Efficient Deniable Authentication for Signatures

Application to Machine-Readable Travel Document

Jean Monnerat, **Sylvain Pasini**, and Serge Vaudenay

ACNS '09

Paris-Rocquencourt, France

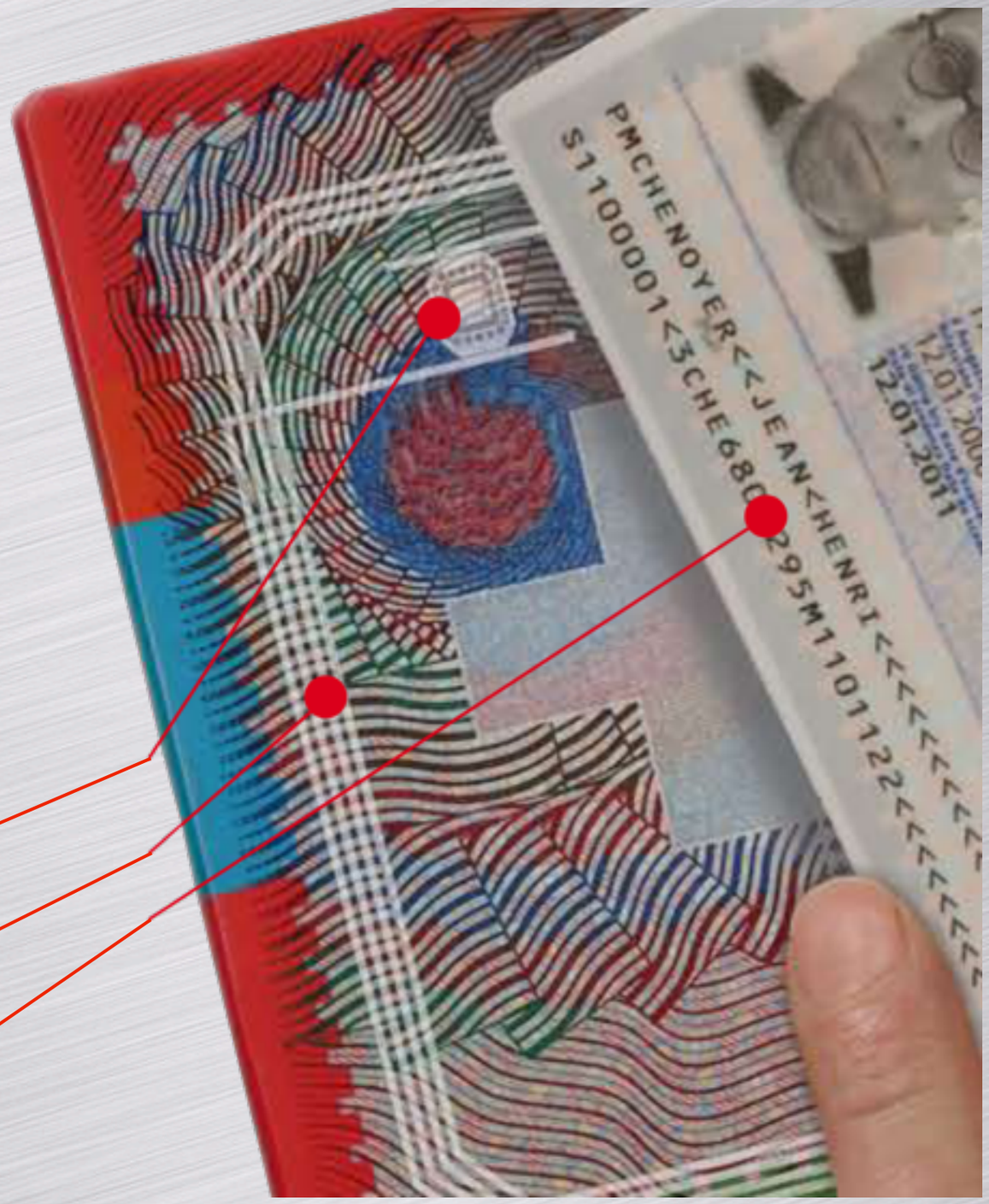
June 4th, 2009

Outline

- Motivation: electronic passports
- New primitive: ONTAP
  - Online Non-Transferable Authentication Protocol
- Proofs of knowledge, zero-knowledge, ...
- Contribution of the paper

Electronic Passports

An Electronic Passport...



RFID chip

Antenna

Machine Readable Zone (MRZ)

Reading an E-passport

Radio channel

Visual channel

Reader

Implementation, use, and security mandated by the International Civil Aviation Organization (ICAO).

Data in the Chip

- Data are stored following a Logical Data Structure (LDS)
  - 19 Data Groups (DG)

Data in the Chip

- Data are stored following a Logical Data Structure (LDS)
  - 19 Data Groups (DG)
- LDS:
  - DG1 - basic data, e.g., name, birth, ... (as in the MRZ)
  - DG2 - face picture
  - DG3 - fingerprint(s)
  - ...
  - DG19

Data in the Chip

- Data are stored following a Logical Data Structure (LDS)
  - 19 Data Groups (DG)
- LDS:
  - DG1 - basic data, e.g., name, birth, ... (as in the MRZ)
  - DG2 - face picture
  - DG3 - fingerprint(s)
  - ...
  - DG19
- Only DG1 and DG2 are mandatory.

Access Control

- By default, no access control

Access Control

- By default, no access control
- Basic Access Control (BAC)
  - Prove to the e-passport that you have visual access
  - Use an encryption key *sk=f(MRZ_info)*

Access Control

- By default, no access control
- Basic Access Control (BAC)
  - Prove to the e-passport that you have visual access
  - Use an encryption key *sk=f(MRZ_info)*
- Extended Access Control (EAC)
  - Terminal authentication
  - PKI for border patrols
  - EU standard (not an ICAO standard)

Access Control

- By default, no access control
- Basic Access Control (BAC)
  - Prove to the e-passport that you have visual access
  - Use an encryption key *sk=f(MRZ_info)*

Usually used

- Extended Access Control (EAC)
  - Terminal authentication
  - PKI for border patrols
  - EU standard (not an ICAO standard)

Data Authentication

- **Passive** versus **active** authentication

Data Authentication

- **Passive** versus **active** authentication

- Passive authentication (mandatory)
  - Aims to prove that the **data is genuine**

Data Authentication

- **Passive** versus **active** authentication

- Passive authentication (mandatory)
  - Aims to prove that the **data is genuine**

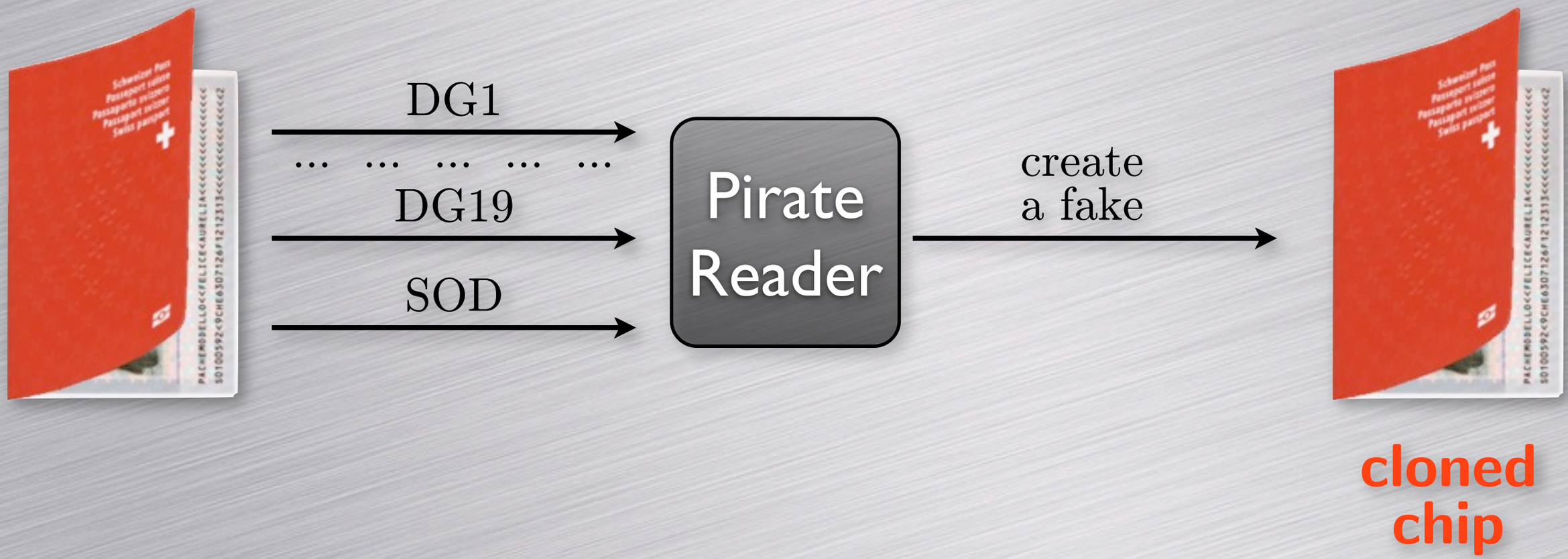
- Active authentication (optional)
  - Aims to prove that the **chip is genuine** (not cloned)
  - In addition to passive authentication

Passive Authentication

- LDS contains a Security Object Document (SOD)
  - Basically, the national authority signed the DGs
- LDS:
  - DG1
  - ...
  - DG19
  - **SOD** which contains

$$H(DG1), \ldots, H(DG19), \quad \mathsf{sign}_{K_{s,NA}}\big(H(DG1), \ldots, H(DG19)\big)$$

Passive Authentication (2)



Active Authentication

- Avoids cloning or substitution of the chip
- The e-passport contains a pair of keys: Kp and Ks
  - Ks stored in a secure memory
  - Kp stored in DG15 (authenticated by SOD)

Reader

DGs and SOD → Verify Kp

challenge c ← Pick c

$\sigma = \mathsf{sign}_{Ks}(c)$

response σ → Verify σ

Privacy Issue

- Anyone having a reader (100 Euros) can obtain all DGs and the SOD

DGs and SOD

Privacy Issue

- Anyone having a reader (100 Euros) can obtain all DGs and the SOD

DGs and SOD

- Publishing the data only (DGs):
  - the owner can still claim that it is incorrect

Privacy Issue

- Anyone having a reader (100 Euros) can obtain all DGs and the SOD

DGs and SOD

- Publishing the data only (DGs):
  - the owner can still claim that it is incorrect
- But, publishing the SOD too:
  - SOD is an evidence of the authenticity of DGs

Solution: The Main Idea

Reader

X

$K_{p,NA}, K_{s,NA}$

$K_{p,NA}$

Solution: The Main Idea

Reader

X

$K_{p,NA}, K_{s,NA}$

$K_{p,NA}$

DGs

σ

Solution: The Main Idea

Reader

X

$K_{p,NA}, K_{s,NA}$

$K_{p,NA}$

DGs

σ

$DGs,\ SOD$

Solution: The Main Idea

Reader

X

$K_{p,NA}, K_{s,NA}$

$K_{p,NA}$

DGs

σ

$DGs,\ SOD$

DGs

SOD

Solution: The Main Idea

Reader

X

$K_{p,NA}, K_{s,NA}$

$K_{p,NA}$

DGs

σ

$DGs,\ SOD$

DGs

SOD

$DGs,\ SOD$

DGs are valid

Privacy issue

Solution: The Main Idea

Reader

X

$K_{p,NA}, K_{s,NA}$

$K_{p,NA}$

DGs

σ

DGs, SOD

DGs

~~SOD~~

DGs, SOD

DGs are valid

Privacy issue

interactive proof
"I know a valid σ"

Online Non Transferable Authentication Protocol (ONTAP)

ONTAP Overview

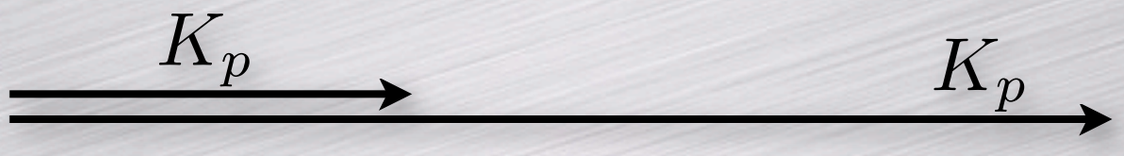
ONTAP Overview

Signer **Prover** **Verifier**

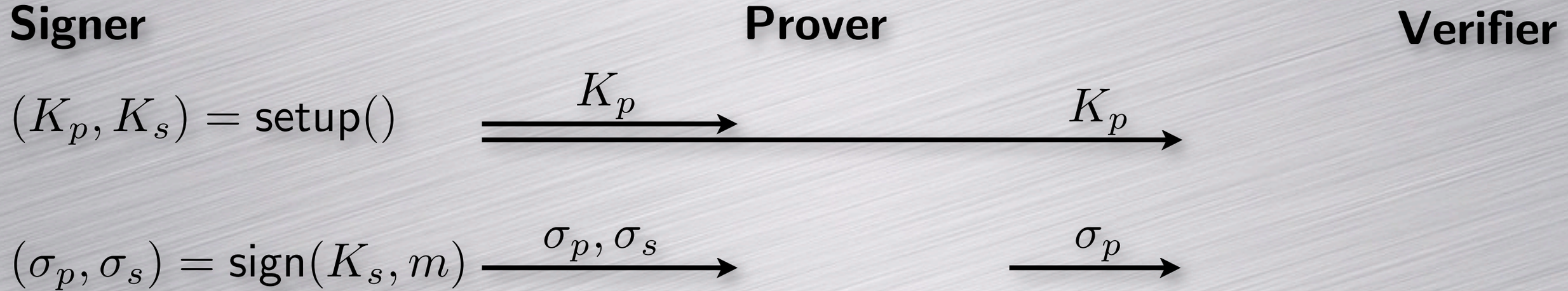
ONTAP Overview

Signer **Prover** **Verifier**

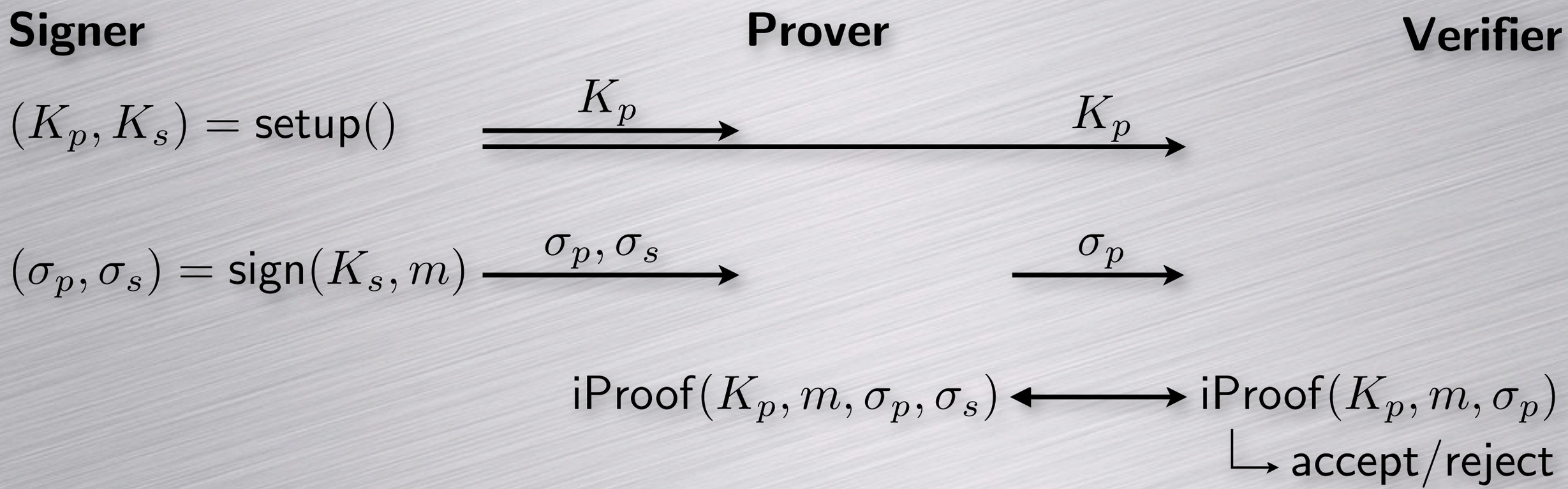
$(K_p, K_s) = \text{setup}()$



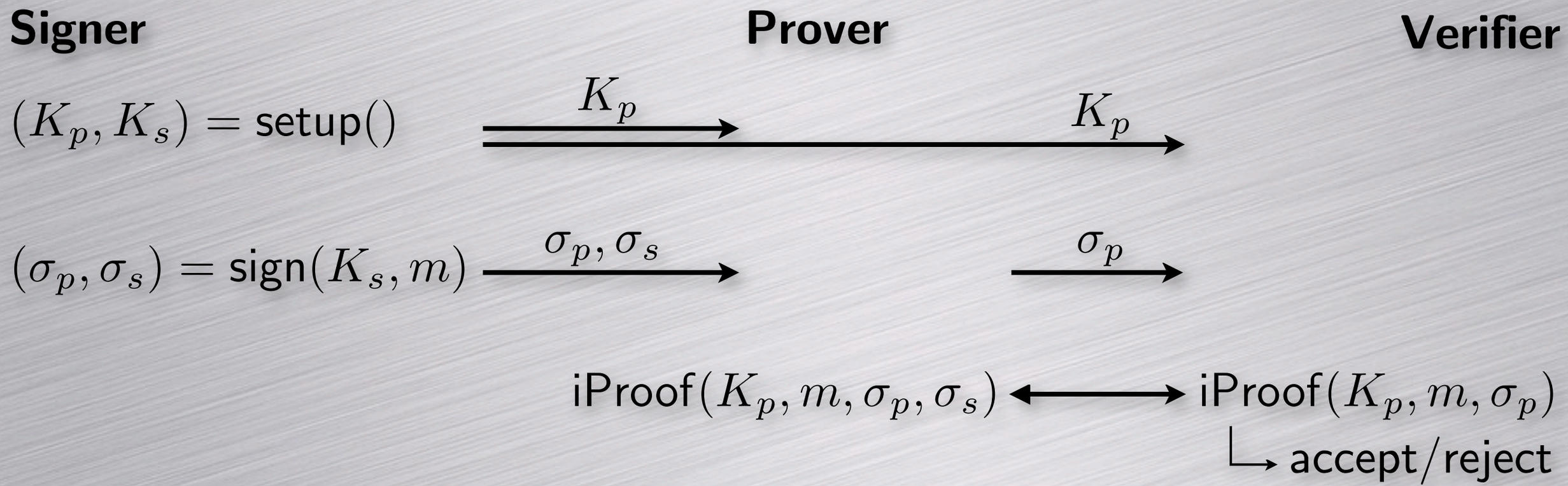
ONTAP Overview



ONTAP Overview



ONTAP Overview



- Properties:
  - Completeness
  - Unforgeability (sign + iProof)
  - Non-transferability (offline)

ONTAP Construction

Theorem

An ONTAP can be build with

- a secure signature scheme such as
  - the signature is splittable in two parts: σ_p and σ_s
  - σ_p is simulatable
- a zero-knowledge proof for witness σ_s

Proofs of Knowledge

Proof of Knowledge

Binary relation R, e.g., the RSA problem:

$$R = \left\{(x, w) : x \equiv w^e \pmod{N}\right\}$$

RSA params: $N{=}pq,\ \ ed \equiv 1 \pmod{\varphi(N)}$

Proof of Knowledge

Binary relation R, e.g., the RSA problem:

$$R = \left\{(x, w) : x \equiv w^e \pmod{N}\right\}$$

RSA params: $N{=}pq,\ \ ed \equiv 1 \pmod{\varphi(N)}$

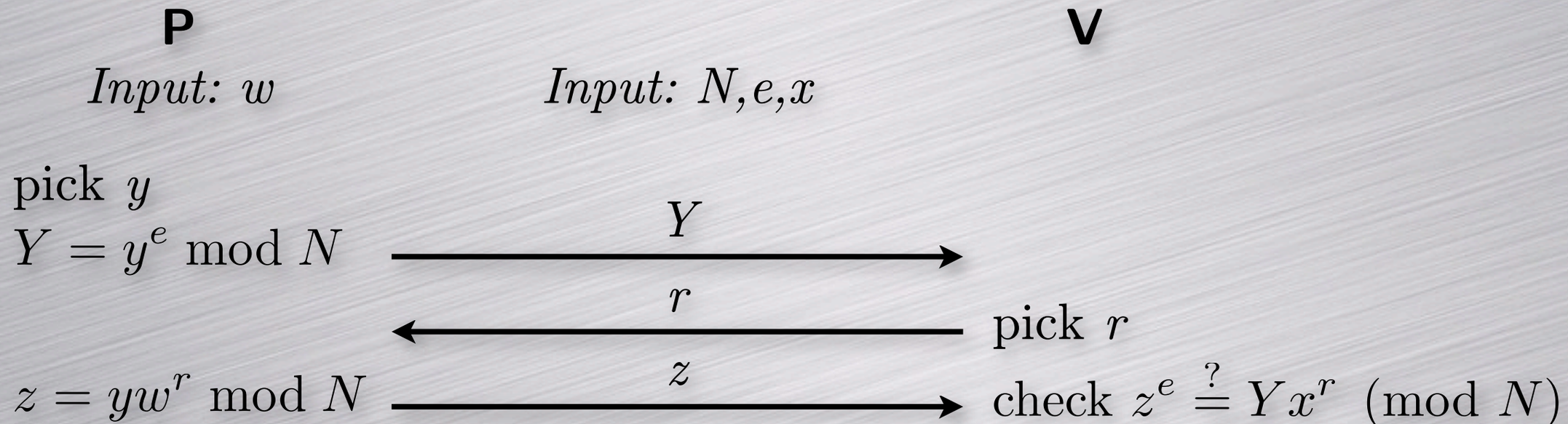
Proof of Knowledge

P — *Input:* x,w — **V** — *Input:* x

- Efficiency
- Completeness: if $(x,w) \in R$, then **V** always accepts
- Soundness: if $(x,w) \notin R$, then **V** rejects (with high prob)

The Guillou-Quisquater Protocol

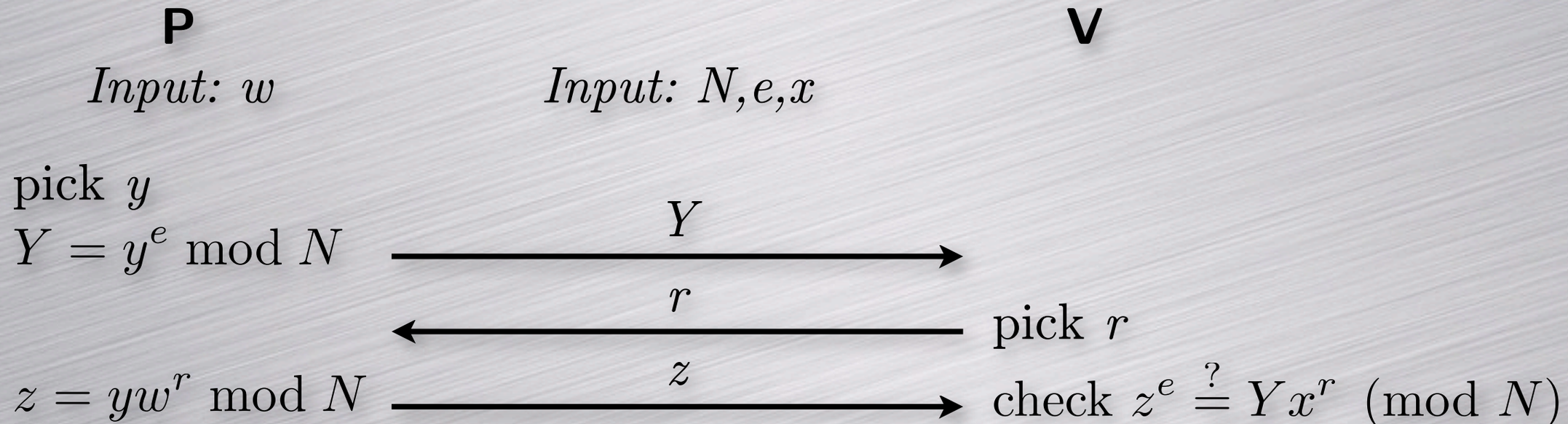
RSA params: $N{=}pq,\ \ ed \equiv 1 \pmod{\varphi(N)}$



- Efficiency
- Completeness
- Soundness

The Guillou-Quisquater Protocol

RSA params: $N{=}pq,\ \ ed \equiv 1 \pmod{\varphi(N)}$



- Efficiency
- Completeness
- Soundness

V is convinced because P replied to the challenge r.

Zero-Knowledge

No information leaks to **V** (except the statement)

Zero-Knowledge

No information leaks to **V** (except the statement)

Zero-knowledge

For any x, there exists **Sim** able to generate the transcript without w.

Zero-Knowledge

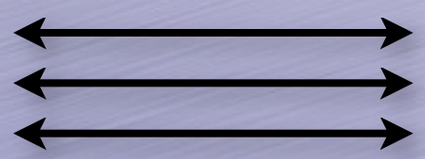
No information leaks to **V** (except the statement)

Zero-knowledge

For any x, there exists **Sim** able to generate the transcript without w.

P *Input: x,w*

V *Input: x*



Zero-Knowledge

No information leaks to **V** (except the statement)

Zero-knowledge

For any x, there exists **Sim** able to generate the transcript without w.

P *Input: x,w*

V *Input: x*

Sim *Input: x*

Zero-Knowledge

No information leaks to **V** (except the statement)

Zero-knowledge

For any x, there exists **Sim** able to generate the transcript without w.

P

Input: x,w

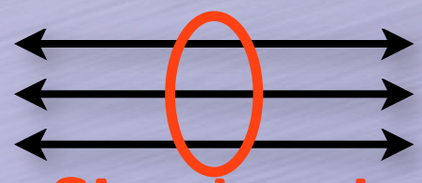
V

Input: x

Sim

Input: x

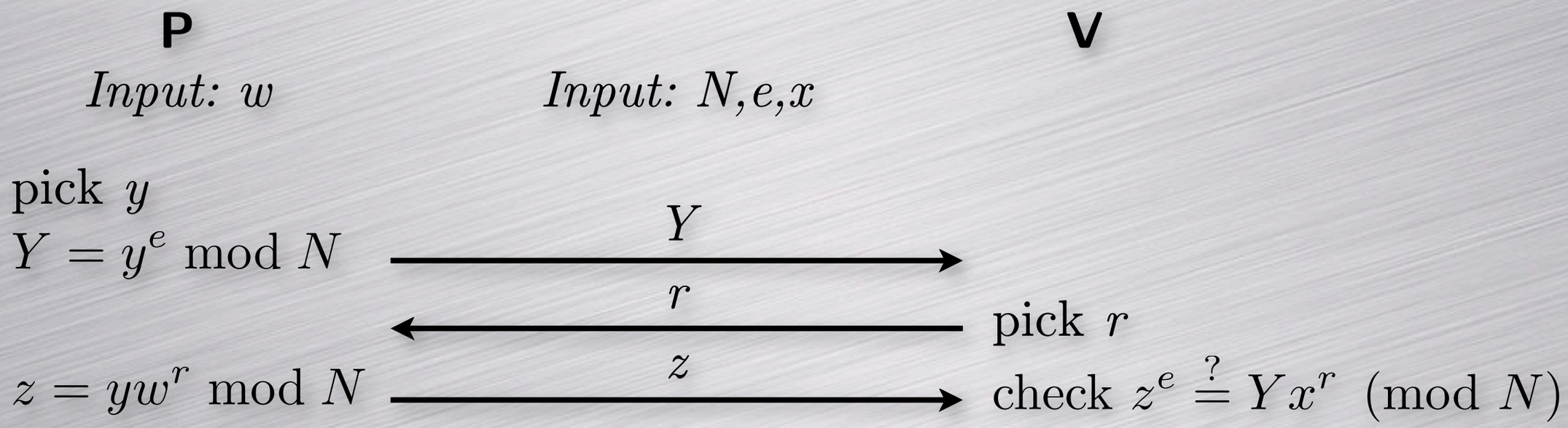
Real transcript



Simulated transcript

Indistinguishable

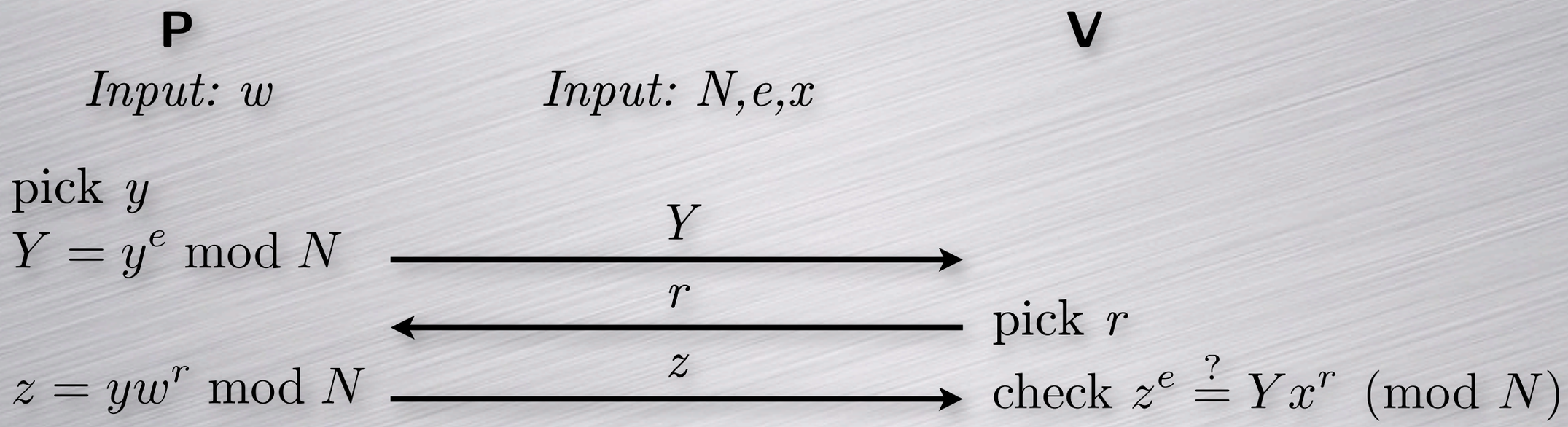
Zero-Knowledge: GQ protocol



Simulated transcript (without w):

given $N,e,x,$ and r
pick z
$Y = z^e / x^r$
output (Y,r,z)

Zero-Knowledge: GQ protocol



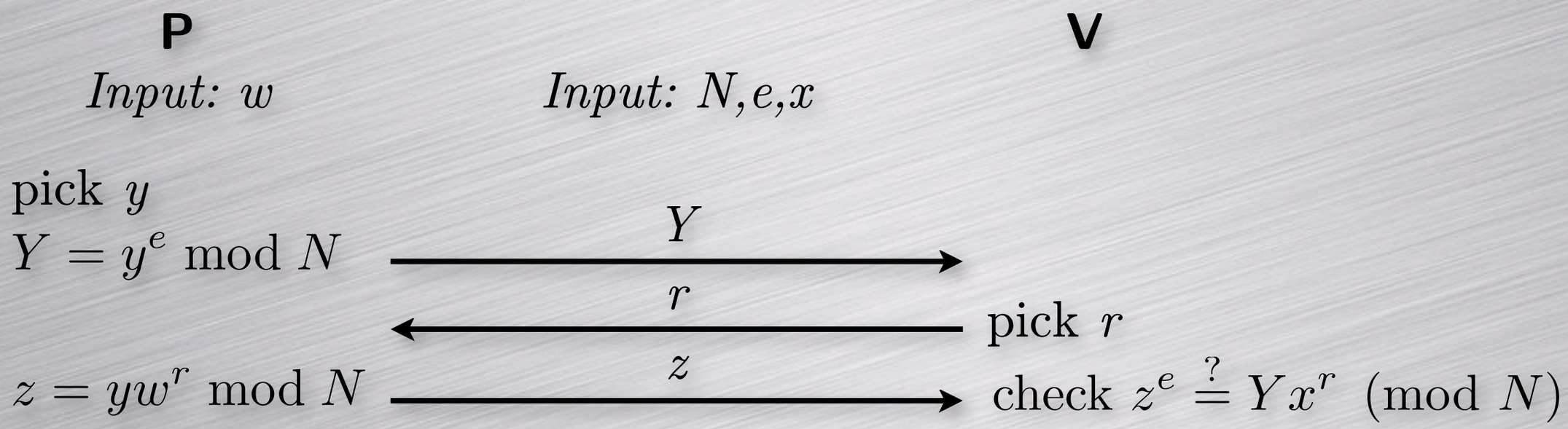
Simulated transcript (without w):

given $N,e,x,$ and r
pick z
$Y = z^e/x^r$
output (Y,r,z)

Everybody is able to generate this transcript, this is not a proof of interaction.

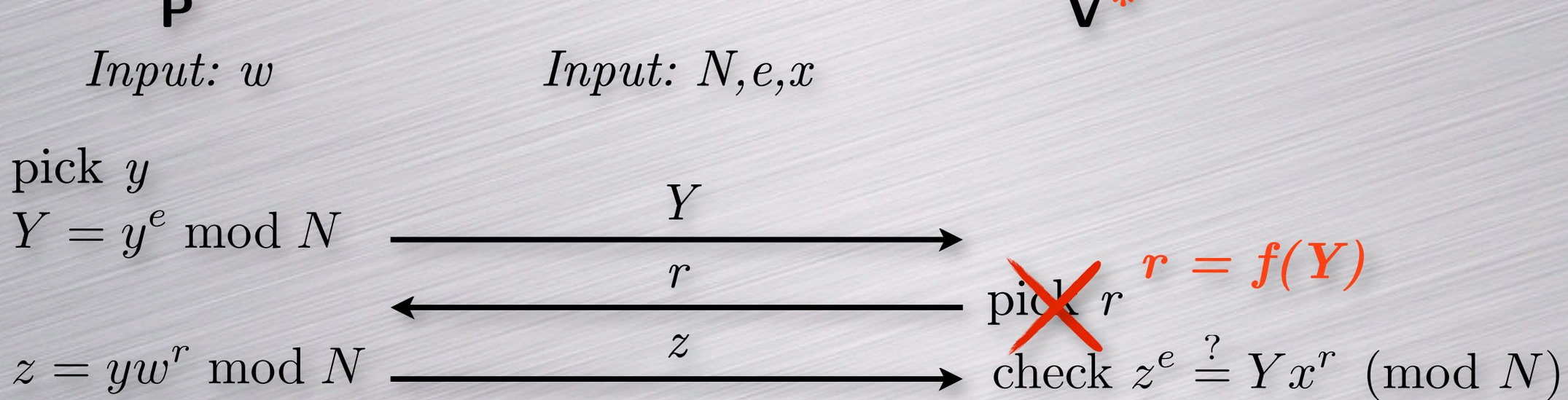
Fiat-Shamir Transform

The GQ protocol is only Honest-Verifier ZK.



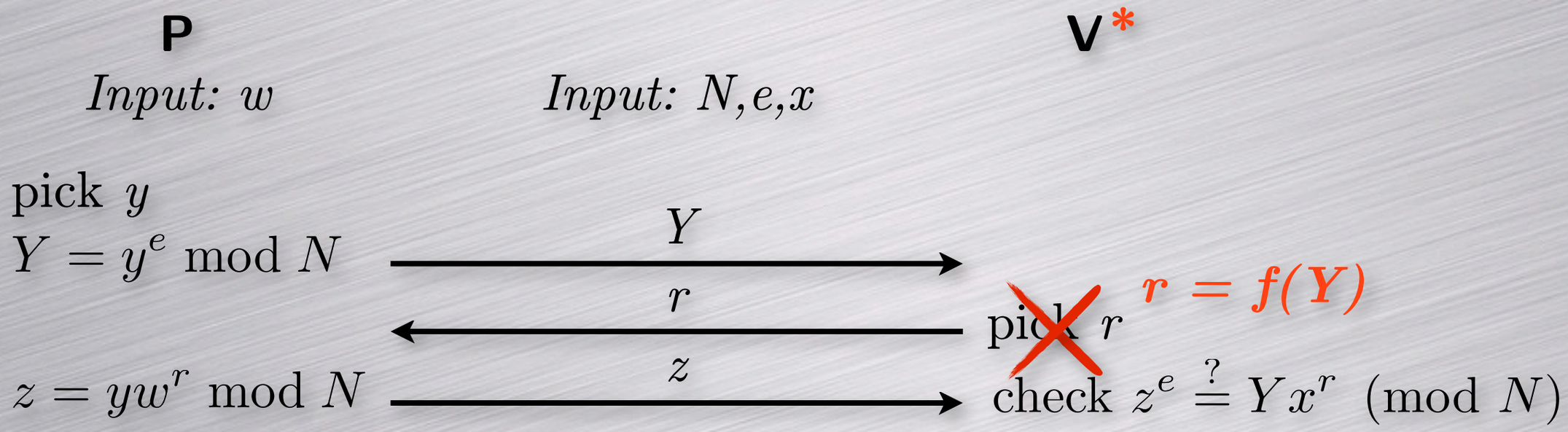
Fiat-Shamir Transform

The GQ protocol is only Honest-Verifier ZK.



Fiat-Shamir Transform

The GQ protocol is only Honest-Verifier ZK.



Considering malicious verifiers:

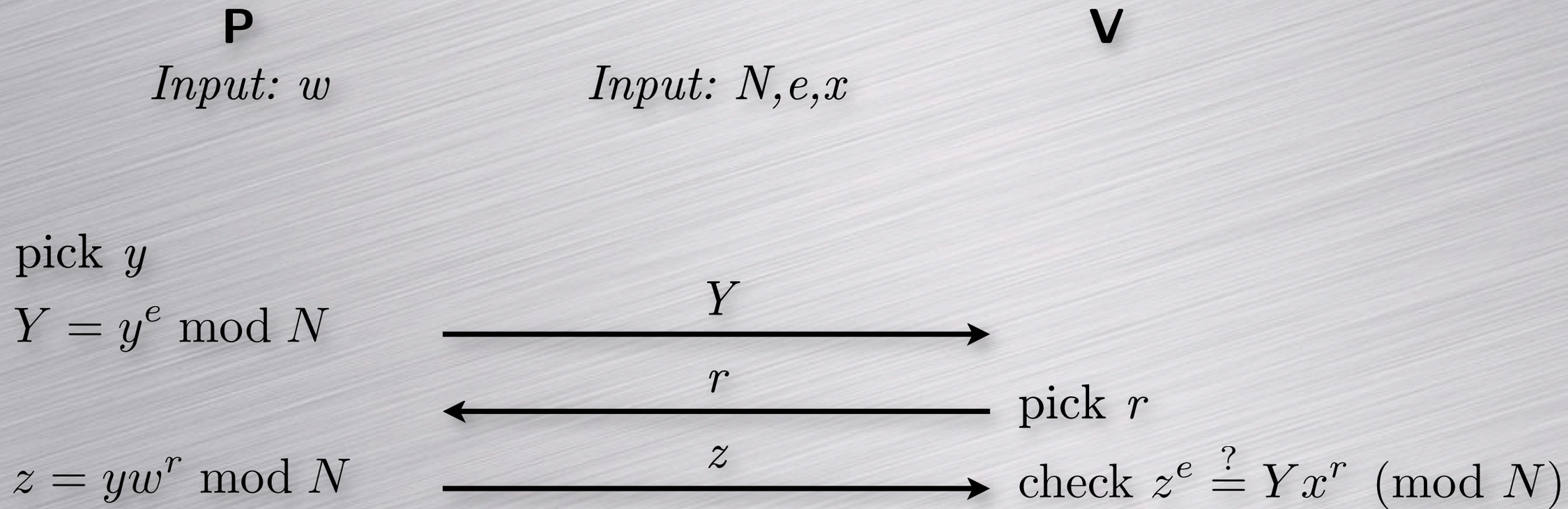
- the proof is not simulatable (without w),
- the proof becomes transferable.

Protocol Transform

To obtain a **full** zero-knowledge protocol,
ensure that r is chosen independently from Y.

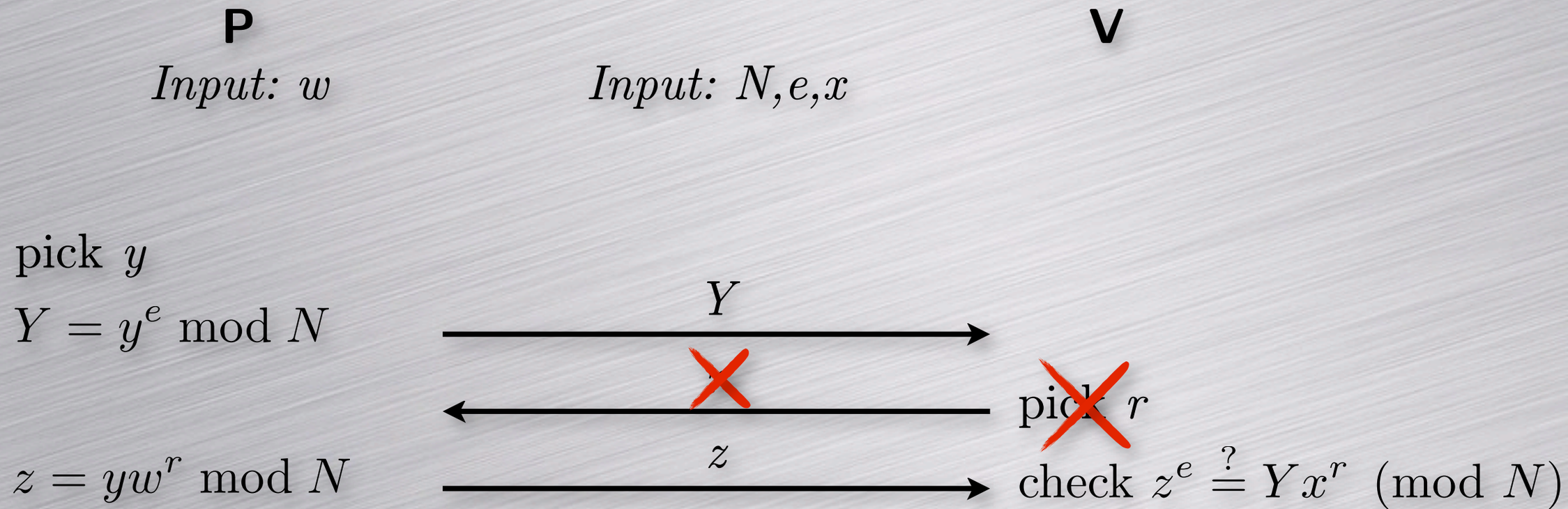
Protocol Transform

To obtain a **full** zero-knowledge protocol,
ensure that r is chosen independently from Y.



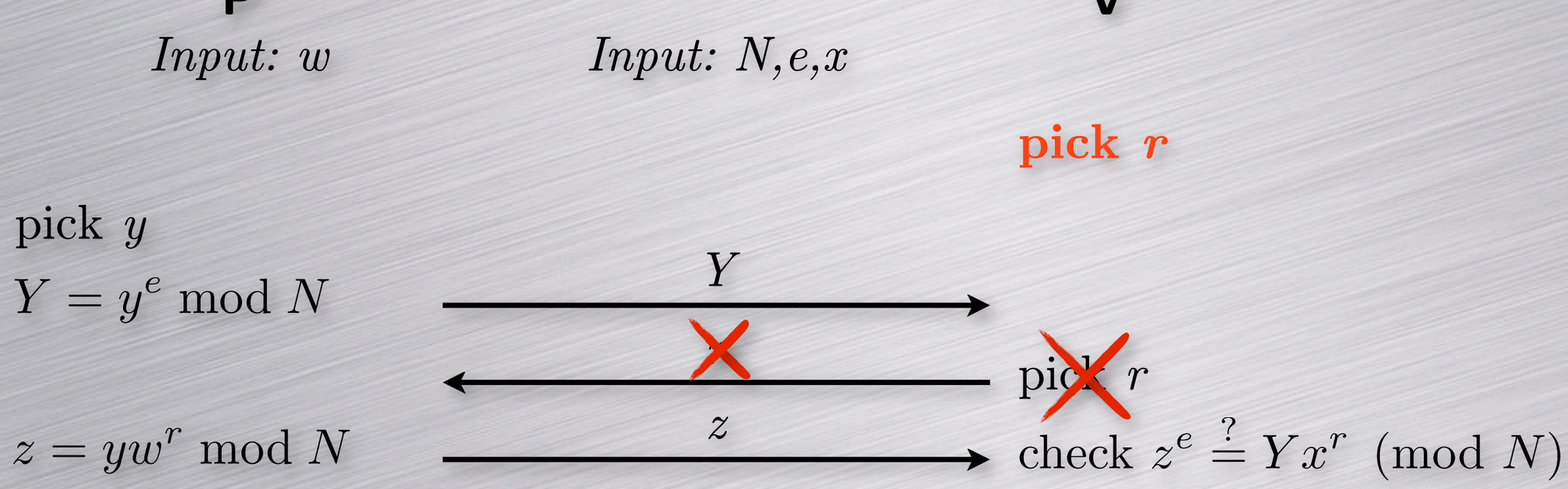
Protocol Transform

To obtain a **full** zero-knowledge protocol,
ensure that r is chosen independently from Y.



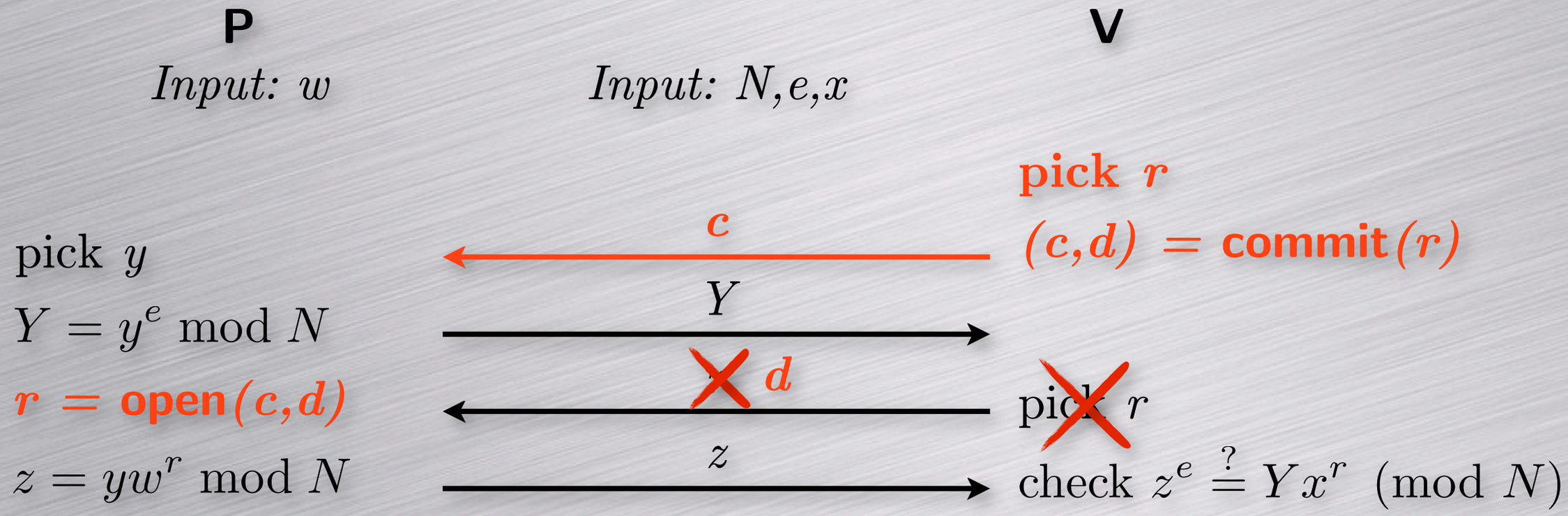
Protocol Transform

To obtain a **full** zero-knowledge protocol,
ensure that r is chosen independently from Y.

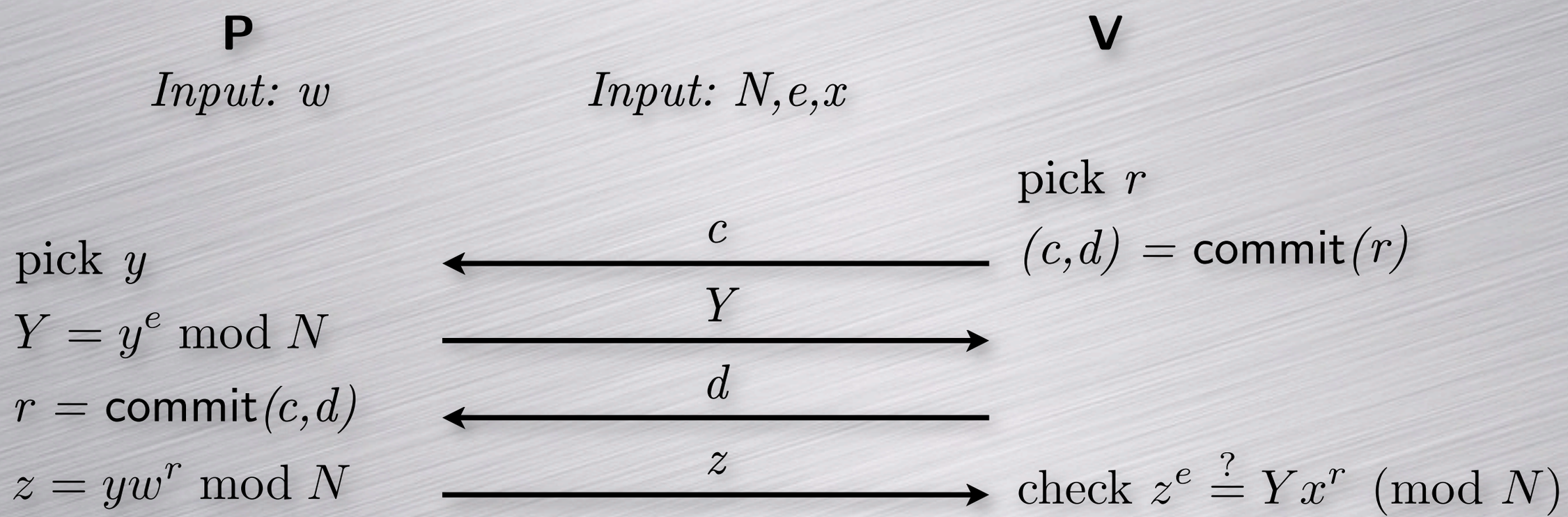


Protocol Transform

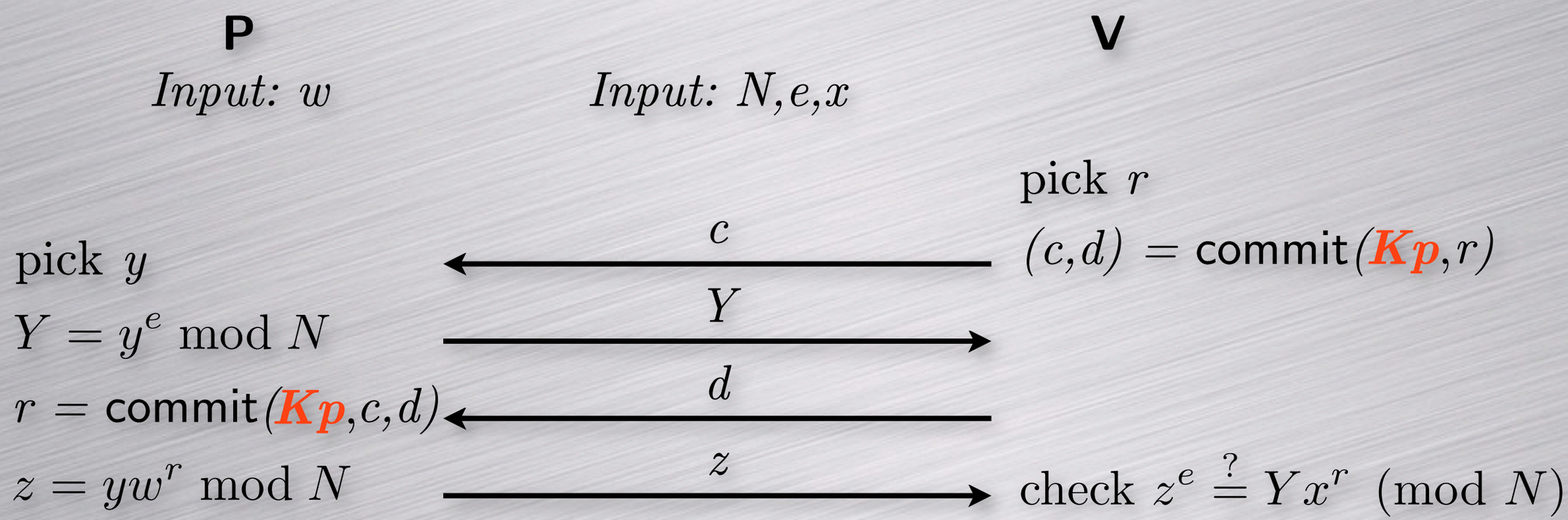
To obtain a **full** zero-knowledge protocol,
ensure that r is chosen independently from Y.



Require the CRS Model...

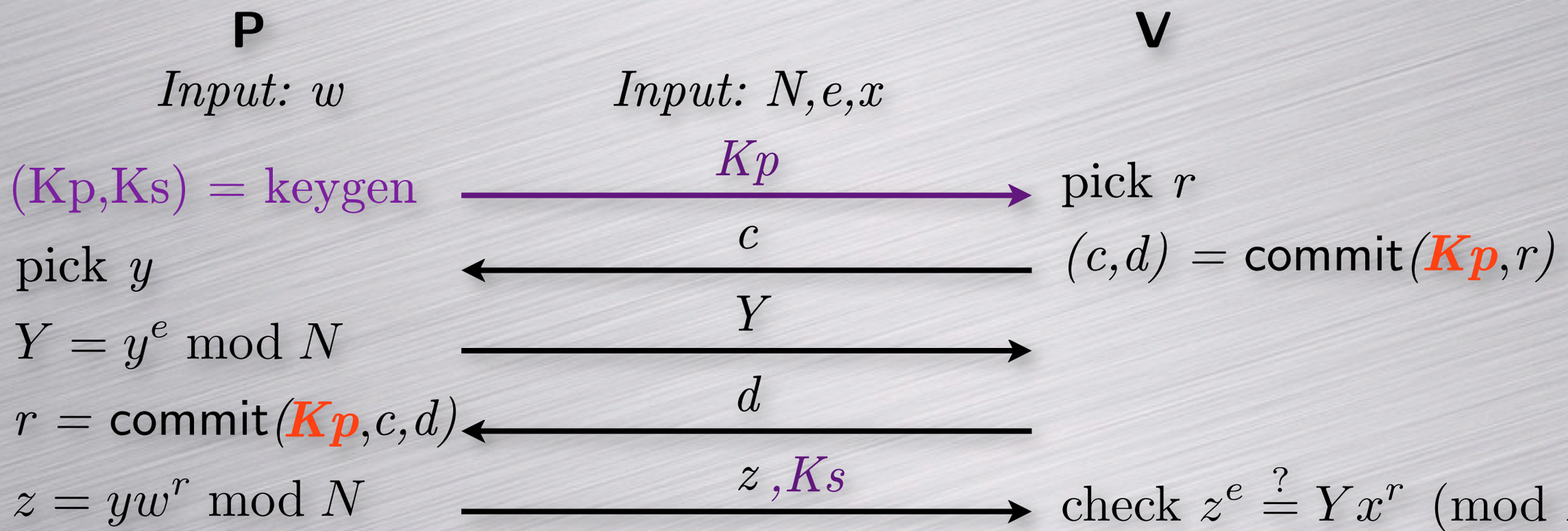


Require the CRS Model...



To prove the soundness, we should add a trapdoor.

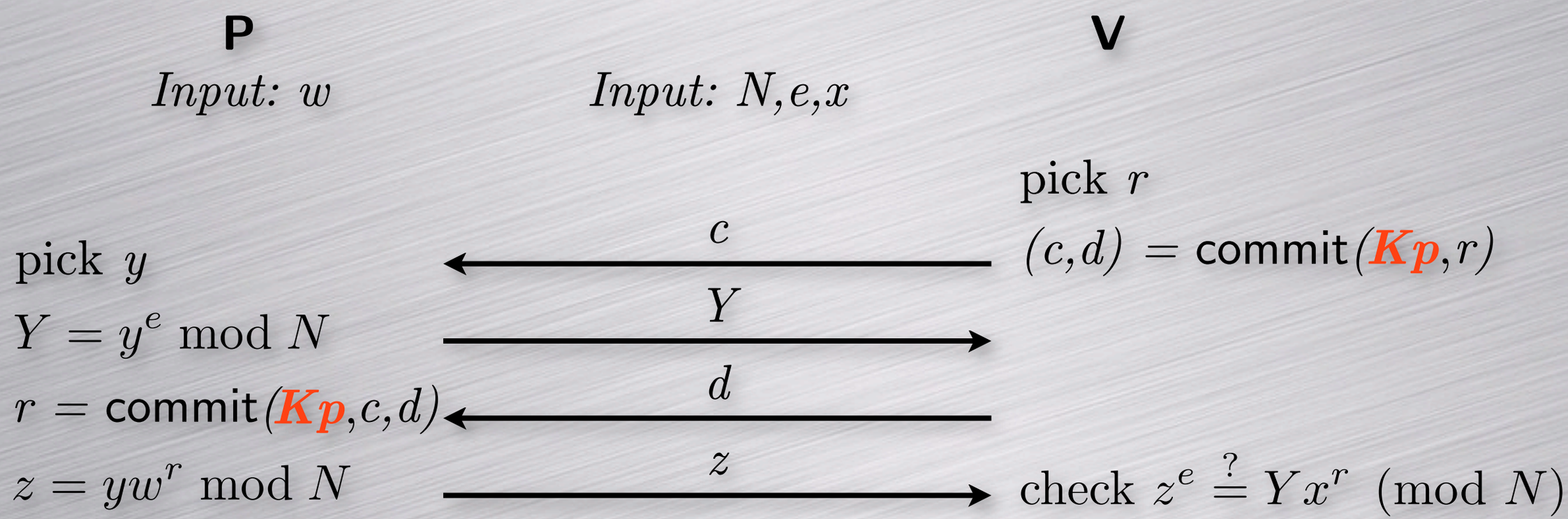
Require the CRS Model...



To prove the soundness, we should add a trapdoor.

- in the plain model, we add a move.

Require the CRS Model...



To prove the soundness, we should add a trapdoor.

- in the plain model, we add a move.
- in the CRS/RO model, Kp is a global setup.

Deniable Zero-Knowledge

Honest-Verifier ZK:

Deniable Zero-Knowledge

Honest-Verifier ZK:

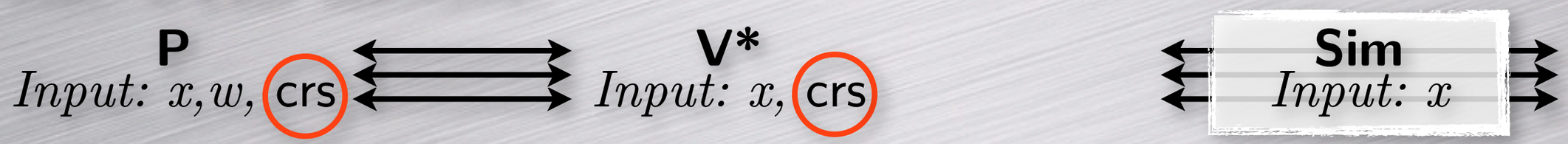
ZK:

Deniable Zero-Knowledge

Honest-Verifier ZK:

ZK:

ZK in the CRS model:

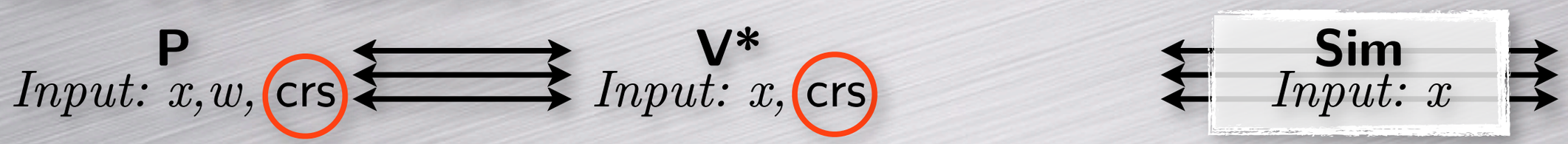


Deniable Zero-Knowledge

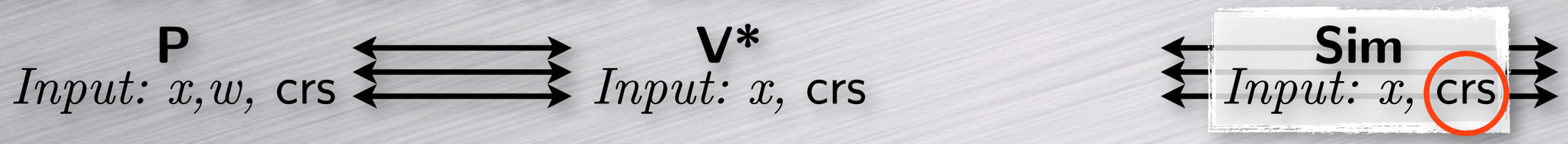
Honest-Verifier ZK:

ZK:

ZK in the CRS model:



Deniable ZK in the CRS model:



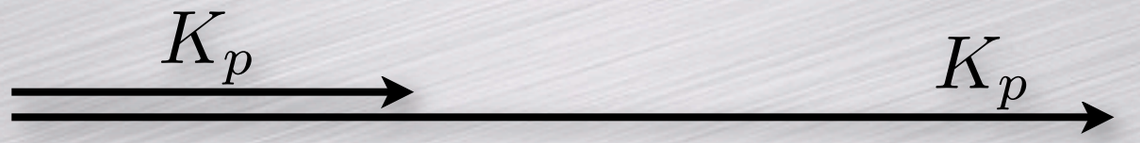
Back to ONTAP: RSA example

Signer **Prover** **Verifier**

Back to ONTAP: RSA example

Signer **Prover** **Verifier**

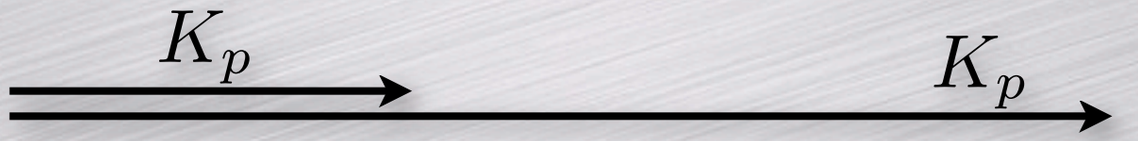
RSA : p, q, N, e, d
$K_p = (N, e)$
$K_s = d$



Back to ONTAP: RSA example

Signer **Prover** **Verifier**

RSA : p, q, N, e, d
$K_p = (N, e)$
$K_s = d$



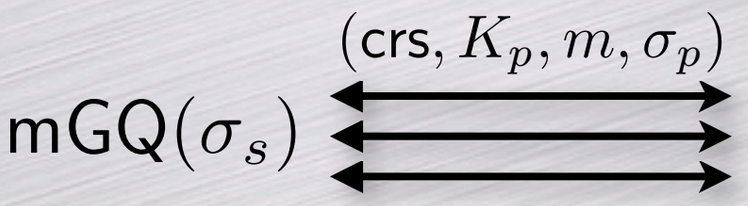
$\sigma_p = \mathsf{H}_{\mathsf{seed}}(m)$
$\sigma_s = \sigma_p^d \bmod N$

Back to ONTAP: RSA example

Signer **Prover** **Verifier**

RSA : p, q, N, e, d
$K_p = (N, e)$
$K_s = d$

$\sigma_p = \mathsf{H}_{\mathsf{seed}}(m)$
$\sigma_s = \sigma_p^d \bmod N$



Back to ONTAP: RSA example

Signer **Prover** **Verifier**

RSA : p, q, N, e, d
$K_p = (N, e)$
$K_s = d$

K_p K_p

$\sigma_p = \mathsf{H}_{\mathsf{seed}}(m)$
$\sigma_s = \sigma_p^d \bmod N$

σ_p, σ_s σ_p

$(\mathsf{crs}, K_p, m, \sigma_p)$

$\mathsf{mGQ}(\sigma_s)$ $\mathsf{mGQ}()$

↳ accept/reject

Reader

In the Paper...

In the Paper...

- Formal ONTAP definition
  - Online Non-Transferable Authentication Protocol

In the Paper...

- Formal ONTAP definition
  - Online Non-Transferable Authentication Protocol
- Formal security proof of the generic transform
  - in the plain
  - in the random oracle model
  - in the common reference string model

In the Paper...

- Formal ONTAP definition
  - Online Non-Transferable Authentication Protocol
- Formal security proof of the generic transform
  - in the plain
  - in the random oracle model
  - in the common reference string model
- Efficient ONTAP implementations
  - for RSA-based signature schemes (GQ proof)
  - for ElGamal-based signature schemes (Schnorr proof)

Thank you for your attention!