Dual-Mode NIZKs:

Possibility and Impossibility Results for Property Transfer

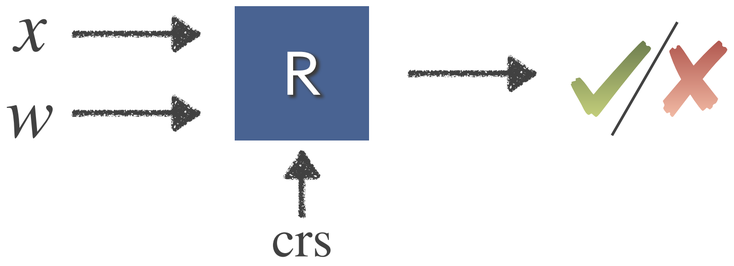
Vivek Arte

Mihir Bellare

UC San Diego

https://eprint.iacr.org/2020/629

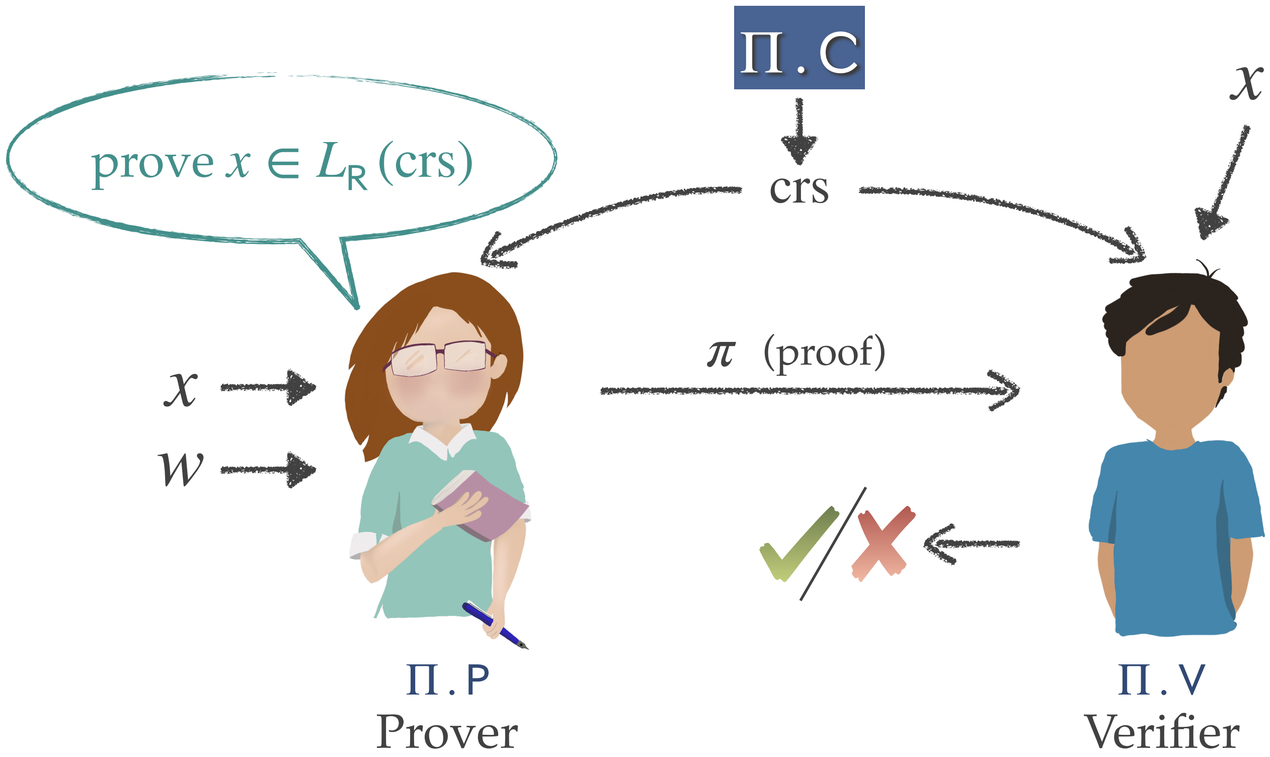
Non-interactive Proof Systems [BFM88]



NP relation

language associated with R and crs

$$L_{\mathsf{R}}(\mathrm{crs}) = \left\{ x \mid \exists w \text{ s.t. } \mathsf{R}(\mathrm{crs}, x, w) = \mathsf{true} \right\}$$



Syntax

$\mathrm{crs} \leftarrow \Pi.\mathsf{C}(1^\lambda)$ — CRS generation

$\pi \leftarrow \Pi.\mathsf{P}(1^\lambda, \mathrm{crs}, x, w)$ — Proof generation

$d \leftarrow \Pi.\mathsf{V}(1^\lambda, \mathrm{crs}, x, \pi)$ — Verification

Properties for Non-Interactive Proof Systems

Soundness

An adversary (given the crs) should **not** be able to find $x \notin L_{\mathsf{R}}(\mathrm{crs})$ and a proof π such that $\Pi \,.\, \mathsf{V}(1^{\lambda}, \mathrm{crs}, x, \pi) = \mathsf{true}$

There are different variants of soundness present. We will consider : SND-E and SND-P

Extractability [GMR89,BG93,DP92]

has access to a trapdoor underlying the crs

If an adversary produces a valid proof for a statement, there is an extractor that can extract the witness from the information available to the adversary

Witness-indistinguishability

$\mathsf{R}(\mathrm{crs}, x, w_0) = \mathsf{R}(\mathrm{crs}, x, w_1) = \mathsf{true}$

If one knows $x \in L_{\mathsf{R}}(\mathrm{crs})$ and two witnesses w_0 and w_1 for x, then it is hard to tell which witness was used for proof generation

Zero-knowledge

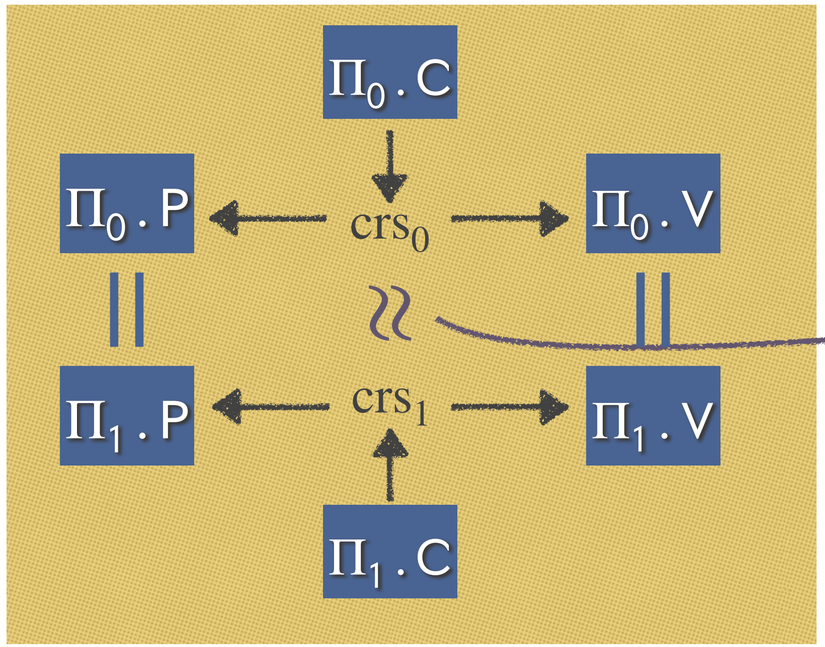
A proof generated for a statement $x \in L_{\mathsf{R}}(\mathrm{crs})$ should reveal no information about the witness for the statement.

Dual-mode Proof Systems

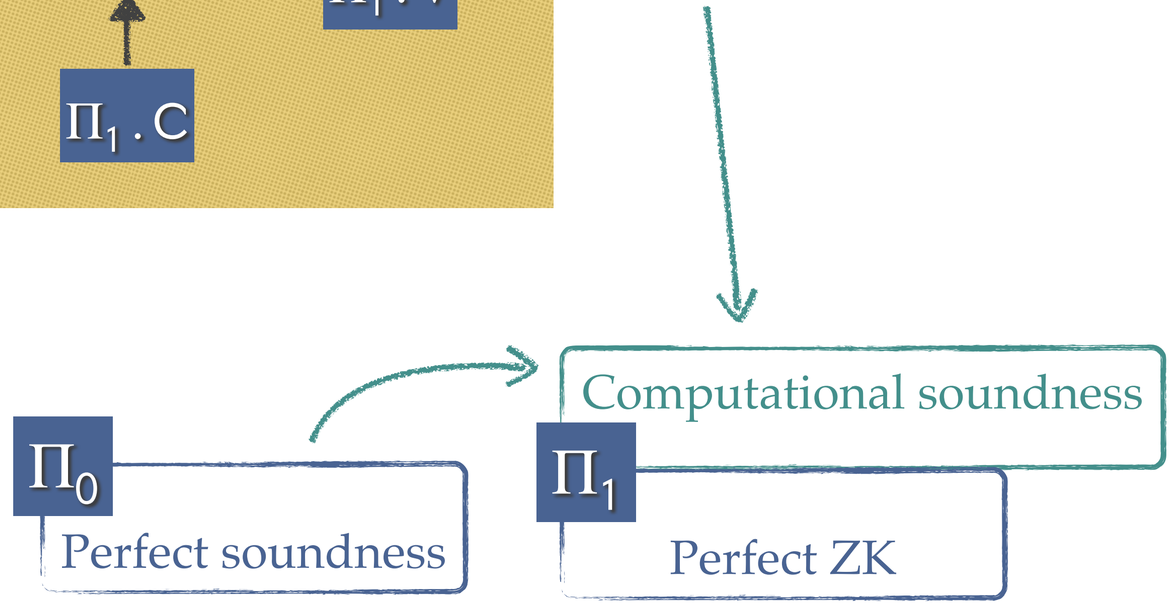
First built in [GOS06, GOS12].

Two proof systems

Π_0 Π_1



computational indistinguishability

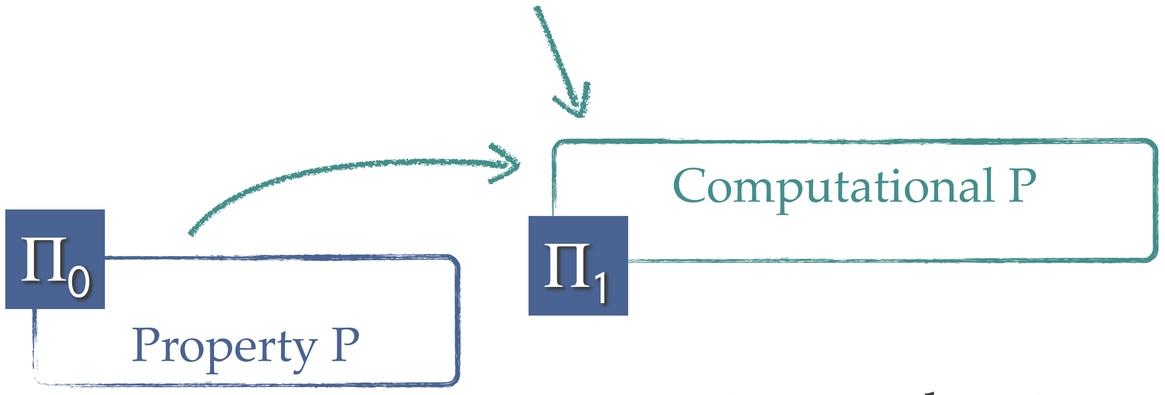


Why? [GOS06]

Prior definitions and work

	mode 0 requirements	mode 1 requirements	
[AFHLP16]	perfect soundness and extractability	perfect ZK and WI	*for multi-linear maps*
[HU19]	statistical soundness and extractability	statistical WI	*construct dual-mode NIZKs*
[LPWW20]	statistical soundness	statistical ZK	*construct dual-mode NIZKs*
[GOS06]	perfect soundness	perfect ZK	*construct dual-mode NIZKs*
[BCCKLS09]	perfect soundness	perfect WI	*for anonymous credentials*

Transference



We say that Property P **transfers** if this diagram is true

The purpose and applications of prior work depend on property transference

P
SND-E
ZK
WI
XT

Which properties P transfer?

Contributions

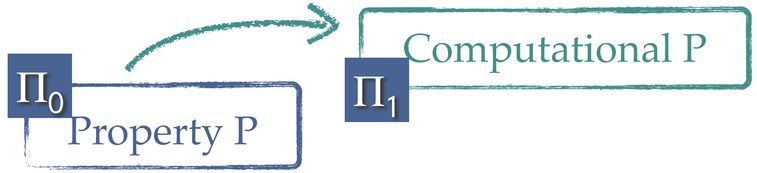
Definitions

mode-indistinguishability

- dual-mode proof systems are defined with only a CRS indistinguishability requirement

Formulating the transference question

computational indistinguishability of CRS



Negative results

for dual-mode proof systems

- SND-P soundness does not transfer
- separation between SND-E and SND-P

for regular proof systems

Positive results

- property specifications
- transfer theorem

} abstraction to capture all positive results simultaneously

- standard definitions of ZK, WI, extractability transfer

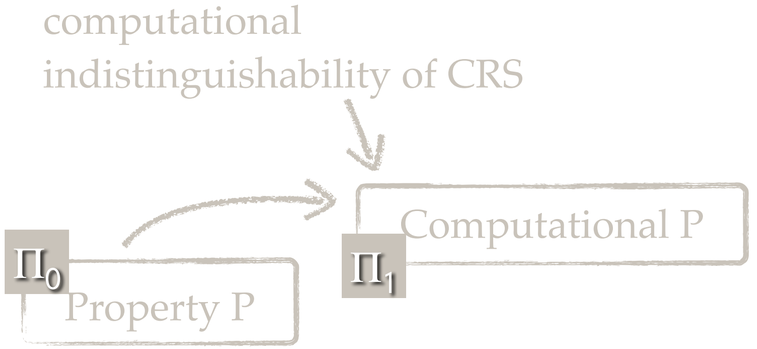
Contributions

Definitions

mode-indistinguishability

- **dual-mode proof systems are defined with only a CRS indistinguishability requirement**

Formulating the transference question



Negative results

for dual-mode proof systems

- SND-P soundness does not transfer
- separation between SND-E and SND-P

for regular proof systems

Positive results

- property specifications
- transfer theorem

} abstraction to capture all positive results simultaneously

- standard definitions of ZK, WI, extractability transfer

Dual-mode Proof System Syntax

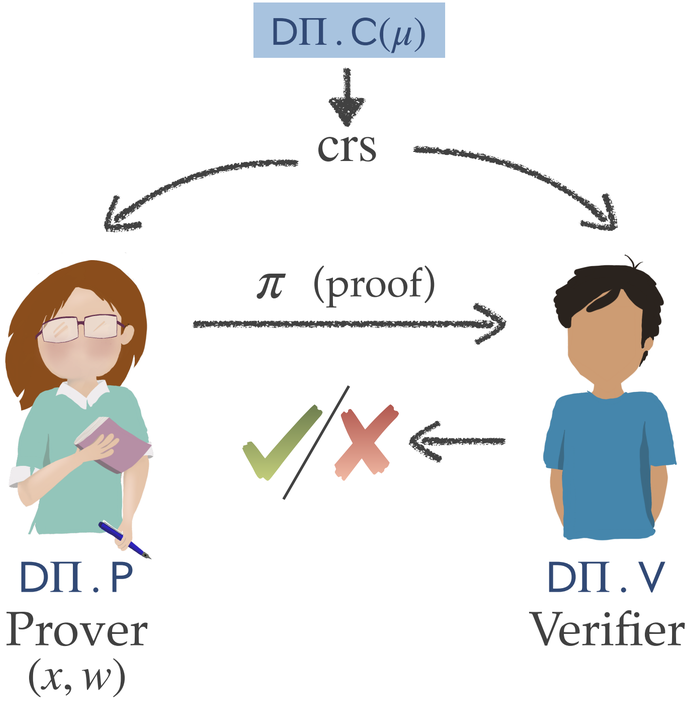
$\mathsf{crs} \leftarrow \mathsf{D\Pi.C}(1^\lambda, \mu)$ — CRS generation

$\pi \leftarrow \mathsf{D\Pi.P}(1^\lambda, \mathsf{crs}, x, w)$ — Proof generation

$d \leftarrow \mathsf{D\Pi.V}(1^\lambda, crs, x, \pi)$ — Verification

Two induced proof systems : Π_0 and Π_1

non-interactive proof systems



MODE-INDISTINGUISHABILITY

computational indistinguishability

$\mathsf{D\Pi.C}(1^\lambda, 0) \rightarrow \mathsf{crs}_0 \approx \mathsf{crs}_1 \leftarrow \mathsf{D\Pi.C}(1^\lambda, 1)$

This is the only property we require of dual-mode proof systems

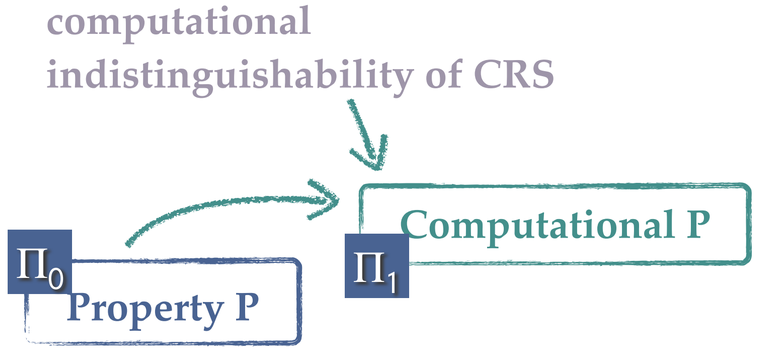
Contributions

Definitions

mode-indistinguishability

- dual-mode proof systems are defined with only a CRS indistinguishability requirement

Formulating the transference question



Negative results

for dual-mode proof systems

- SND-P soundness does not transfer
- separation between SND-E and SND-P

for regular proof systems

Positive results

- property specifications
- transfer theorem

} abstraction to capture all positive results simultaneously

- standard definitions of ZK, WI, extractability transfer

Transference of a property P

Examples of properties P

- SND-P
- SND-E
- zero-knowledge
- witness-indistinguishability
- extractability (proof of knowledge)

A property P transfers if it can be specified in polynomial-time

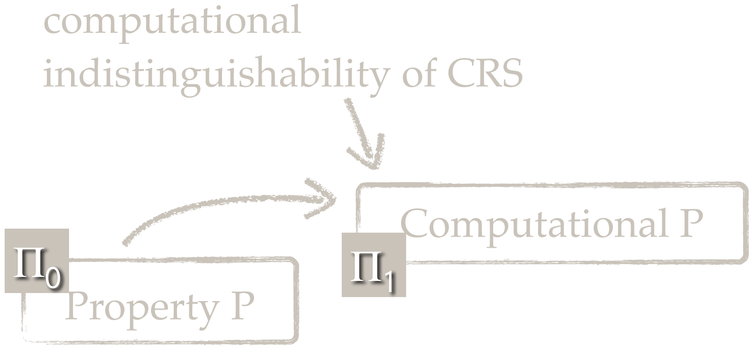
Contributions

Definitions

mode-indistinguishability

- dual-mode proof systems are defined with only a CRS indistinguishability requirement

Formulating the transference question



Negative results

for dual-mode proof systems

- **SND-P soundness does not transfer**
- **separation between SND-E and SND-P**

for regular proof systems

Positive results

- property specifications
- transfer theorem

} abstraction to capture all positive results simultaneously

- standard definitions of ZK, WI, extractability transfer

Types of Soundness for relation R

regular proof systems

Penalty and Exclusion [BHK15]

Game $G^{\text{snd-p}}_{\Pi,R,\lambda}$

INIT():
1 $\text{crs} \leftarrow\!\!\$\ \Pi.\mathsf{C}(1^\lambda)$; Return crs

FIN(x, pf):
2 If $(x \in \mathsf{L}_R(\text{crs}))$ then return false
3 Return $\Pi.\mathsf{V}(1^\lambda, \text{crs}, x, \text{pf})$

Game $G^{\text{snd-e}}_{\Pi,R,\lambda}$

INIT():
1 $\text{crs} \leftarrow\!\!\$\ \Pi.\mathsf{C}(1^\lambda)$; Return crs

FIN(x, pf):
2 If $(x \in \mathsf{L}_R(\text{crs}))$ then bad $\leftarrow$ true
3 Return $\Pi.\mathsf{V}(1^\lambda, \text{crs}, x, \text{pf})$

Membership-conscious adversary
picks $x \in L_R$ with negligible probability
i.e. sets bad $\leftarrow$ true with negligible probability

		win condition	restriction on PT adversary	good for applications?
Penalty-style	SND-P	$(x \notin L_R) \wedge (\Pi.\mathsf{V}(\ldots) \rightarrow \checkmark)$	none	yes
Exclusion-style	SND-E	$(\Pi.\mathsf{V}(\ldots) \rightarrow \checkmark)$	membership-conscious	no

We consider digital signatures [BG90] as a canonical application

Relating SND-P and SND-E

regular proof systems

SND-P $\Rightarrow$ SND-E

Any (membership-conscious) adversary that attacks the SND-E notion also attacks the SND-P notion

SND-E $\not\Rightarrow$ SND-P

This shows SND-E is strictly weaker than SND-P

We show this via a counter-example (assuming the hardness of DDH)

We build a non-interactive proof system Π and relation R such that

(1) Π satisfies SND-E

(2) Π does not satisfy SND-P.

We show this via an explicit attack that succeeds with probability $\frac{1}{2}$

SND-P does not transfer!

dual-mode proof systems

Intuition : SND-P fails to transfer because transference would require a reduction adversary to perform a test of membership (which would be inefficient for languages $\in$ **NP**)

Recall: SND-P win condition

$(x \notin L_R) \wedge (\Pi \,.\, V(\ldots) \rightarrow \checkmark\ )$

Theorem : Assume there exists a group generator for which DDH is hard. There exists a dual-mode proof system DΠ and a relation R such that

- DΠ is mode-indistinguishable
- $D\Pi_1$ is SND-P for R
- $D\Pi_0$ is **not** SND-P for R

COUNTER-EXAMPLE

assumes DDH is hard in group G → MODE-INDISTINGUISHABILITY

assumes DDH is hard in group G → SND-P FOR $D\Pi_1$

$D\Pi \,.\, C(1^\lambda, \mu) \rightarrow \text{crs} = (G, g, g^a, g^b, g^c)$

- $\mu = 0 \implies c = ab$
- $\mu = 1 \implies c \leftarrow_\$ \mathbb{Z}_{|G|}$

Proof generation is trivial

Verification accepts all $x \in G$

$L_R(\text{crs}) = G \backslash \{g^{ab}\}$

ATTACK AGAINST SND-P FOR $D\Pi_0$

Breaking soundness requires picking $x = g^{ab}$

Return $x = g^c$ and the trivial proof

Contributions

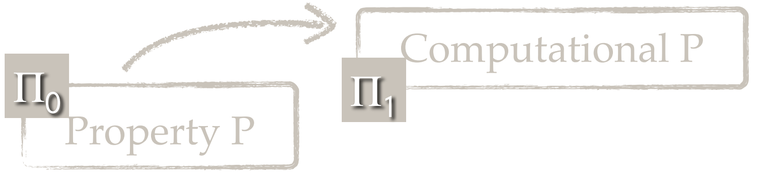
Definitions

mode-indistinguishability

- dual-mode proof systems are defined with only a CRS indistinguishability requirement

Formulating the transference question

computational indistinguishability of CRS



Negative results

for dual-mode proof systems

- SND-P soundness does not transfer
- separation between SND-E and SND-P

for regular proof systems

Positive results

- **property specifications**
- **transfer theorem**

} **abstraction to capture all positive results simultaneously**

- **standard definitions of ZK, WI, extractability transfer**

SND-E does transfer!

We are given that one mode of the dual-mode proof system satisfies SND-E soundness

We also know that the dual-mode proof system satisfies mode indistinguishability

The main idea is that if the other mode of the proof system did **not** satisfy SND-E soundness, then this difference in behavior would be used to break mode-indistinguishability

This works because there is no code in the SND-E game that is not polynomial-time, and therefore it can be simulated by the polynomial-time mode-indistinguishability adversary

Property Specifications and Transfer Theorem

We formalize properties via the abstraction of **property specifications**.

The property specification for P captures the game defined for the property P

Our constructed property specifications perfectly match the game for the target property

Transfer Theorem : (informal)

Let DΠ be a dual-mode proof system satisfying mode-indistinguishability.

If one mode of DΠ satisfies a **polynomial-time** property specification PS, then the other mode satisfies the computational counterpart of PS.

zero-knowledge

witness-indistinguishability

extractability (proof of knowledge)

SND-E

} PS is polynomial-time

PS is not polynomial-time

Recall: SND-P win condition

$(x \notin L_R) \wedge (\Pi \,.\, V(\ldots) \rightarrow$ ✓ $)$

SND-P

Capturing other models

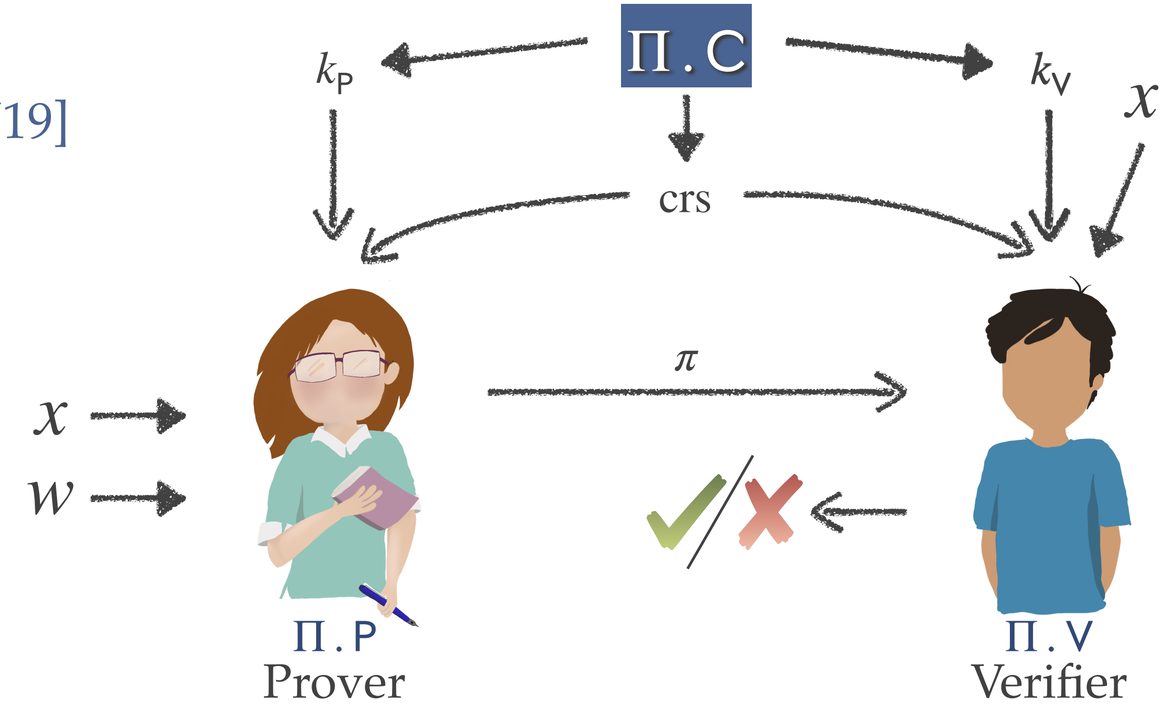
So far : we have only discussed the CRS model

Designated Verifier Model [ES02, PsV06, DFN06]

Designated Prover Model [KW18, KNYY19]

Preprocessing Model [DMP90]

	k_P	k_V
CRS Model	✗	✗
Designated Verifier Model	✗	✓
Designated Prover Model	✓	✗
Preprocessing Model	✓	✓



Summary

We defined dual-mode proof systems with only the mode-indistinguishability requirement

We define what it means for a property to transfer

We ask which properties transfer

We prove that SND-P does not transfer via a counter-example

We prove via a general framework, that many properties like ZK, WI, XT, SND-E do transfer

We show that SND-P is a strictly stronger notion than SND-E

- We must be careful when using dual-mode systems in applications!
- We must check that we actually do get the properties we require from the induced proof systems, and not expect it to be implicit due to transference

https://eprint.iacr.org/2020/629