

Secure Communication using Authenticated Channels

Sylvain Pasini

Private PhD Defense

June 17th, 2009

Outline

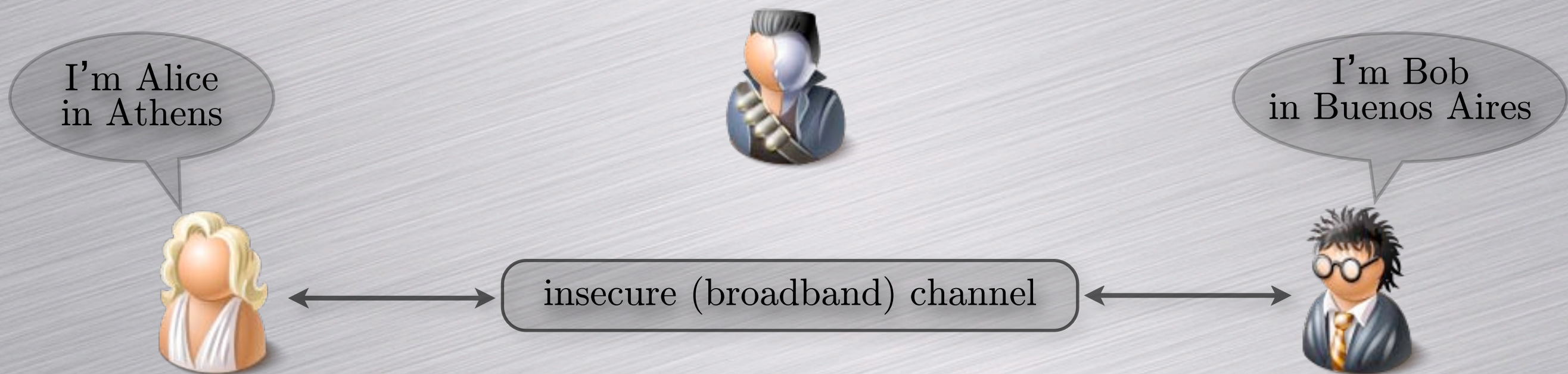
- Motivation
- SAS-based cryptography
 - Security model
 - Generic attacks, optimality
 - Overview of different protocols
- Signature schemes
 - Privacy protection
 - (Strengthening hash-and-sign implementations)

Motivation

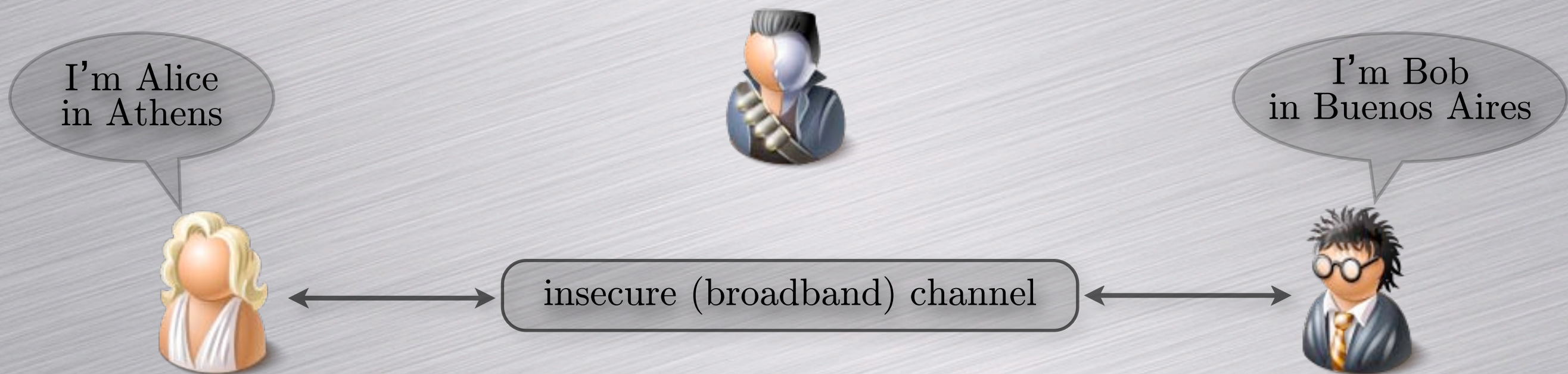
**How to establish
a secure communication?**

Hypothesis

Hypothesis



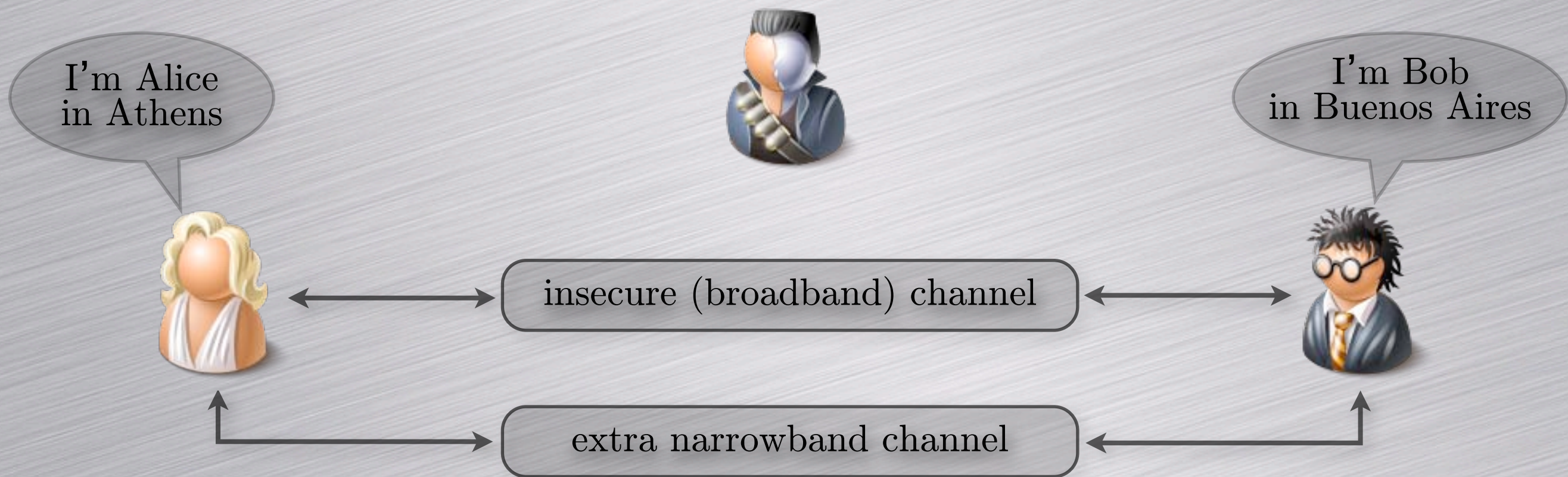
Hypothesis



Goal

Communicate securely

Hypothesis



Goal

Communicate securely

Symmetric cryptography



Need to **share a secret key k** .

Symmetric encryption is **secure** and **fast**.

Secret key exchange in reality

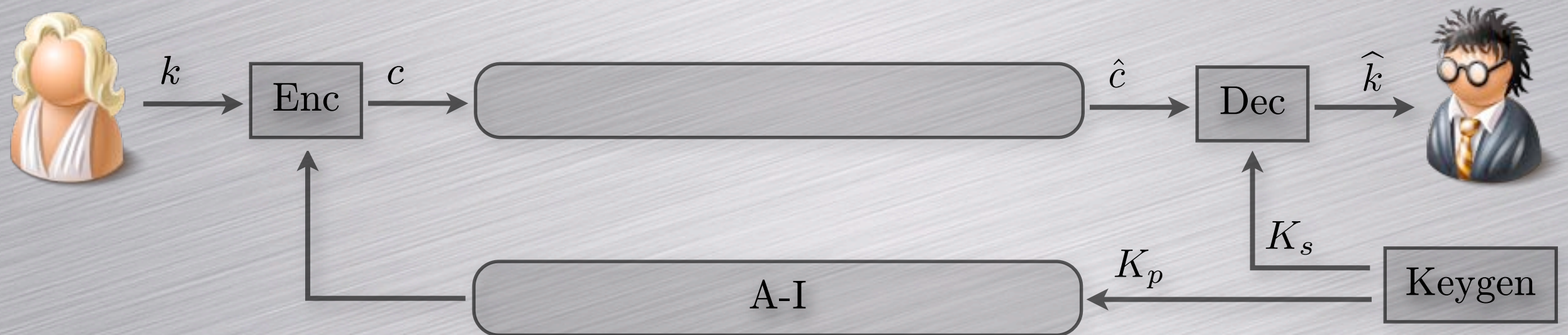
	Encounter	Telephone	Voice mail	E-mail
Confidentiality	😊			
Authenticity	😊	😊	😊	
Low cost		😊	😊	😊
Availability			😊	😊
Speed rate				😊

Confidential channel: expensive and bad availability.

Can we avoid confidentiality and only use authentication?

Asymmetric cryptography

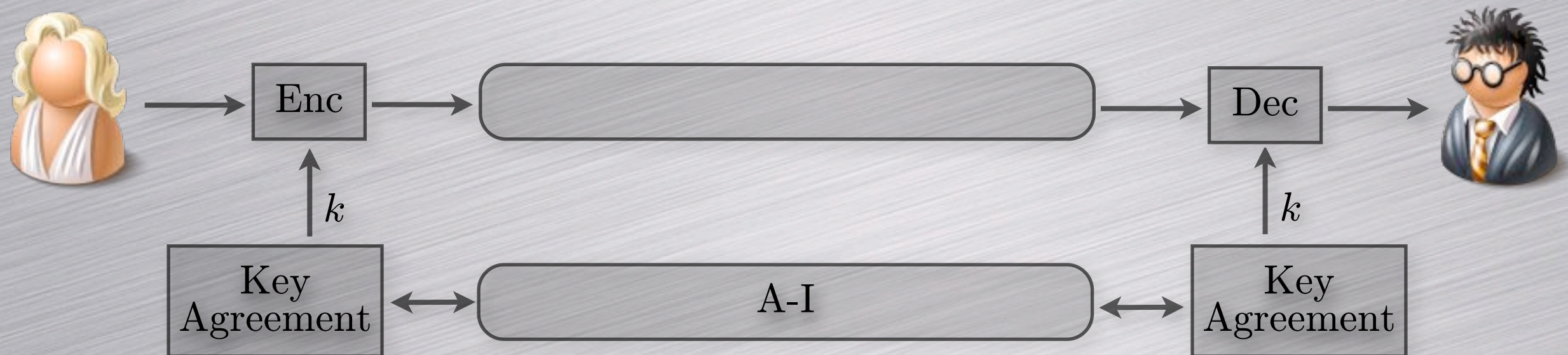
Semi-authenticated key transfer:



Confidentiality is no longer required.
Authentication is enough.

Key agreement

Merkle-Diffie-Hellman model:



Confidentiality is no longer required.
Authentication is enough.

In a nutshell

In a nutshell

- Goal:
 - Alice and Bob want to communicate securely

In a nutshell

- Goal:
 - Alice and Bob want to communicate securely
- Hypothesis:
 - no prior exchanged data (no PSK, no PKI)

In a nutshell

- Goal:
 - Alice and Bob want to communicate securely
- Hypothesis:
 - no prior exchanged data (no PSK, no PKI)
- A secure channel can be setup with a secret key

In a nutshell

- Goal:
 - Alice and Bob want to communicate securely
- Hypothesis:
 - no prior exchanged data (no PSK, no PKI)
- A secure channel can be setup with a secret key
- A secret key can be setup by
 - exchanging (and authenticating) a public-key
 - or running an authenticated key agreement

In a nutshell (2)

Claim

As long as parties are able to authenticate data,
they are able to setup a secure communication.

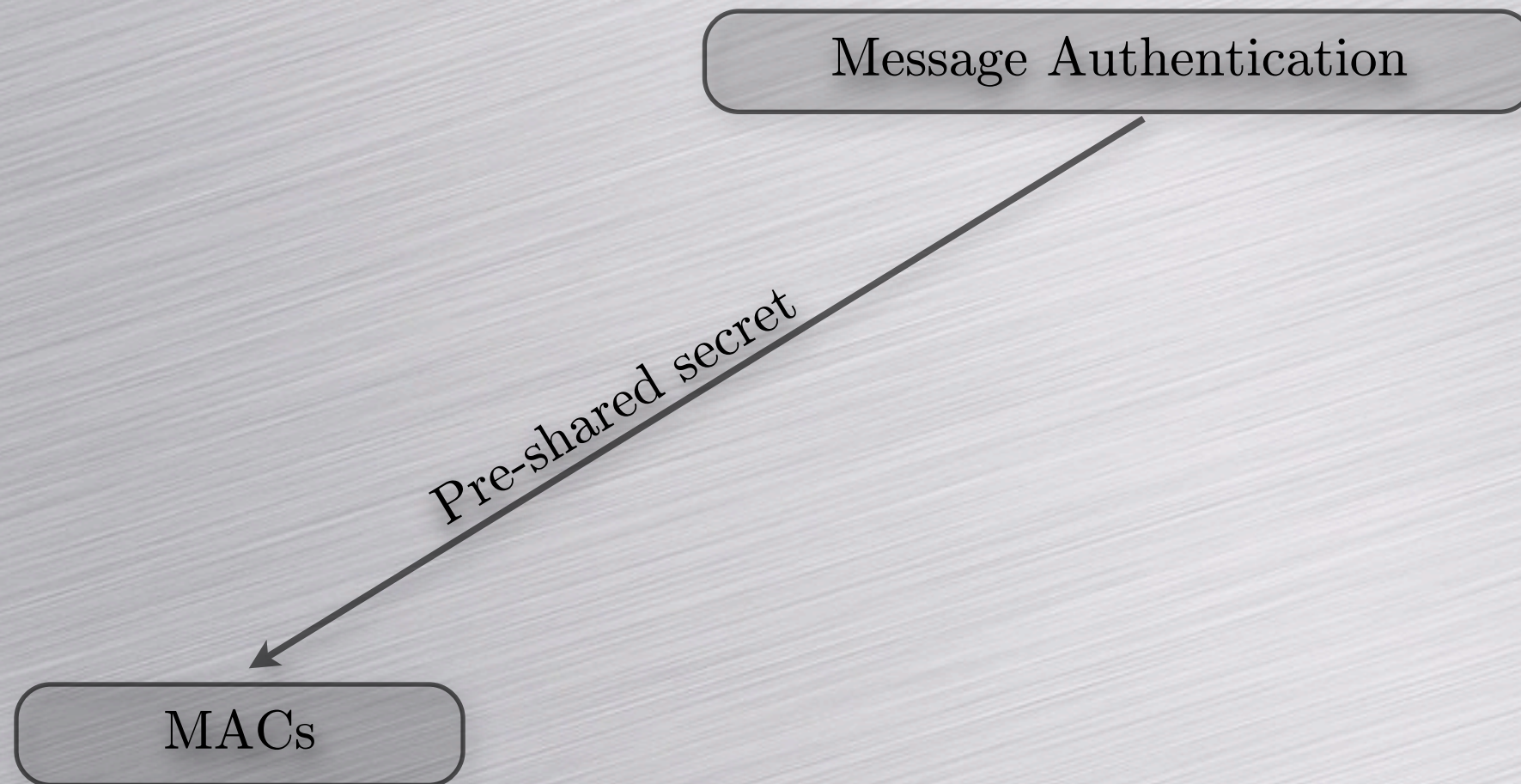
Motivation

How to authenticate messages?

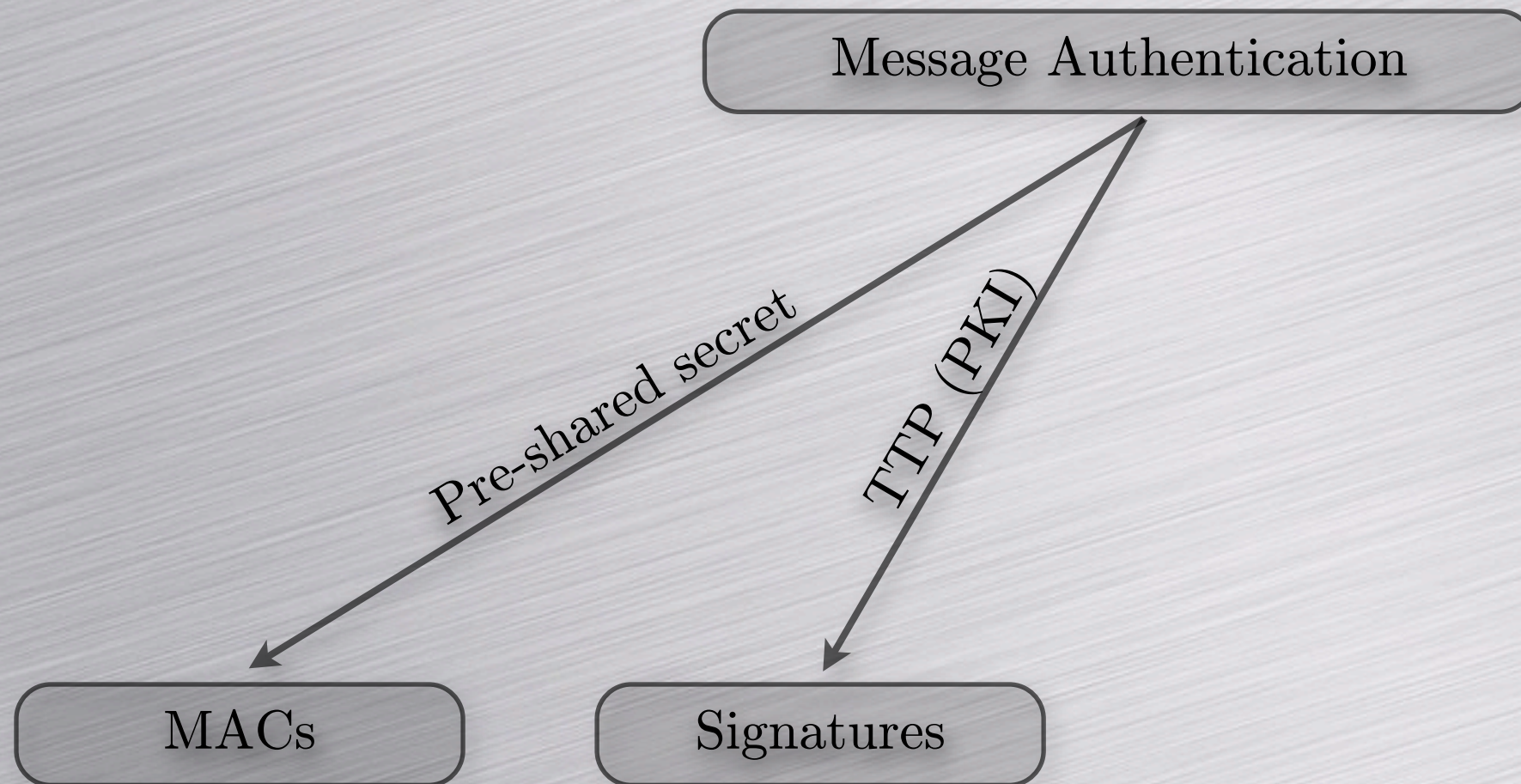
Authentication Overview

Message Authentication

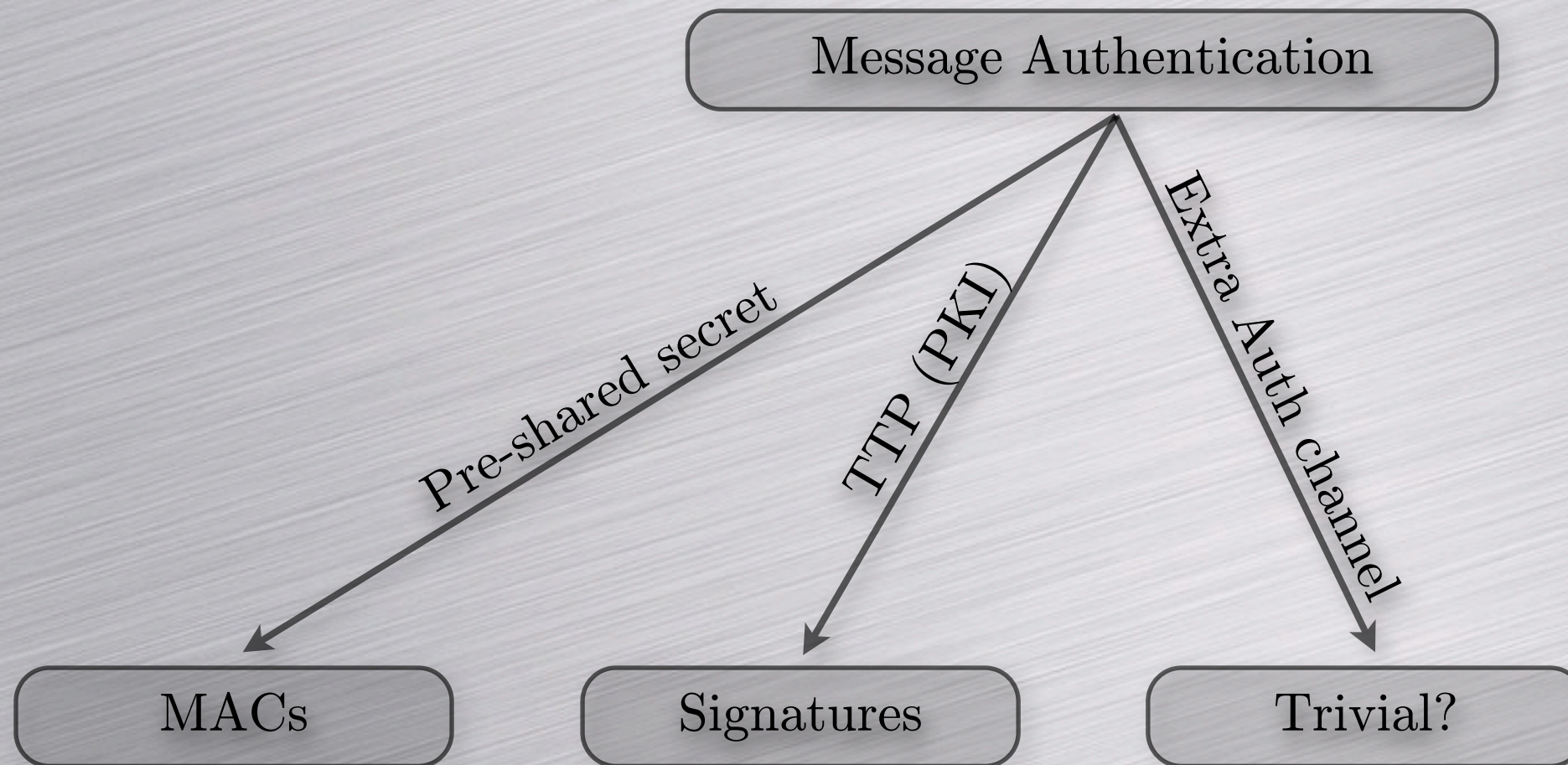
Authentication Overview



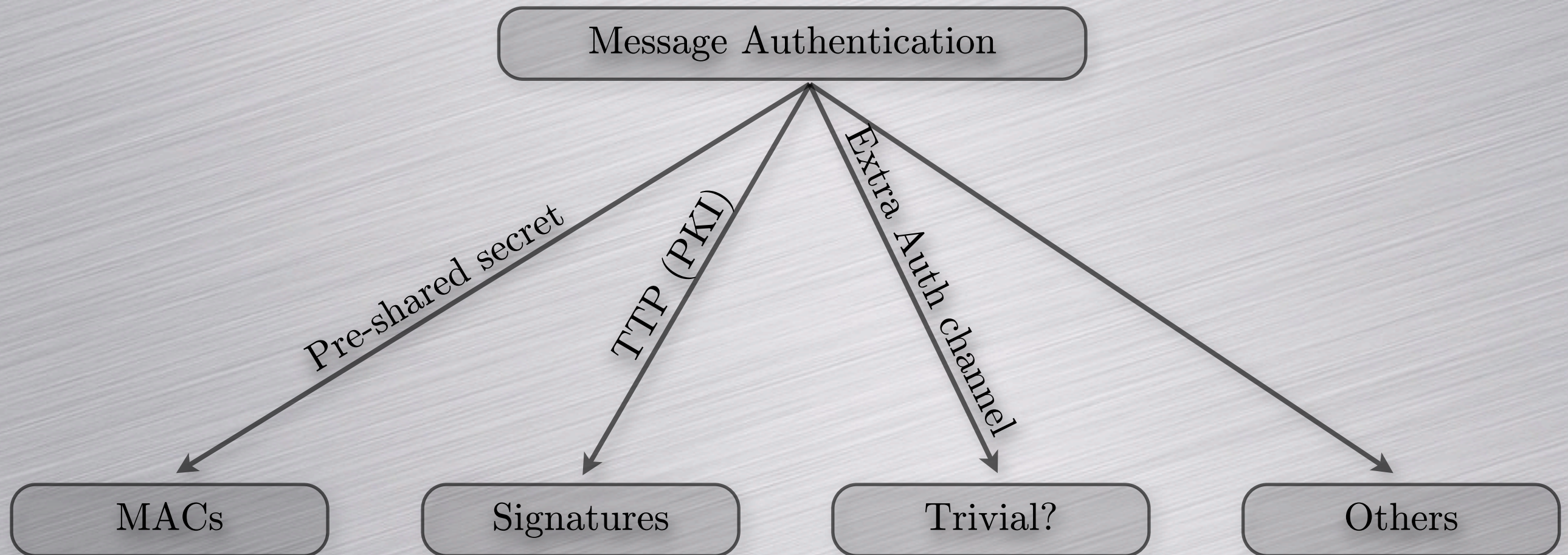
Authentication Overview



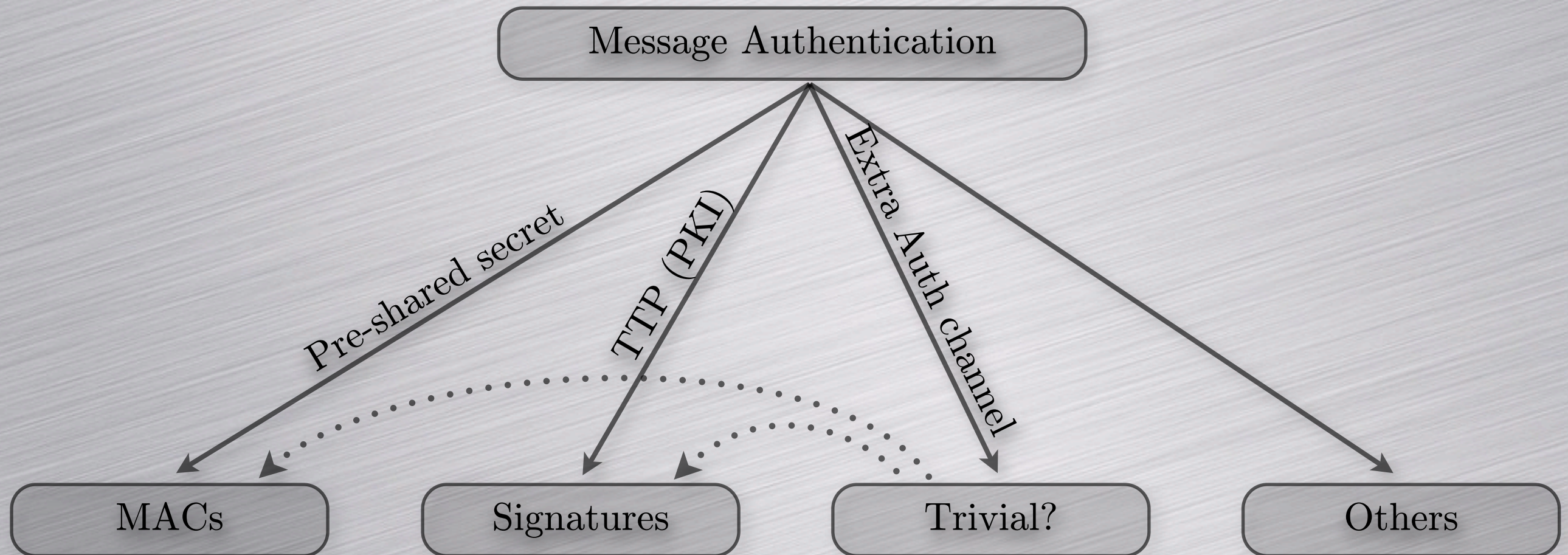
Authentication Overview



Authentication Overview

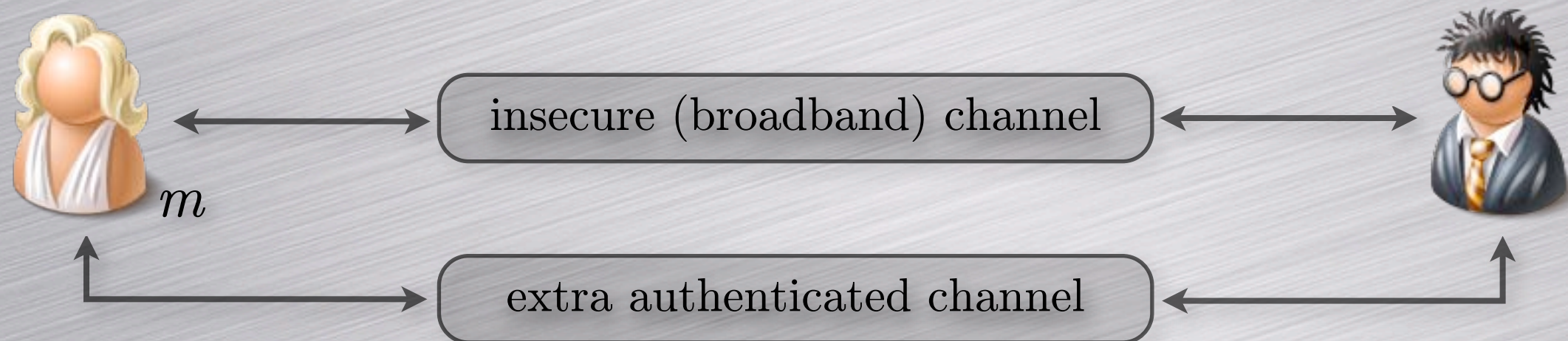


Authentication Overview



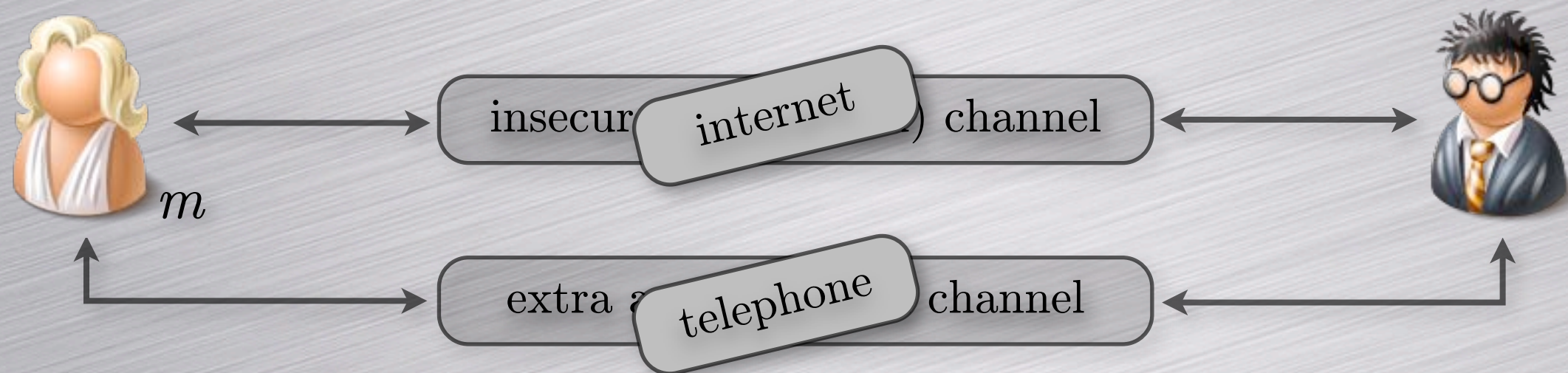
Trivial solution

Goal: authenticate the message m .



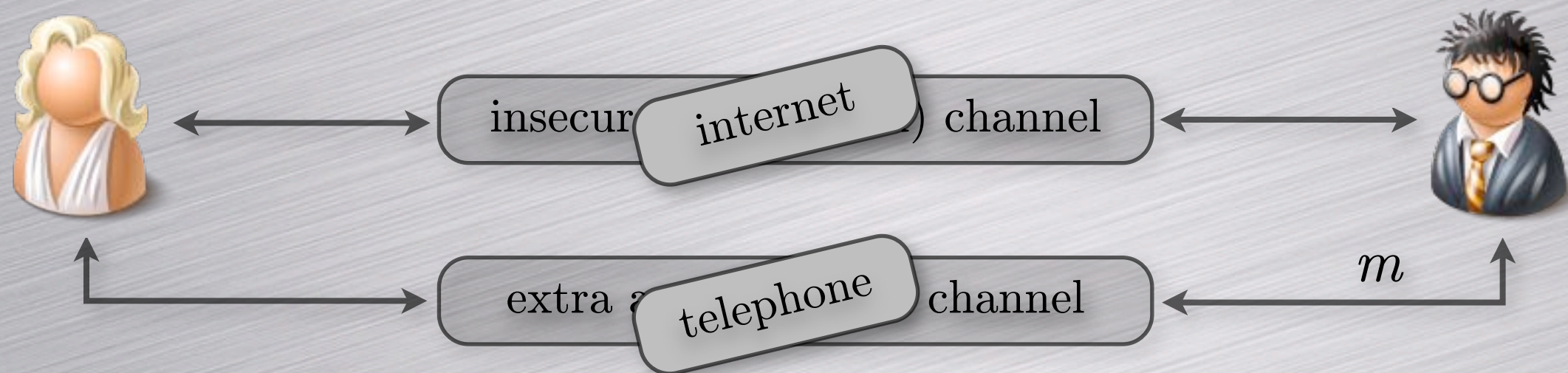
Trivial solution

Goal: authenticate the message m .



Trivial solution

Goal: authenticate the message m .



User-friendly...

Example of an RSA 1024-bit key:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEApZTXilQgosFxe
vR9ewub/qE1/BoHXCkpzWwopTHkiY2e8pMxMXOc/
DzKV0qgsdC3X9pQODRy+awoANAgttPX
h6JM4ZlYgaEN6azJSyrK0SlOLDn
+YmjhaKEn1ufLbroQ6Cpg0lj3lXvHEN52P32IfhY08ivC
0pBmO4Y eyErBiE=
```

By telephone... good luck!

User-friendly...

Example of an RSA 1024-bit key:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEApZTXilQgosFxe
vR9ewub/qE1/BoHXCkpzWwopTHkiY2e8pMxMXOc/
DzKV0qgsdC3X9pQODRy+awoANAgttPX
h6JM4ZlYgaEN6azJSyrK0SlOLDn
+YmjhaKEn1ufLbroQ6Cpg0lj3lXvHEN52P32IfhY08ivC
0pBmO4Y eyErBiE=
```

By telephone... good luck!

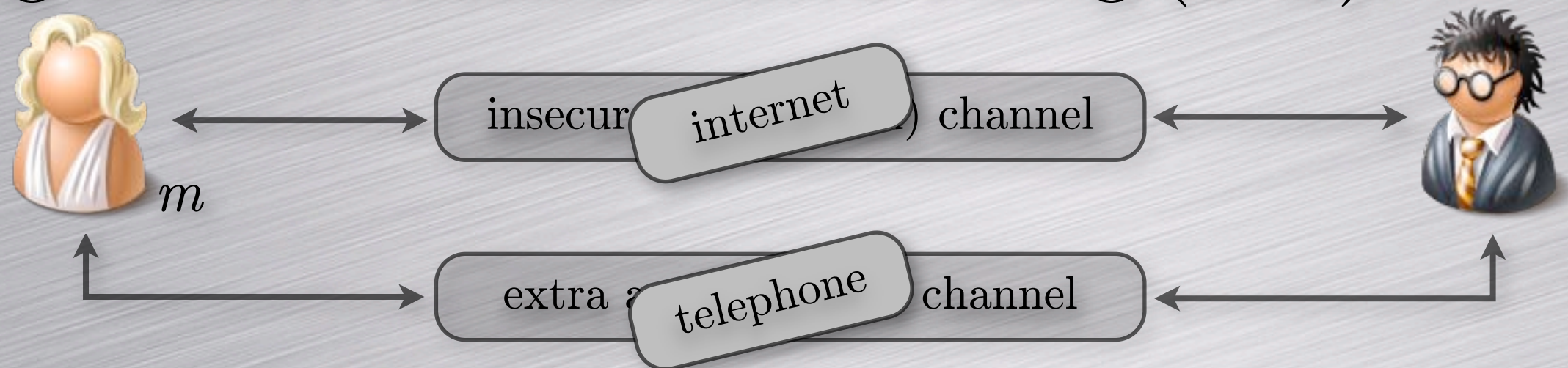
Objective

Design user-friendly protocols.
So, authenticated data should be as short as possible.

In practice...

Goal: authenticate the message m .

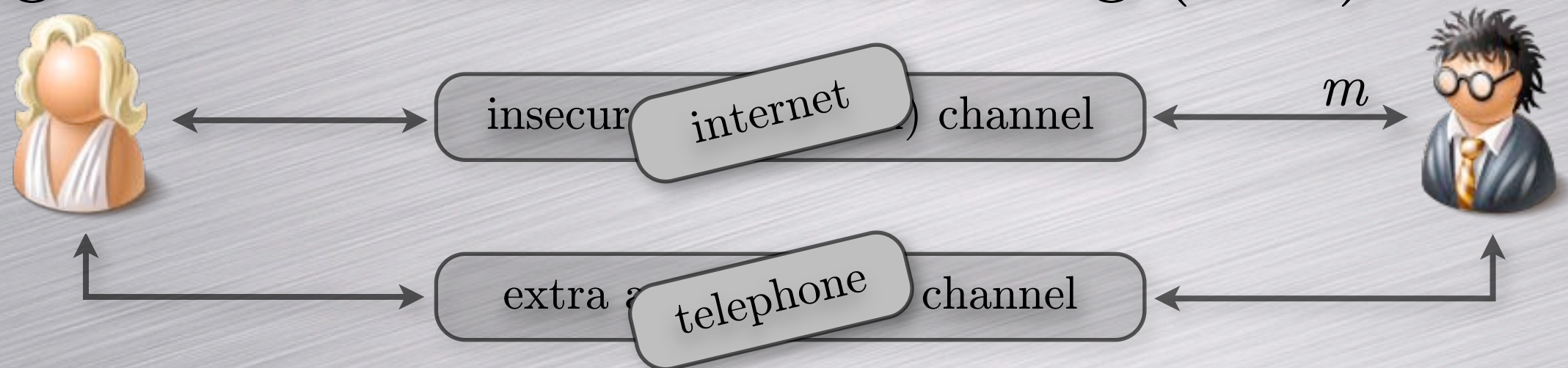
Using a Short Authenticated String (SAS):



In practice...

Goal: authenticate the message m .

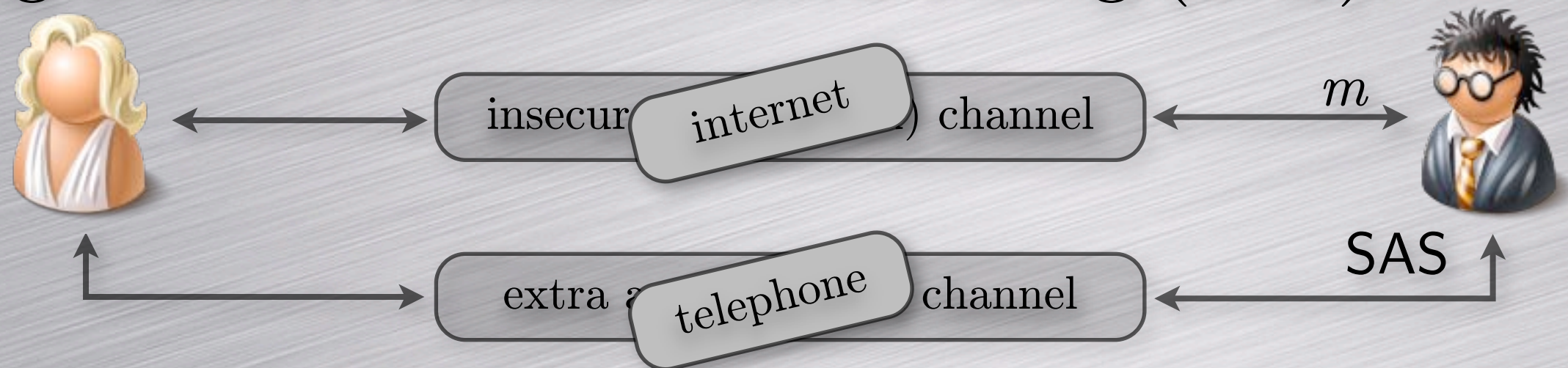
Using a Short Authenticated String (SAS):



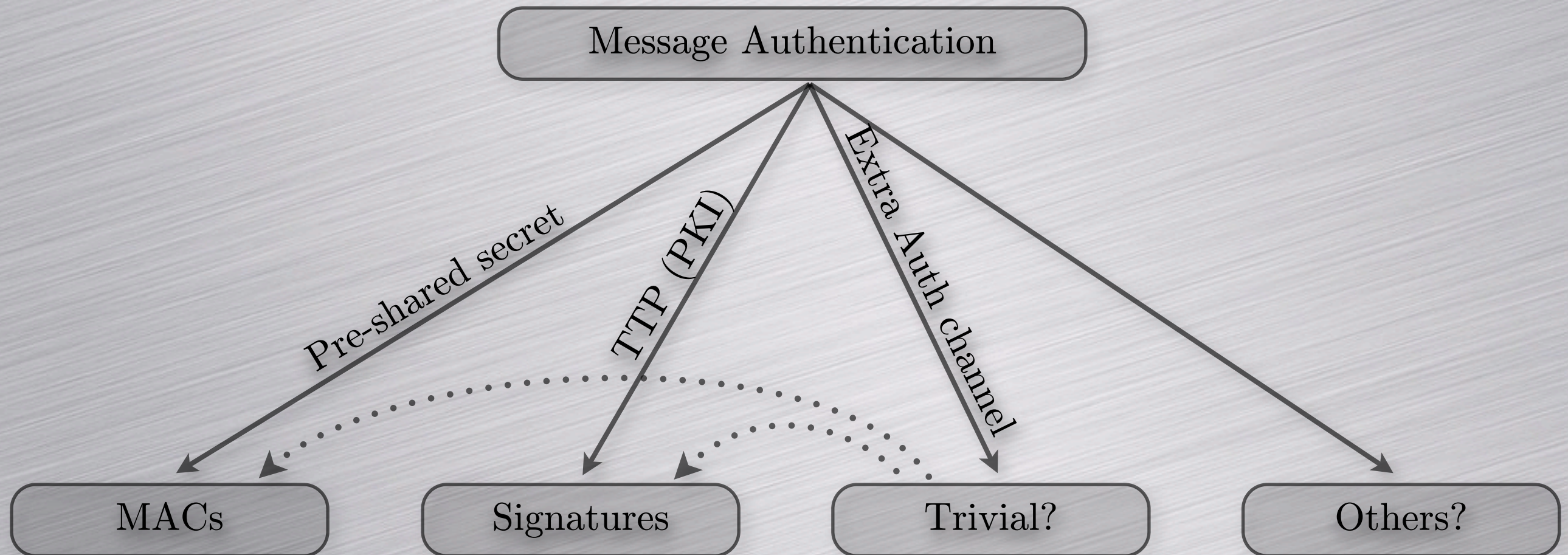
In practice...

Goal: authenticate the message m .

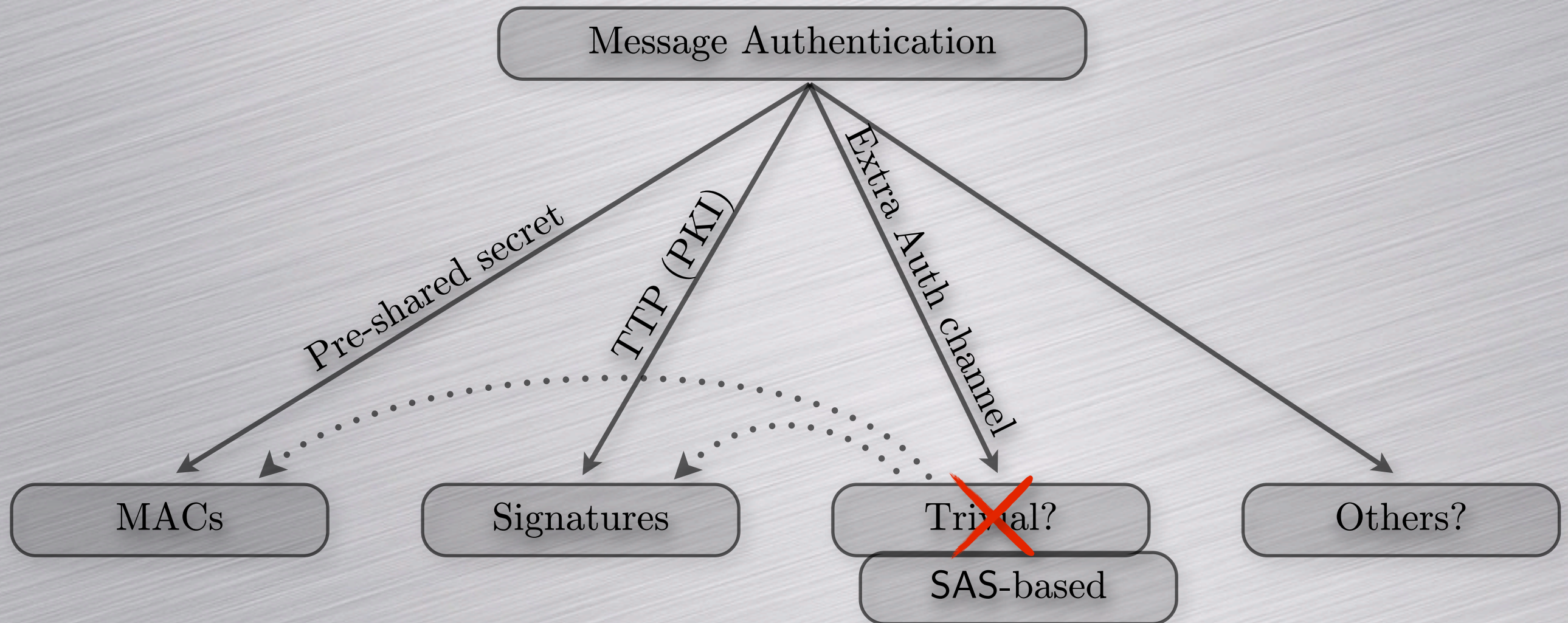
Using a Short Authenticated String (SAS):



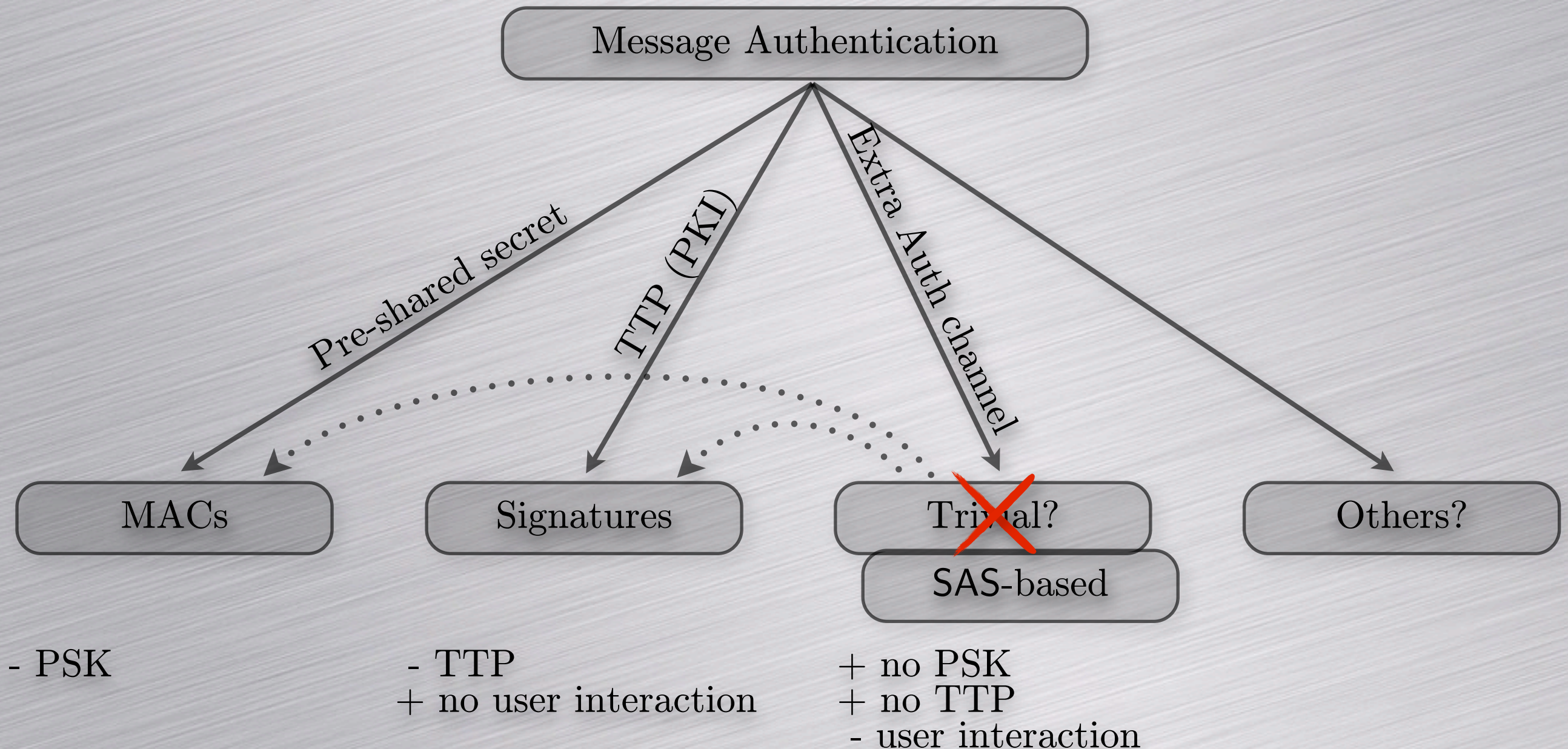
Authentication Overview



Authentication Overview



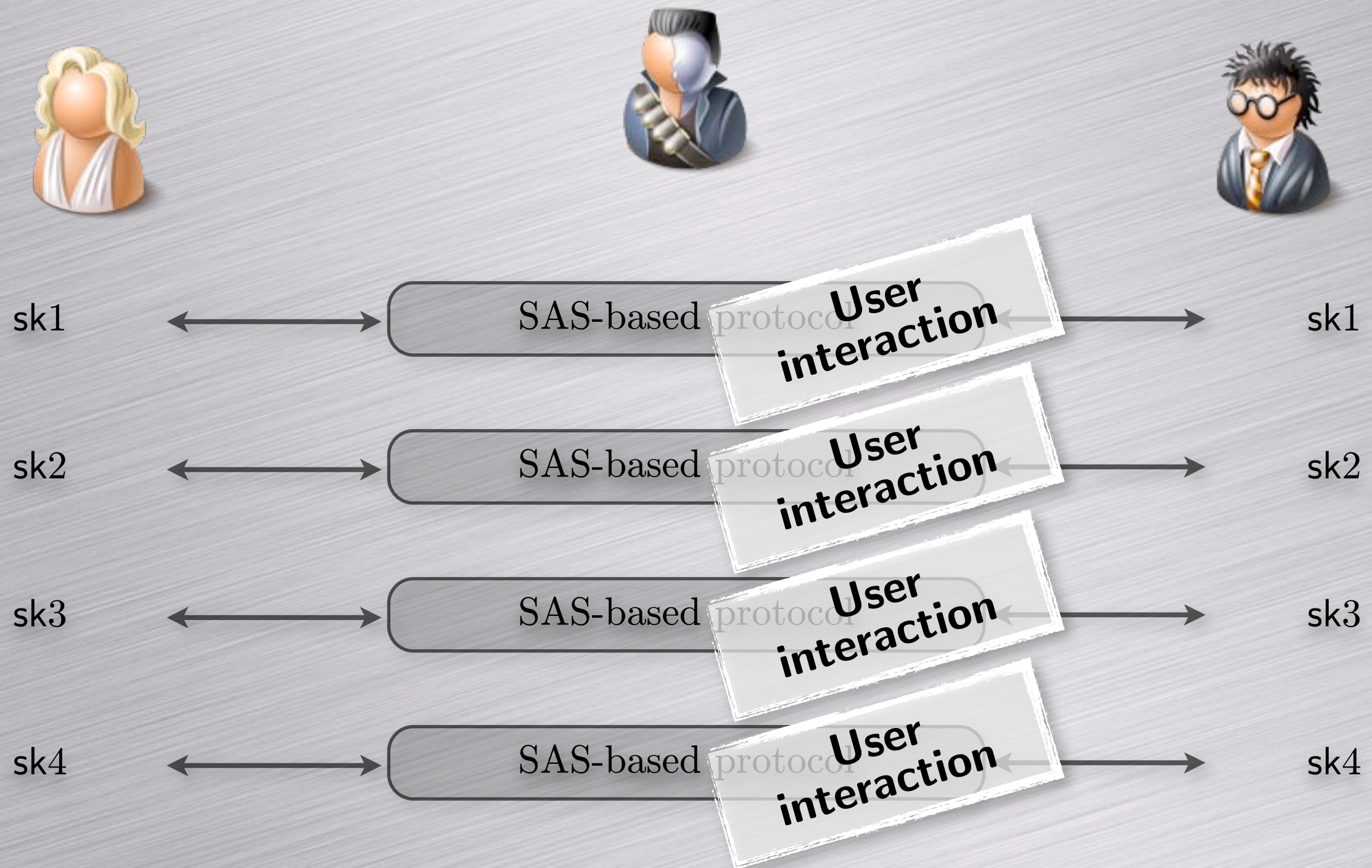
Authentication Overview



Using SAS-based Protocols



Using SAS-based Protocols



Trusted Setup



Trusted Setup



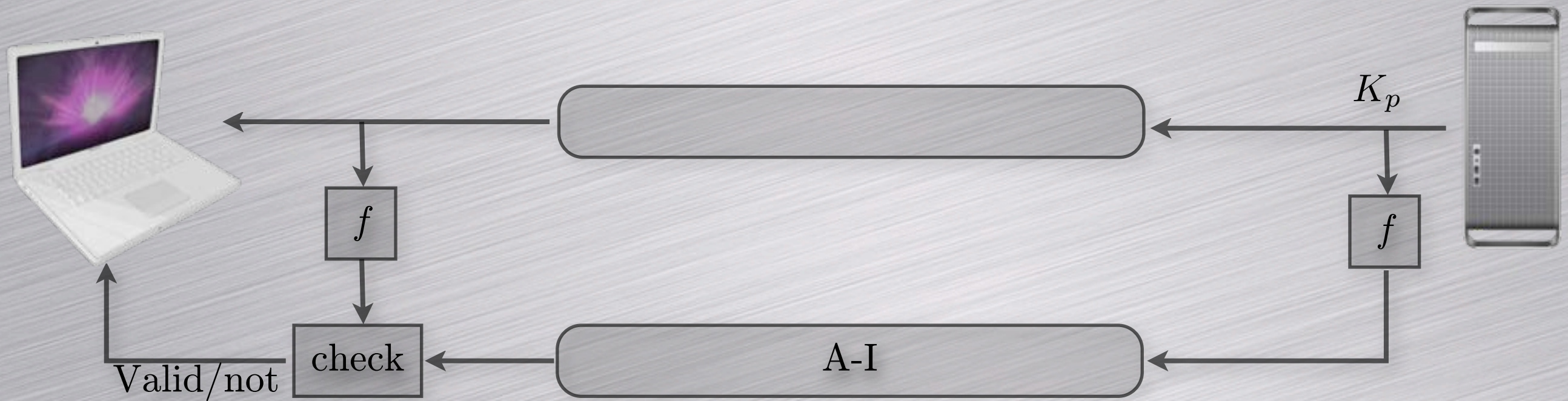
Trusted Setup



+ no PSK, + no TTP, + one user interaction

Example: Secure Shell (SSH)

Goal: authenticate the server's public key.



Check done the first time only (trusted setup)

The fingerprint is of the form

bc:a1:12:30:bc:17:08:eb:31:43:eb:e1:15:12:ca:1a (hexa)

It is better, but who **really** check this?

SAS-based Cryptography

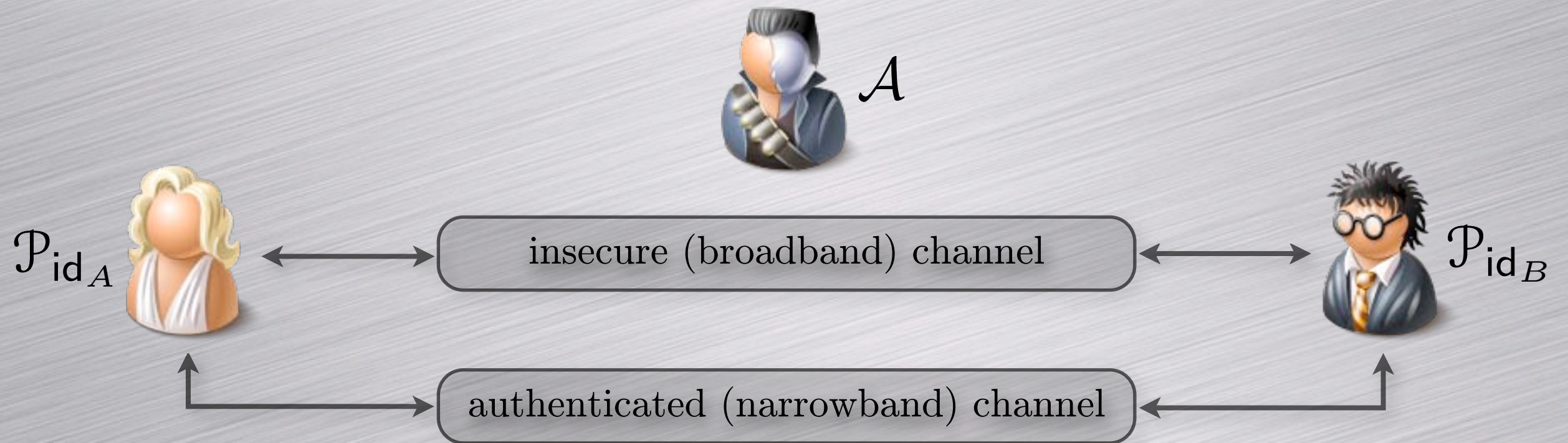
SAS also known as...

- MANual Authentication (MANA)
 - Gehrman, Mitchell, Nyberg, and Laur.
- Short Authenticated String (SAS)
 - Vaudenay and Pasini.
- Two-channel cryptography
 - Mashatan and Stinson.
- User-aided data authentication
 - Peyrin, Vaudenay, and recently Laur and Pasini.

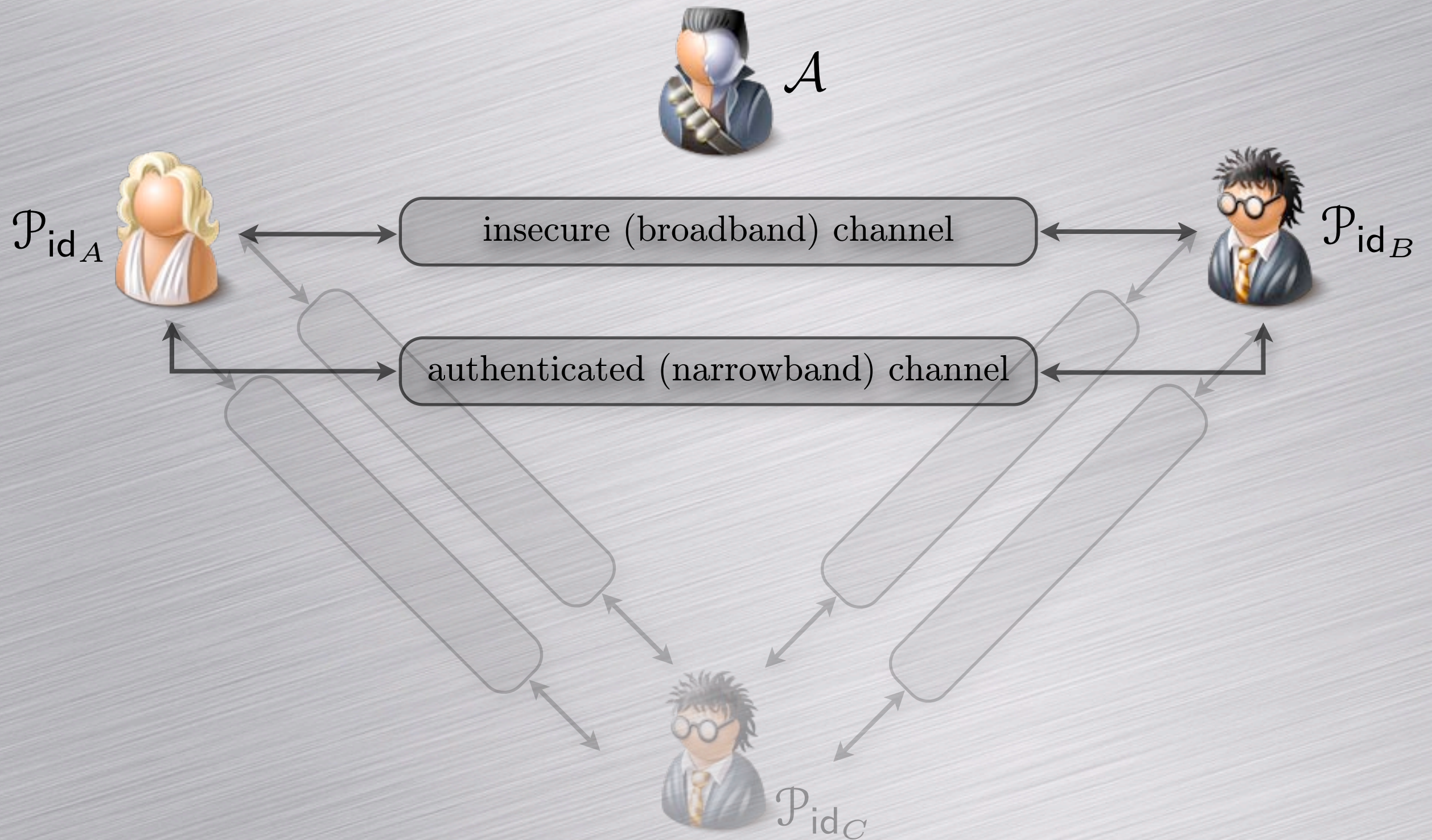
SAS-based Cryptography

Security model

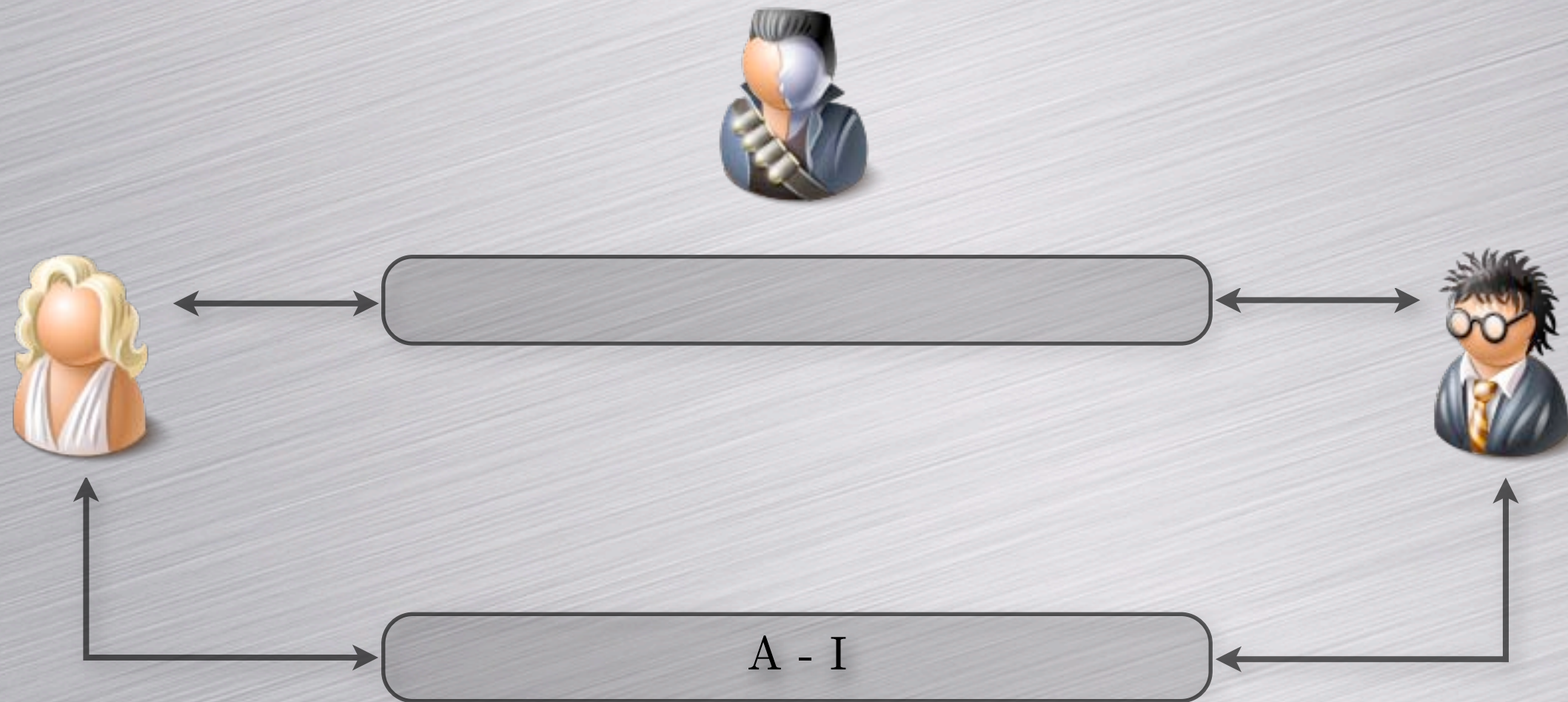
Network model



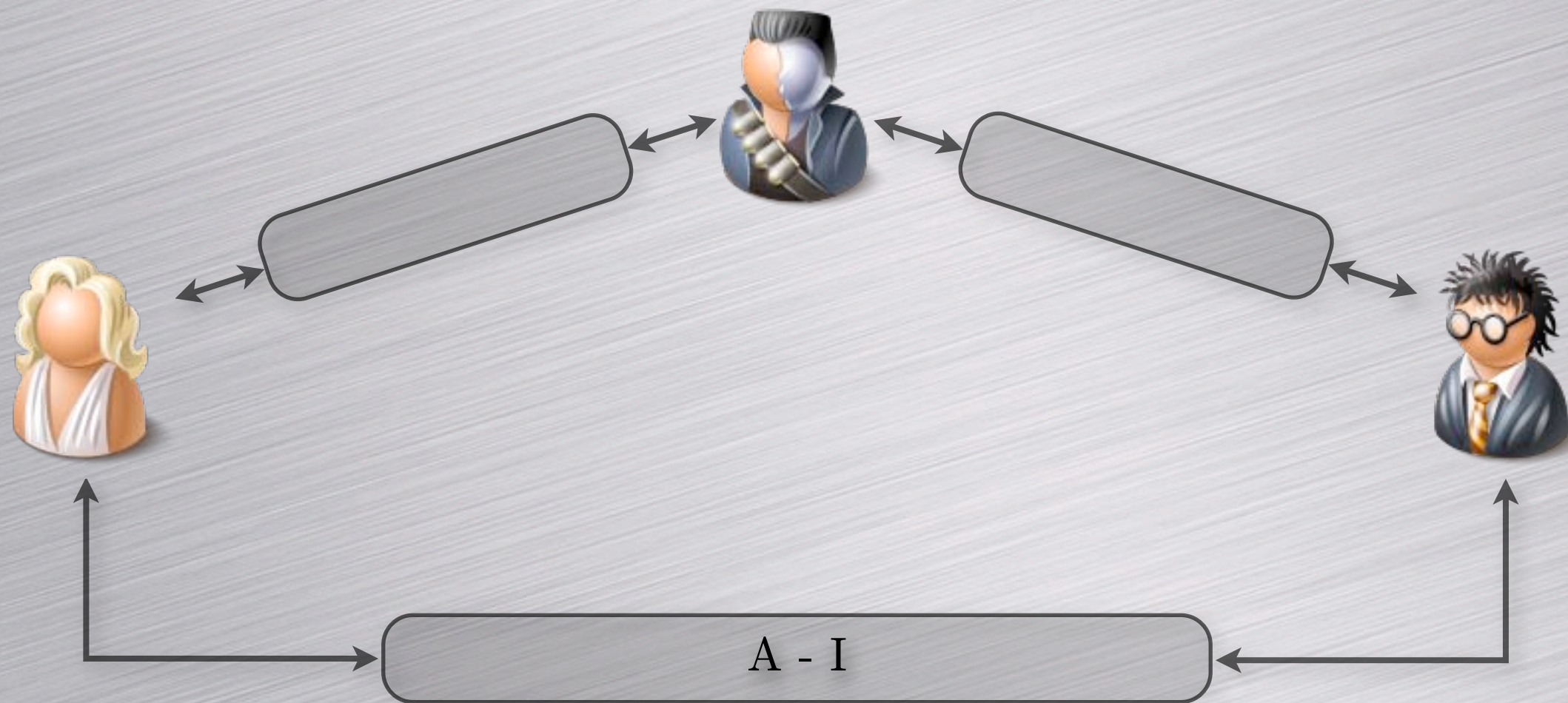
Network model



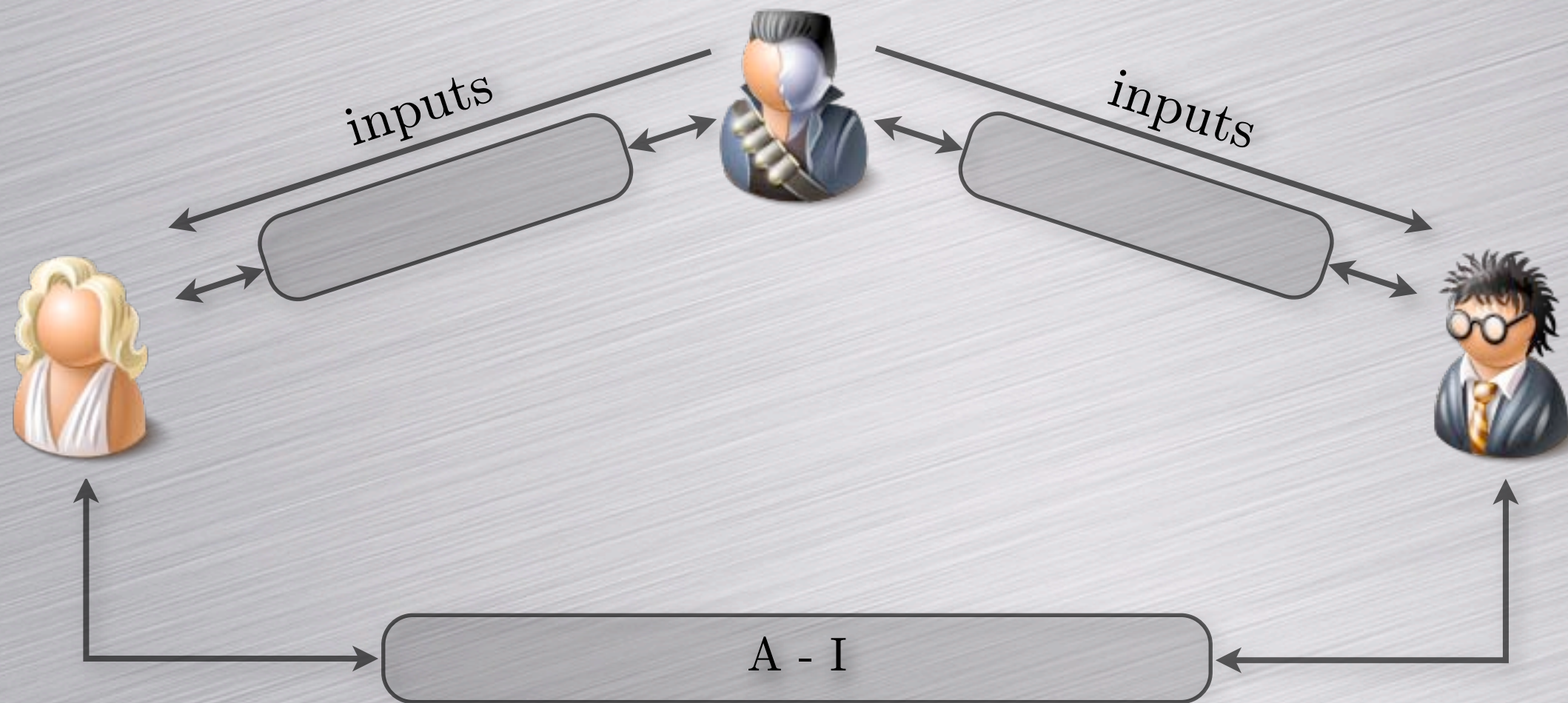
Adversarial model



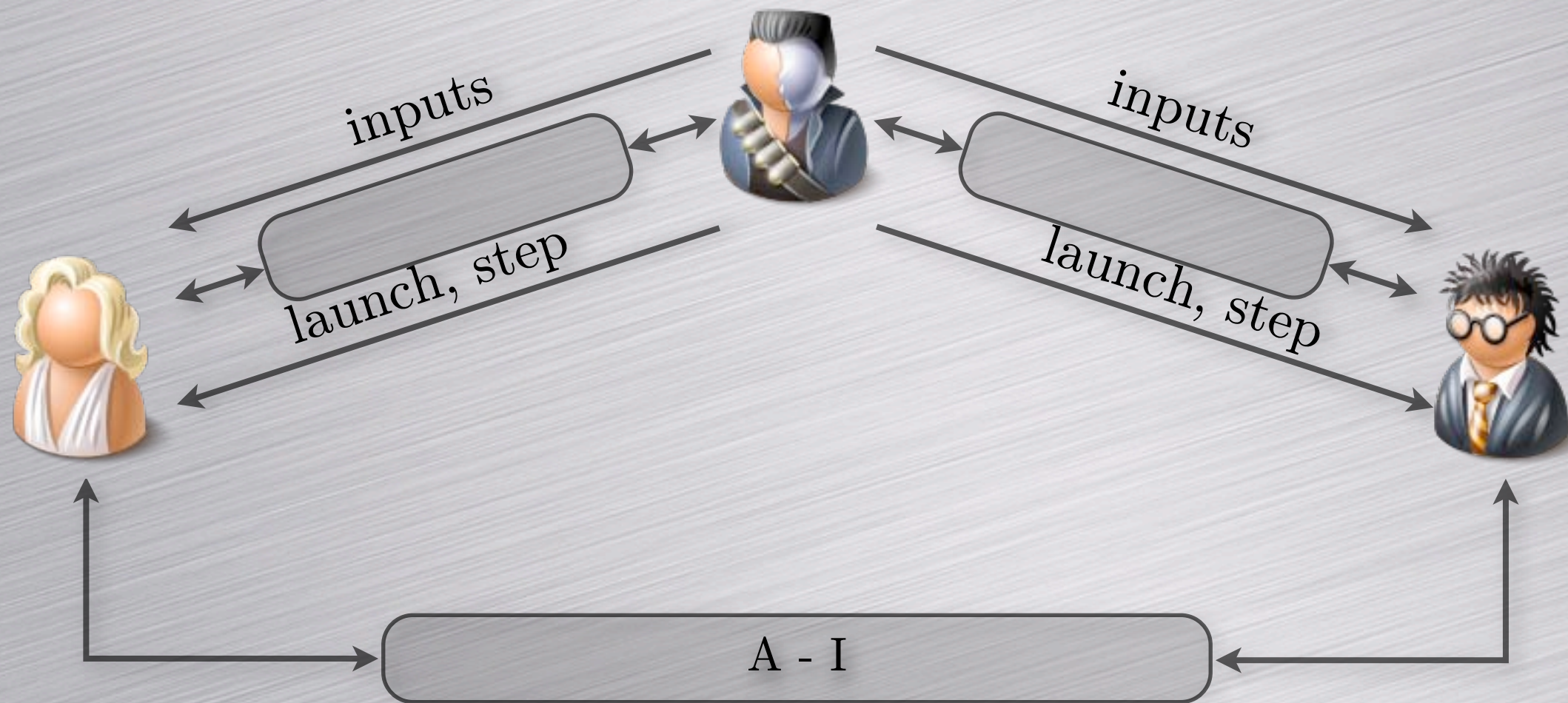
Adversarial model



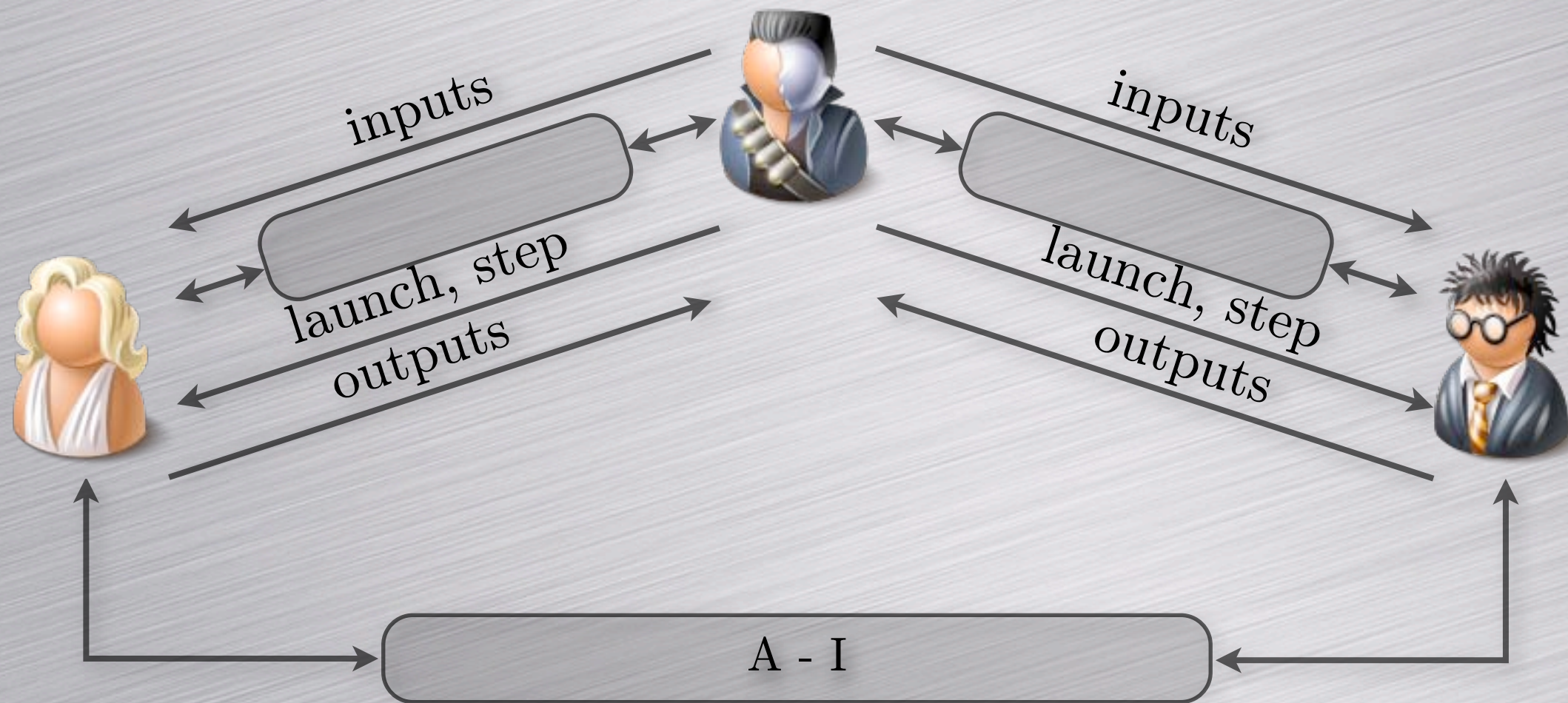
Adversarial model



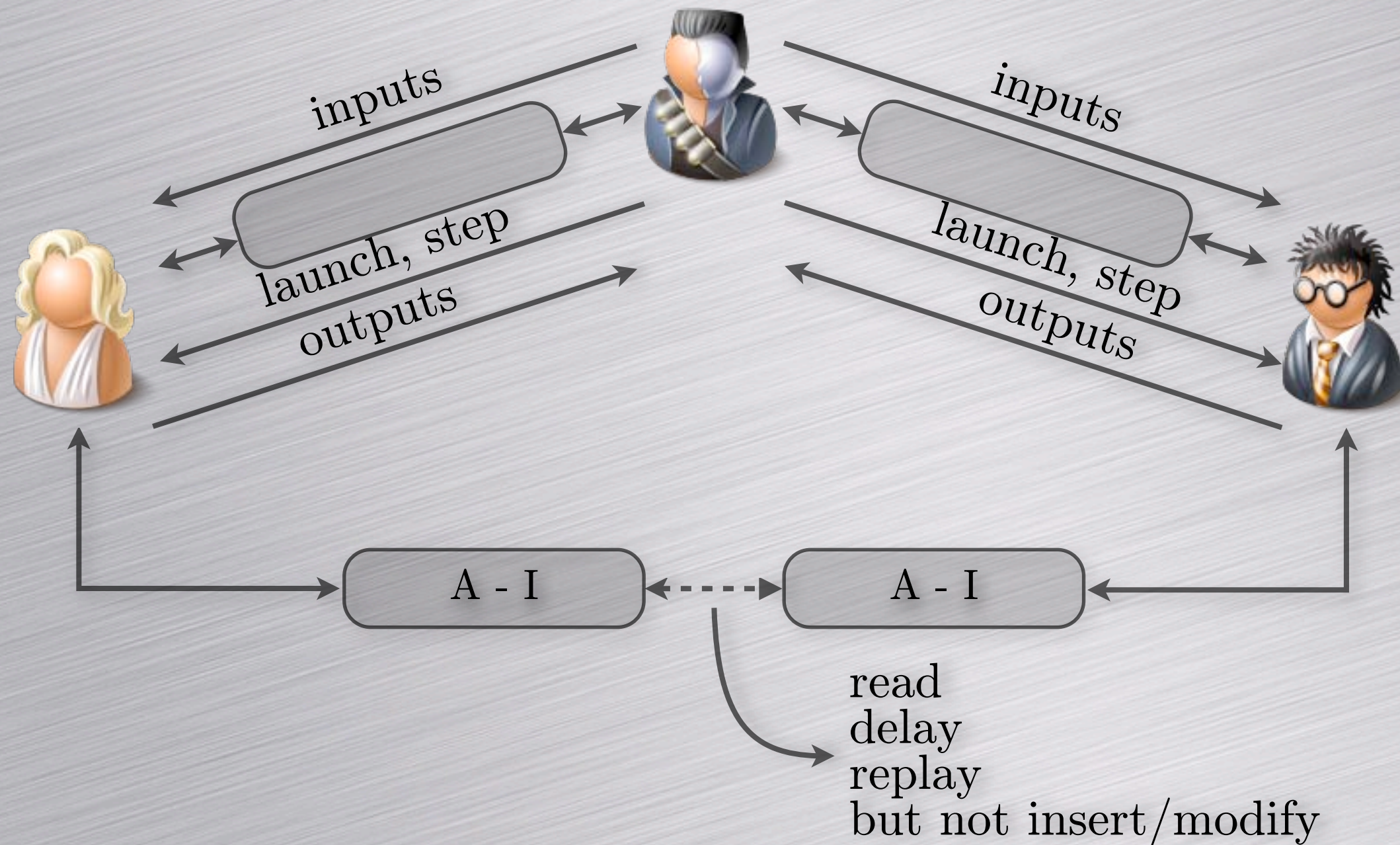
Adversarial model



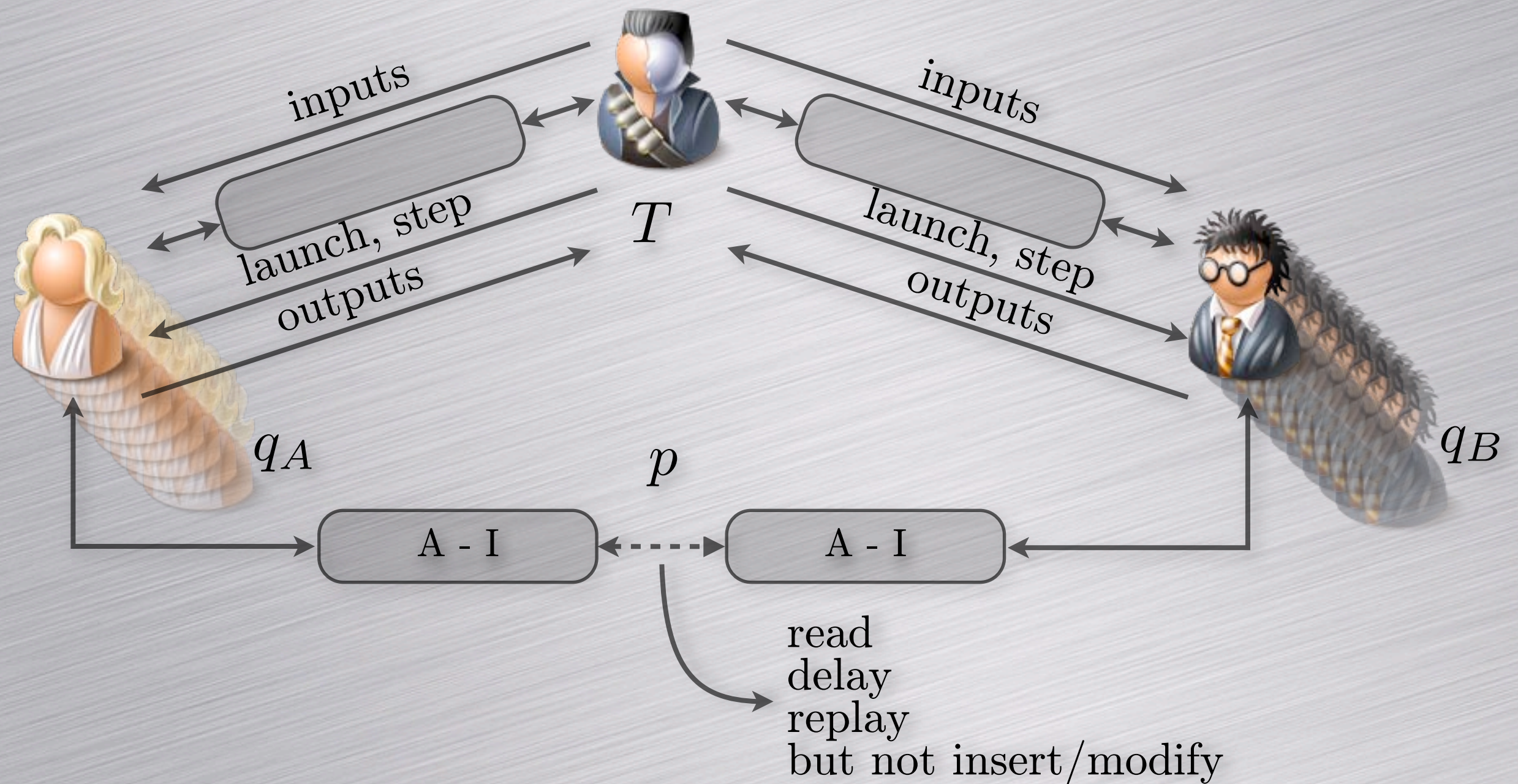
Adversarial model



Adversarial model

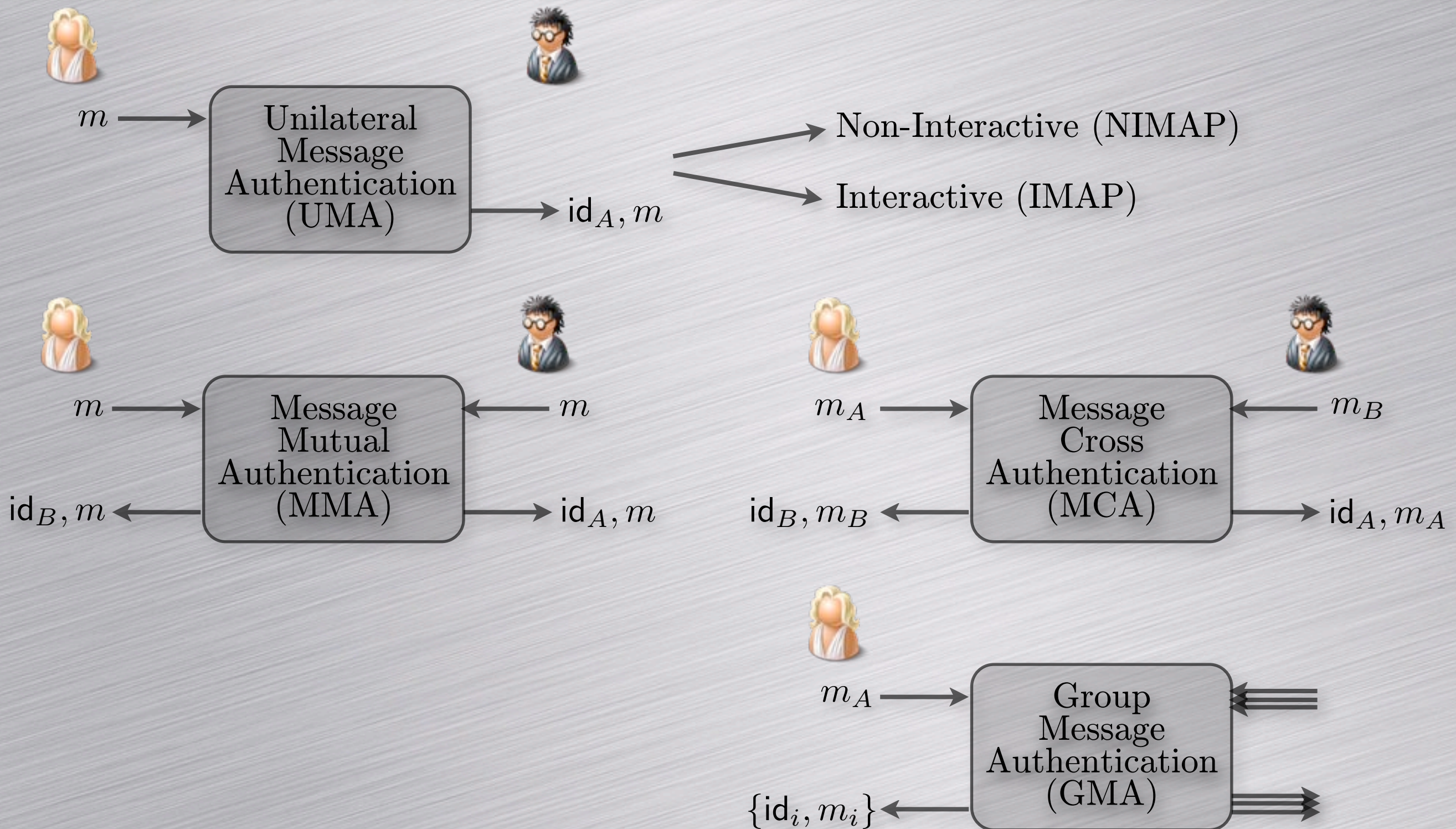


Adversarial model



The attack cost is measured by (T, q, p) .

Message Authentication



SAS-based Cryptography

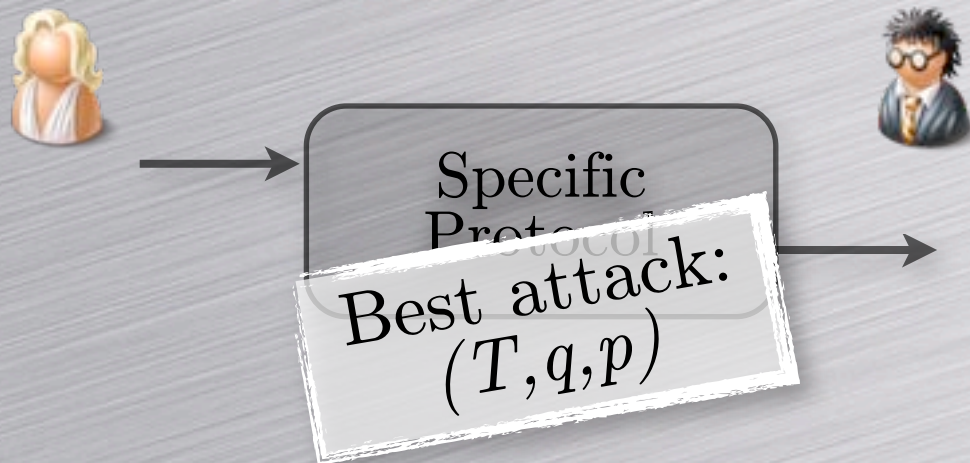
Generic attacks, optimality

What is the maximal security?

- Suppose
 - no limit on the insecure channel
 - limit on the authenticated channel: k bits
 - fixed bound on complexities q and T

What is the maximal security?

- Suppose
 - no limit on the insecure channel
 - limit on the authenticated channel: k bits
 - fixed bound on complexities q and T



- The protocol is at least (T, q, p) -secure

What is the maximal security?

- Suppose
 - no limit on the insecure channel
 - limit on the authenticated channel: k bits
 - fixed bound on complexities q and T



- The protocol is at least (T, q, p) -secure
- Every protocols are at most (T, q, P) -secure

What is the maximal security?

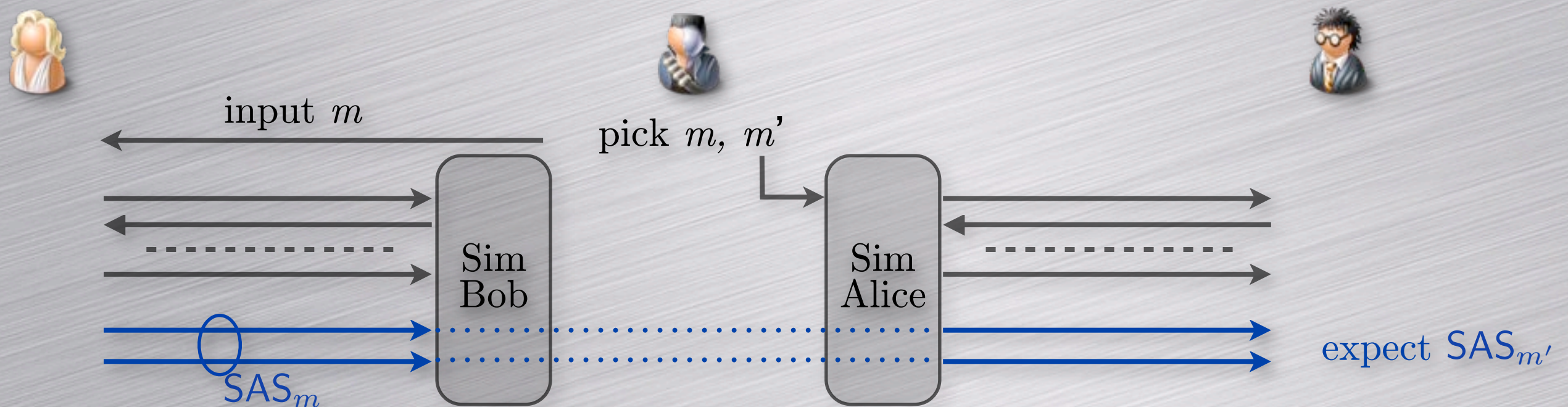
- Suppose
 - no limit on the insecure channel
 - limit on the authenticated channel: k bits
 - fixed bound on complexities q and T



- The protocol is at least (T, q, p) -secure
- Every protocols are at most (T, q, P) -secure
- When $p \rightarrow P$, the protocol is said **optimal**

Generic One-shot Attack

- Consider a generic UMA
 - goal: impersonation of Alice
 - one protocol run only



$$p = \Pr[\text{success}] = \Pr[SAS_m = SAS_{m'} \text{ and } m \neq m']$$

Generic One-shot Attack (2)

$$p = \Pr[\text{success}] = \Pr[\text{SAS}_m = \text{SAS}_{m'} \text{ and } m \neq m']$$

$$\begin{aligned} \Pr[\text{SAS}_m = \text{SAS}_m] &= \Pr[\text{SAS}_m = \text{SAS}_m \text{ and } m \neq m'] \\ &\quad + \Pr[\text{SAS}_m = \text{SAS}_m \text{ and } m = m'] \end{aligned}$$

$$\begin{aligned} p &= \Pr[\text{SAS}_m = \text{SAS}_{m'}] - \Pr[\text{SAS}_m = \text{SAS}_{m'} \text{ and } m = m'] \\ &\geq \Pr[\text{SAS}_m = \text{SAS}_{m'}] - \Pr[m = m'] \end{aligned}$$

$$\begin{aligned} &\geq \Pr[\text{SAS}_m = \text{SAS}_{m'} | \mathcal{D} \text{ is uniform}] \\ &= \frac{1}{n} \end{aligned}$$

2^{-t}

$$p \geq \frac{1}{n} - 2^{-t}$$

Optimal SAS Distribution

Set of possible SAS: $\mathcal{S} = \{s_1, \dots, s_n\}$

Let p_i denote $\Pr[\text{SAS} = s_i]$

Let $\text{SAS}_1, \text{SAS}_2 \in_{\mathcal{D}} \mathcal{S}$

Optimal SAS Distribution

Set of possible SAS: $\mathcal{S} = \{s_1, \dots, s_n\}$

Let p_i denote $\Pr[\text{SAS} = s_i]$

Let $\text{SAS}_1, \text{SAS}_2 \in_{\mathcal{D}} \mathcal{S}$

$$p = \Pr[\text{SAS}_1 = \text{SAS}_2] = \sum_{i=1}^n p_i^2$$

Optimal SAS Distribution

Set of possible SAS: $\mathcal{S} = \{s_1, \dots, s_n\}$

Let p_i denote $\Pr[\text{SAS} = s_i]$

Let $\text{SAS}_1, \text{SAS}_2 \in_{\mathcal{D}} \mathcal{S}$

$$p = \Pr[\text{SAS}_1 = \text{SAS}_2] = \sum_{i=1}^n p_i^2$$

$\mathcal{D}$ is uniform

$\mathcal{D}$ is non-uniform

Optimal SAS Distribution

Set of possible SAS: $\mathcal{S} = \{s_1, \dots, s_n\}$

Let p_i denote $\Pr[\text{SAS} = s_i]$

Let $\text{SAS}_1, \text{SAS}_2 \in_{\mathcal{D}} \mathcal{S}$

$$p = \Pr[\text{SAS}_1 = \text{SAS}_2] = \sum_{i=1}^n p_i^2$$

$\mathcal{D}$ is uniform

$$p_i = 1/n$$

$$\begin{aligned} p &= \sum (1/n)^2 \\ &= 1/n \end{aligned}$$

$\mathcal{D}$ is non-uniform

Optimal SAS Distribution

Set of possible SAS: $\mathcal{S} = \{s_1, \dots, s_n\}$

Let p_i denote $\Pr[\text{SAS} = s_i]$

Let $\text{SAS}_1, \text{SAS}_2 \in_{\mathcal{D}} \mathcal{S}$

$$p = \Pr[\text{SAS}_1 = \text{SAS}_2] = \sum_{i=1}^n p_i^2$$

$\mathcal{D}$ is uniform

$$p_i = 1/n$$

$$\begin{aligned} p &= \sum (1/n)^2 \\ &= 1/n \end{aligned}$$

$\mathcal{D}$ is non-uniform

$$p_i = 1/n + \delta_i \quad \text{with} \quad \sum_{i=1}^n \delta_i = 0$$

$$\begin{aligned} p &= \sum (1/n + \delta_i)^2 \\ &= \sum (1/n)^2 + 1/n \sum \delta_i + \sum \delta_i^2 \\ &> 1/n \end{aligned}$$

Optimal SAS Distribution

Set of possible SAS: $\mathcal{S} = \{s_1, \dots, s_n\}$

Let p_i denote $\Pr[\text{SAS} = s_i]$

Let $\text{SAS}_1, \text{SAS}_2 \in_{\mathcal{D}} \mathcal{S}$

$$p = \Pr[\text{SAS}_1 = \text{SAS}_2] = \sum_{i=1}^n p_i^2$$

$\mathcal{D}$ is uniform

$$p_i = 1/n$$

$$\begin{aligned} p &= \sum (1/n)^2 \\ &= \boxed{1/n} \text{optimal} \end{aligned}$$

$\mathcal{D}$ is non-uniform

$$p_i = 1/n + \delta_i \quad \text{with} \quad \sum_{i=1}^n \delta_i = 0$$

$$p = \sum (1/n + \delta_i)^2$$

$$\begin{aligned} &= \sum (1/n)^2 + 1/n \sum \delta_i + \sum \delta_i^2 \\ &> 1/n \end{aligned}$$

Generic Multi-shot Attack

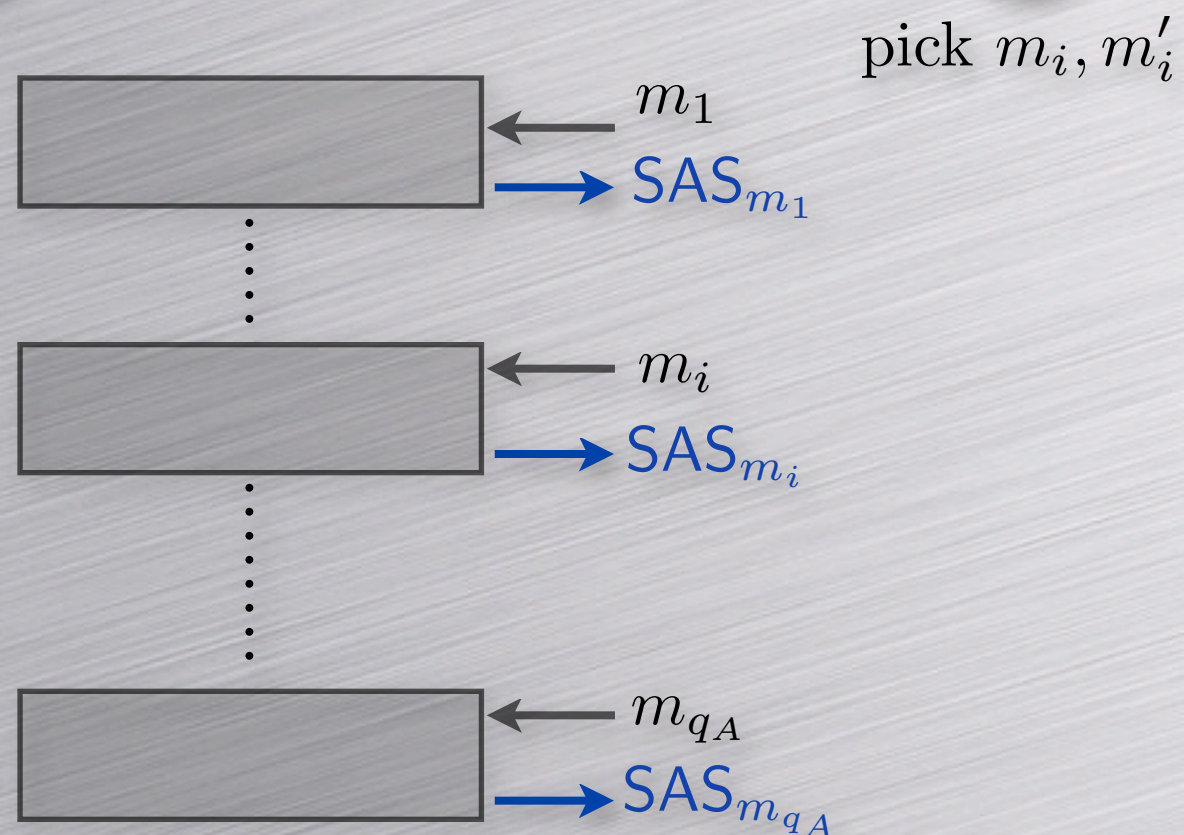
Now, the adversary may use several protocol runs...



pick m_i, m'_i

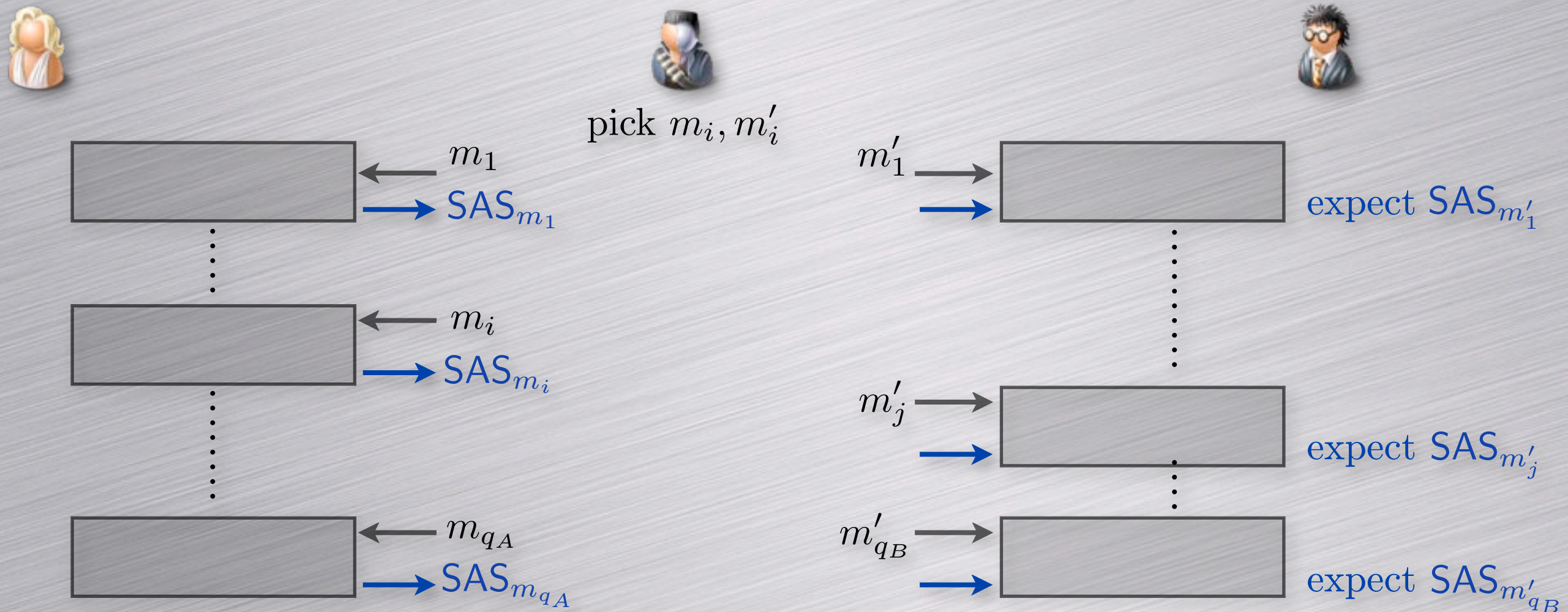
Generic Multi-shot Attack

Now, the adversary may use several protocol runs...



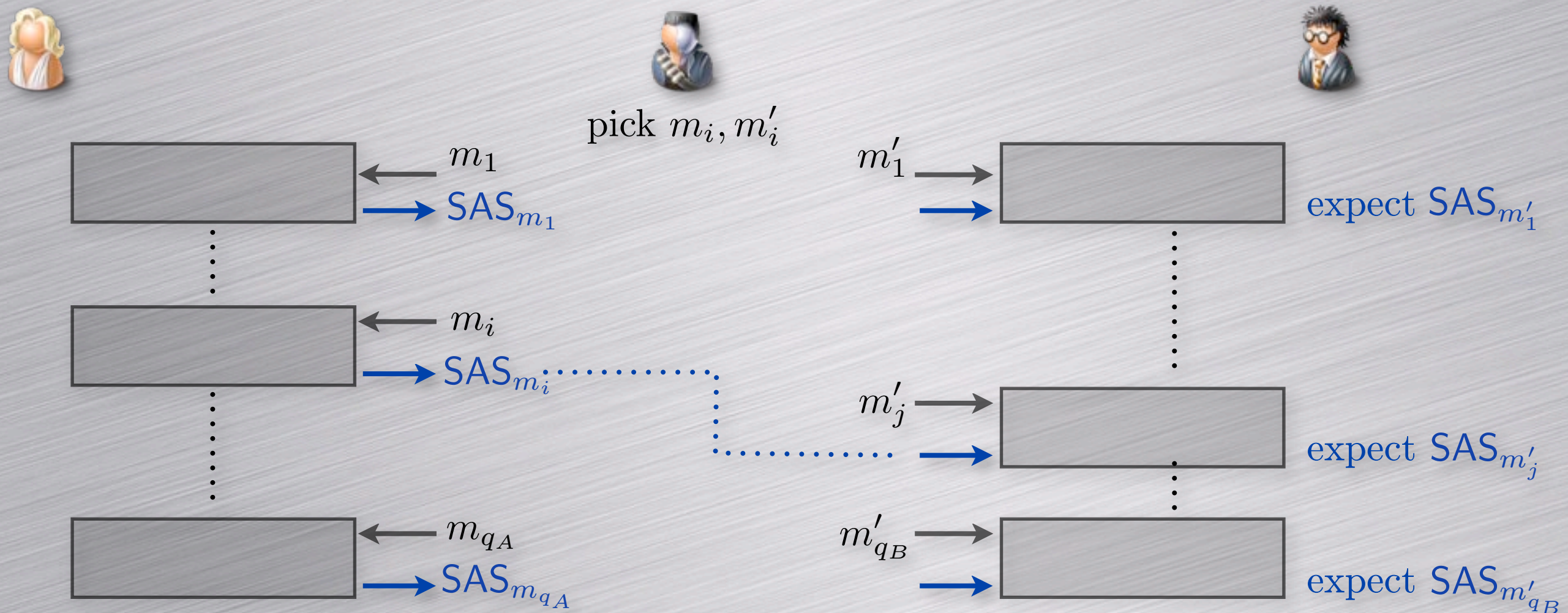
Generic Multi-shot Attack

Now, the adversary may use several protocol runs...



Generic Multi-shot Attack

Now, the adversary may use several protocol runs...



$$p = \Pr[\exists i, j \text{ such that } SAS_{m_i} = SAS_{m'_j} \text{ and } m_i \neq m'_j]$$

Generic Multi-shot Attack (2)

$$\begin{aligned}
 p &= \Pr[\exists i, j \text{ such that } \text{SAS}_{m_i} = \text{SAS}_{m'_j} \text{ and } m_i \neq m'_j] \\
 &\geq \frac{\Pr[\exists i, j \text{ such that } \text{SAS}_{m_i} = \text{SAS}_{m'_j}]}{\Pr[\forall k, \ell \text{ such that } \text{SAS}_{m_k} = \text{SAS}_{m'_\ell} : m_k = m'_\ell]} \\
 &\quad \downarrow \qquad \qquad \qquad \downarrow \\
 &\geq \Pr[\exists i, j \text{ such that } \text{SAS}_{m_i} = \text{SAS}_{m'_j} | \mathcal{D} \text{ is uniform}] \\
 &\geq 1 - \exp^{-\frac{q_A q_B}{n}} \\
 &\quad \leq \Pr[\forall k, \ell : m_k = m'_\ell] \\
 &\quad \leq q_A q_B 2^{-t} \\
 p &\geq 1 - \exp^{-\frac{q_A q_B}{n}} - q_A q_B 2^{-t}
 \end{aligned}$$

Optimal SAS Split

1 k -bit SAS

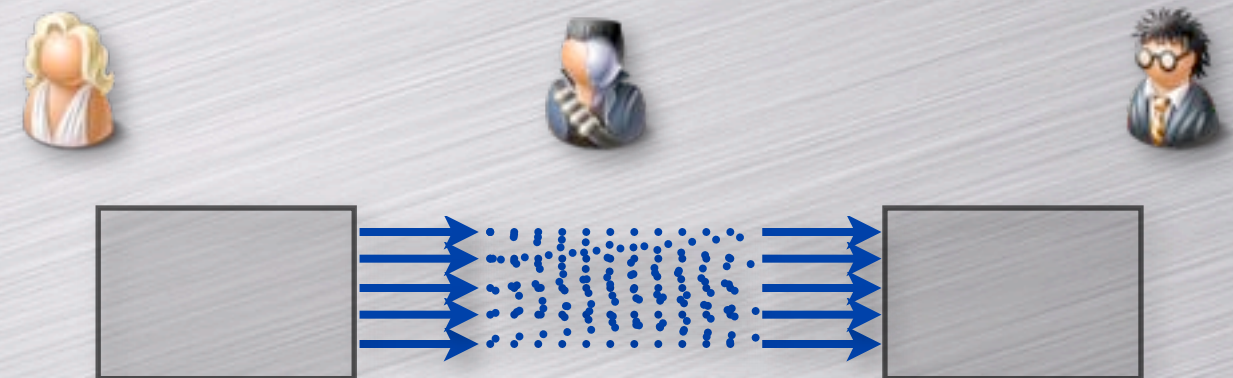
Size of SAS catalog: 2^k



$$p \approx \frac{1}{2^k}$$

k 1-bit SAS

Size of SAS catalog: 2

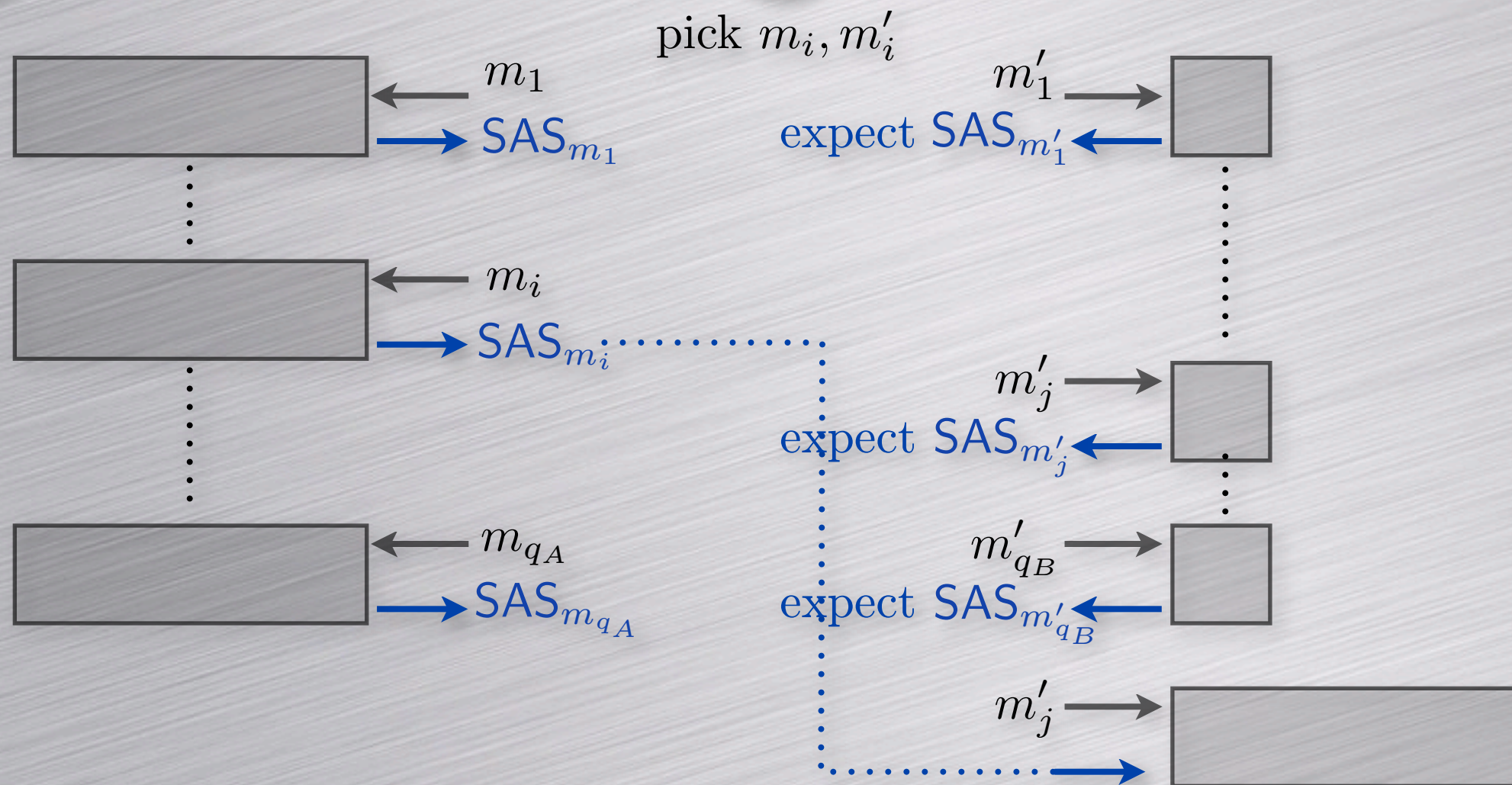


If Alice release a '0' and a '1',
then the attack succeeds...

$$p \approx 1$$

Generic Multi-shot Attack (NI)

Now, the protocol is **non-interactive**.



q_B is now an offline complexity.

Overview of Generic Attacks

$$p \approx 1 - \exp^{-\frac{q_A q_B}{n}}$$
$$p \approx 1 - \exp^{-\frac{q_A T}{n}}$$

Overview of Generic Attacks

- Optimal SAS are
 - uniformly distributed
 - sent in one piece

$$p \approx 1 - \exp^{-\frac{q_A q_B}{n}}$$

$$p \approx 1 - \exp^{-\frac{q_A T}{n}}$$

Overview of Generic Attacks

- Optimal SAS are
 - uniformly distributed
 - sent in one piece
- Generic attack against *any* UMAP:
 - one-shot attack with $p \approx \frac{1}{n}$
$$p \approx 1 - \exp^{-\frac{q_A q_B}{n}}$$
$$p \approx 1 - \exp^{-\frac{q_A T}{n}}$$

Overview of Generic Attacks

- Optimal SAS are
 - uniformly distributed
 - sent in one piece
- Generic attack against *any* UMAP:
 - one-shot attack with $p \approx \frac{1}{n}$
 - multi-shot attack with $p \approx 1 - \exp^{-\frac{q_A q_B}{n}}$
 $p \approx 1 - \exp^{-\frac{q_A T}{n}}$

Overview of Generic Attacks

- Optimal SAS are
 - uniformly distributed
 - sent in one piece
- Generic attack against *any* UMAP:
 - one-shot attack with $p \approx \frac{1}{n}$
 - multi-shot attack with $p \approx 1 - \exp^{-\frac{q_A q_B}{n}}$
 - [NIMAP] multi-shot attack with $p \approx 1 - \exp^{-\frac{q_A T}{n}}$

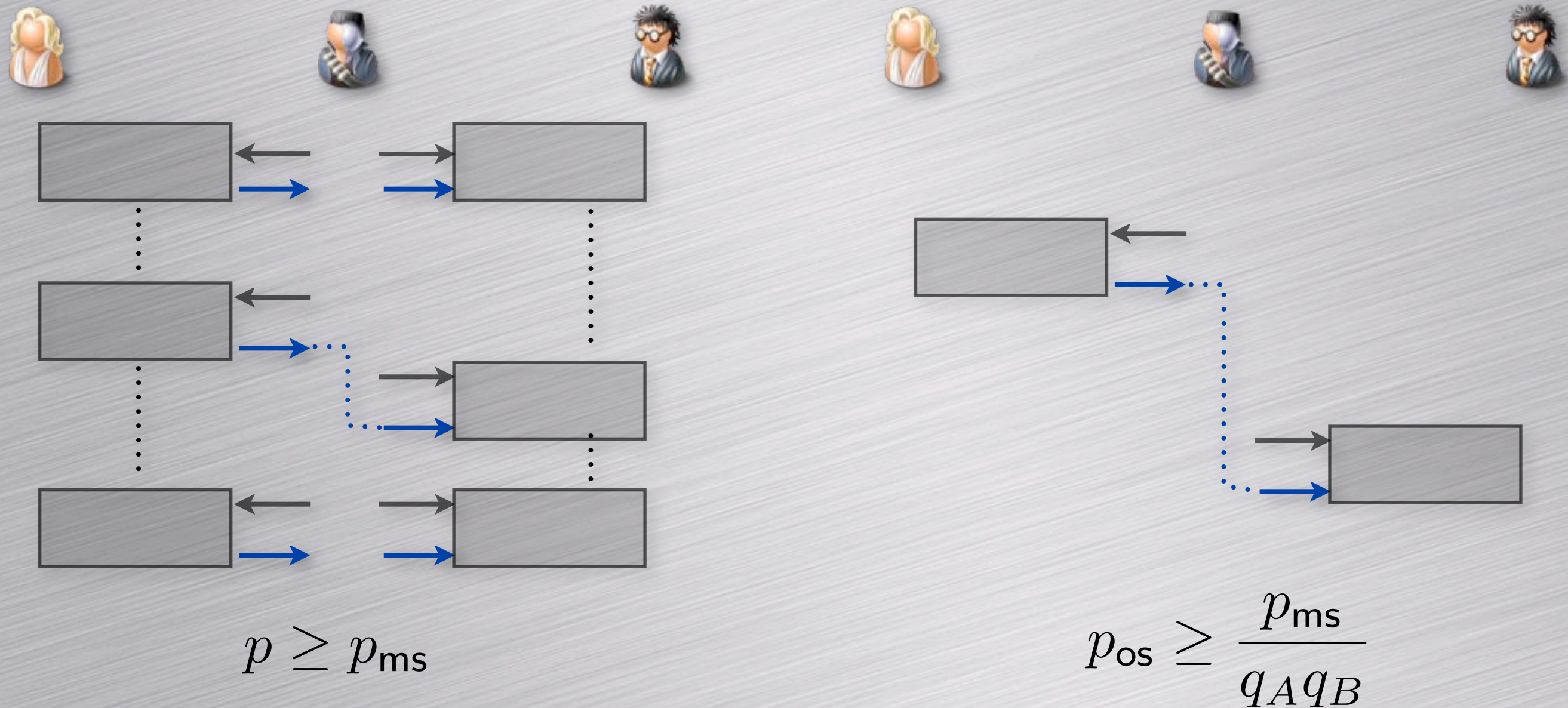
Overview of Generic Attacks

- Optimal SAS are
 - uniformly distributed
 - sent in one piece
- Generic attack against *any* UMAP:
 - one-shot attack with $p \approx \frac{1}{n}$
 - multi-shot attack with $p \approx 1 - \exp^{-\frac{q_A q_B}{n}}$
 - [NIMAP] multi-shot attack with $p \approx 1 - \exp^{-\frac{q_A T}{n}}$
 - If the best attack is the generic one: **optimal**

Overview of Generic Attacks

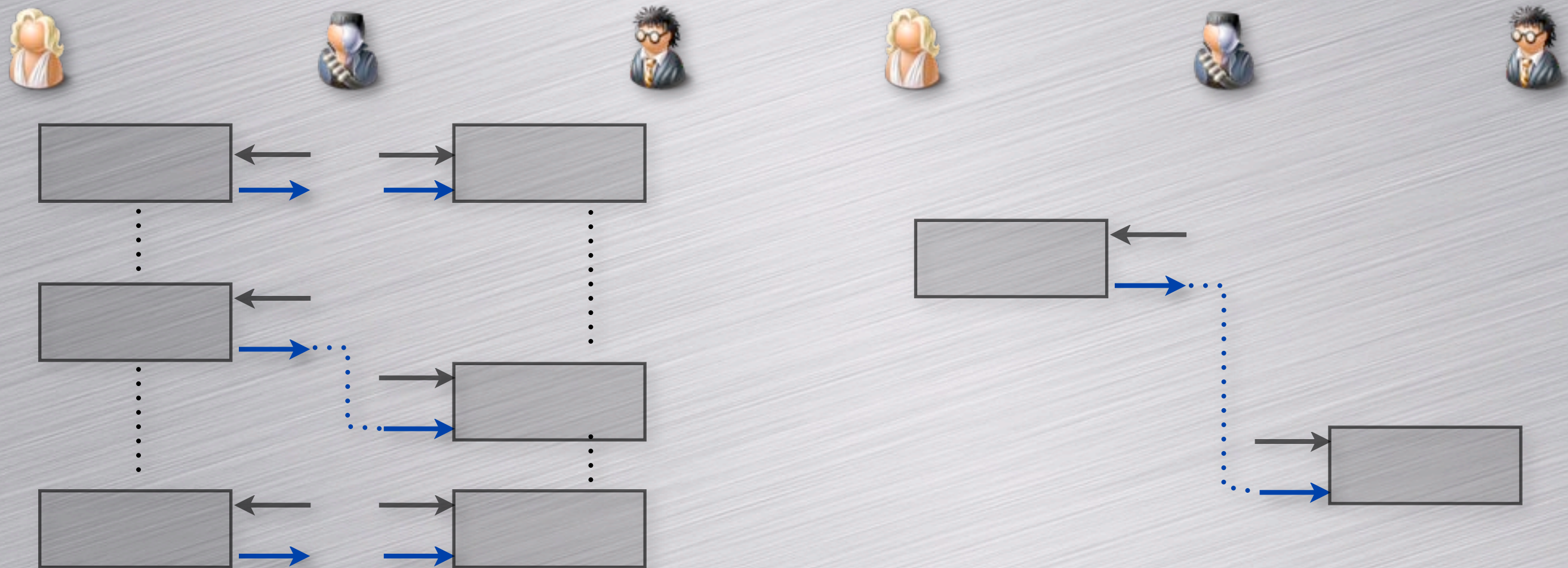
- Optimal SAS are
 - uniformly distributed
 - sent in one piece
- Generic attack against *any* UMAP:
 - one-shot attack with $p \approx \frac{1}{n}$
 - multi-shot attack with $p \approx 1 - \exp^{-\frac{q_A q_B}{n}}$
 - [NIMAP] multi-shot attack with $p \approx 1 - \exp^{-\frac{q_A T}{n}}$
 - If the best attack is the generic one: **optimal**
- [LN06] an optimal protocol has at least 3 (interactive) moves

One-shot versus Multi-shot [Vau05]



$$p_{os} \geq \frac{p_{ms}}{q_A q_B}$$

One-shot versus Multi-shot [Vau05]

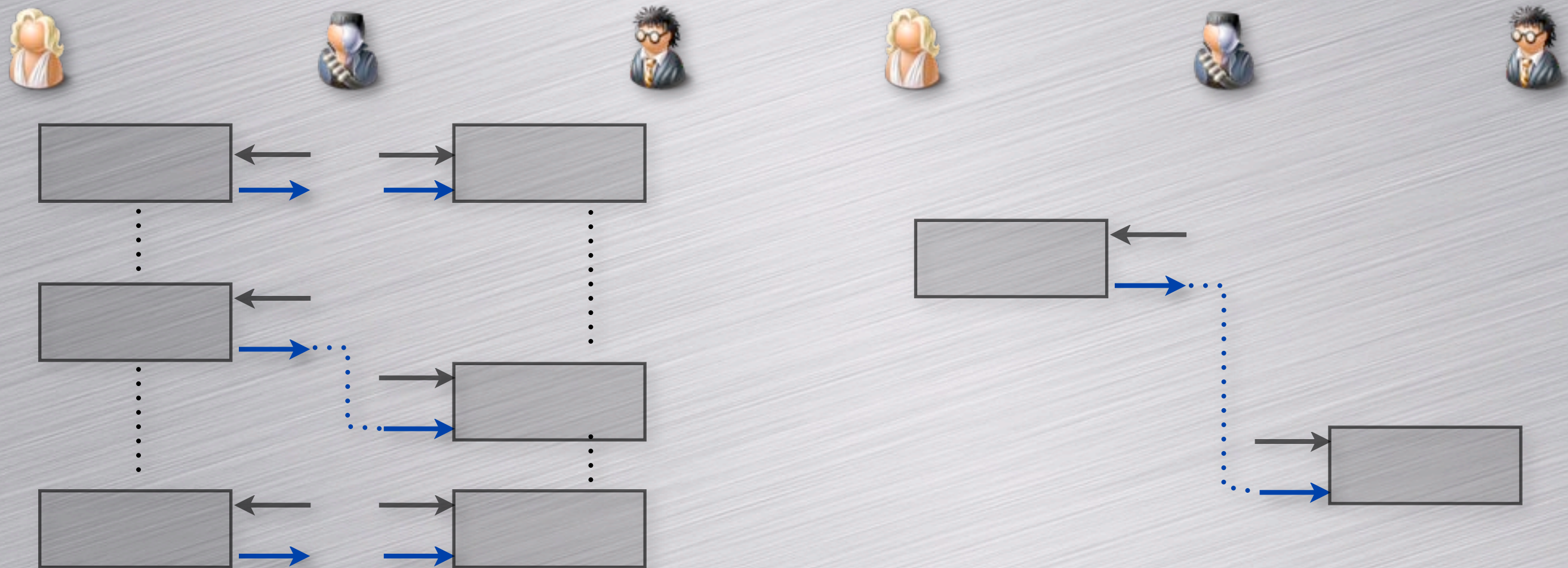


$$p \geq p_{\text{ms}}$$

$$p_{\text{ms}} \leq q_A q_B p_{\text{os}}$$

$$p_{\text{os}} \geq \frac{p_{\text{ms}}}{q_A q_B}$$

One-shot versus Multi-shot [Vau05]



$$p \geq p_{\text{ms}}$$

$$p_{\text{ms}} \leq q_A q_B p_{\text{os}}$$

$$p_{\text{os}} \geq \frac{p_{\text{ms}}}{q_A q_B}$$

$(T, 2, p_{\text{os}})$ implies $(T, q_A + q_B, q_A q_B p_{\text{os}})$

SAS-based Cryptography

Unilateral Message Authentication Protocols

CRHF-based NIMAP [BSSW02]

Used in SSH, GPG, ...

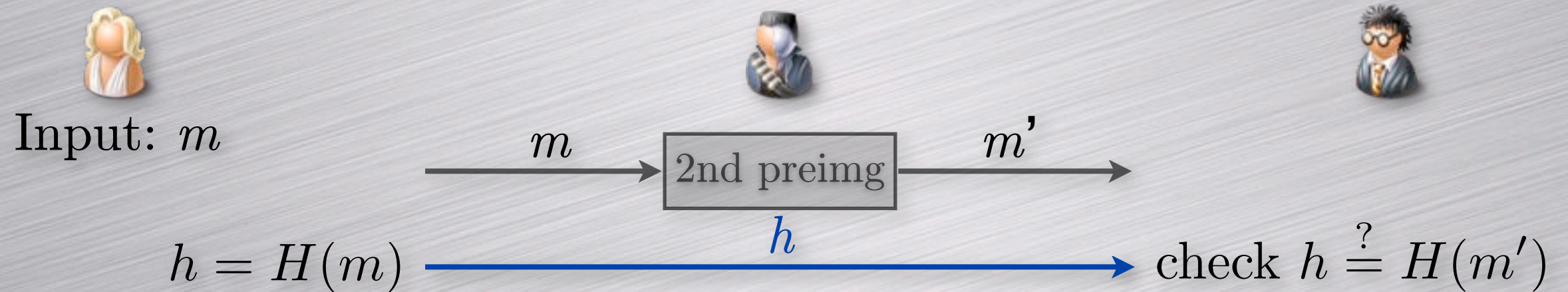


Input: m



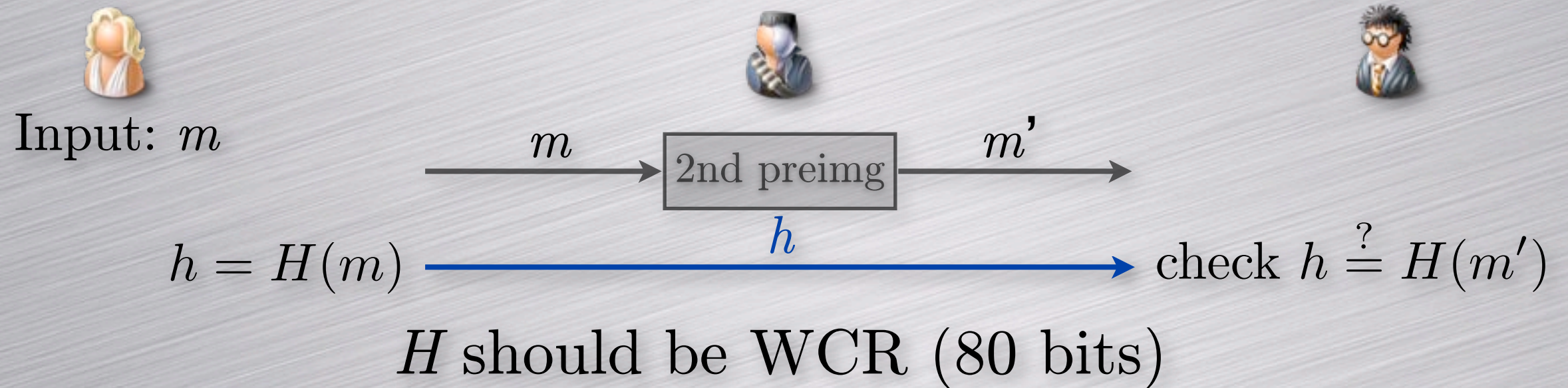
CRHF-based NIMAP [BSSW02]

Known message attack:



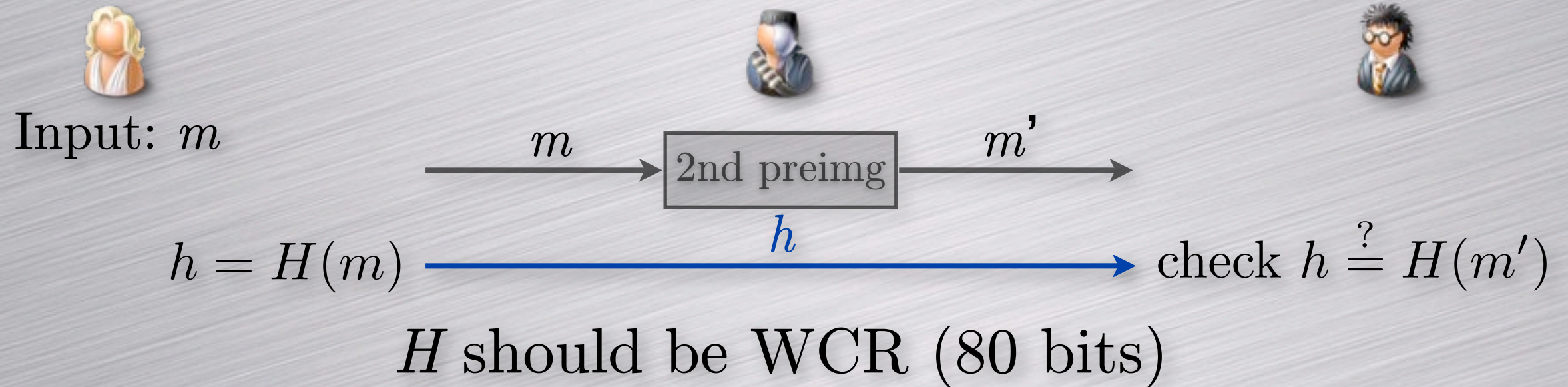
CRHF-based NIMAP [BSSW02]

Known message attack:



CRHF-based NIMAP [BSSW02]

Known message attack:

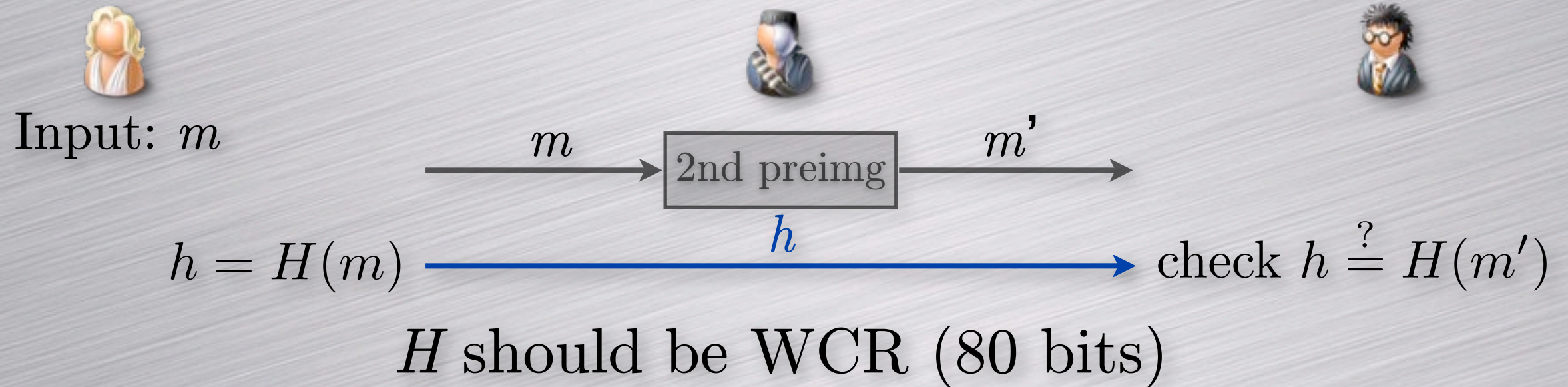


Chosen message attack:

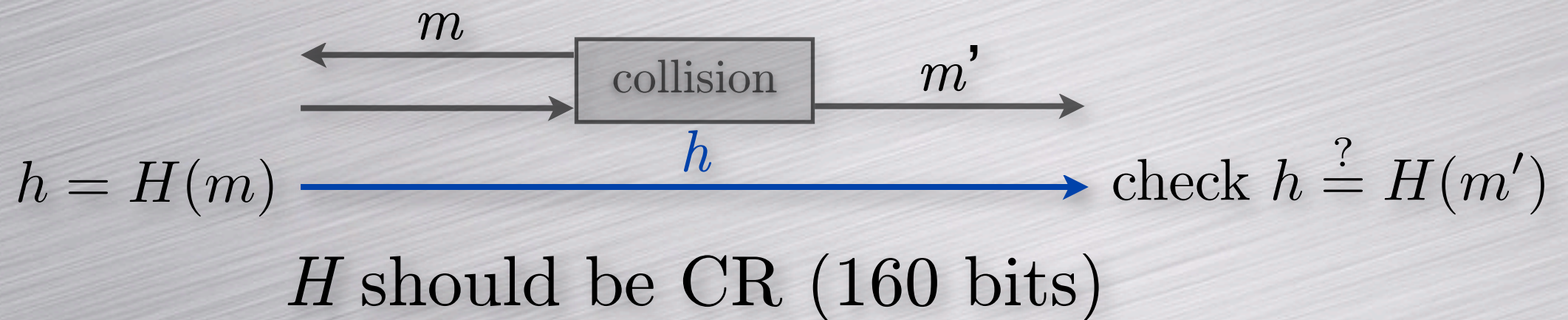


CRHF-based NIMAP [BSSW02]

Known message attack:



Chosen message attack:



PV-NIMAP [PV06a]

CRHF-based NIMAP:

collision attack due to a predictable $H(m)$

Main idea of PV-NIMAP

Avoid the authenticated message to be predictable.

PV-NIMAP [PV06a]

CRHF-based NIMAP:

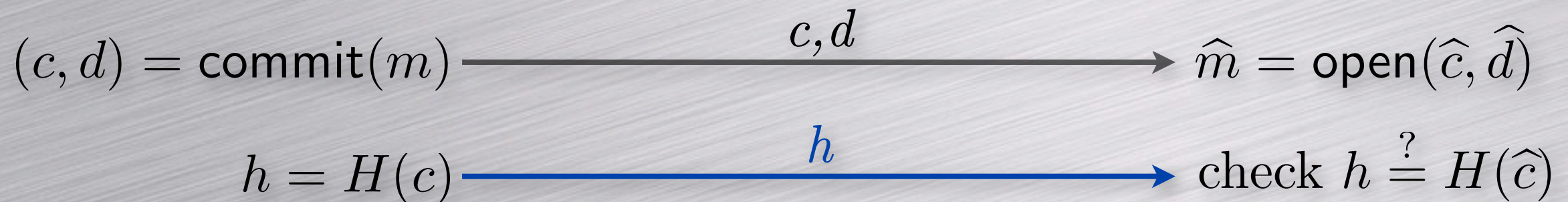
collision attack due to a predictable $H(m)$

Main idea of PV-NIMAP

Avoid the authenticated message to be predictable.



Input: m



PV-NIMAP [PV06a]

CRHF-based NIMAP:

collision attack due to a predictable $H(m)$

Main idea of PV-NIMAP

Avoid the authenticated message to be predictable.



Input: m

pick r , $c = R(m, r)$
 $(c, d) = \text{commit}(m)$

c, m, r
 c, d

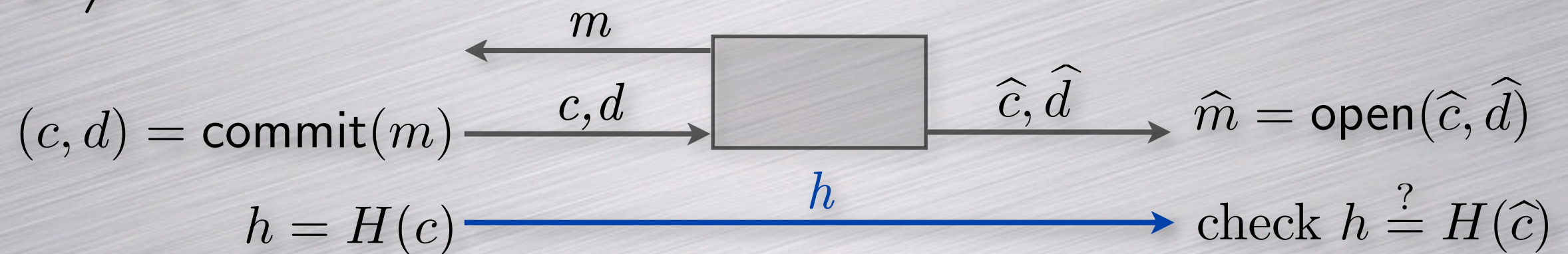
check $\hat{c} \stackrel{?}{=} R(\hat{m}, \hat{r})$
 $\hat{m} = \text{open}(\hat{c}, \hat{d})$

$h = H(c)$ h check $h \stackrel{?}{=} H(\hat{c})$



PV-NIMAP: intuitive security

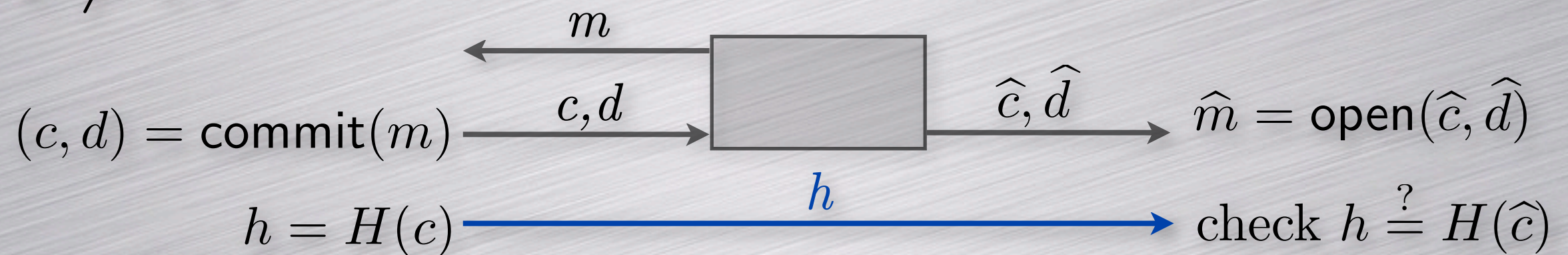
Case $\hat{c} \neq c$:



Require to find a 2nd preimage on H .

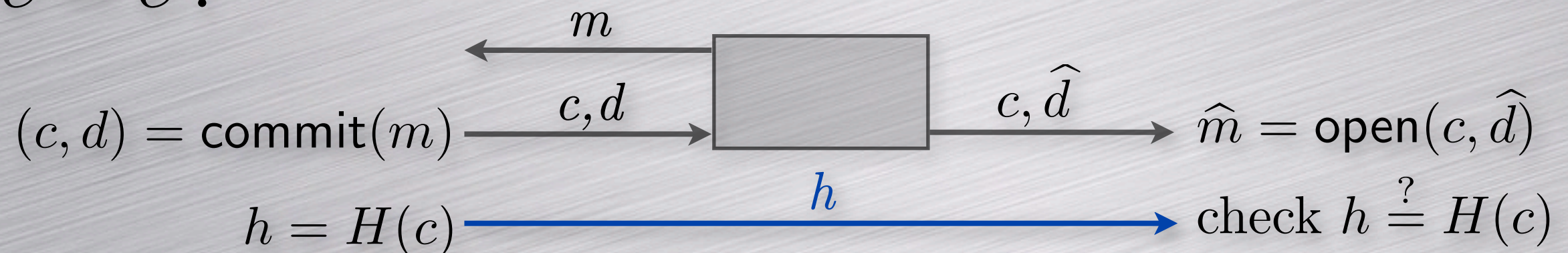
PV-NIMAP: intuitive security

Case $\hat{c} \neq c$:



Require to find a 2nd preimage on H .

Case $\hat{c} = c$:



Require to defeat the binding property.

PV-NIMAP [PV06a]

Theorem

Assume a (T, ε_c) -binding commitment

a (T, ε_h) -WCR function

Then, PV-NIMAP is $(T, q_A + 1, q_A(\varepsilon_c + \varepsilon_h))$

PV-NIMAP [PV06a]

Theorem

Assume a (T, ε_c) -binding commitment

a (T, ε_h) -WCR function

Then, PV-NIMAP is $(T, q_A + 1, q_A(\varepsilon_c + \varepsilon_h))$

- c is sent over the insecure channel
 - ε_c as small as desired

PV-NIMAP [PV06a]

Theorem

Assume a (T, ε_c) -binding commitment

a (T, ε_h) -WCR function

Then, PV-NIMAP is $(T, q_A + 1, q_A(\varepsilon_c + \varepsilon_h))$

- c is sent over the insecure channel
 - ε_c as small as desired
- WCR-resistance on H (not CR)

What about interactivity?

- Interactivity allows to avoid offline attacks.
- As a consequence, SAS are shorter.

What about interactivity?

- Interactivity allows to avoid offline attacks.
- As a consequence, SAS are shorter.
- As example, Vau-SAS-IMAP:



Input: m

pick $R_A \in \{0, 1\}^k$

$(c, d) = \text{commit}(m, R_A)$

m, c

R_B

d

$\text{SAS} = R_A \oplus \hat{R}_B$

SAS



pick $R_B \in \{0, 1\}^k$

$\hat{R}_A = \text{open}(\hat{m}, \hat{c}, \hat{d})$

check $\text{SAS} \stackrel{?}{=} \hat{R}_A \oplus R_B$

Vau-SAS-IMAP [Vau05]

Theorem

Assume a (T, ε_c) -equivocable or extractable commitment

Then, Vau-SAS-IMAP is $(T, q_A + q_B, q_A q_B(2^{-k} + \varepsilon_c))$

- Optimal
- Vau-SAS-IMAP requires 20-50-bit SAS
- PV-NIMAP requires 100-bit SAS

SAS-based Cryptography

Bilateral Message Authentication Protocols

Vau-SAS-MCA



Input: m_A

pick $R_A \in \{0, 1\}^k$

$(c_A, d_A) = \text{commit}(0 \| m_A, R_A)$

m_A, c_A

m_B, c_B

d_A

d_B

$\hat{R}_B = \text{open}(1 \| \hat{m}_B, \hat{c}_B, \hat{d}_B)$

$SAS = R_A \oplus \hat{R}_B$

check SAS are the same

SAS

SAS

check $SAS \stackrel{?}{=} \hat{R}_A \oplus R_B$



Input: m_B

pick $R_B \in \{0, 1\}^k$

$(c_B, d_B) = \text{commit}(1 \| m_B, R_B)$

$\hat{R}_A = \text{open}(0 \| \hat{m}_A, \hat{c}_A, \hat{d}_A)$

- Two interleaved Vau-SAS-IMAP
- May a 3-move (optimal) protocol exist?

Vau-SAS-MCA



Input: m_A

pick $R_A \in \{0, 1\}^k$

$(c_A, d_A) = \text{commit}(0 \| m_A, R_A)$

m_A, c_A

m_B, c_B

d_A

d_B

$\hat{R}_B = \text{open}(1 \| \hat{m}_B, \hat{c}_B, \hat{d}_B)$

$SAS = \hat{R}_B \oplus h(\hat{m}_B, R_A)$

~~$SAS = R_A \oplus \hat{R}_B$~~

check SAS are the same

SAS

SAS



Input: m_B

pick $R_B \in \{0, 1\}^k$

$(c_B, d_B) = \text{commit}(1 \| m_B, R_B)$

$\hat{R}_A = \text{open}(0 \| \hat{m}_A, \hat{c}_A, \hat{d}_A)$

$R_B \oplus h(m_B, \hat{R}_A)$

check SAS $\stackrel{?}{=} \hat{R}_A \oplus R_B$

- Two interleaved Vau-SAS-IMAP
- May a 3-move (optimal) protocol exist?

Vau-SAS-MCA



Input: m_A

pick $R_A \in \{0, 1\}^k$

$(c_A, d_A) = \text{commit}(0 \| m_A, R_A)$

m_A, c_A

$m_B, \cancel{c_B}, R_B$

d_A

$\cancel{d_B}$

~~$\hat{R}_B = \text{open}(1 \| \hat{m}_B, \hat{c}_B, \hat{d}_B)$~~

$SAS = \hat{R}_B \oplus h(\hat{m}_B, R_A)$

~~$SAS = R_A \oplus \hat{R}_B$~~

check SAS are the same

SAS

SAS



Input: m_B

pick $R_B \in \{0, 1\}^k$

~~$(c_B, d_B) = \text{commit}(1 \| m_B, R_B)$~~

$\hat{R}_A = \text{open}(0 \| \hat{m}_A, \hat{c}_A, \hat{d}_A)$

check $SAS \stackrel{?}{=} \hat{R}_A \oplus R_B$

- Two interleaved Vau-SAS-IMAP
- May a 3-move (optimal) protocol exist?

Vau-SAS-MCA



Input: m_A

pick $R_A \in \{0, 1\}^k$

$(c_A, d_A) = \text{commit}(0 \parallel m_A, R_A)$

m_A, c_A

m_B, c_B, R_B

d_A

d_B

~~$\hat{R}_B = \text{open}(1 \parallel \hat{m}_B, \hat{c}_B, \hat{d}_B)$~~

$SAS = \hat{R}_B \oplus h(\hat{m}_B, R_A)$

~~$SAS = R_A \oplus \hat{R}_B$~~

check SAS are the same

SAS

SAS



Input: m_B

pick $R_B \in \{0, 1\}^k$

~~$(c_B, d_B) = \text{commit}(1 \parallel m_B, R_B)$~~

$\hat{R}_A = \text{open}(0 \parallel \hat{m}_A, \hat{c}_A, \hat{d}_A)$

$R_B \oplus h(m_B, \hat{R}_A)$

check $SAS \stackrel{?}{=} \hat{R}_A \oplus R_B$

- Two interleaved Vau-SAS-IMAP
- May a 3-move (optimal) protocol exist?

Vau-SAS-MCA



Input: m_A

pick $R_A \in \{0, 1\}^{\ell}$

$(c_A, d_A) = \text{commit}(0 \parallel m_A, R_A)$

m_A, c_A

m_B, c_B, R_B

d_A

d_B

~~$\hat{R}_B = \text{open}(1 \parallel \hat{m}_B, \hat{c}_B, \hat{d}_B)$~~

$SAS = \hat{R}_B \oplus h(\hat{m}_B, R_A)$

~~$SAS = R_A \oplus \hat{R}_B$~~

check SAS are the same

SAS

SAS



Input: m_B

pick $R_B \in \{0, 1\}^k$

~~$(c_B, d_B) = \text{commit}(1 \parallel m_B, R_B)$~~

$\hat{R}_A = \text{open}(0 \parallel \hat{m}_A, \hat{c}_A, \hat{d}_A)$

check $SAS \stackrel{?}{=} \hat{R}_A \oplus R_B$

- Two interleaved Vau-SAS-IMAP
- May a 3-move (optimal) protocol exist?

PV-SAS-MCA [PV06b]



Input: m_A

pick $R_A \in \{0, 1\}^\ell$

$(c, d) = \text{commit}(m_A, R_A)$

m_A, c

m_B, R_B

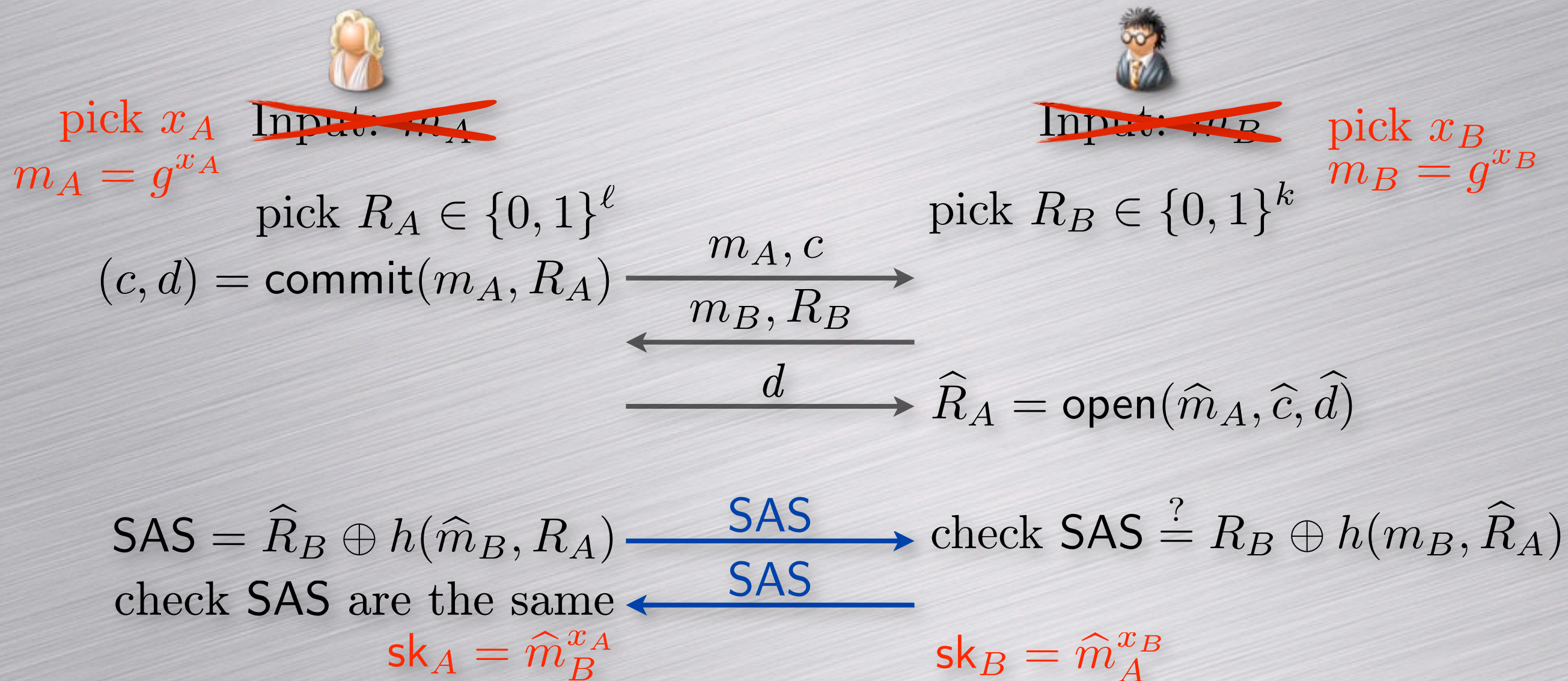
d

pick $R_B \in \{0, 1\}^k$

$\hat{R}_A = \text{open}(\hat{m}_A, \hat{c}, \hat{d})$

$\text{SAS} = \hat{R}_B \oplus h(\hat{m}_B, R_A)$ $\xrightarrow{\text{SAS}}$ check $\text{SAS} \stackrel{?}{=} R_B \oplus h(m_B, \hat{R}_A)$
 check SAS are the same $\xleftarrow{\text{SAS}}$

PV-SAS-MCA [PV06b]



o PV-SAS-AKA

PV-SAS-MCA [PV06b]



Input: m_A

pick $R_A \in \{0, 1\}^\ell$

$(c, d) = \text{commit}(\cancel{m_A}, R_A)$

m_A, c

m_B, R_B

d

pick $R_B \in \{0, 1\}^k$

$\hat{R}_A = \text{open}(\cancel{\hat{m}_A}, \hat{c}, \hat{d})$

$SAS = h(m_A || \hat{m}_B, R_A, \hat{R}_B)$

$SAS = \hat{R}_B \oplus h(\hat{m}_B, R_A)$

check SAS are the same

SAS

SAS

check $SAS \stackrel{?}{=} R_B \oplus h(m_B, \hat{R}_A)$

- PV-SAS-AKA

- Comparison with MANA IV [LN06]

PV-SAS-MCA [PV06b]

Theorem

Assume a (T, ε_c) -equivocable commitment
a (T, ε_h) -almost strongly universal function

Then, PV-SAS-MCA is

$$(T, q_A + q_B, q_A(q_A - 1 + q_B)(2^{-k} + \varepsilon_c + \varepsilon_h))$$

SAS-based Cryptography

Towards Group Settings

Group implications...

- More than two parties implies that
 - DH cannot be used.
 - Instead, we can use the Burmester-Desmedt (BD).
 - No group-MCA protocol exist?
- Security proofs become more complex:
 - More parties
 - Increase in communication
 - The same message may be received differently by each

LP-SAS-GMA [LP08]

- use commitment to temporarily hide secret keys
- direct authentication (as in MANA IV)



$\mathcal{P}_{\text{id}_i}$

Input: m_i



pick r_i
 $(c_i, d_i) = \text{commit}(\text{crs}, i, r_i)$

→ i, m_i, c_i

$\forall j : (j, \hat{r}_{ji}) = \text{open}(\text{crs}, \hat{c}_{ji}, \hat{d}_{ji})$

→ d_i

$\text{SAS}_i = H\left((\hat{\mathcal{G}}_i, \hat{\vec{m}}_i), \hat{\vec{r}}_i\right)$

check $\text{SAS}_i = \text{SAS}_j$

→ SAS

LP-SAS-GMA [LP08]

Theorem

Assume a (T, ε_b) -binding and
 (T, ε_{nm}) -non-malleable commitment
 a (T, ε_h) -almost strongly universal function

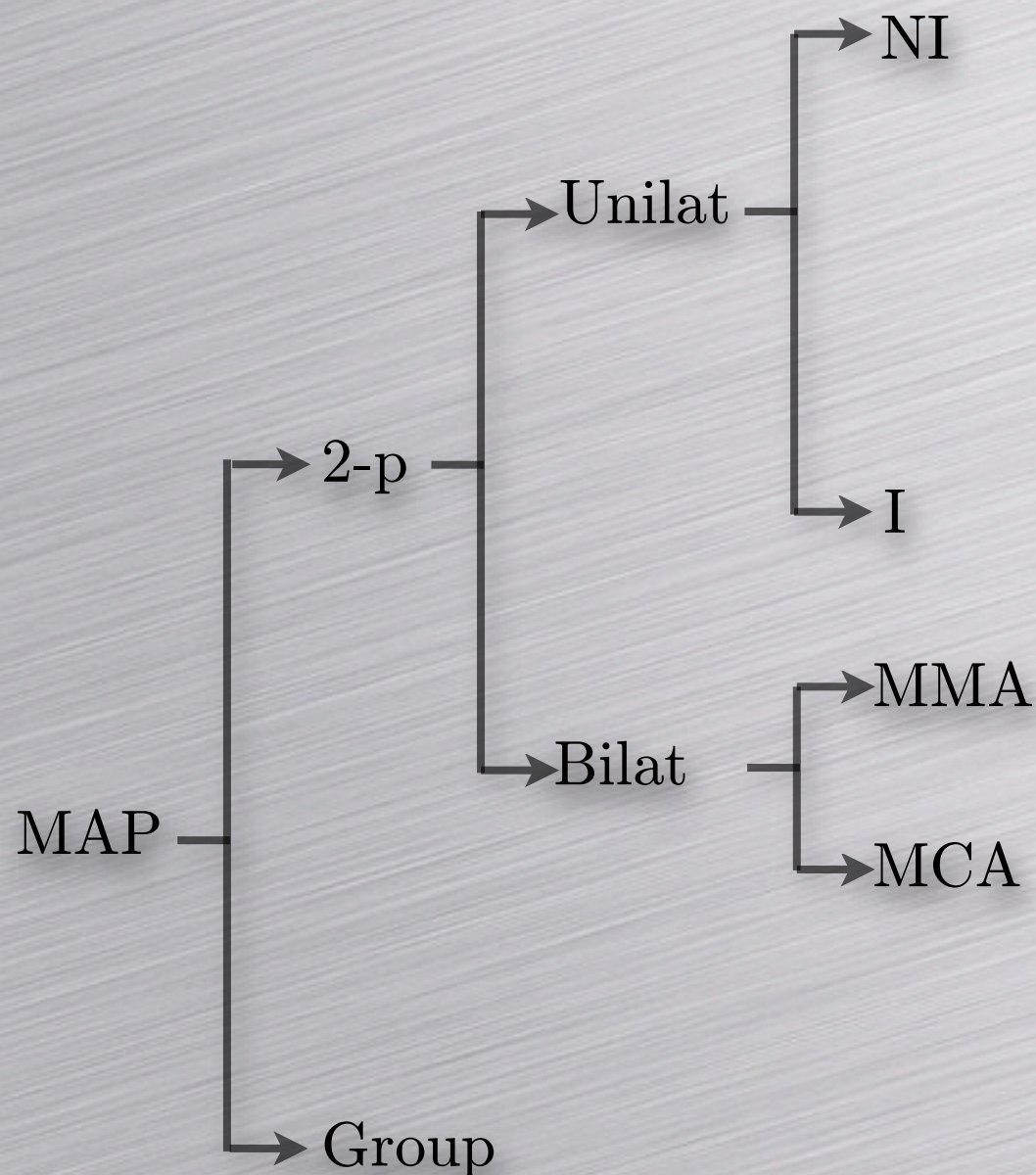
Then, LP-SAS-GMA is

$$(T, q, q(2^{-k} + n\varepsilon_{nm} + \varepsilon_b + \varepsilon_h))$$

SAS-based Cryptography

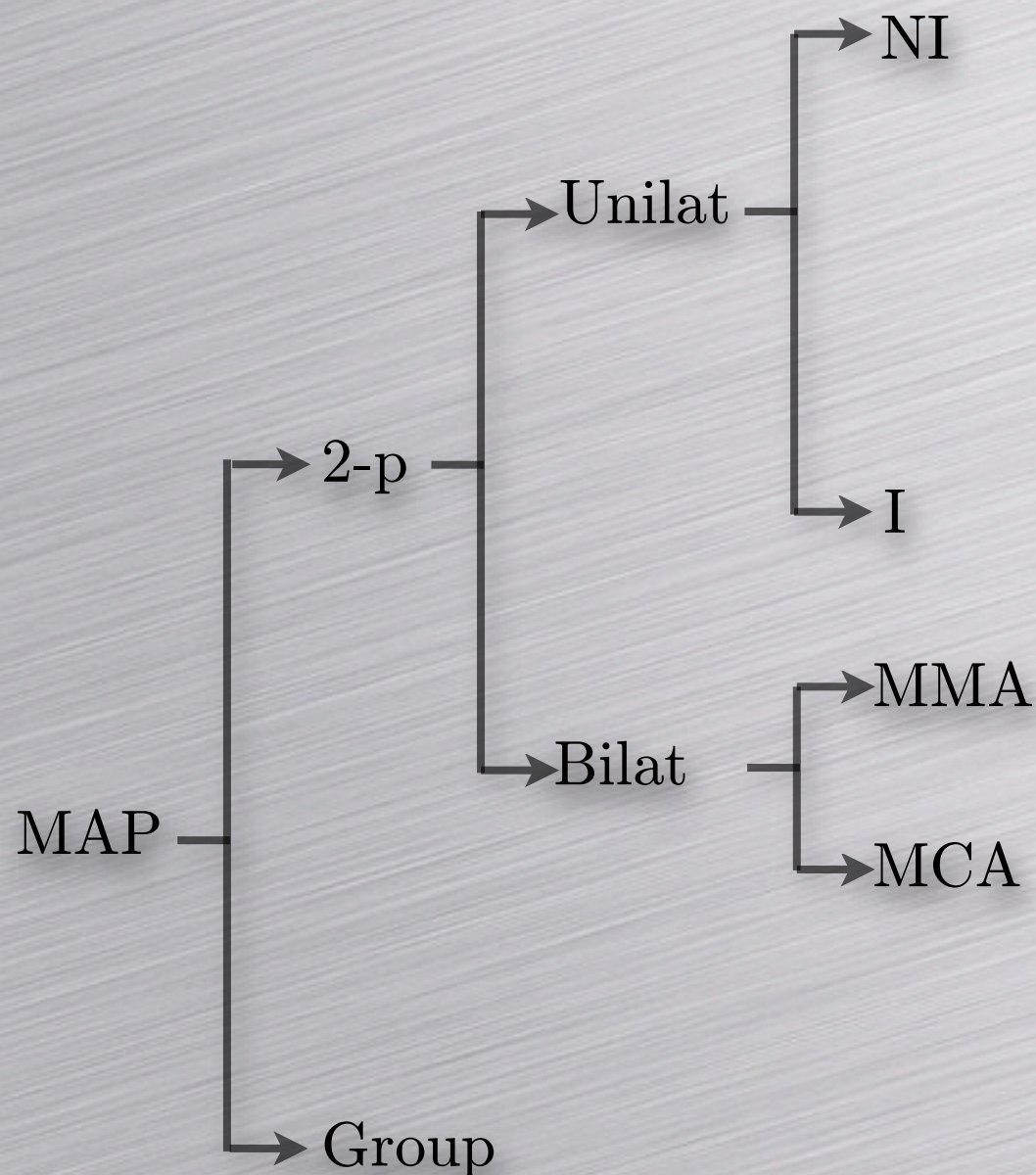
Summary

Summary



	Auth channel	Optimal	Sec proof
CRHF-based [BSSW02]	weak		y
MANA I [GMN04]	strong		y
PV-NIMAP [PV06a]	weak	y	y
eTCR-based [RWSN07]	weak	y	y
HCR-based [MS07]	weak	?	y
Vau-SAS-IMAP [Vau05]	weak	y	y
ICR-based [MS08]	weak	?	y
MANA III [GMN04]	strong		y
PV-SAS-MMA [PV06b]	weak	y	y
Vau-SAS-MCA [Vau05]	weak		
PV-SAS-MCA [PV06b]	weak	y	y
MANA IV [LN06]	weak	y	y
Group-MANA IV [VAN06]	weak		y
LP-SAS-GMA [LP08]	weak	y	y

Summary

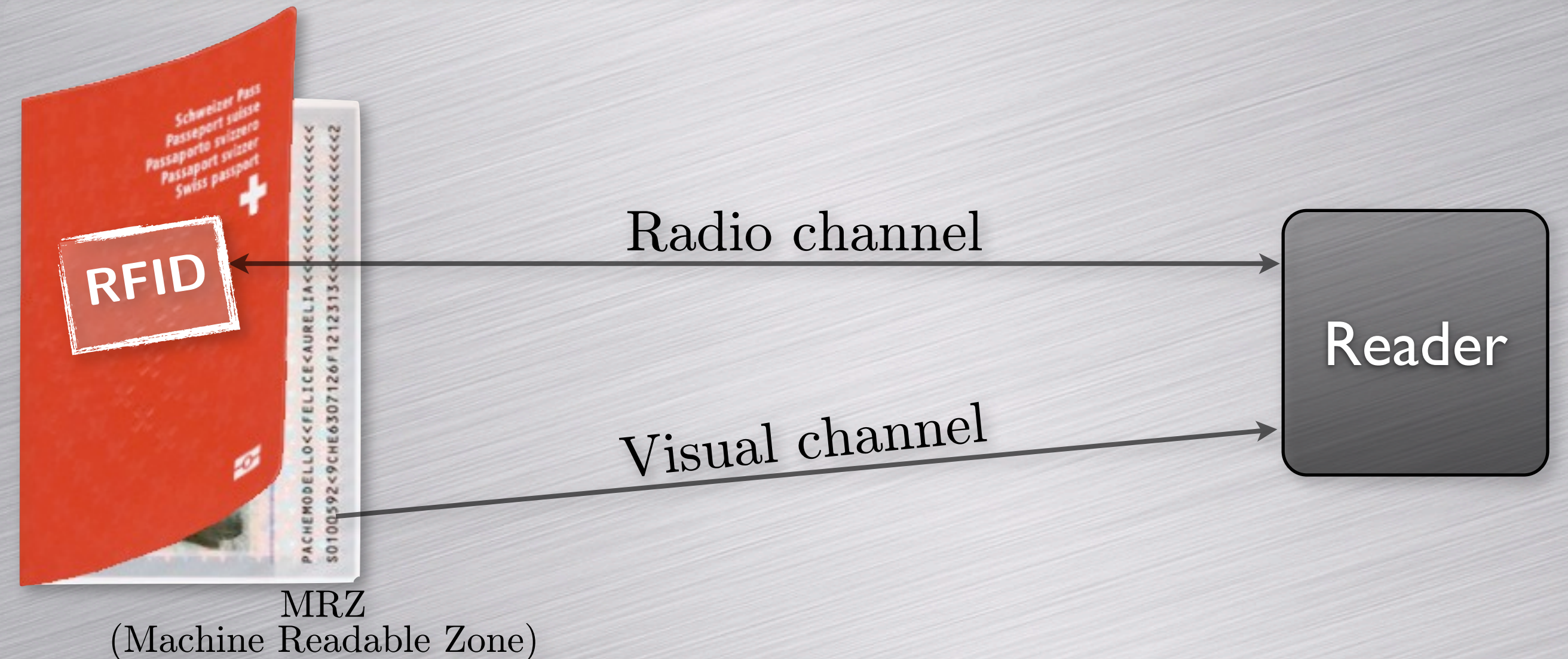


	Auth channel	Optimal	Sec proof
CRHF-based [BSSW02]	weak		y
MANA I [GMN04]	strong		y
PV-NIMAP [PV06a]	weak	y	y
eTCR-based [RWSN07]	weak	y	y
HCR-based [MS07]	weak	?	y
Vau-SAS-IMAP [Vau05]	weak	y	y
ICR-based [MS08]	weak	?	y
MANA III [GMN04]	strong		y
PV-SAS-MMA [PV06b]	weak	y	y
Vau-SAS-MCA [Vau05]	weak		
PV-SAS-MCA [PV06b]	weak	y	y
LP-SAS-AKA [PV06b]	weak	y	y
MANA IV [LN06]	weak	y	y
Group-MANA IV [VAN06]	weak		y
LP-SAS-GMA [LP08]	weak	y	y

LP-SAS-GKA [LP08]

Efficient Deniable Authentication for Signatures

Reading an E-passport



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

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 $sk=f(MRZ)$

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 $sk=f(MRZ)$
- Extended Access Control (EAC)
 - Terminal authentication, PKI for border patrols
 - EU standard (not an ICAO standard)
 - Basic data must remain accessible

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 $sk=f(MRZ)$
- Extended Access Control (EAC)
 - Terminal authentication, PKI for border patrols
 - EU standard (not an ICAO standard)
 - Basic data must remain accessible

Usually used

Passive Authentication

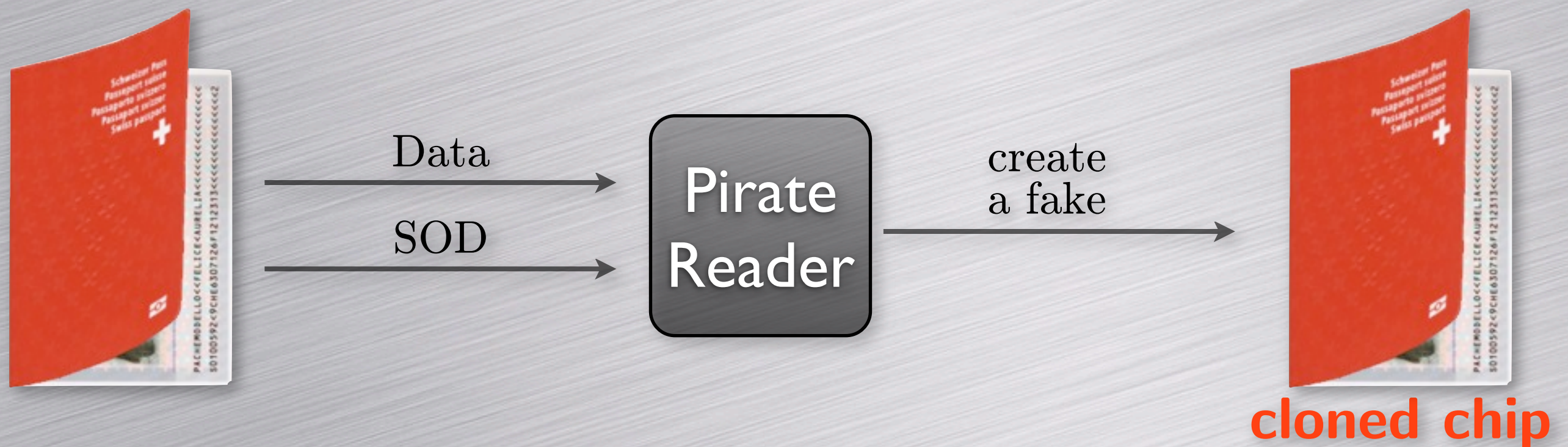
- Aims to prove that the **data is genuine**
- The chip has a Security Object Document (SOD)
- Basically, the national authority signed the data

$$\text{SOD} = \text{sign}_{K_{s,NA}}(\text{data})$$

Passive Authentication

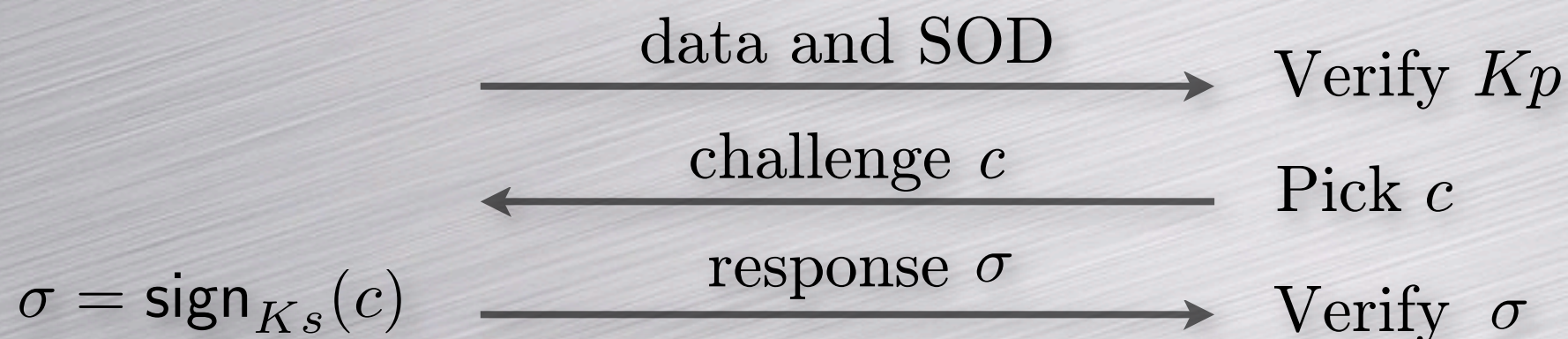
- Aims to prove that the **data is genuine**
- The chip has a Security Object Document (SOD)
- Basically, the national authority signed the data

$$\text{SOD} = \text{sign}_{K_s, N_A}(\text{data})$$



Active Authentication

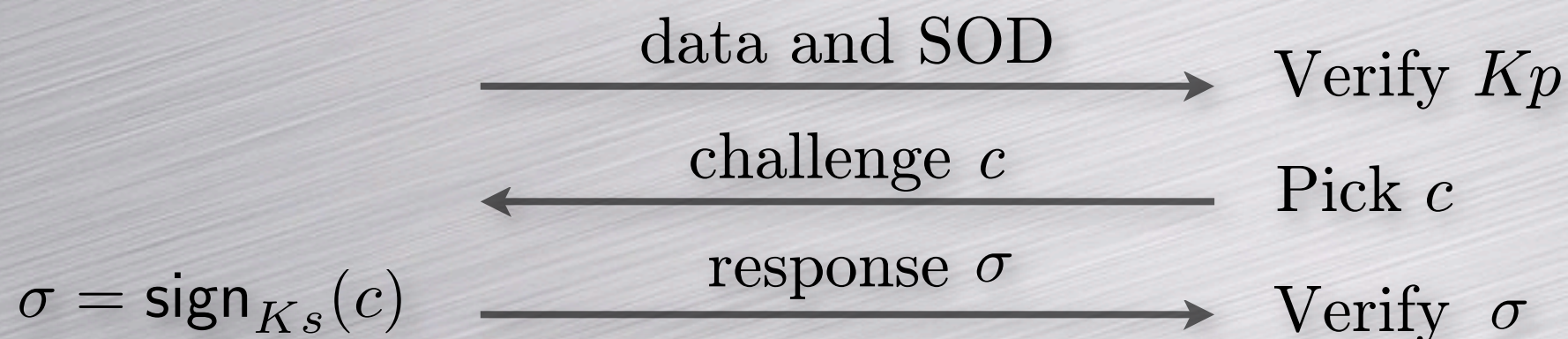
- Aims to prove that the **chip is genuine**
 - no cloning and no substitution possible
- The e-passport contains a pair of keys: K_p and K_s
 - K_s stored in a secure memory
 - K_p is a standard data (authenticated by SOD)



Reader

Active Authentication

- Aims to prove that the **chip is genuine**
 - no cloning and no substitution possible
- The e-passport contains a pair of keys: K_p and K_s
 - K_s stored in a secure memory
 - K_p is a standard data (authenticated by SOD)



Reader

The passport is able to sign...

Privacy Issue

- Anyone having a reader (50\$) can obtain all data and the SOD
- Publishing the data only:
 - the owner can still claim that it is incorrect
- But, publishing the SOD too:
 - SOD is an evidence of the authenticity of DGs

Privacy Issue

- Anyone having a reader (50\$) can obtain all data and the SOD
- Publishing the data only:
 - the owner can still claim that it is incorrect
- But, publishing the SOD too:
 - SOD is an evidence of the authenticity of DGs

Goal

Protect the SOD...

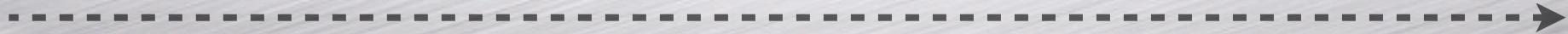
(Remember that data should be accessible.)

Solution: The Main Idea



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

$K_{p,NA}$



Solution: The Main Idea

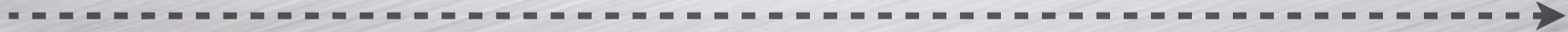


$K_{p,NA}, K_{s,NA}$

$K_{p,NA}$

data

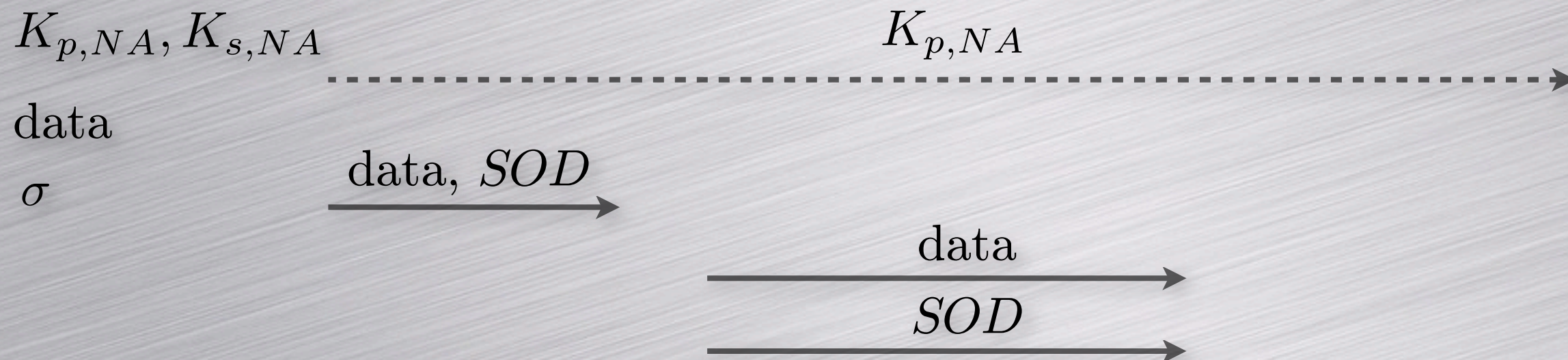
σ



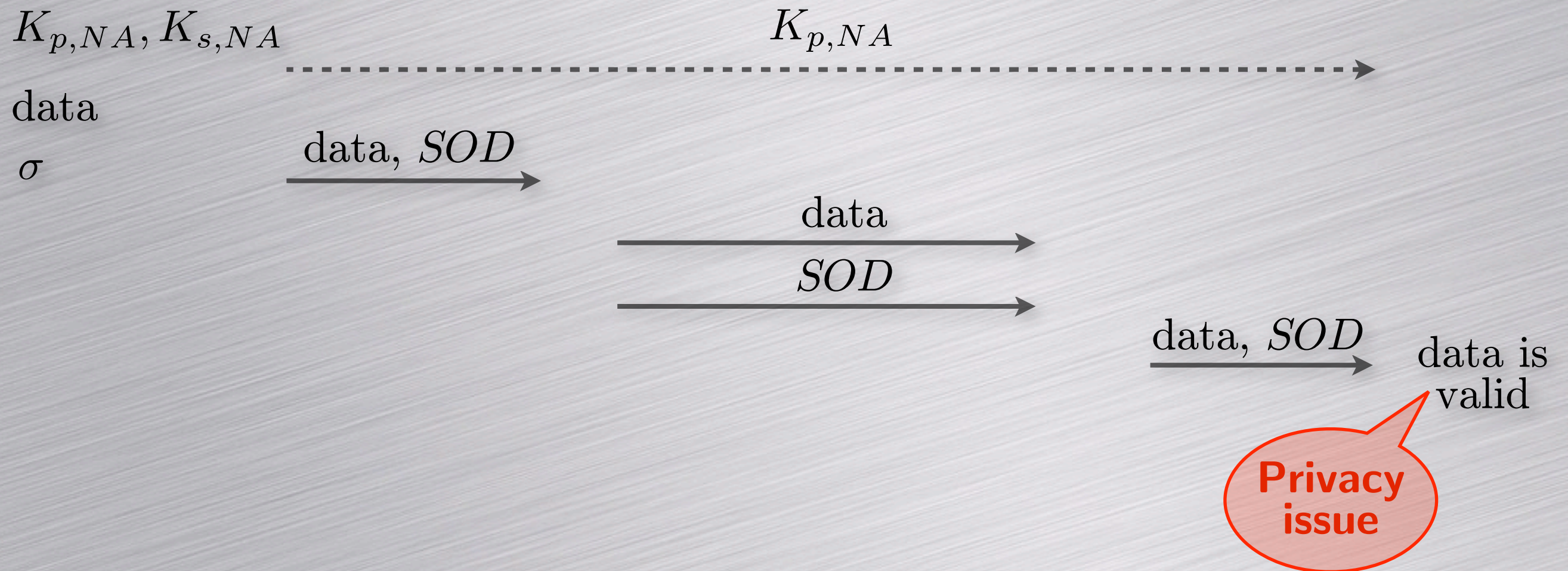
Solution: The Main Idea



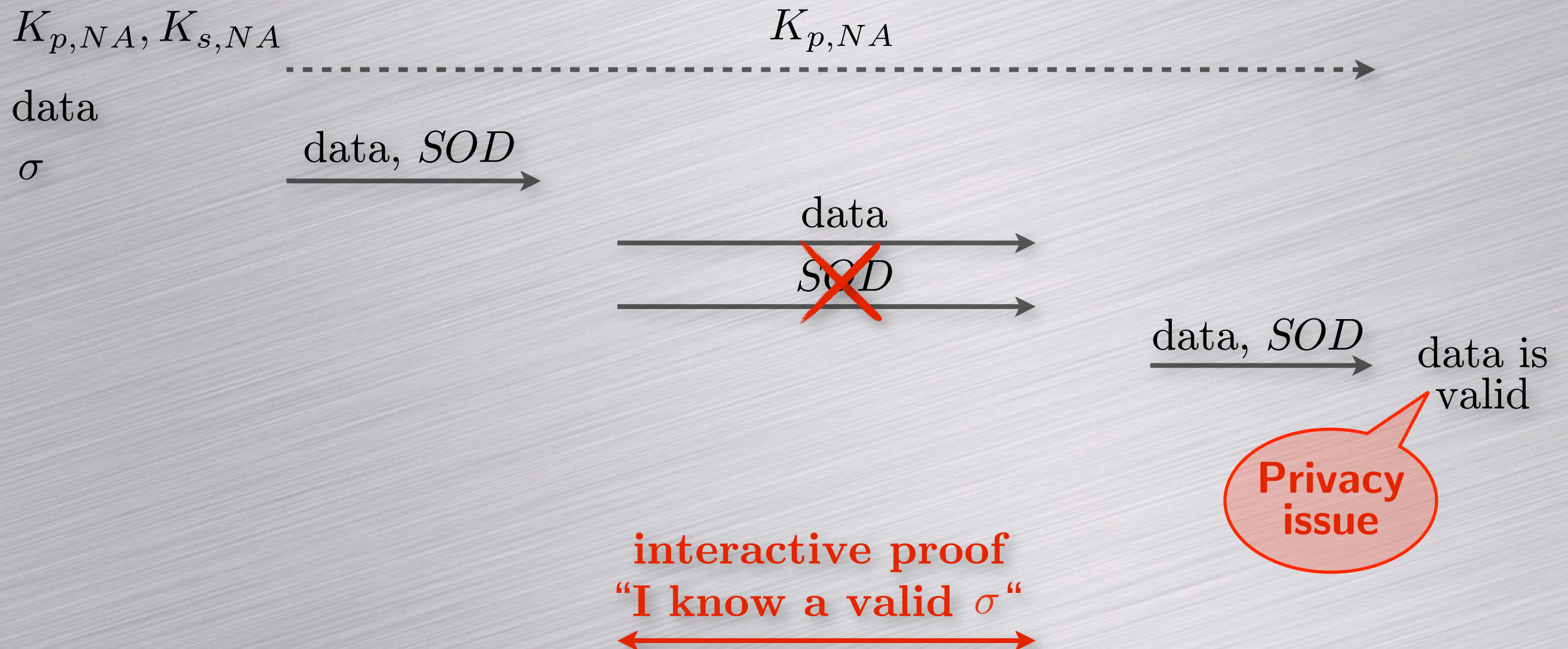
Solution: The Main Idea



Solution: The Main Idea



Solution: The Main Idea



ONTAP Overview

ONTAP Overview

Signer

Prover

Verifier

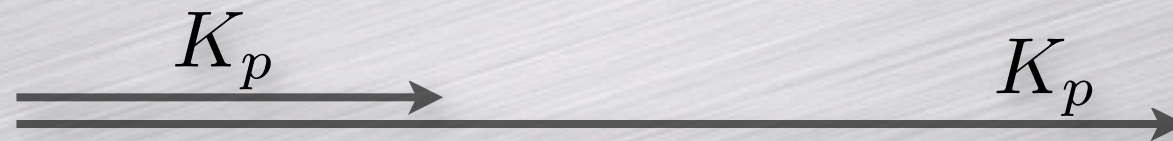
ONTAP Overview

Signer

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

Prover

Verifier



ONTAP Overview

Signer

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

$(\sigma_p, \sigma_s) = \text{sign}(K_s, m)$

Prover

$\xrightarrow{K_p}$

$\xrightarrow{\sigma_p, \sigma_s}$

Verifier

$\xrightarrow{K_p}$

$\xrightarrow{\sigma_p}$

ONTAP Overview

Signer

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

$(\sigma_p, \sigma_s) = \text{sign}(K_s, m)$

Prover

$\xrightarrow{K_p}$

$\xrightarrow{\sigma_p, \sigma_s}$

Verifier

$\xrightarrow{K_p}$

$\xrightarrow{\sigma_p}$

$\text{iProof}(K_p, m, \sigma_p, \sigma_s) \longleftrightarrow \text{iProof}(K_p, m, \sigma_p)$
 $\quad \quad \quad \searrow \text{accept/reject}$

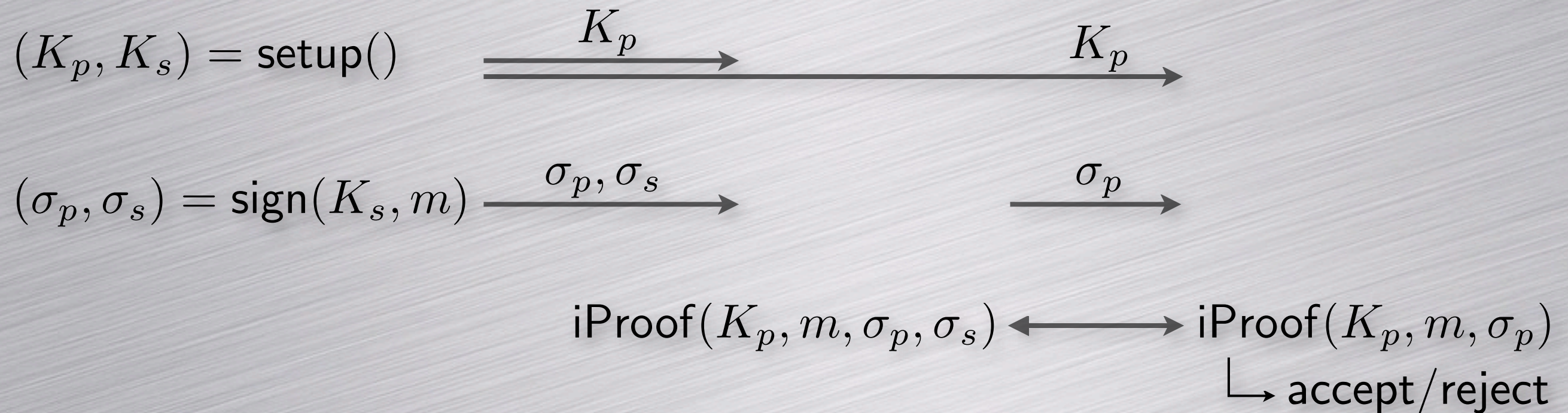
ONTAP Overview

Signer

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

Prover

Verifier



○ Properties:

- Completeness
- Unforgeability (sign) + soundness (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

ONTAP Construction

Theorem

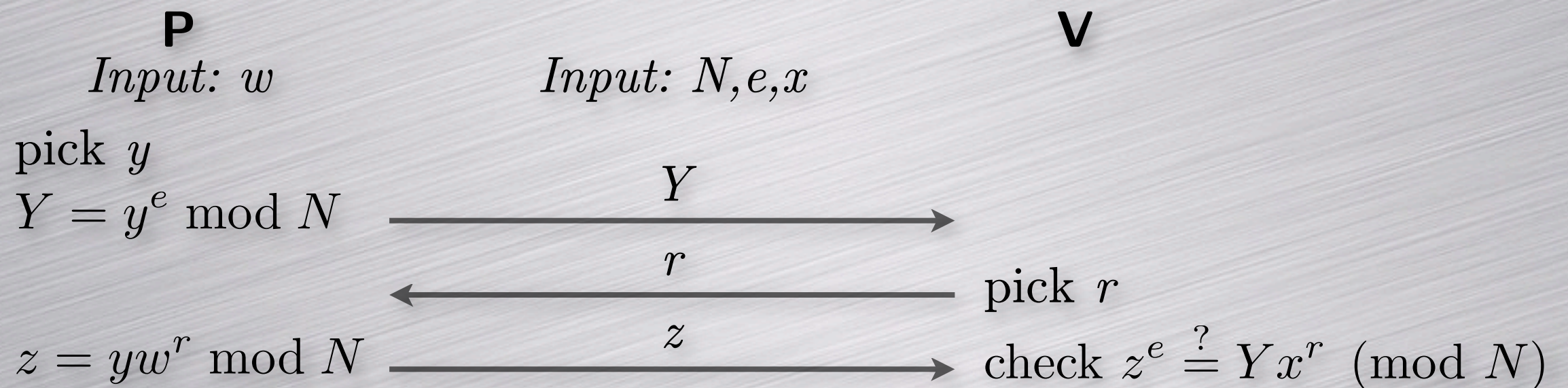
An ONTAP can be build with

- 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

An e-passport uses RSA, DSA, or ECDSA.

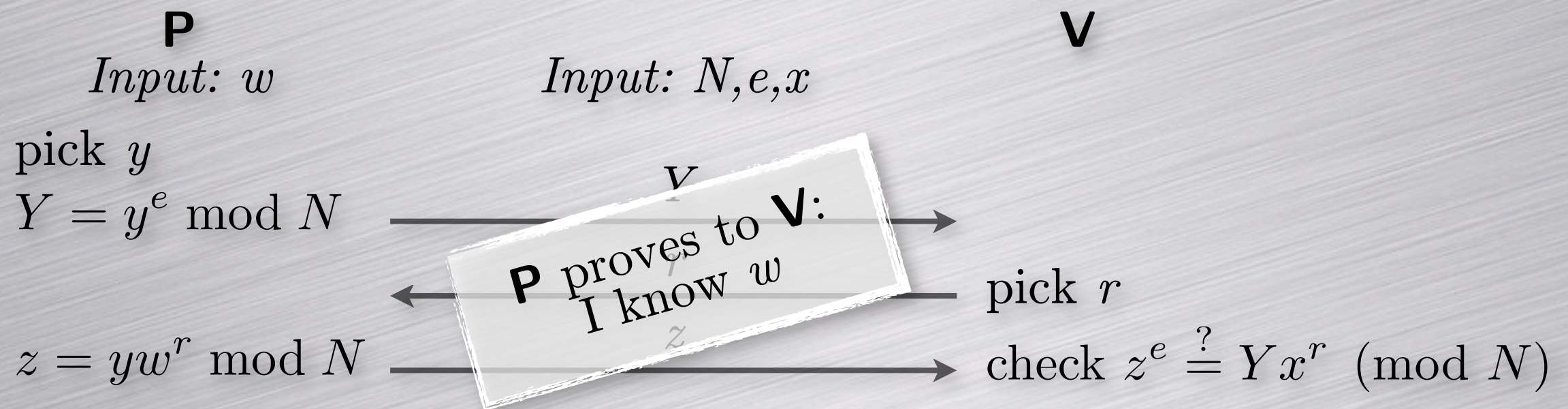
The Guillou-Quisquater Protocol

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



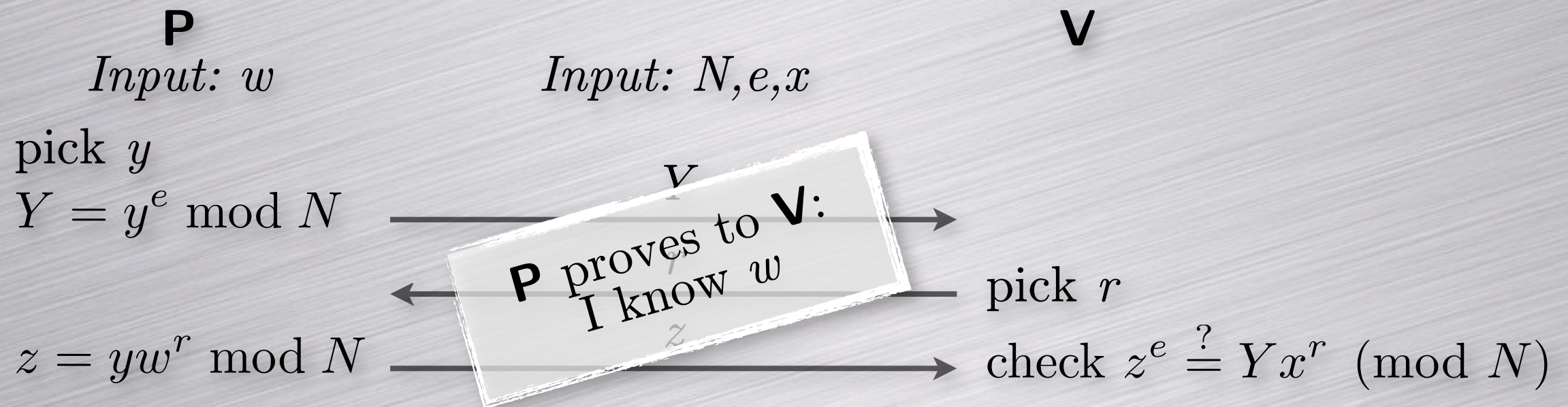
The Guillou-Quisquater Protocol

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



The Guillou-Quisquater Protocol

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

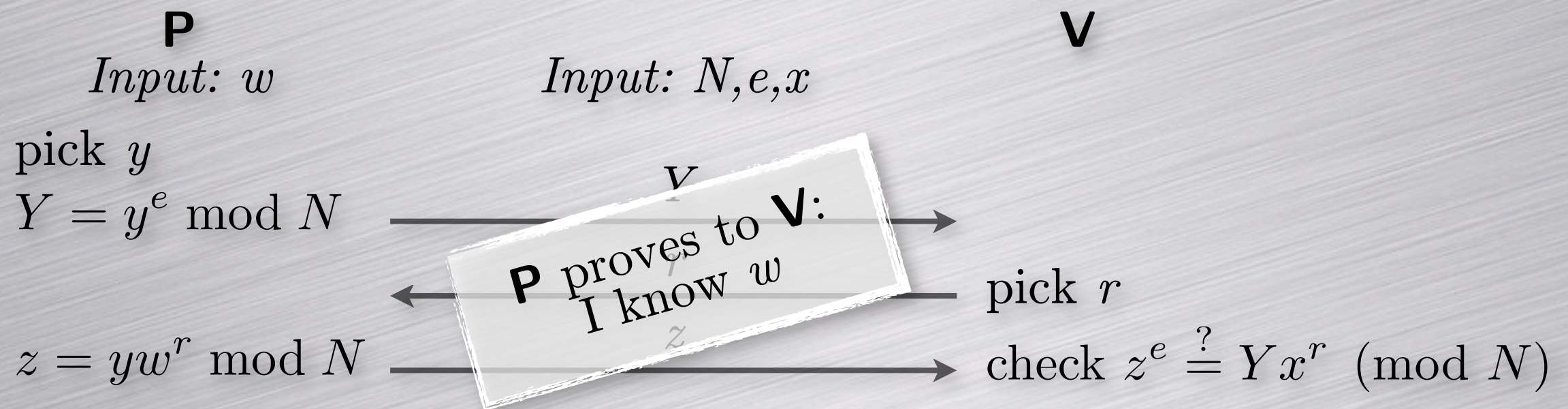


GQ is a proof knowledge with:

- ☑ Efficiency
- ☑ Completeness
- ☑ Soundness

The Guillou-Quisquater Protocol

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



GQ is a proof knowledge with:

- ☑ 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 .

$$\left\{ \text{View}_V \left(\text{proof}_{P(w), V(z)}(x) \right) \right\}_{z \in \{0,1\}^*, x \in L_R, w \in R(x)} \quad \{ \text{Sim}(x, z) \}_{z \in \{0,1\}^*, x \in L_R}$$

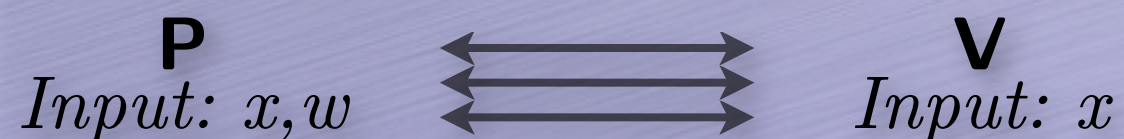
Zero-Knowledge

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

Zero-knowledge

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

$$\left\{ \text{View}_V \left(\text{proof}_{P(w), V(z)}(x) \right) \right\}_{z \in \{0,1\}^*, x \in L_R, w \in R(x)} \quad \{ \text{Sim}(x, z) \}_{z \in \{0,1\}^*, x \in L_R}$$



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 .

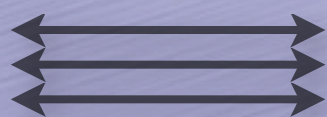
$$\left\{ \text{View}_V \left(\text{proof}_{P(w), V(z)}(x) \right) \right\}_{z \in \{0,1\}^*, x \in L_R, w \in R(x)} \quad \{ \text{Sim}(x, z) \}_{z \in \{0,1\}^*, x \in L_R}$$

**Real
transcript**

Indistinguishable

**Simulated
transcript**

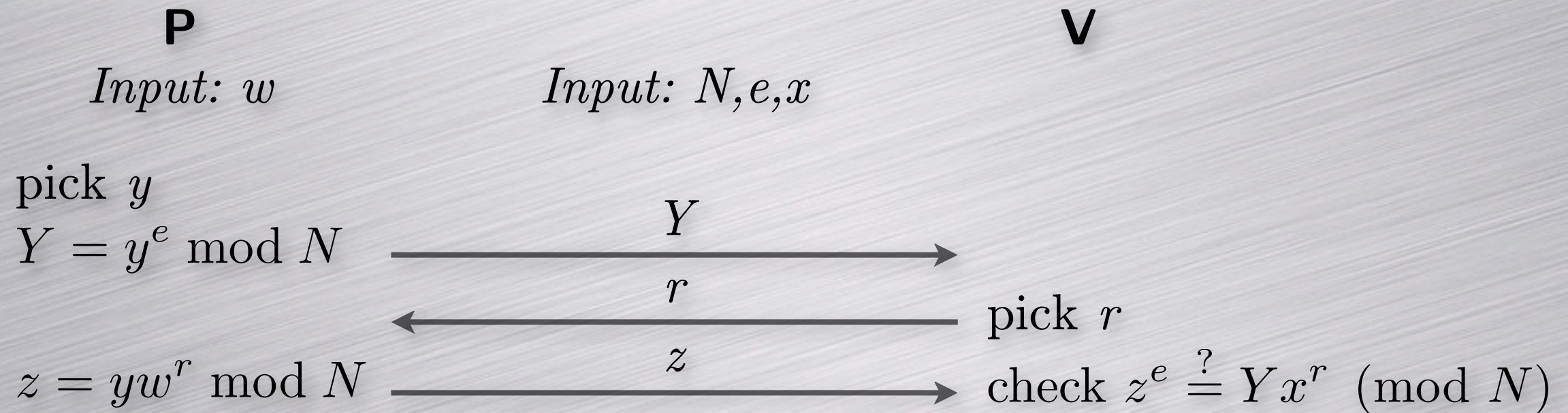
P
Input: x, w



V
Input: x



Zero-Knowledge: GQ protocol



Simulated transcript (without w):

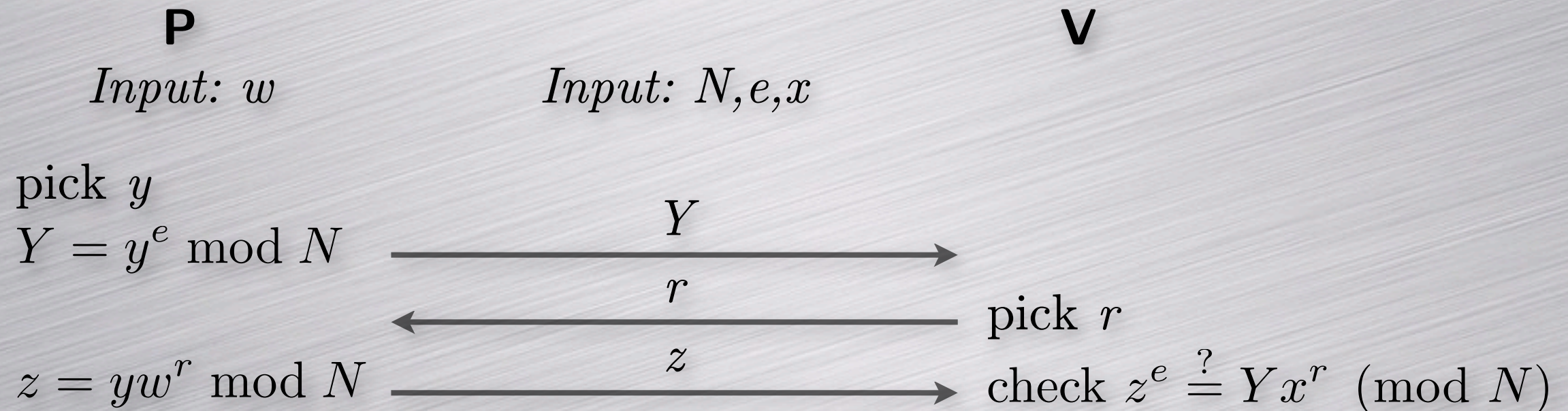
given N, e, x , and r

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

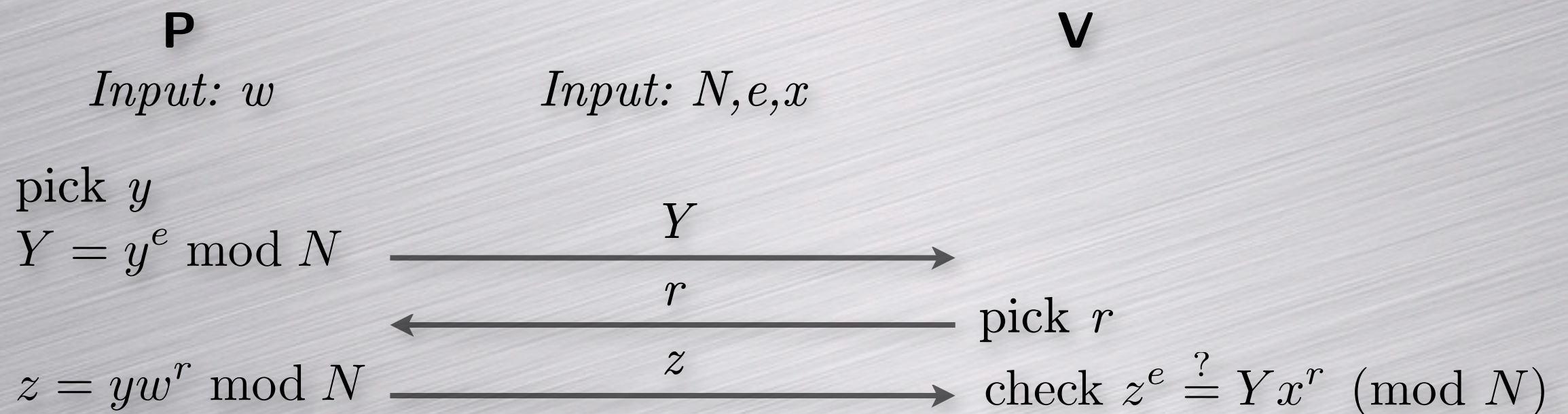
$$Y = z^e / x^r$$

output (Y, r, z)

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

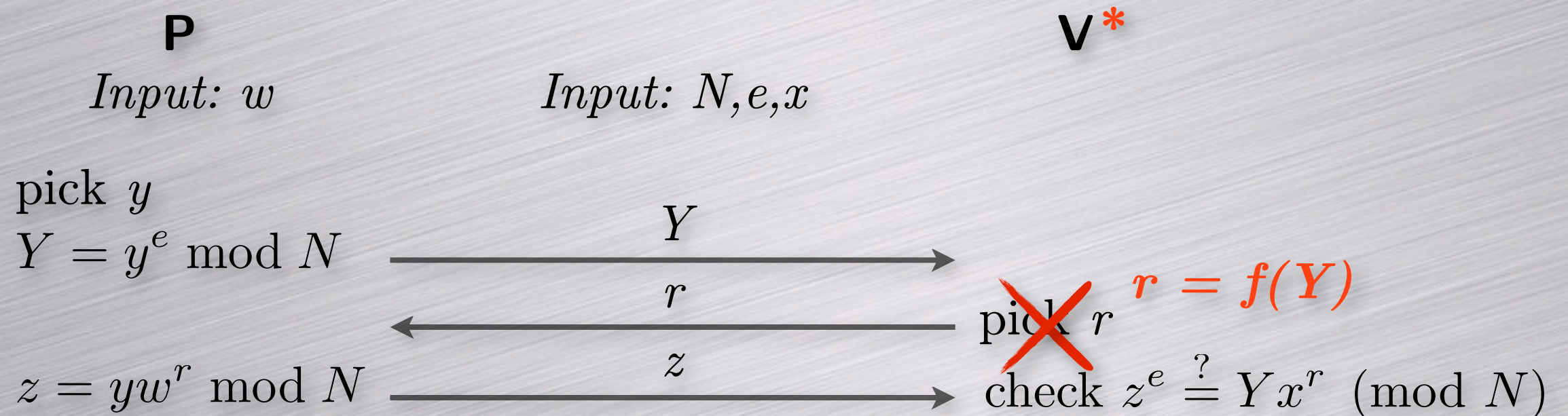
Fiat-Shamir Transform

The GQ protocol is only Honest-Verifier ZK.



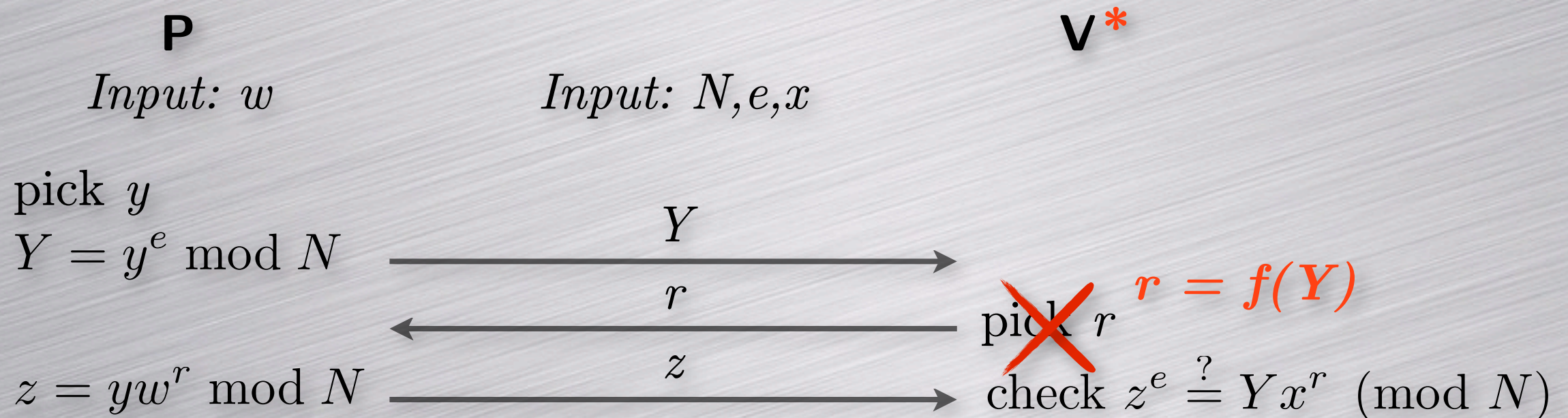
Fiat-Shamir Transform

The GQ protocol is only Honest-Verifier ZK.



Fiat-Shamir Transform

The GQ protocol is only Honest-Verifier ZK.



Considering malicious verifiers:

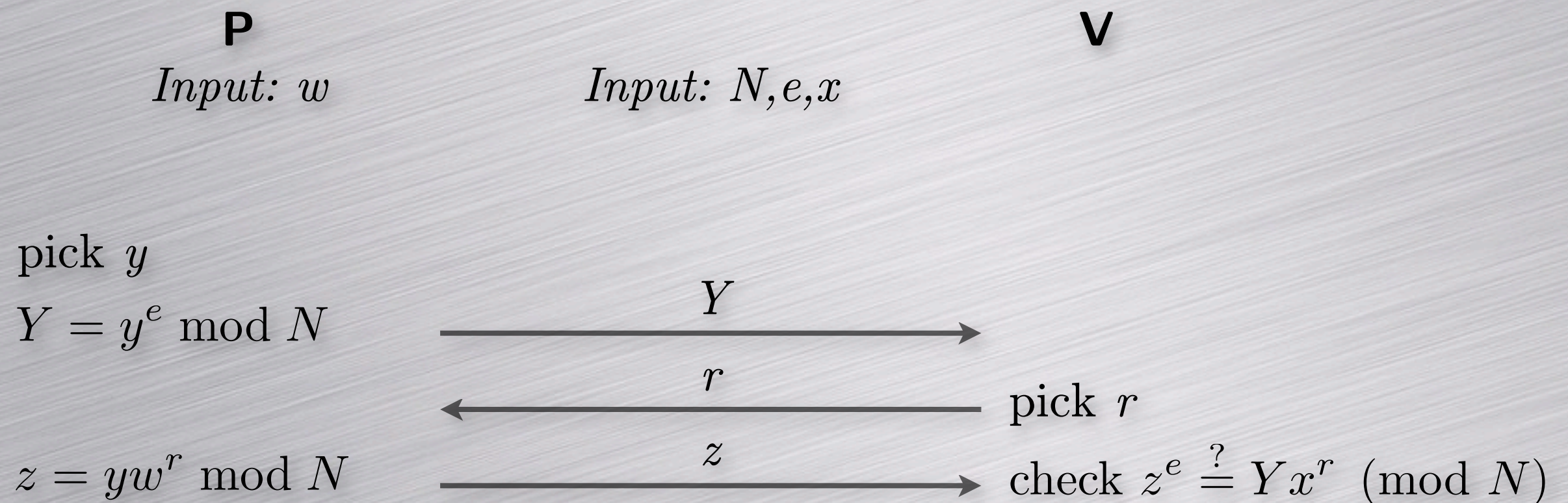
- ❑ the proof is not simulatable (without w),
- ❑ the proof becomes transferable.

Protocol Transform

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

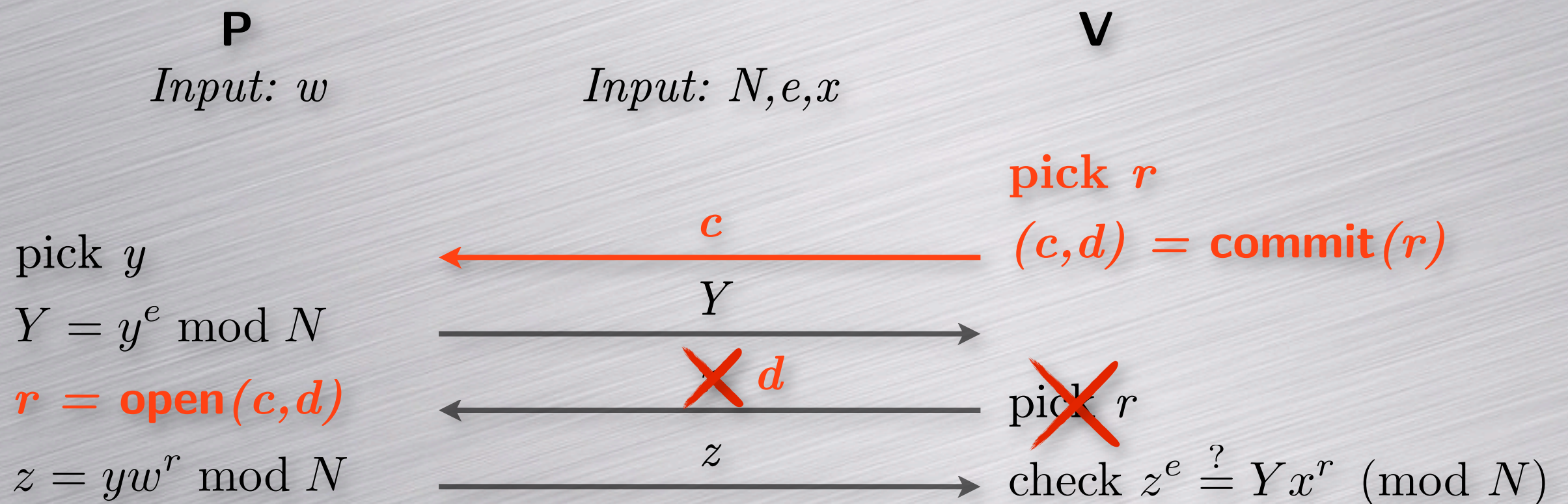
Protocol Transform

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

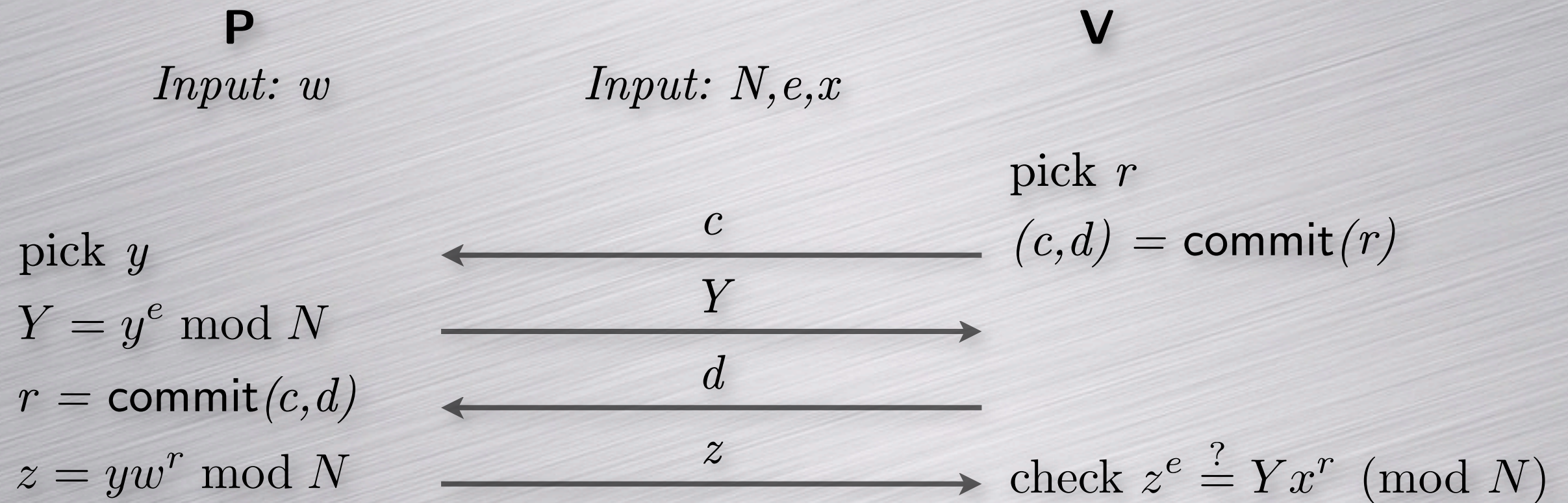


Protocol Transform

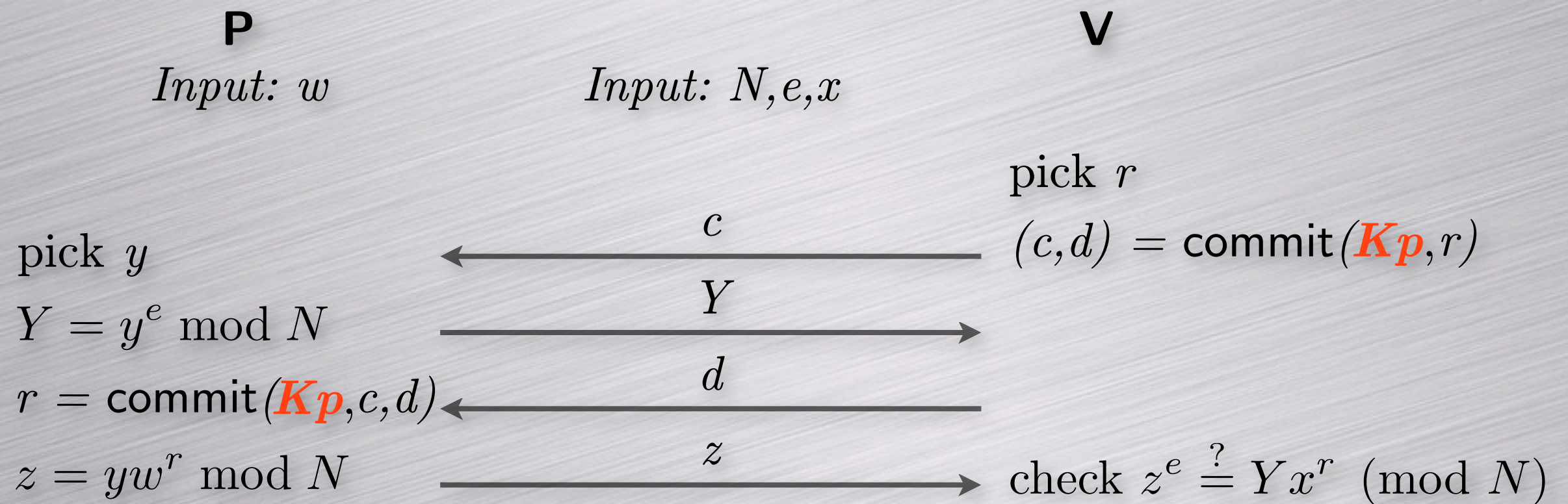
To obtain a **full** zero-knowledge protocol,
ensure that r is chosen independently from Y .



Require the CRS Model...

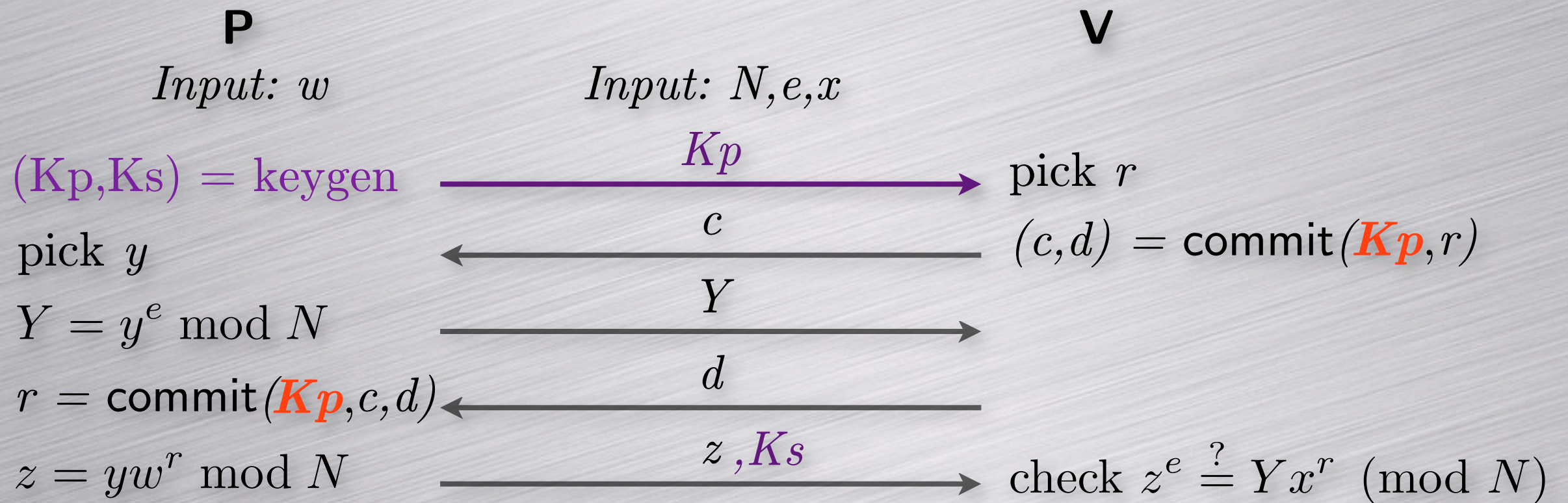


Require the CRS Model...



To prove the soundness, we should add a trapdoor.

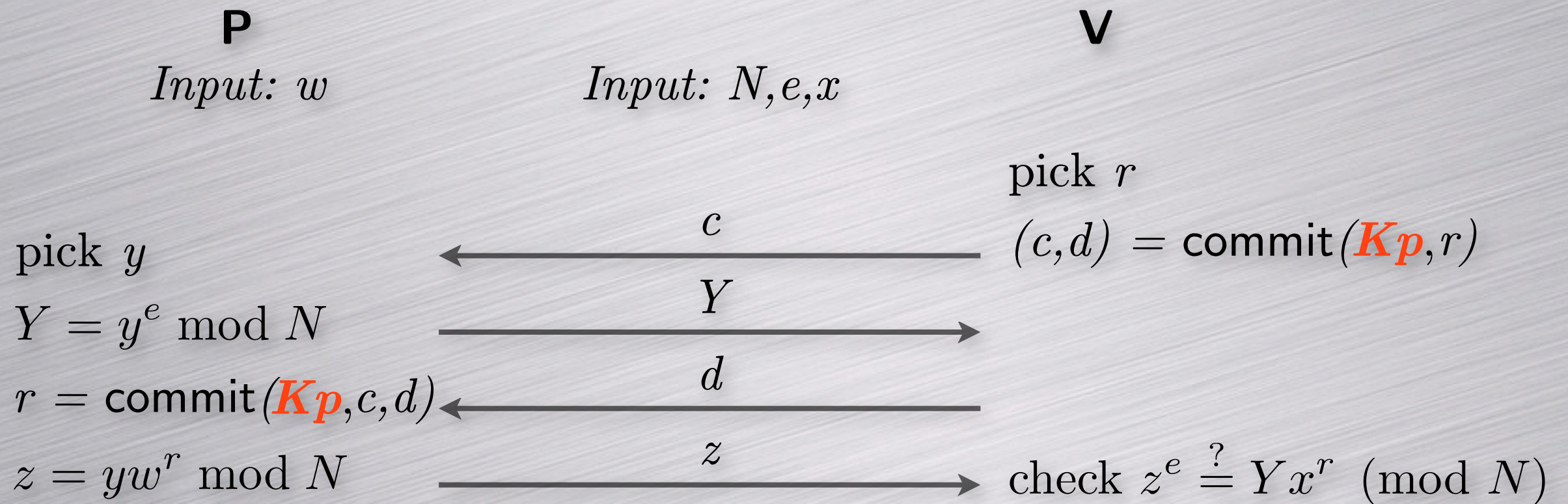
Require the CRS Model...



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.

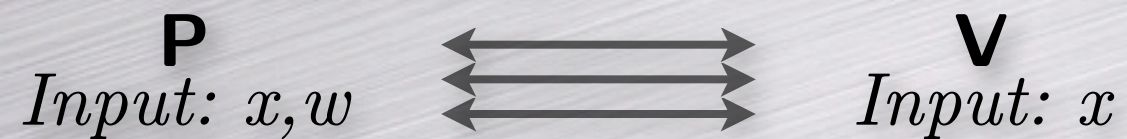
Deniable Zero-Knowledge

Honest-Verifier ZK:

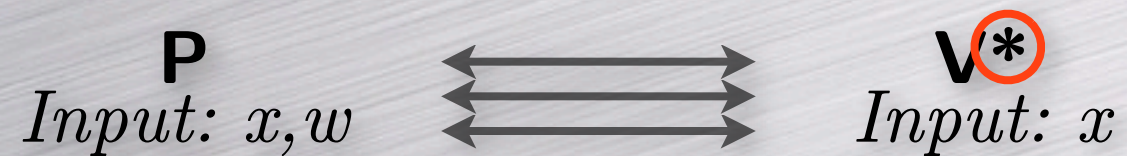


Deniable Zero-Knowledge

Honest-Verifier ZK:

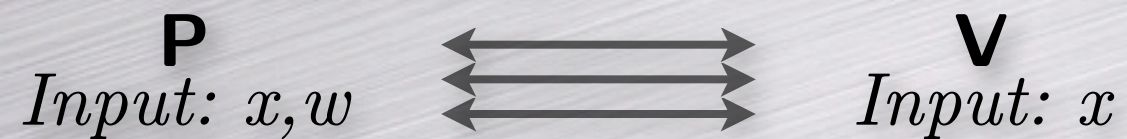


ZK:

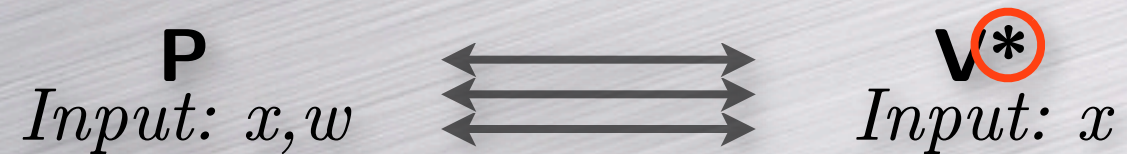


Deniable Zero-Knowledge

Honest-Verifier ZK:



ZK:

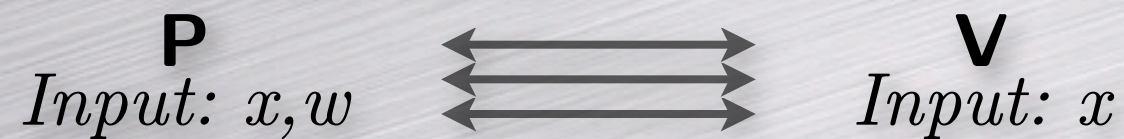


ZK in the CRS model:



Deniable Zero-Knowledge

Honest-Verifier ZK:



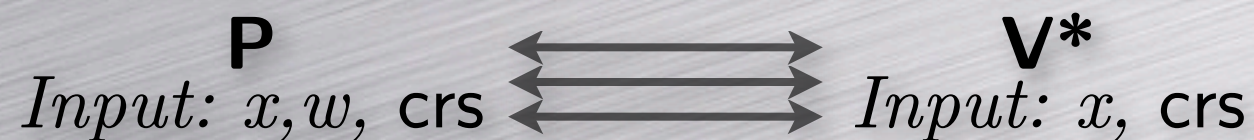
ZK:



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

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

Prover

Verifier



Back to ONTAP: RSA example

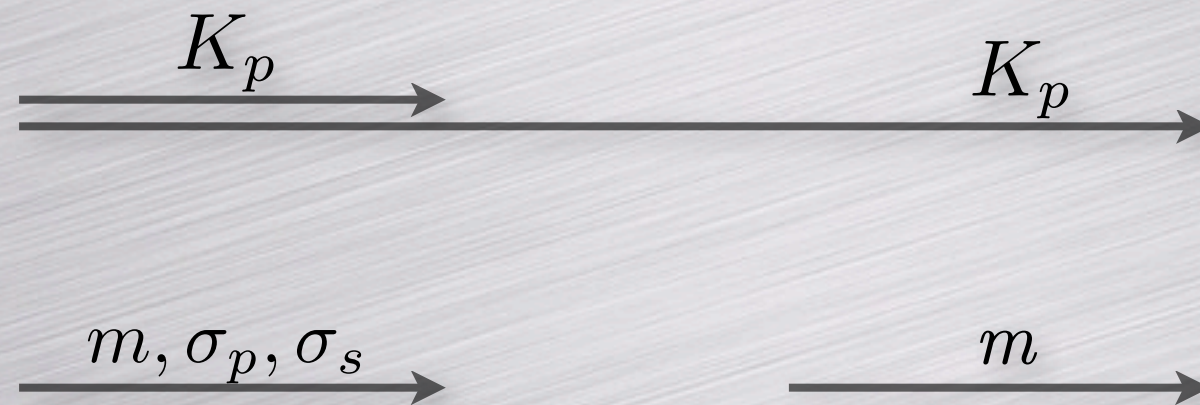
Signer

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

$\sigma_p = H_{\text{seed}}(m)$
 $\sigma_s = \sigma_p^d \bmod N$

Prover

Verifier



Back to ONTAP: RSA example

Signer

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

$\sigma_p = H_{\text{seed}}(m)$
 $\sigma_s = \sigma_p^d \bmod N$

Prover

Verifier

K_p

m, σ_p, σ_s

m

pick y $\leftarrow$ c pick r
 $Y = y^e \bmod N$ $\xrightarrow{Y, \sigma_p}$ $(c, d) = \text{commit}(\text{crs}, r)$
 $r = \text{open}(\text{crs}, c, d)$ $\xleftarrow{d}$ check $V(\sigma_p, m) \stackrel{?}{=} 1$
 $z = y\sigma_s^r \bmod N$ $\xrightarrow{z}$ check $z^e \stackrel{?}{=} Y\sigma_p^r \bmod N$

Back to ONTAP: RSA example

Signer

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

$\sigma_p = H_{\text{seed}}(m)$
 $\sigma_s = \sigma_p^d \bmod N$

Prover

Verifier

K_p

m, σ_p, σ_s

m

pick y $\leftarrow c$ pick r
 $Y = y^e \bmod N$ $\xrightarrow{Y, \sigma_p}$ $(c, d) = \text{commit}(\text{crs}, r)$
 $r = \text{open}(\text{crs}, c, d)$ $\xrightarrow{d}$ check $V(\sigma_p, m) \stackrel{?}{=} 1$
 $z = y\sigma_s^r \bmod N$ $\xrightarrow{z}$ check $z^e \stackrel{?}{=} Y\sigma_p^r \bmod N$



Conclusion

Conclusion

Conclusion

- SAS-based cryptography:
 - dedicated network and adversarial model
 - generic security analysis (notion of optimality)
 - optimal NIMAP, MMA, MCA, and GMA
 - optimal AKA and GKA

Conclusion

- SAS-based cryptography:
 - dedicated network and adversarial model
 - generic security analysis (notion of optimality)
 - optimal NIMAP, MMA, MCA, and GMA
 - optimal AKA and GKA
- Offline Non-Transferable Authentication Protocol
 - solve privacy issue in a three-party setting (e-passport)

Conclusion

- SAS-based cryptography:
 - dedicated network and adversarial model
 - generic security analysis (notion of optimality)
 - optimal NIMAP, MMA, MCA, and GMA
 - optimal AKA and GKA
- Offline Non-Transferable Authentication Protocol
 - solve privacy issue in a three-party setting (e-passport)
- (Hash-and-sign-based signatures)
 - pre-processing strengthening actual implementations

**Thank you
for
your attention!**