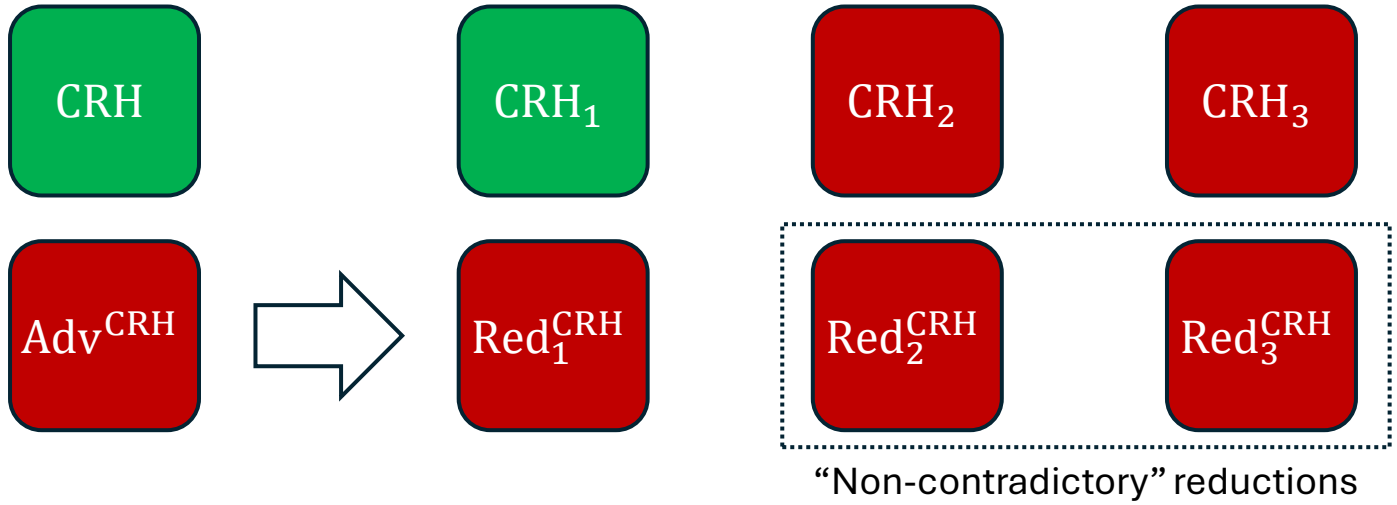
- **Intuition**: a collision for $\mathrm{H}_{\mathrm{comb}}(\mathrm{x})$ implies a collision for $(n - t) + 1$ of the candidates.

[BB06] D. Boneh, X. Boyen, “On the Impossibility of Efficiently Combining Collision Resistant Hash Functions.” CRYPTO’06. https://iacr.org/archive/crypto2006/41170565/41170565.pdf

$n = 3$	$t = 1$
$(n - t) + 1 = 3$	

A simple example: CRH!

$$\mathrm{H}_{\mathrm{comb}}(\mathrm{x}) = \mathrm{H}_1(\mathrm{x}) \,||\, \mathrm{H}_2(\mathrm{x}) \,||\, \mathrm{H}_3(\mathrm{x})$$



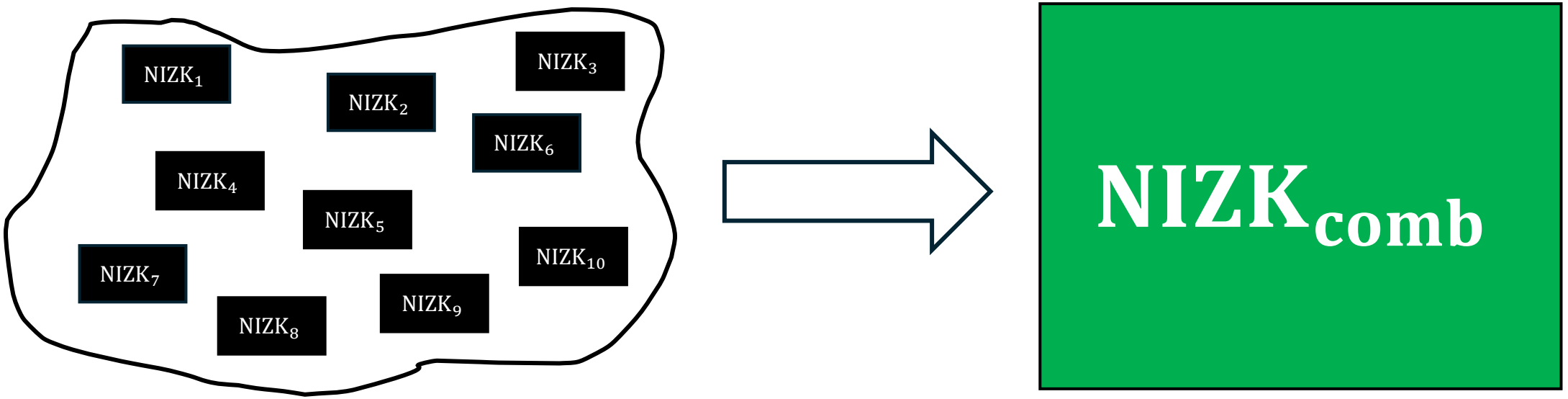
- Optimal security: **one** good candidate suffices.

- **Intuition**: a collision for $\mathrm{H}_{\mathrm{comb}}(\mathrm{x})$ implies a collision for $(n - t) + 1$ of the candidates.

Bird’s eye view

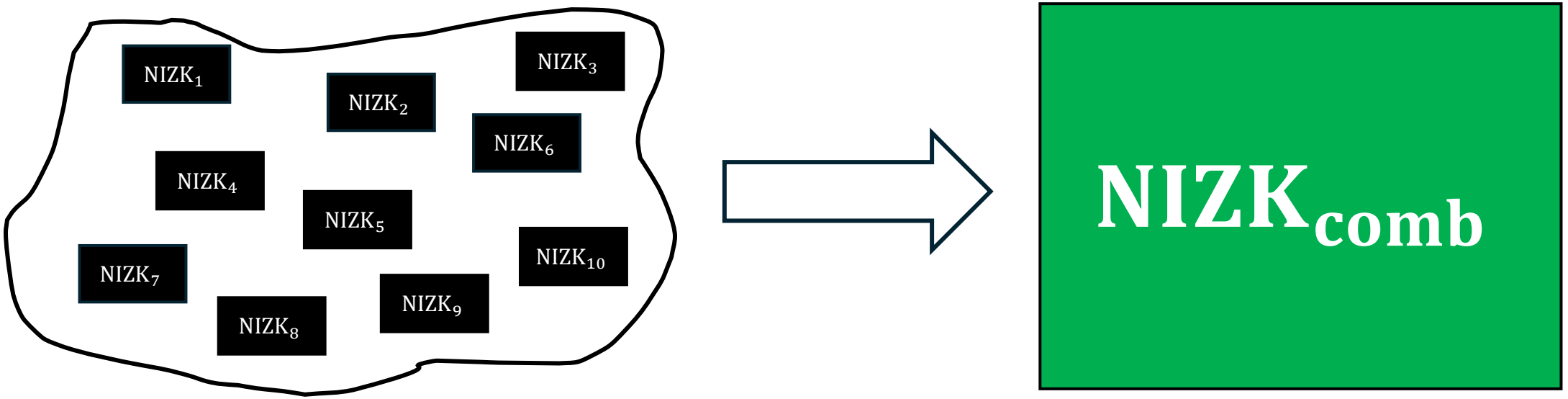
Warm-up: Robust Combiners	**Definitions & Impossibility Results**
Constructions	Wrapping up

Robust NIZK Combiners



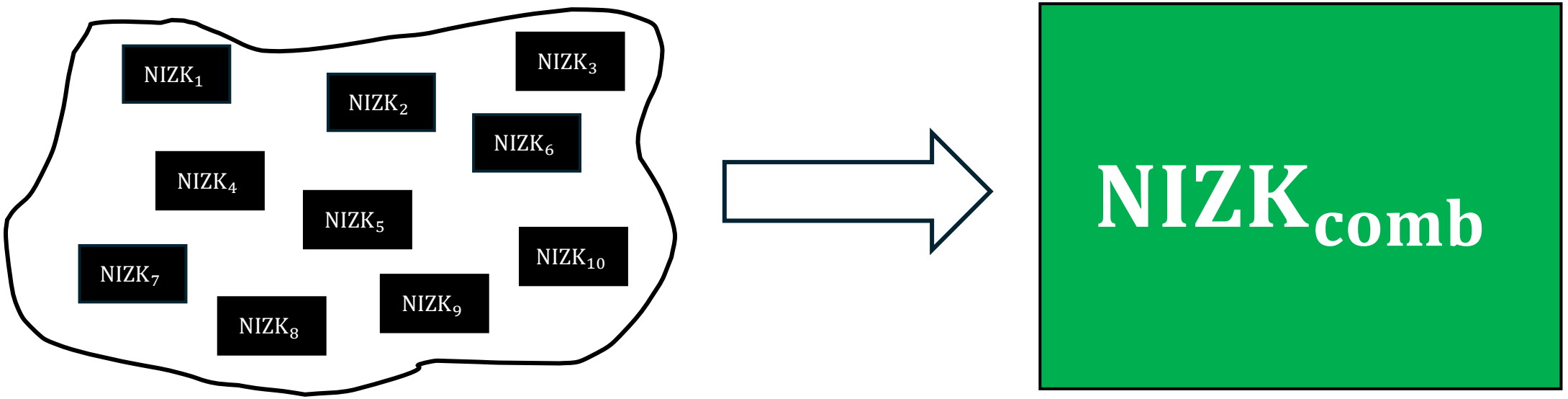
- "As long as at least t out of the n candidates are secure (with $t \leq n$), the combiner is also secure".

Robust NIZK Combiners



- "As long as at least t out of the n candidates are secure (with $t \leq n$), the combiner is also secure".
  - NIZK is **multi-property**.

Robust NIZK Combiners



- "As long as at least t out of the n candidates are secure (with $t \leq n$), the combiner is also secure".
  - NIZK is **multi-property**.
  - What does t mean? What are we breaking?

(Sound, ZK)-Robust Combiner

$n = 3$	$t = 2$
$(n - t) + 1 = 2$	

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2, \mathrm{NIZK}_3)$$

(Sound, ZK)-Robust Combiner

$n = 3$	$t = 2$
$(n - t) + 1 = 2$	

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2, \mathrm{NIZK}_3)$$

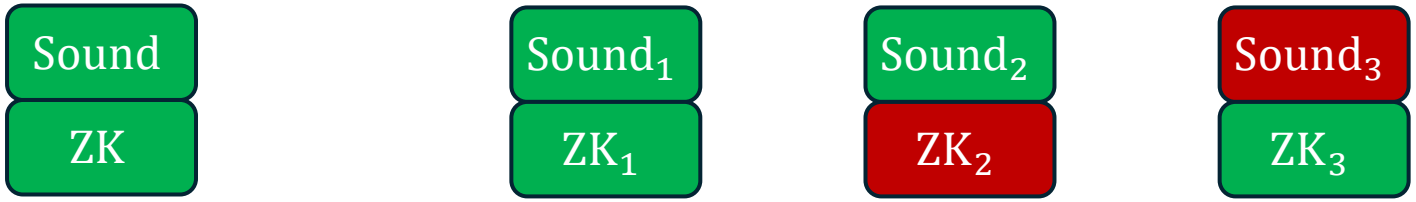
Sound

ZK

(Sound, ZK)-Robust Combiner

$n = 3$	$t = 2$
$(n - t) + 1 = 2$	

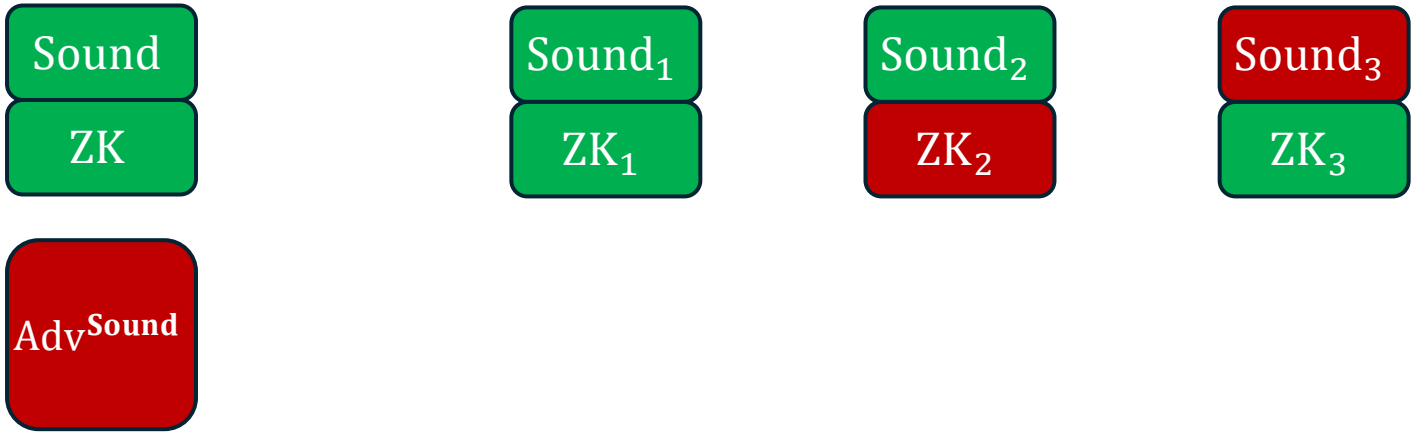
$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2, \mathrm{NIZK}_3)$$



(Sound, ZK)-Robust Combiner

$n = 3$	$t = 2$
$(n - t) + 1 = 2$	

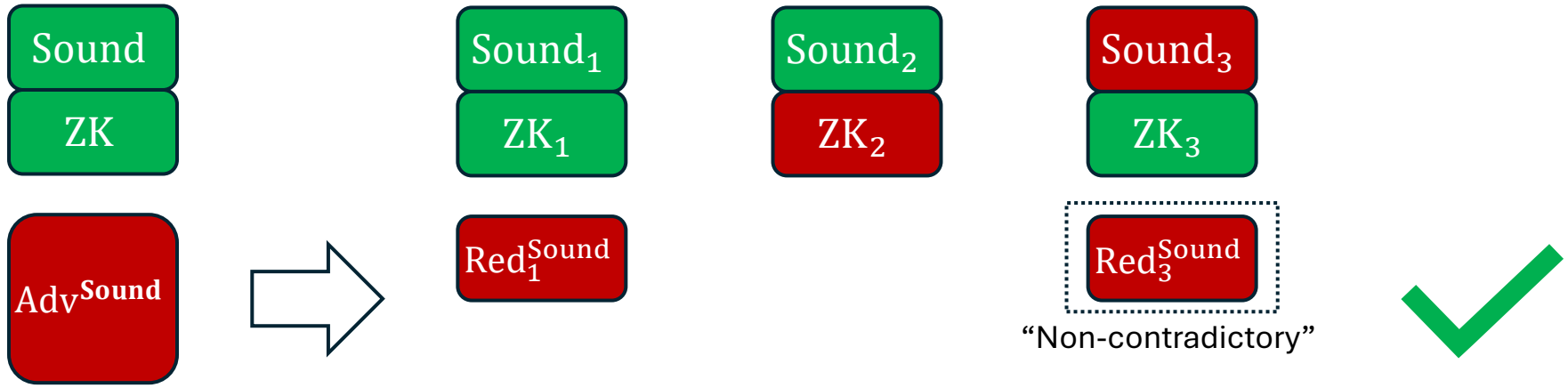
$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2, \mathrm{NIZK}_3)$$



(Sound, ZK)-Robust Combiner

$n = 3$	$t = 2$
$(n - t) + 1 = 2$	

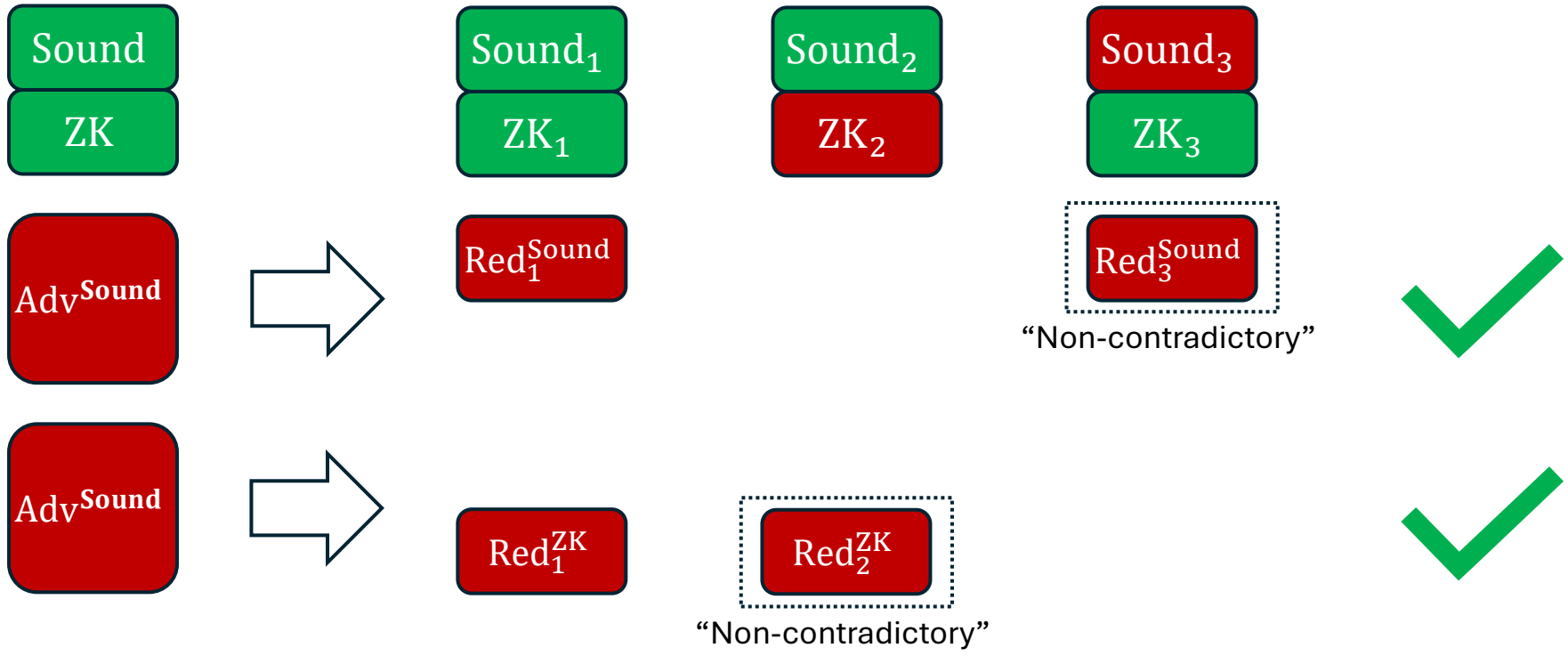
$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2, \mathrm{NIZK}_3)$$



(Sound, ZK)-Robust Combiner

$n = 3$	$t = 2$
$(n - t) + 1 = 2$	

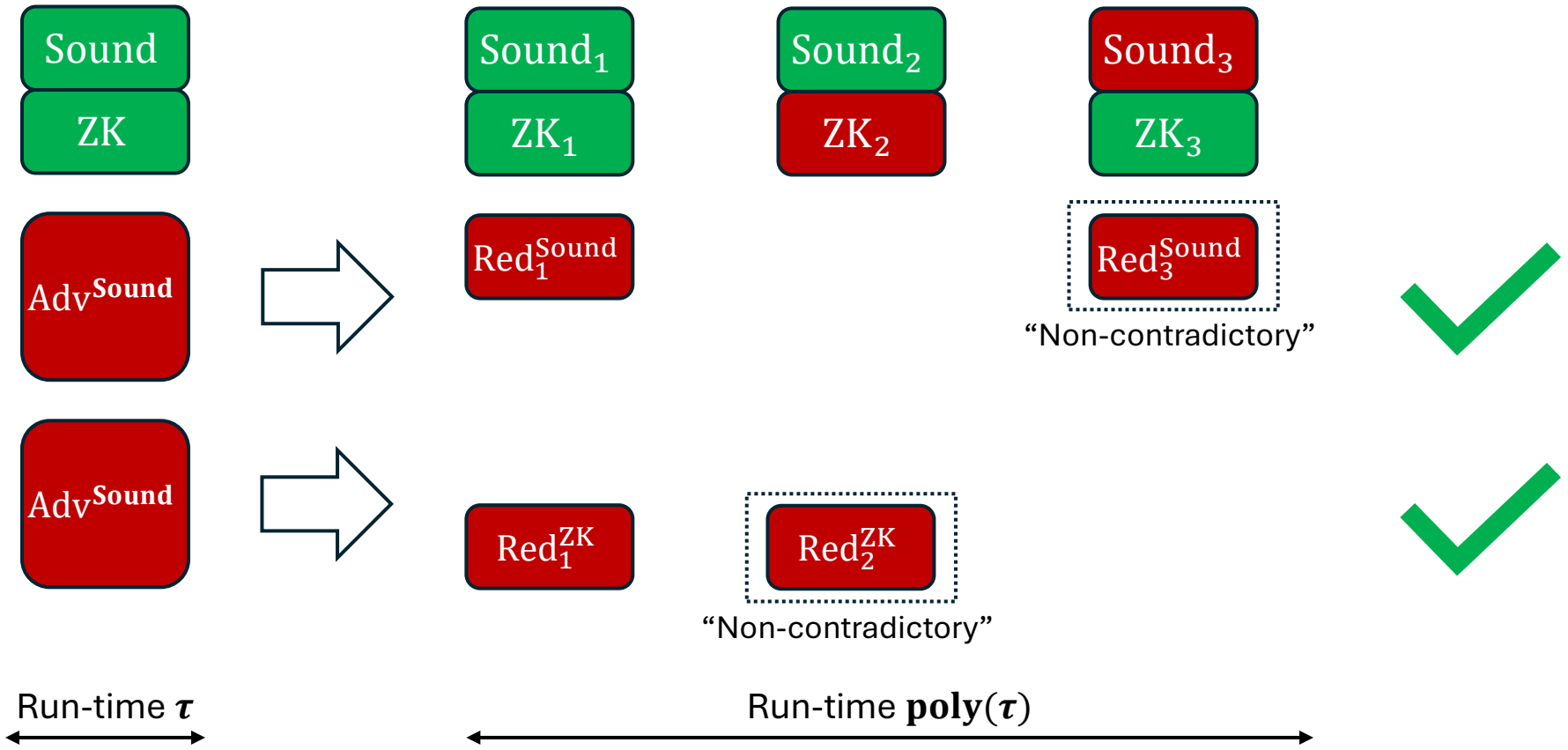
$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2, \mathrm{NIZK}_3)$$



(Sound, ZK)-Robust Combiner

$n = 3$	$t = 2$
$(n - t) + 1 = 2$	

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2, \mathrm{NIZK}_3)$$



Impossibility for $t \leq n/2$

Impossibility for $t \leq n/2$

- Idea: exhibit a **counterexample**!

Impossibility for $t \leq n/2$

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$

- Idea: exhibit a **counterexample**!

Impossibility for $t \leq n/2$

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$







NIZK_1

- $\mathrm{Setup}(1^\lambda)$: Output $\perp$.
- $\mathrm{P}(x, w)$: Output w.
- $\mathrm{V}(x, \pi)$: Check w against x.

NIZK_2

- $\mathrm{Setup}(1^\lambda)$: Output $\perp$.
- $\mathrm{P}(x, w)$: Output 0.
- $\mathrm{V}(x, \pi)$: Output $\pi == 0$.

➢ Idea: exhibit a **counterexample**!

Impossibility for $t \leq n/2$

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$







NIZK_1

- $\mathrm{Setup}(1^\lambda)$: Output $\perp$.
- $\mathrm{P}(x, w)$: Output w.
- $\mathrm{V}(x, \pi)$: Check w against x.

NIZK_2

- $\mathrm{Setup}(1^\lambda)$: Output $\perp$.
- $\mathrm{P}(x, w)$: Output 0.
- $\mathrm{V}(x, \pi)$: Output $\pi == 0$.

➢ Idea: exhibit a **counterexample**!

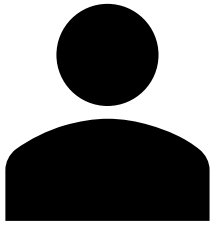
➢ We also adapt this counterexample to more restrictive definitions of robust combiners.

Bird’s eye view

Warm-up: Robust Combiners	Definitions & Impossibility Results
Constructions	Wrapping up

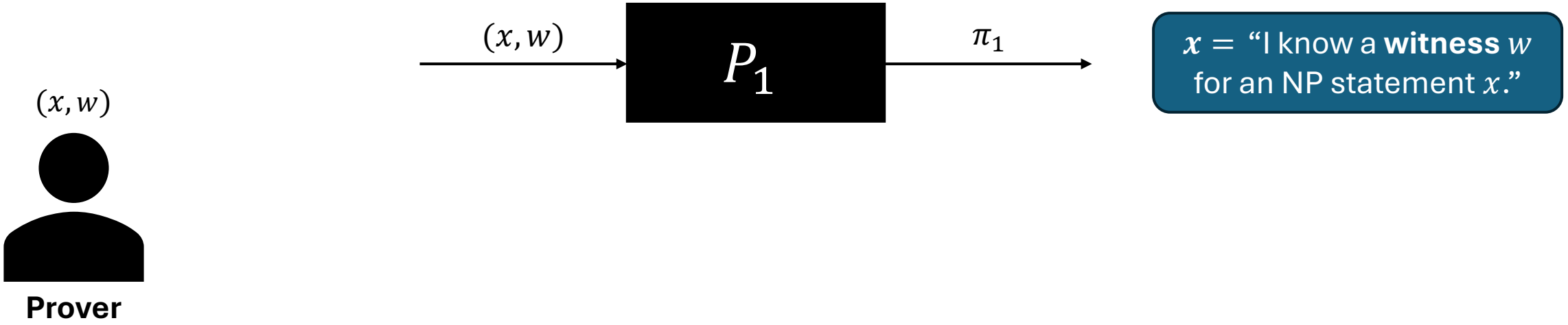
Recursive NIZK

(x, w)

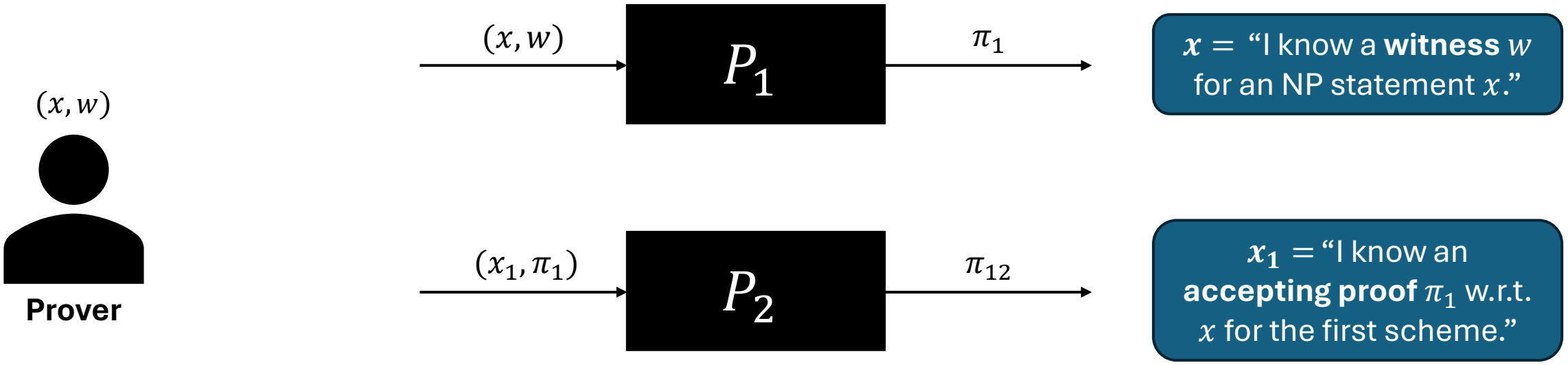


Prover

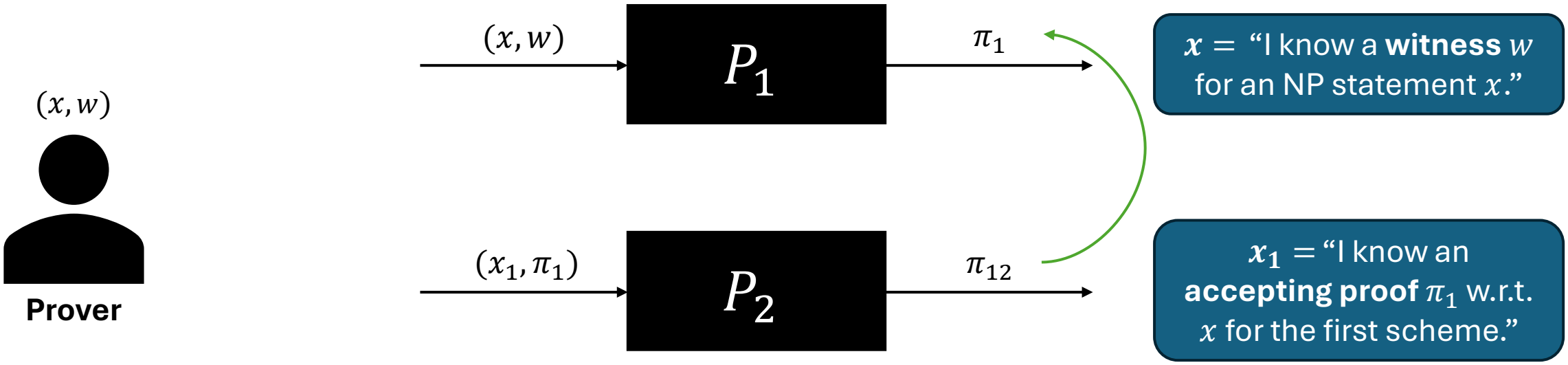
Recursive NIZK



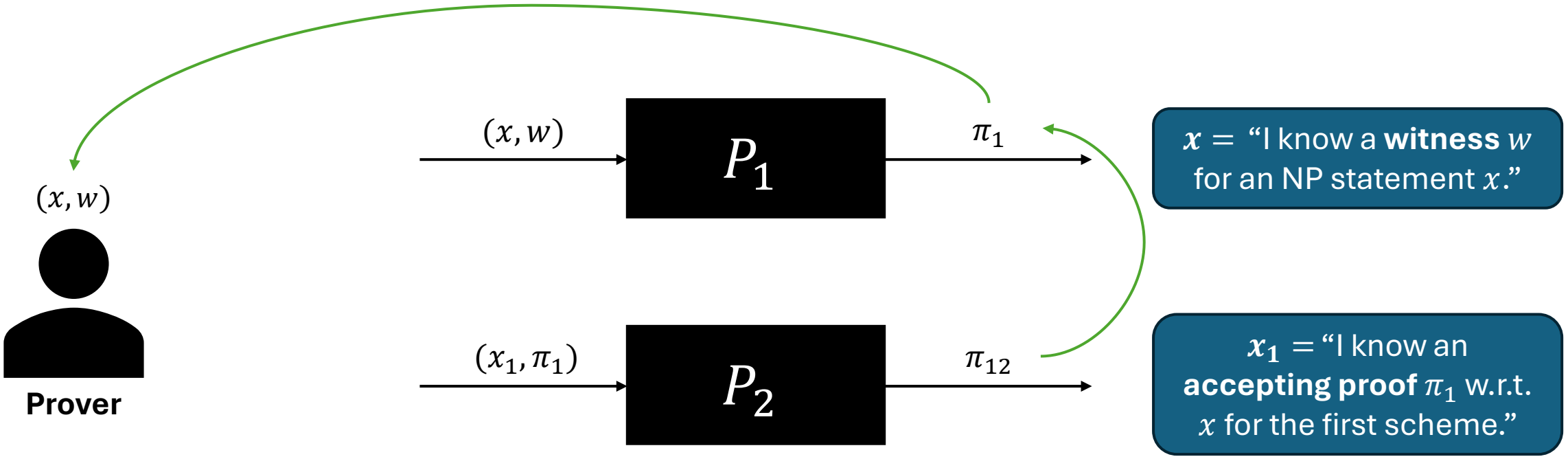
Recursive NIZK



Recursive NIZK



Recursive NIZK

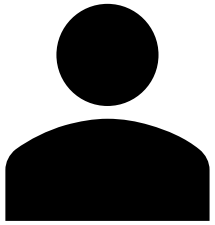


- **Core idea**: hiding π_1 while preserving knowledge soundness.

Robust combiner from recursive NIZK

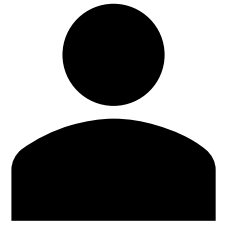
$n = 3$	$t = 2$
$(n - t) + 1 = 2$	

(x, w)



Prover

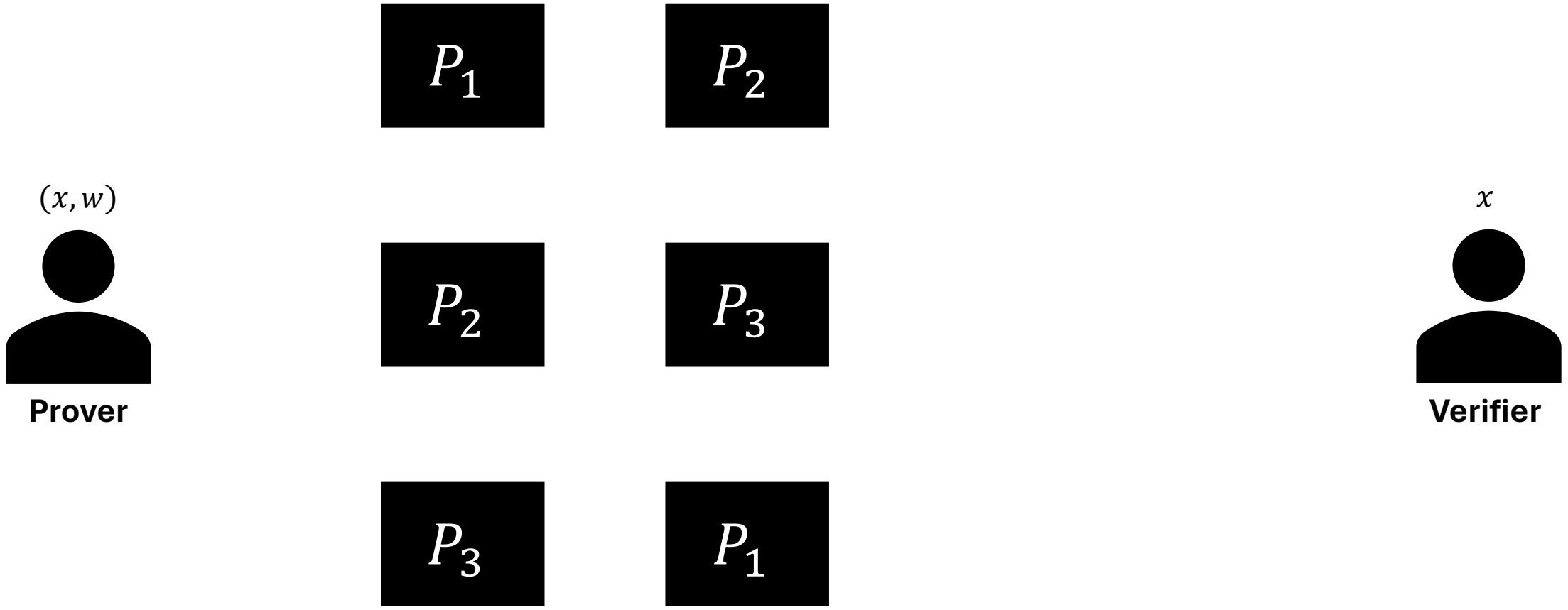
x



Verifier

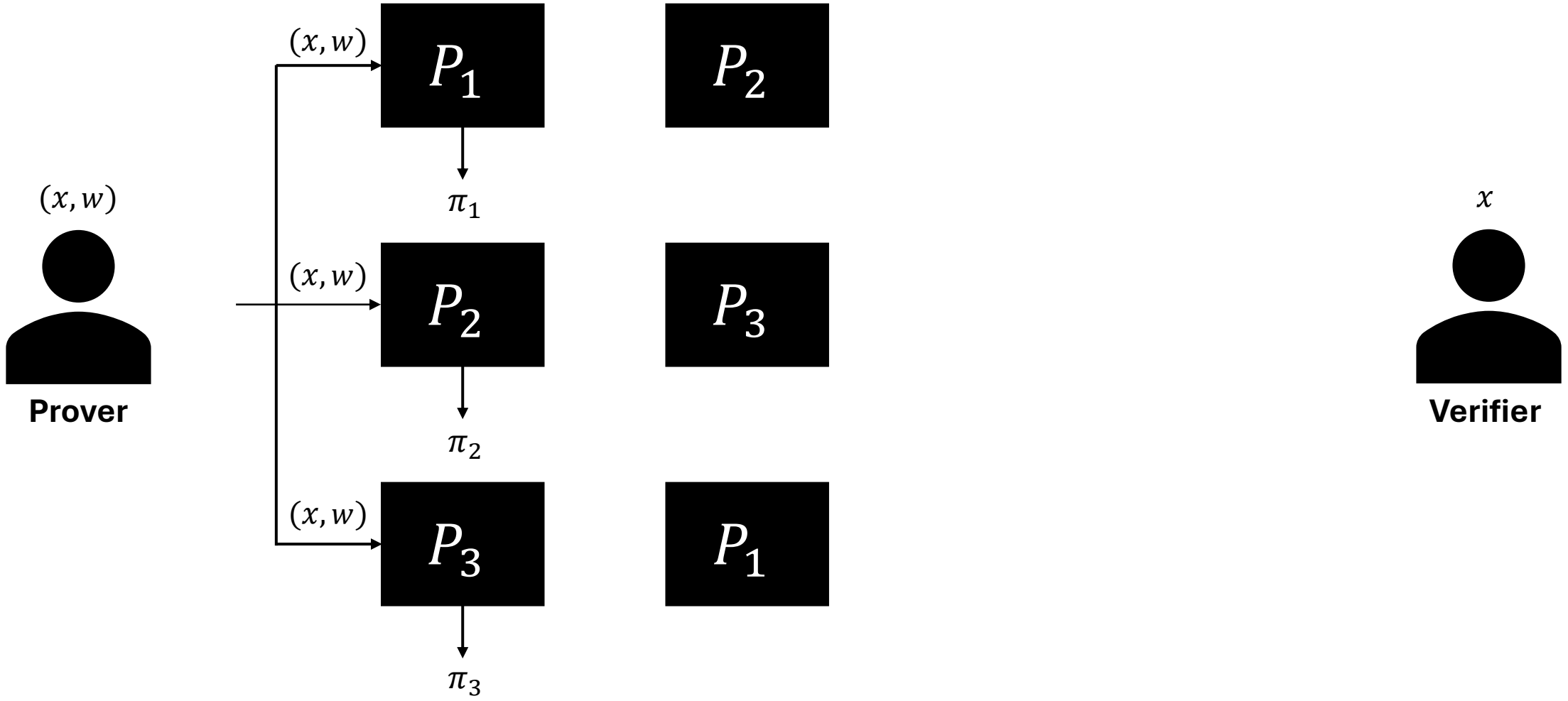
Robust combiner from recursive NIZK

$n = 3$	$t = 2$
$(n - t) + 1 = 2$	



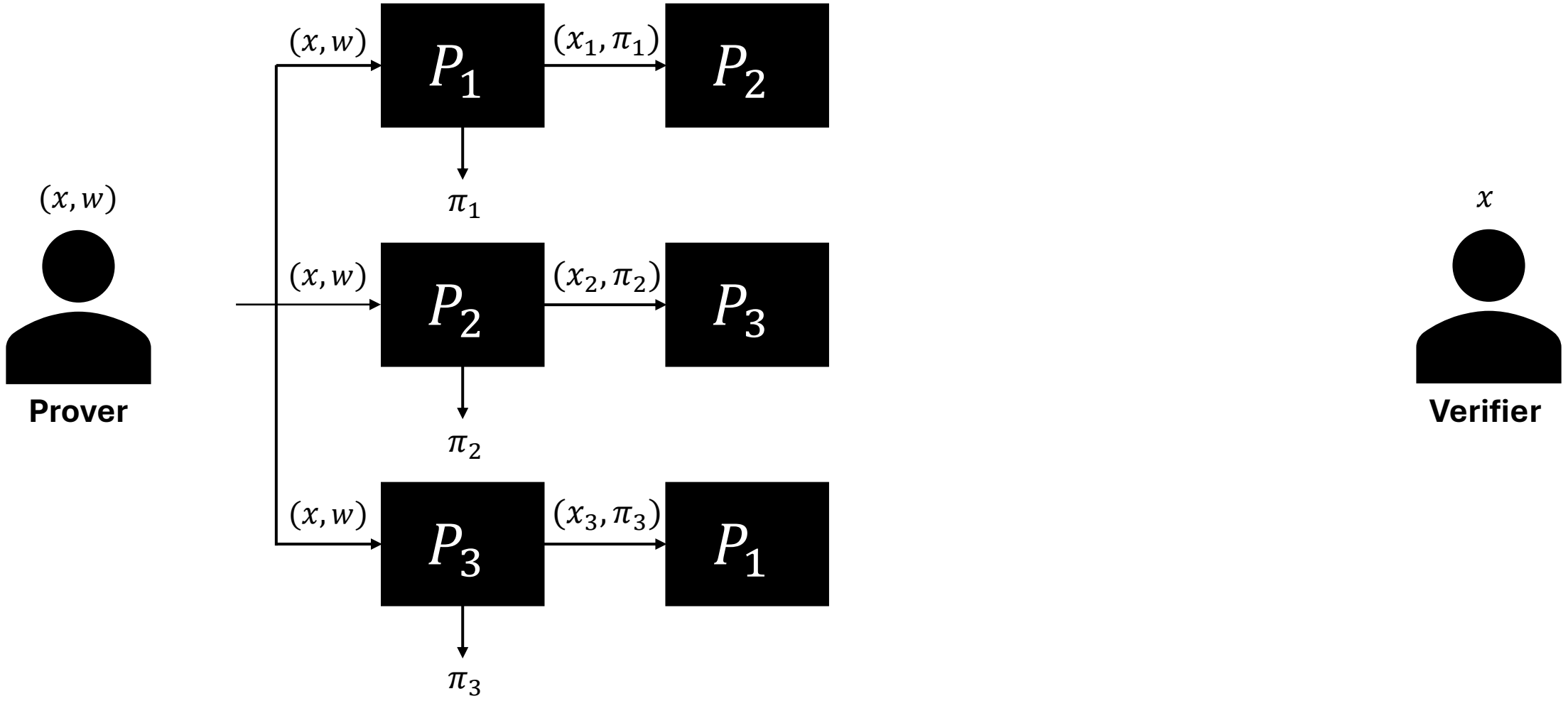
Robust combiner from recursive NIZK

$n = 3$	$t = 2$
$(n - t) + 1 = 2$	



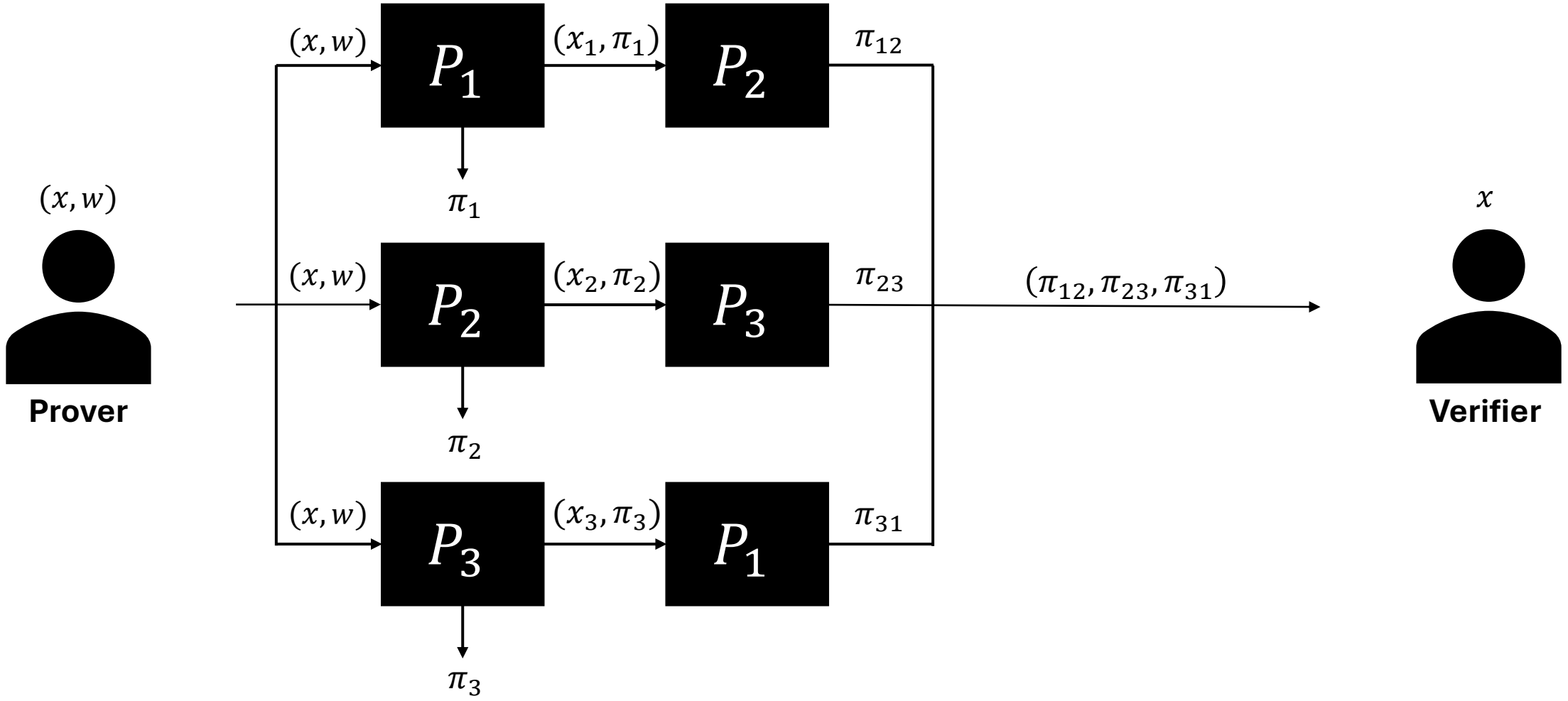
Robust combiner from recursive NIZK

$n = 3$	$t = 2$
$(n - t) + 1 = 2$	



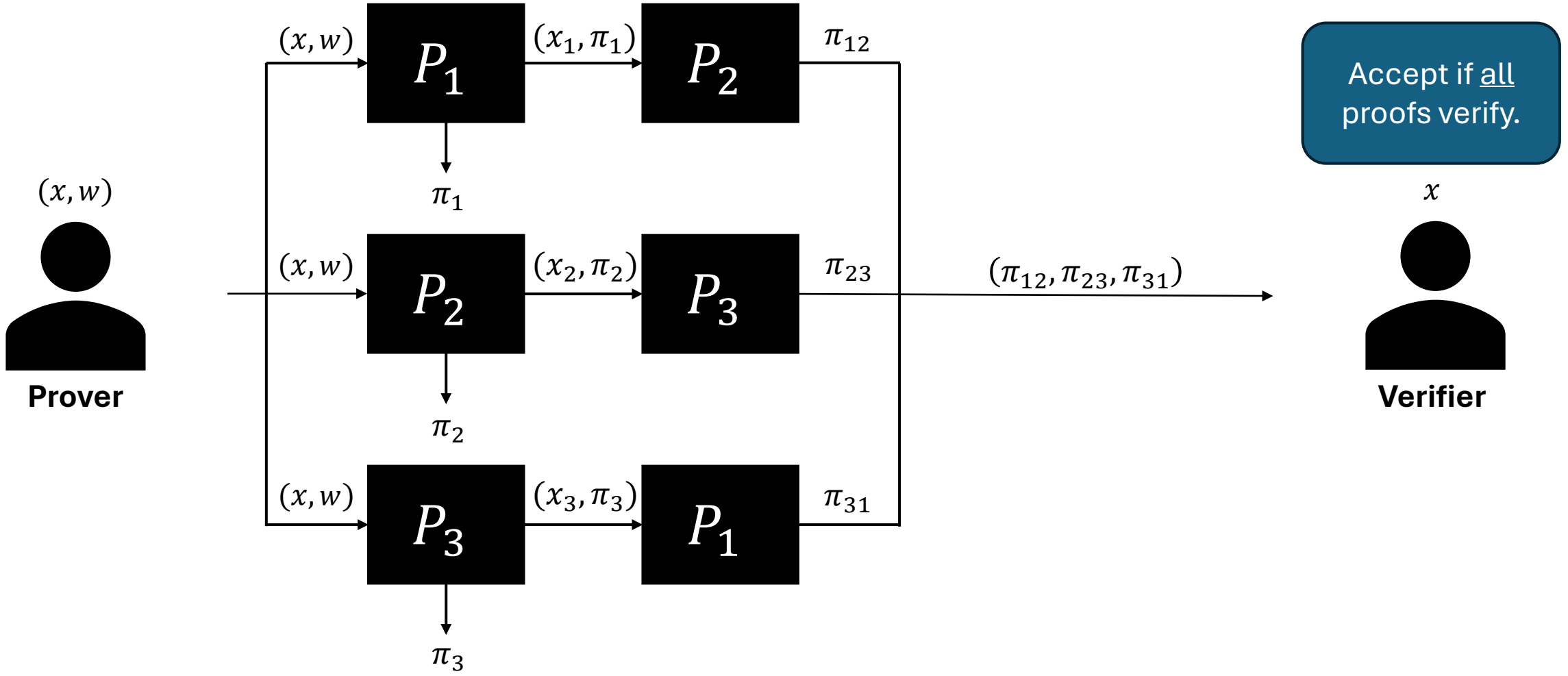
Robust combiner from recursive NIZK

$n = 3$	$t = 2$
$(n - t) + 1 = 2$	

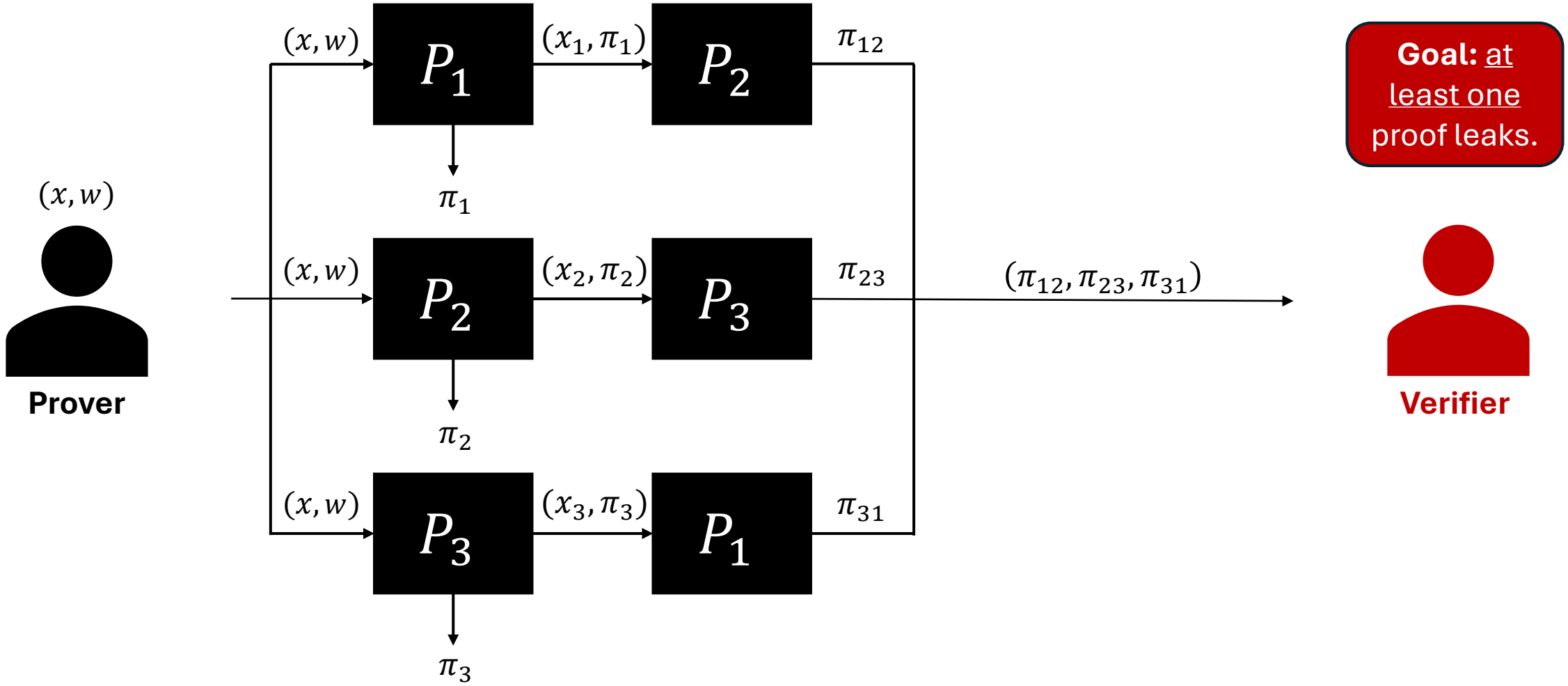


Robust combiner from recursive NIZK

$n = 3$	$t = 2$
$(n - t) + 1 = 2$	

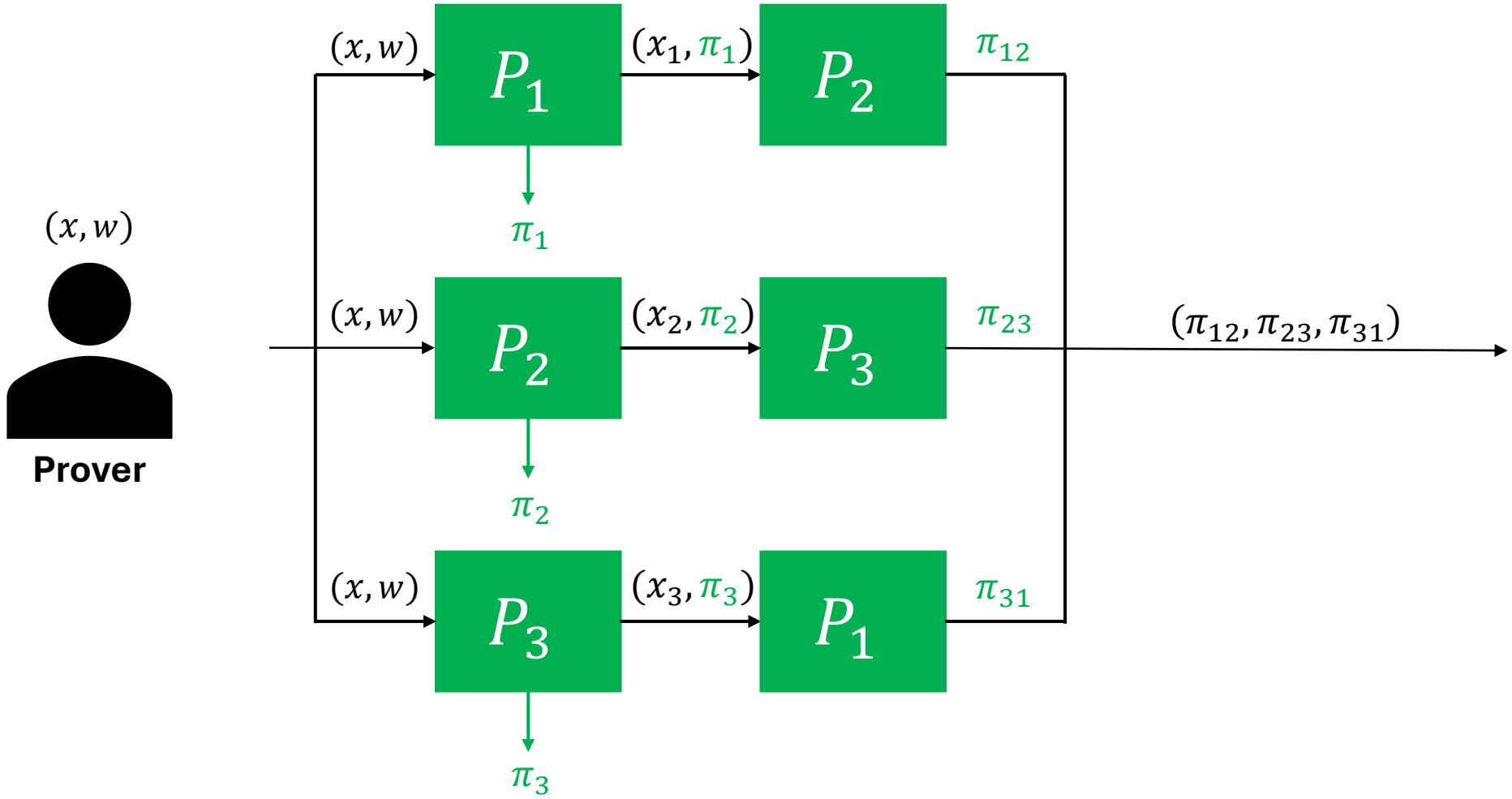


Zero-knowledge



Zero-knowledge

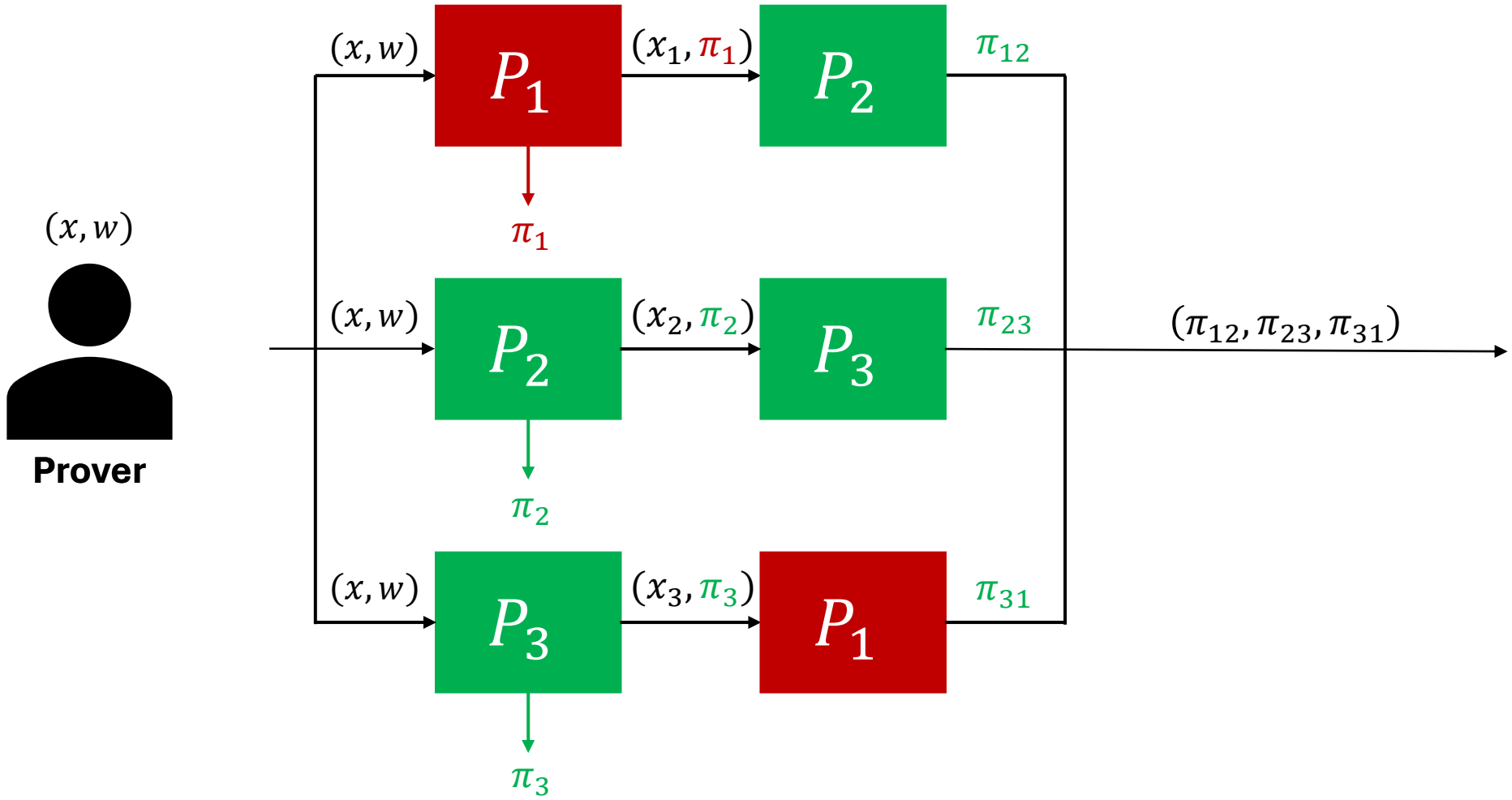
Color Coding
Green: no info on w.
Red: leaks w.



Goal: at least one proof leaks.

Zero-knowledge

Color Coding
Green: no info on w.
Red: leaks w.



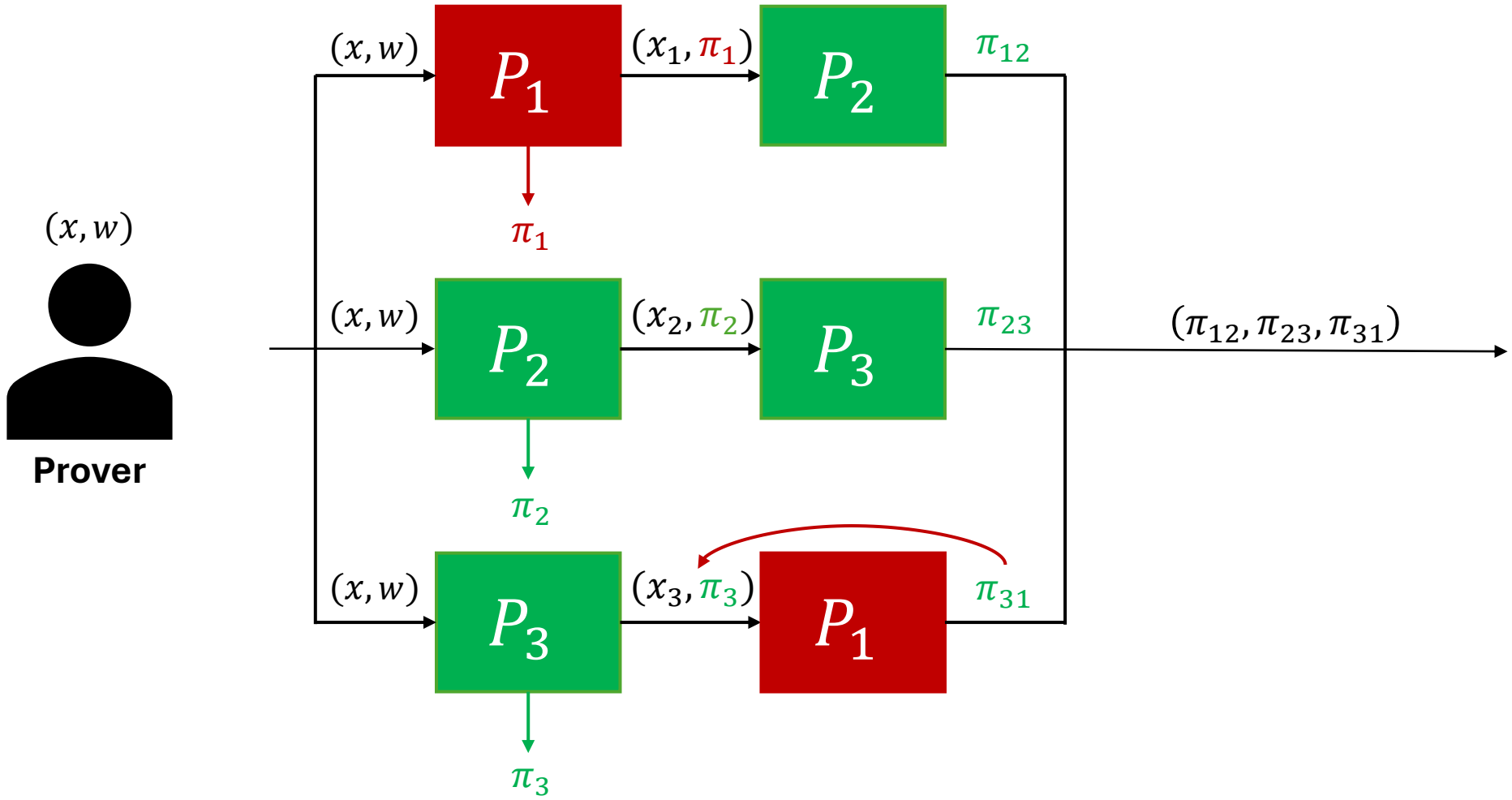
Goal: at least one proof leaks.

Verifier

Red_1^{ZK}

Zero-knowledge

Color Coding
Green: no info on w.
Red: leaks w.



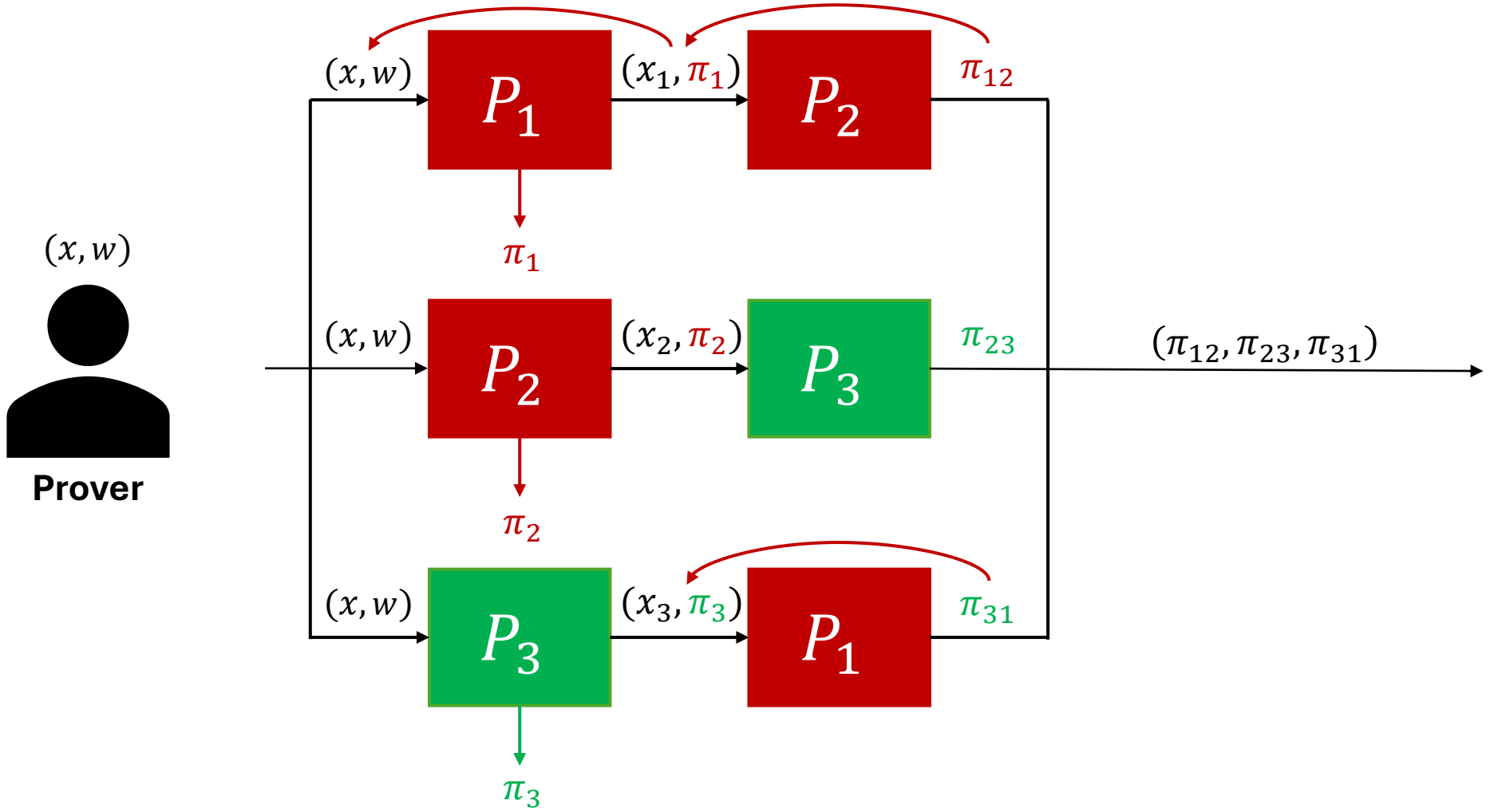
Goal: at least one proof leaks.

Verifier

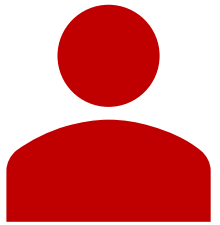
Red_1^{ZK}

Zero-knowledge

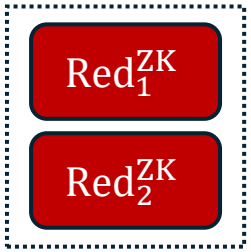
Color Coding
Green: no info on w.
Red: leaks w.



Goal: at least one proof leaks.



Verifier



$(\boldsymbol{n} - \boldsymbol{t}) + \mathbf{1} = 2$ reductions



Constructions overview

Construction	Supported Languages	Threshold	Number of Candidates
“Recursive Proofs”	NP	$t > \lfloor n/2 \rfloor$	$n, t \in \mathrm{O}(1)$

Constructions overview

Construction	Supported Languages	Threshold	Number of Candidates
"Recursive Proofs"	NP	$t > \lfloor n/2 \rfloor$	$n, t \in O(1)$
"Homomorphic Secret Sharing"	Homomorphic Languages	$t > \lfloor n/2 \rfloor$	$n, t \in \text{poly}(\lambda)$
"MPC in the head"	NP	$t > \lfloor 2n/3 \rfloor$	$n, t \in \text{poly}(\lambda)$

Bird’s eye view

Warm-up: Robust Combiners	Definitions & Impossibility Results
Constructions	**Wrapping up**

Wrapping up

- **Full version**: https://ia.cr/2025/240.
  - Formal definitions and impossibility results.
  - Full details of the three constructions.
  - Security proofs (**non-trivial techniques** to find reductions).



Wrapping up

- **Full version**: https://ia.cr/2025/240.
  - Formal definitions and impossibility results.
  - Full details of the three constructions.
  - Security proofs (**non-trivial techniques** to find reductions).

- **Open problems:**
  - Definitions in alternative models (ROM, separate threshold for each property, …).
  - Alternative security properties (witness indistinguishability, simulation soundness, …).
  - **More constructions!**



Wrapping up

- **Full version**: https://ia.cr/2025/240.
  - Formal definitions and impossibility results.
  - Full details of the three constructions.
  - Security proofs (**non-trivial techniques** to find reductions).

- **Open problems:**
  - Definitions in alternative models (ROM, separate threshold for each property, …).
  - Alternative security properties (witness indistinguishability, simulation soundness, …).
  - **More constructions!**

- **Key takeaway**: combiners are yet another formal tool to distribute trust assumptions!



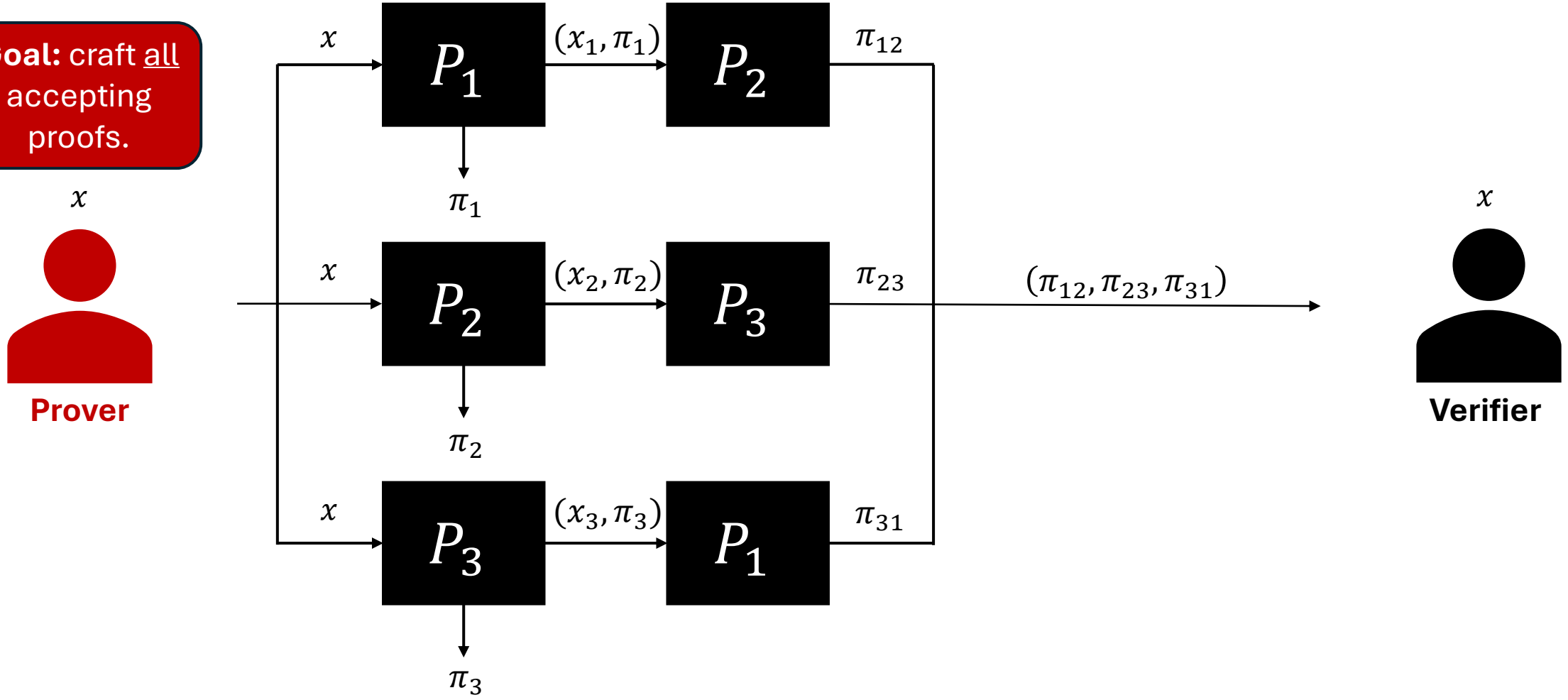
Thanks!

Backup Slides A

Knowledge soundness of the combiner from recursive NIZK

Knowledge soundness

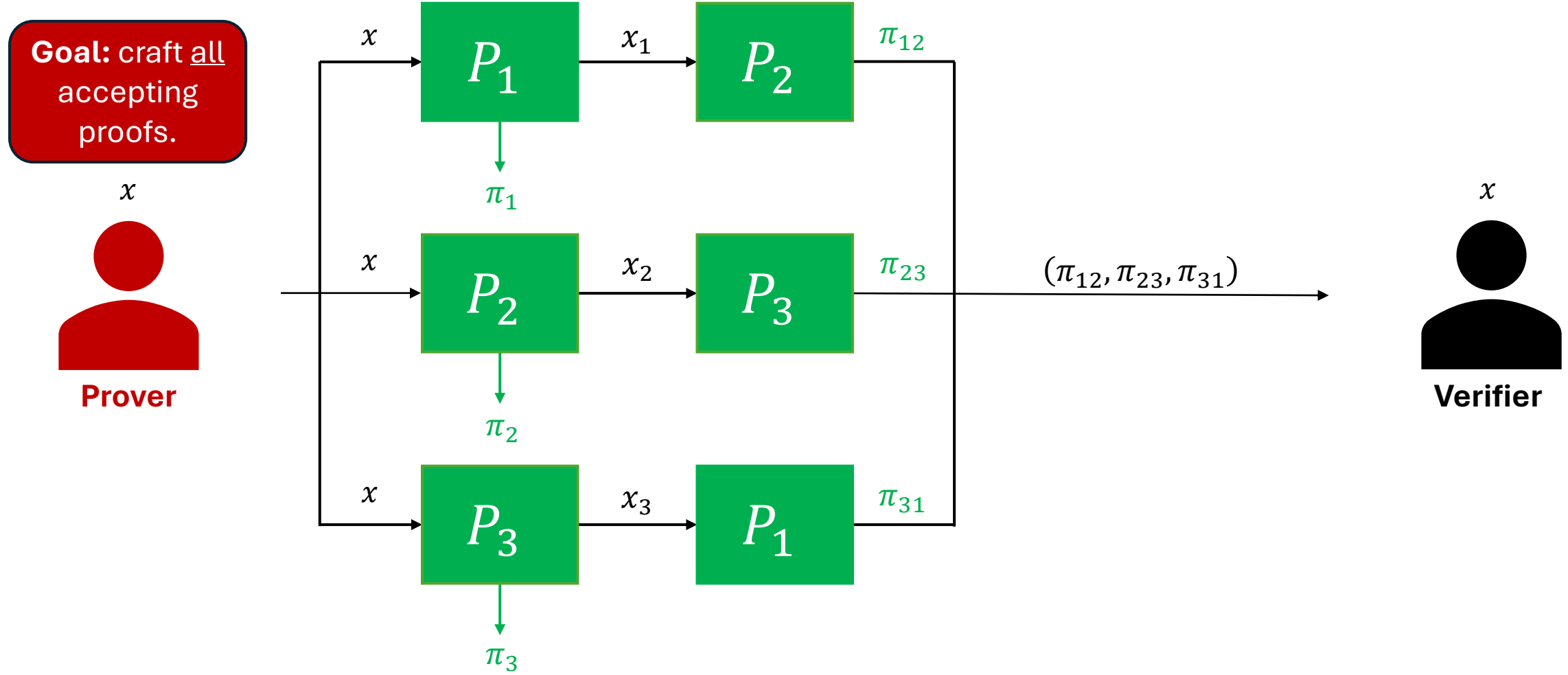
Goal: craft <u>all</u> accepting proofs.



Knowledge soundness

Color Coding
Green: non-accepting.
Red: accepting.

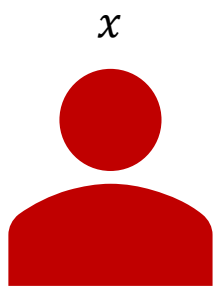
Goal: craft <u>all</u> accepting proofs.



Knowledge soundness

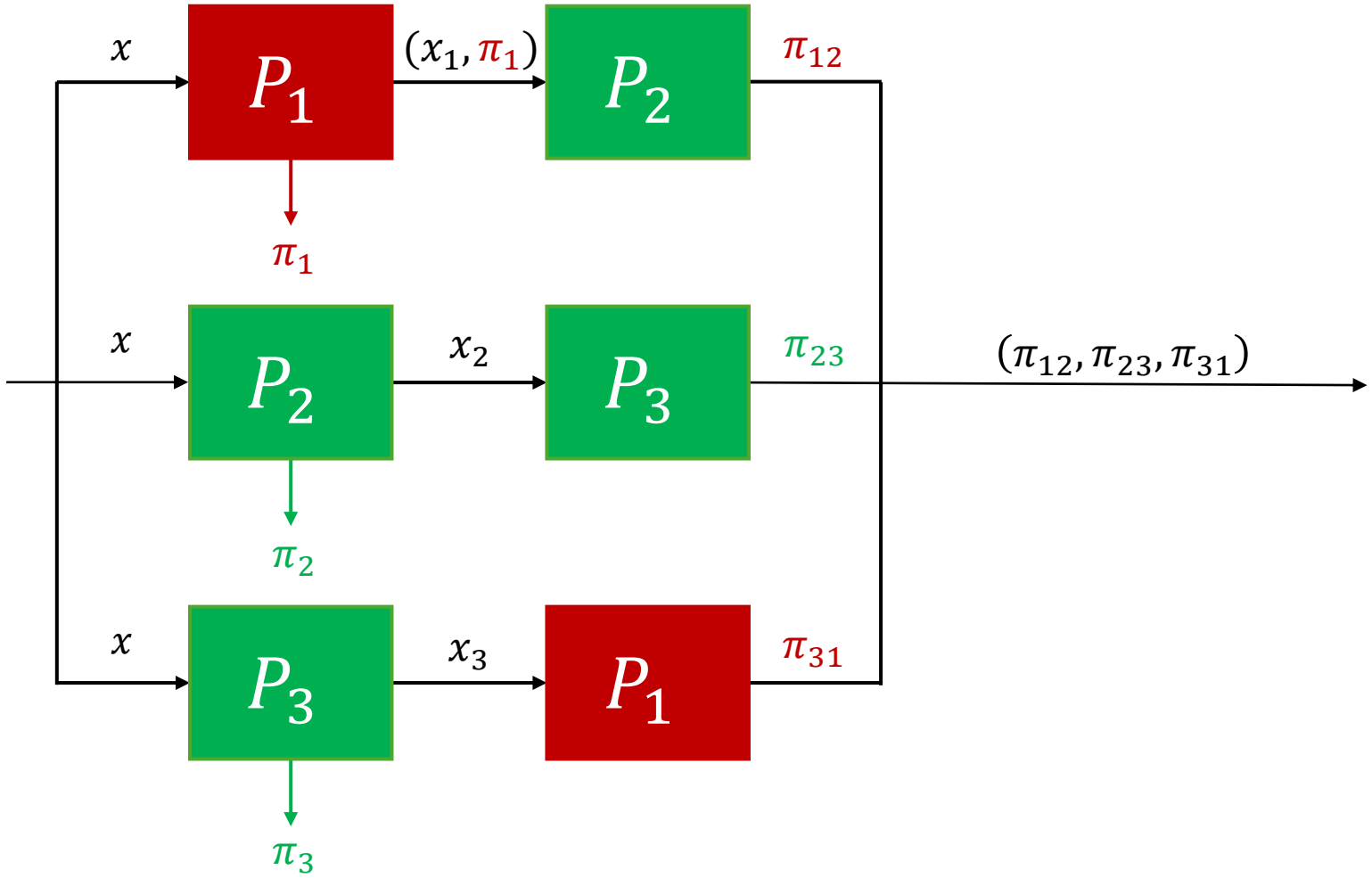
Color Coding
Green: non-accepting.
Red: accepting.

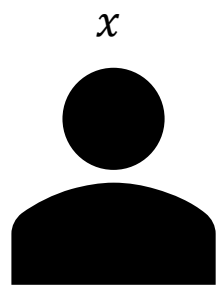
Goal: craft <u>all</u> accepting proofs.



Prover

$\text{Red}_1^{\text{PoK}}$



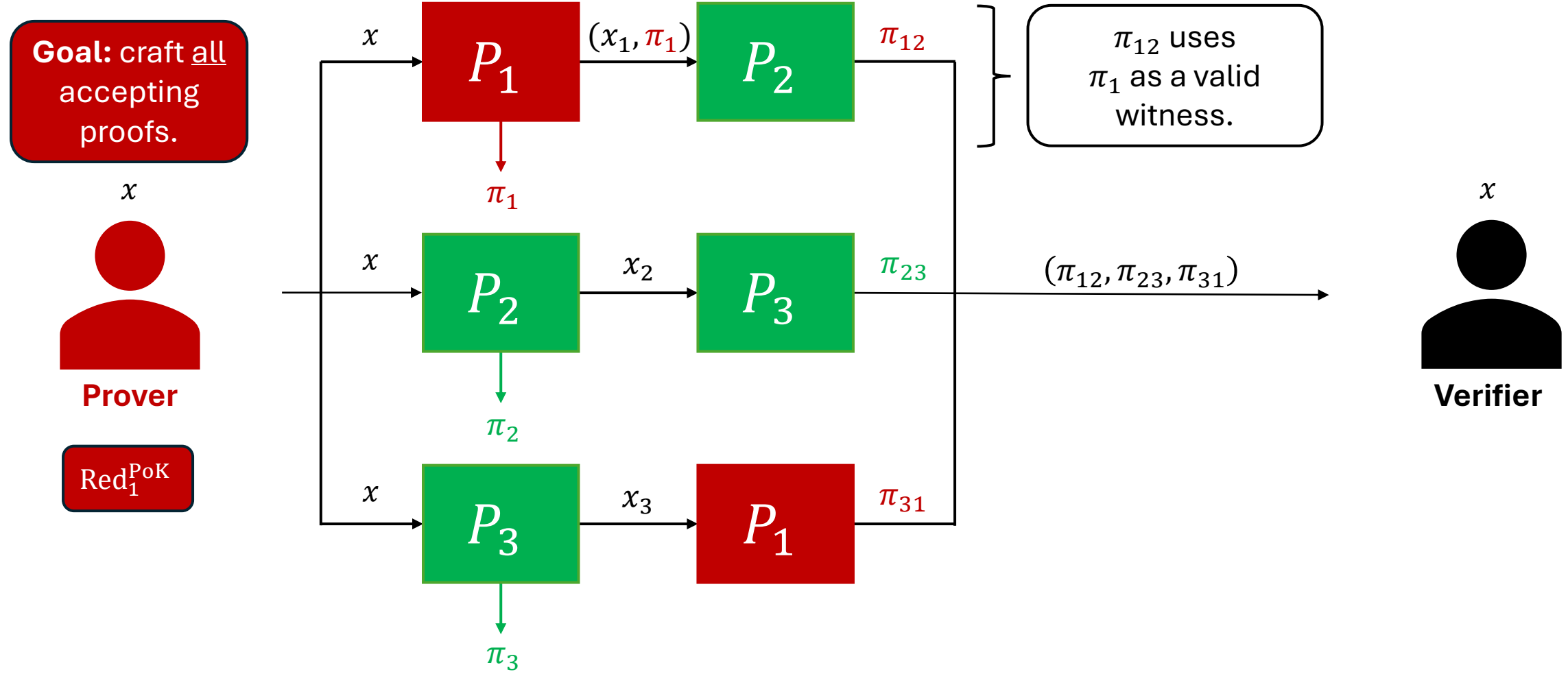


Verifier

Knowledge soundness

Color Coding
Green: non-accepting.
Red: accepting.

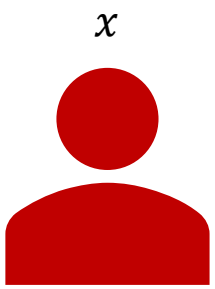
Goal: craft <u>all</u> accepting proofs.



Knowledge soundness

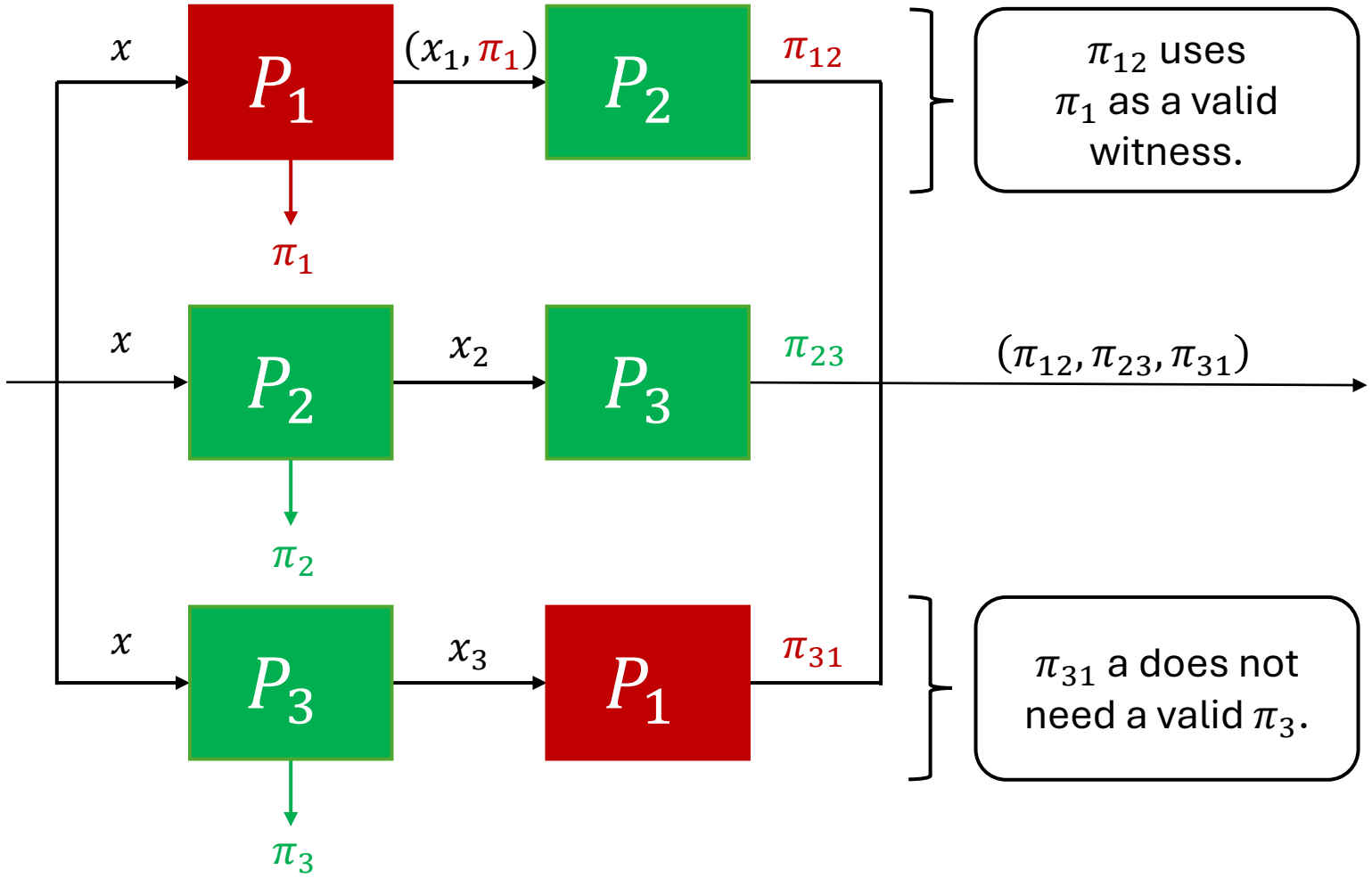
Color Coding
Green: non-accepting.
Red: accepting.

Goal: craft <u>all</u> accepting proofs.



Prover

$\text{Red}_1^{\text{PoK}}$

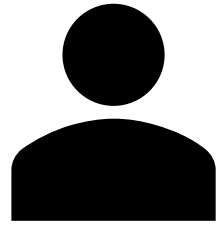


π_{12} uses π_1 as a valid witness.

$(\pi_{12}, \pi_{23}, \pi_{31})$

π_{31} a does not need a valid π_3.

x

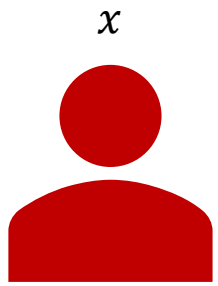


Verifier

Knowledge soundness

Color Coding
Green: non-accepting.
Red: accepting.

Goal: craft <u>all</u> accepting proofs.

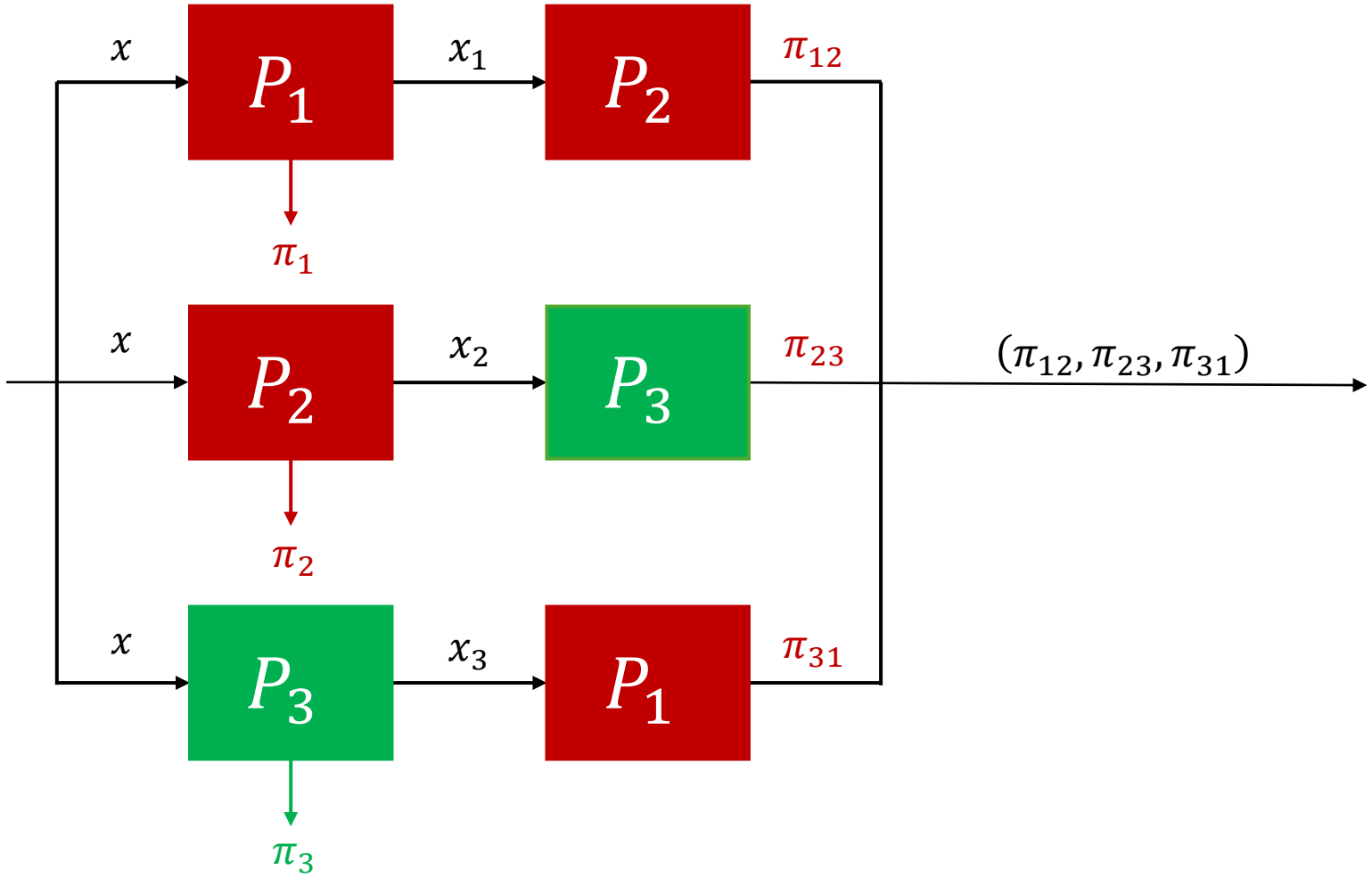


Prover

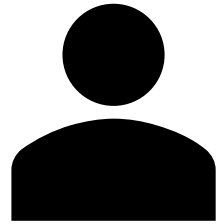
$\mathrm{Red}_1^{\mathrm{PoK}}$

$\mathrm{Red}_2^{\mathrm{PoK}}$

$(n - t) + 1 = 2$ reductions



x



Verifier

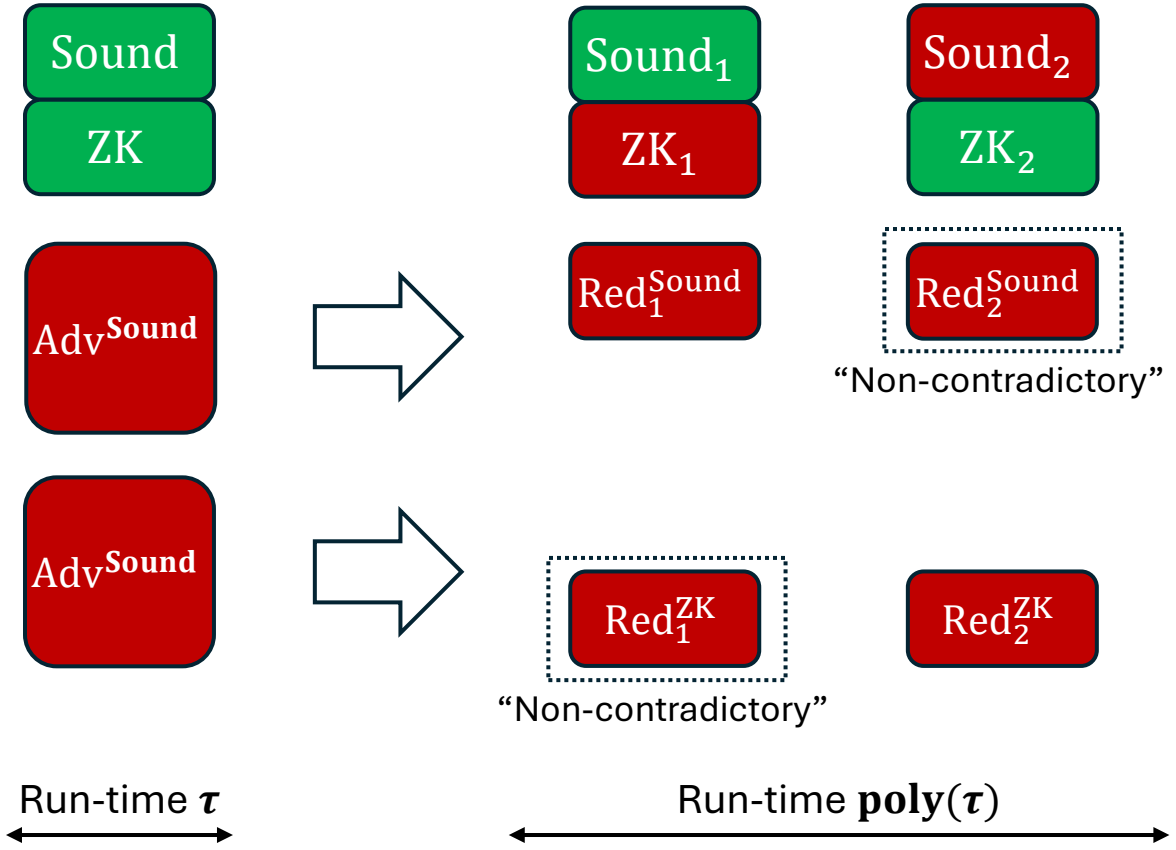
Backup Slides B

Impossibility Sketch

Impossibility for $t \leq n/2$

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$



Impossibility for $t \leq n/2$

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$







NIZK_1

- $\mathrm{Setup}(1^\lambda)$: Output $\perp$.
- $\mathrm{P}(x, w)$: Output w.
- $\mathrm{V}(x, \pi)$: Check w against x.

NIZK_2

- $\mathrm{Setup}(1^\lambda)$: Output $\perp$.
- $\mathrm{P}(x, w)$: Output 0.
- $\mathrm{V}(x, \pi)$: Output $\pi == 0$.

➢ NIZK_1 is **unconditionally** sound, NIZK_2 is **unconditionally** zero-knowledge.

Impossibility for $t \leq n/2$

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$







NIZK_1

- $\mathrm{Setup}(1^\lambda)$: Output $\perp$.
- $\mathrm{P}(x, w)$: Output w.
- $\mathrm{V}(x, \pi)$: Check w against x.

NIZK_2

- $\mathrm{Setup}(1^\lambda)$: Output $\perp$.
- $\mathrm{P}(x, w)$: Output 0.
- $\mathrm{V}(x, \pi)$: Output $\pi == 0$.

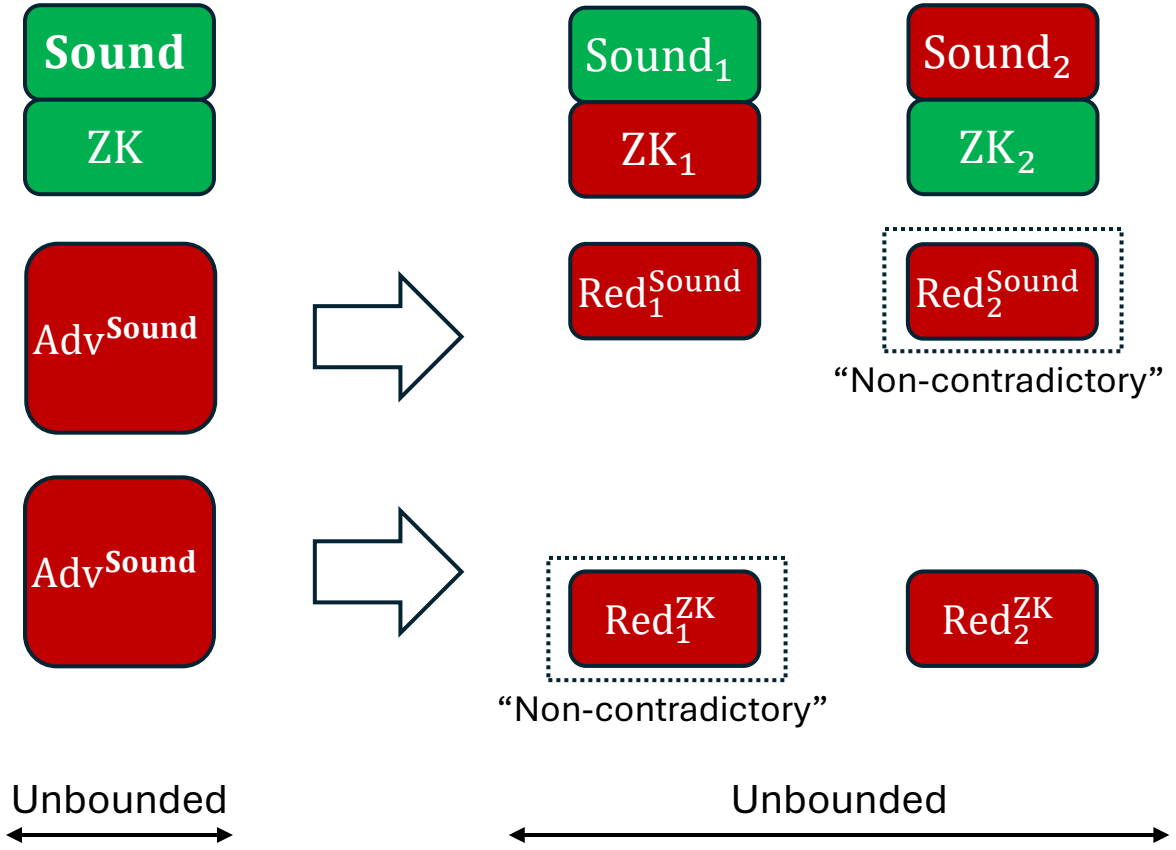
- NIZK_1 is **unconditionally** sound, NIZK_2 is **unconditionally** zero-knowledge.

- By contradiction, $\mathrm{NIZK}_{\mathrm{comb}}$ should output a **secure NIZK** upon input NIZK_1 and NIZK_2 as above.

Impossibility for $t \leq n/2$

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

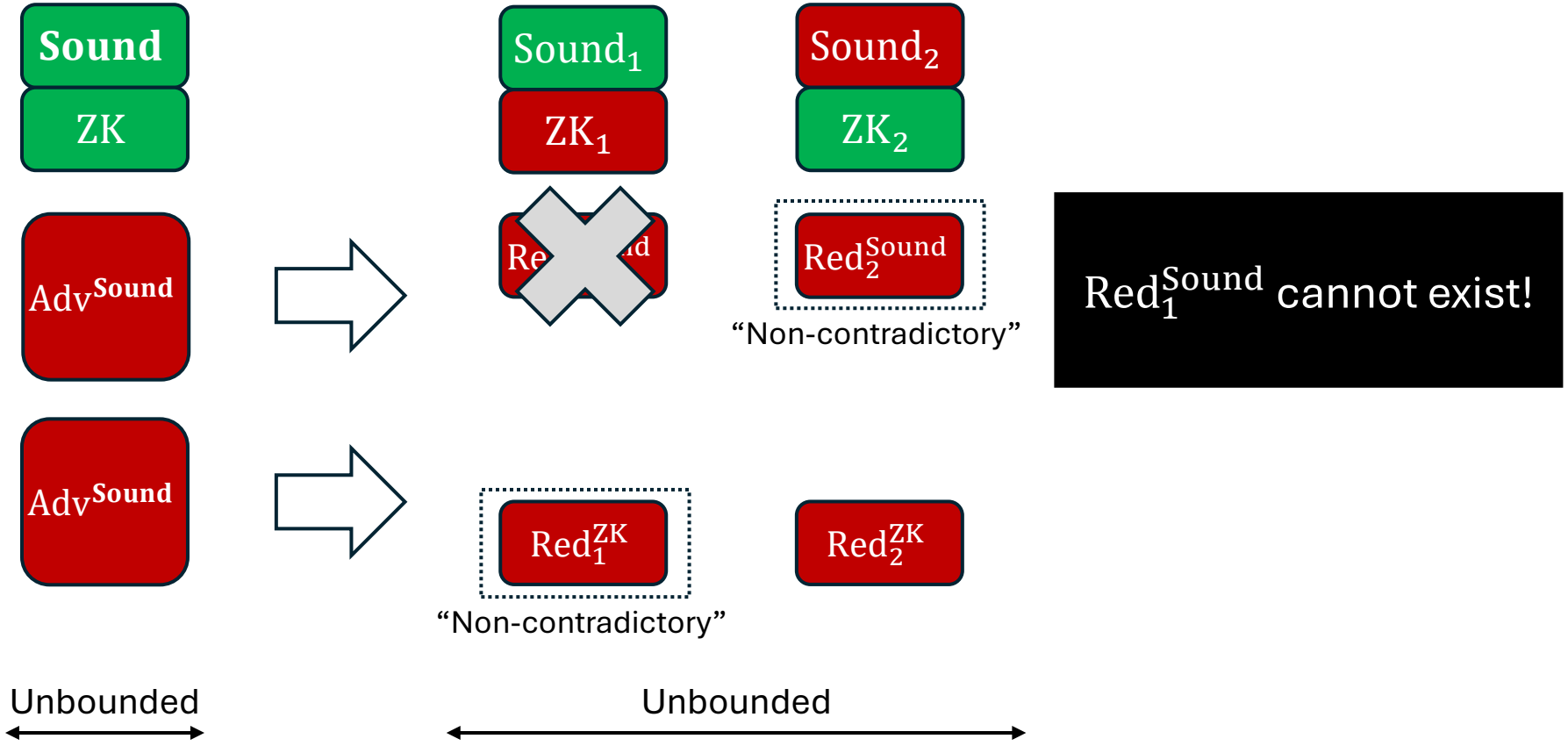
$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$



Impossibility for $t \leq n/2$

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

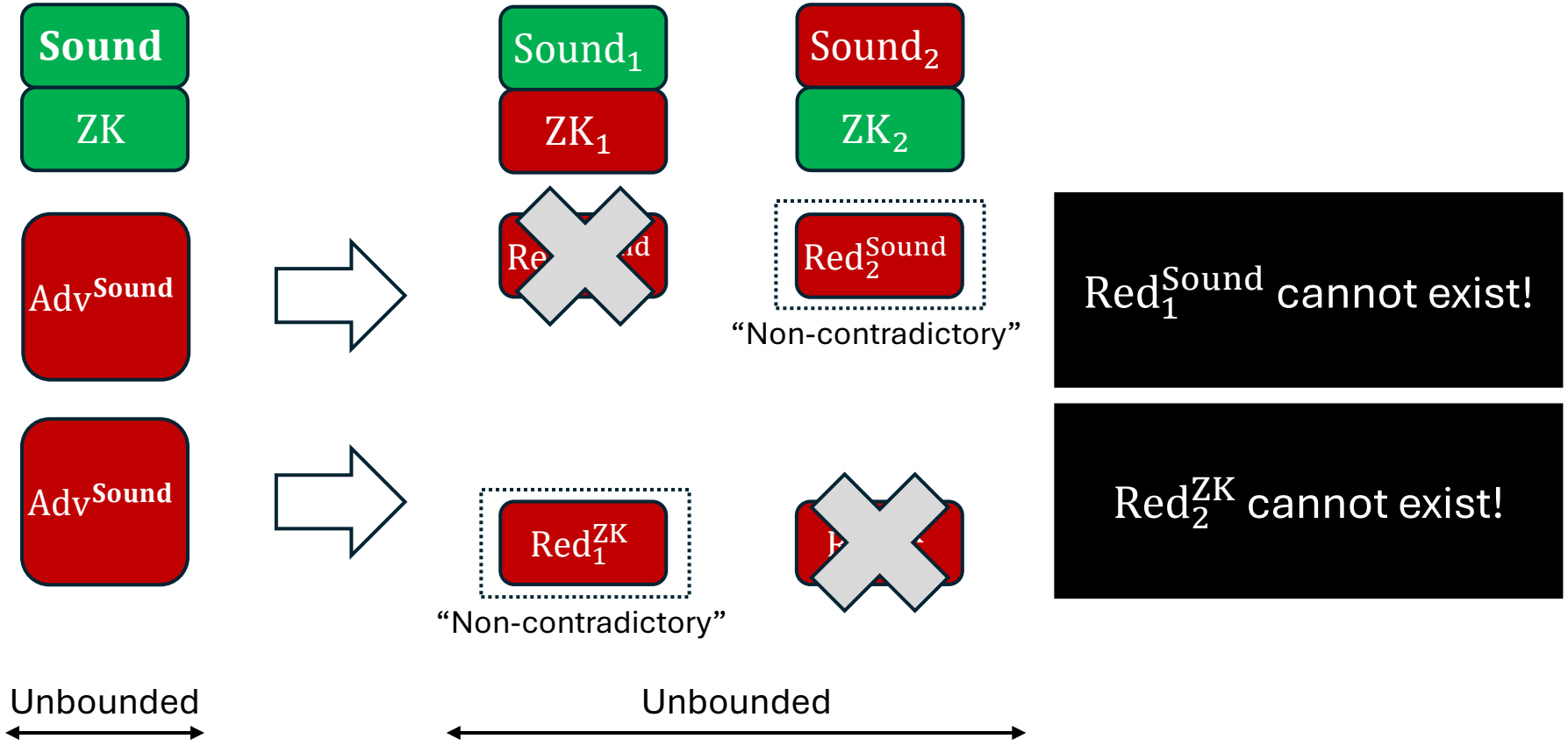
$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$



Impossibility for $t \leq n/2$

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

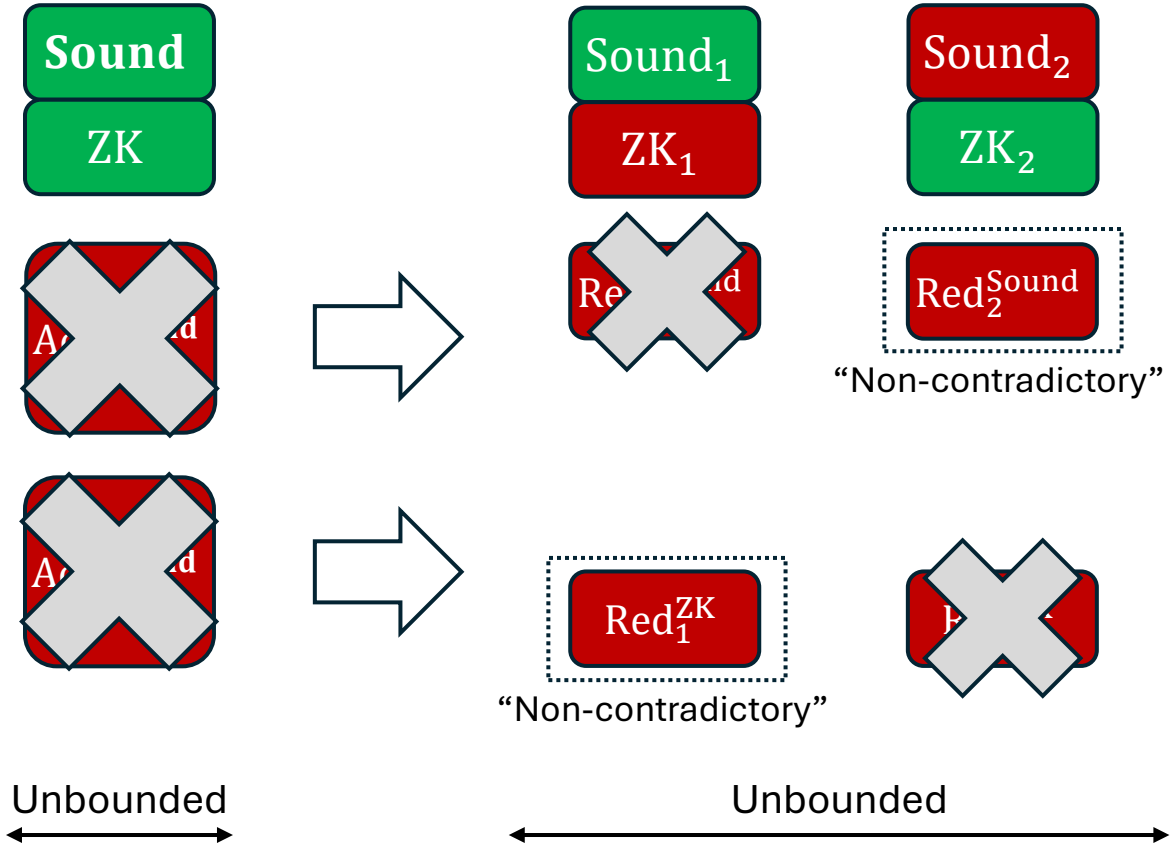
$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$



Impossibility for $t \leq n/2$

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$



$\mathrm{Adv}^{\mathbf{Sound}}$ cannot exist!

$\mathrm{Red}_1^{\mathrm{Sound}}$ cannot exist!

$\mathrm{Red}_2^{\mathrm{ZK}}$ cannot exist!

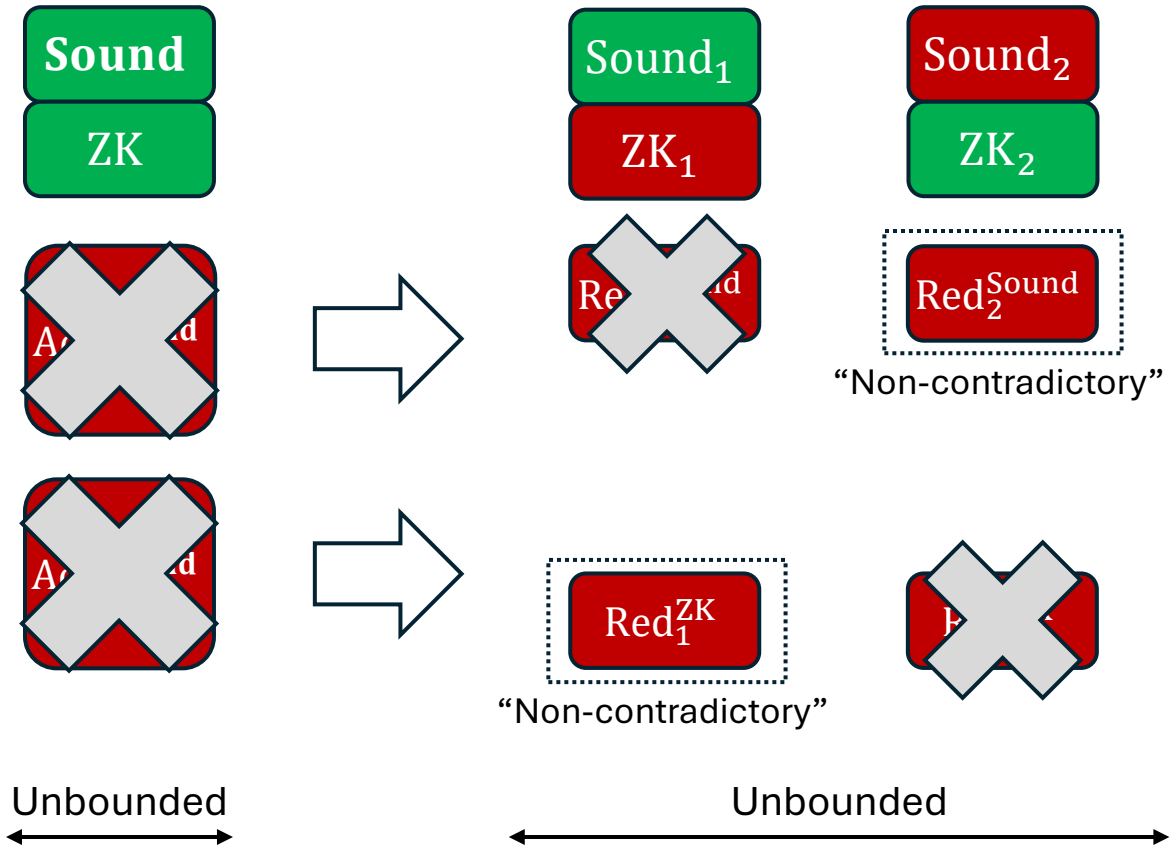
Impossibility for $t \leq n/2$

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$

$\mathrm{NIZK}_{\mathrm{comb}}$ retains soundness even against unbounded adversaries.

$\mathrm{Adv}^{\mathbf{Sound}}$ cannot exist!



$\mathrm{Red}_1^{\mathrm{Sound}}$ cannot exist!

$\mathrm{Red}_2^{\mathrm{ZK}}$ cannot exist!

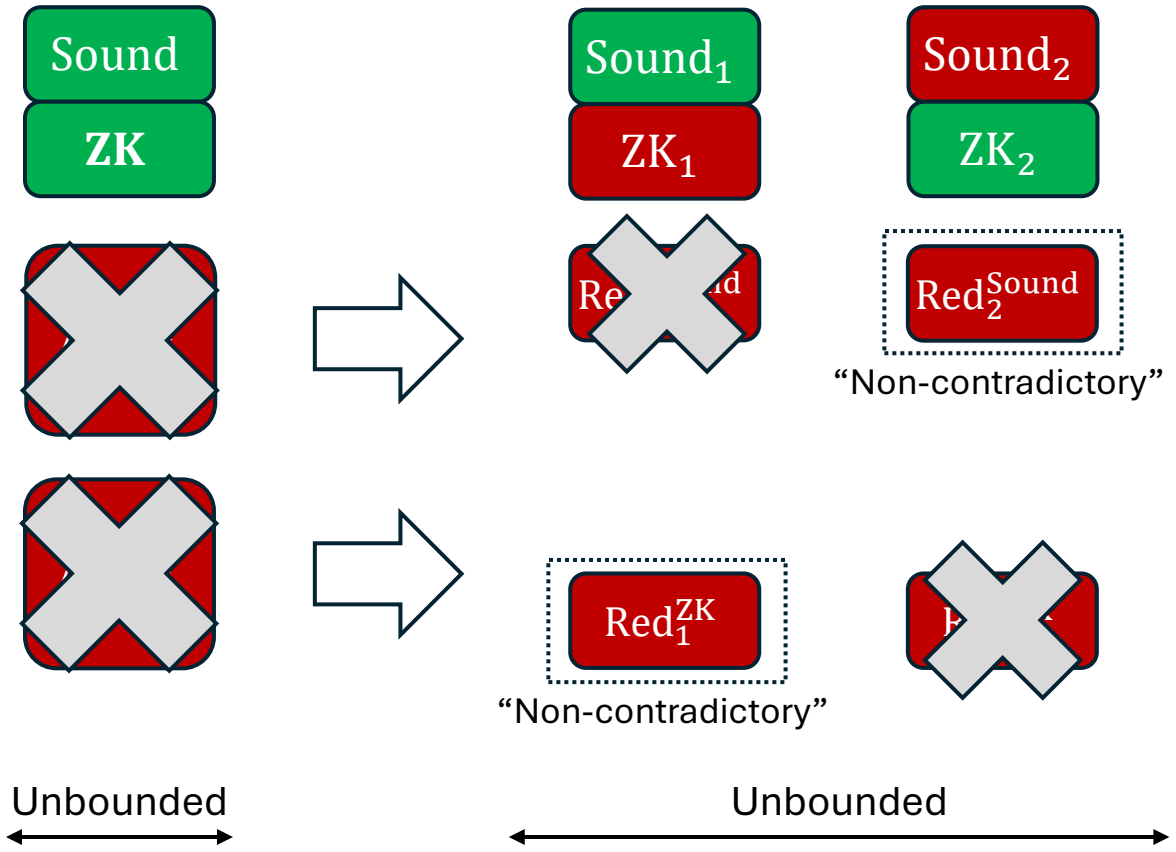
Impossibility for $t \leq n/2$

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$

$\mathrm{NIZK}_{\mathrm{comb}}$ retains zero-knowledge even against unbounded adversaries.

$\mathrm{Adv}^{\mathbf{ZK}}$ cannot exist!



$\mathrm{Red}_1^{\mathrm{Sound}}$ cannot exist!

$\mathrm{Red}_2^{\mathrm{ZK}}$ cannot exist!

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

Impossibility for $t \leq n/2$

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$







$\mathrm{NIZK}_{\mathrm{comb}}$ retains soundness even against unbounded adversaries.

$\mathrm{NIZK}_{\mathrm{comb}}$ retains zero-knowledge even against unbounded adversaries.

Impossibility for $t \leq n/2$

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$







$\mathrm{NIZK}_{\mathrm{comb}}$ retains soundness even against unbounded adversaries.

$\mathrm{NIZK}_{\mathrm{comb}}$ retains zero-knowledge even against unbounded adversaries.

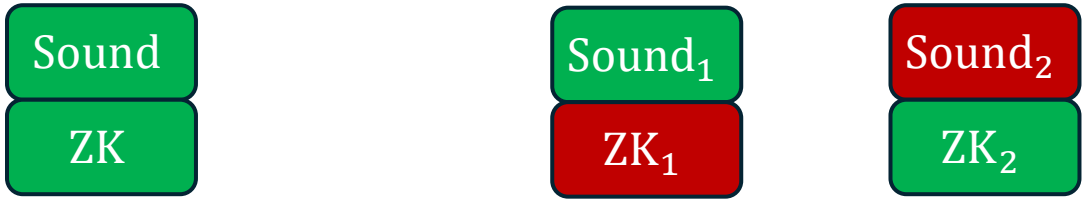
- $\mathrm{NIZK}_{\mathrm{comb}}$ is both unconditionally sound **and** unconditionally zero-knowledge.

[PS05] R. Pass, A. Shelat, "Unconditional characterizations of non-interactive zero-knowledge." CRYPTO'05. https://www.iacr.org/archive/crypto2005/36210114/36210114.pdf

$n = 2$	$t = 1$
$(n - t) + 1 = 2$	

Impossibility for $t \leq n/2$

$$\mathrm{NIZK}_{\mathrm{comb}} = f(\mathrm{NIZK}_1, \mathrm{NIZK}_2)$$



$\mathrm{NIZK}_{\mathrm{comb}}$ retains soundness even against unbounded adversaries.

$\mathrm{NIZK}_{\mathrm{comb}}$ retains zero-knowledge even against unbounded adversaries.

- $\mathrm{NIZK}_{\mathrm{comb}}$ is both unconditionally sound **and** unconditionally zero-knowledge.
- Such a NIZK cannot exist for NP, unless the polynomial hierarchy collapses [PS05]!