RUB

RUHR-UNIVERSITÄT BOCHUM

Selective Opening Security from Simulatable Data Encapsulation

Asiacrypt 2016, Hanoi, 5th of December 2016

Felix Heuer, Bertram Poettering
Horst Görtz Institute for IT Security
Ruhr University Bochum

hgi
Horst Görtz Institut
für IT-Sicherheit

Selective Opening Attacks

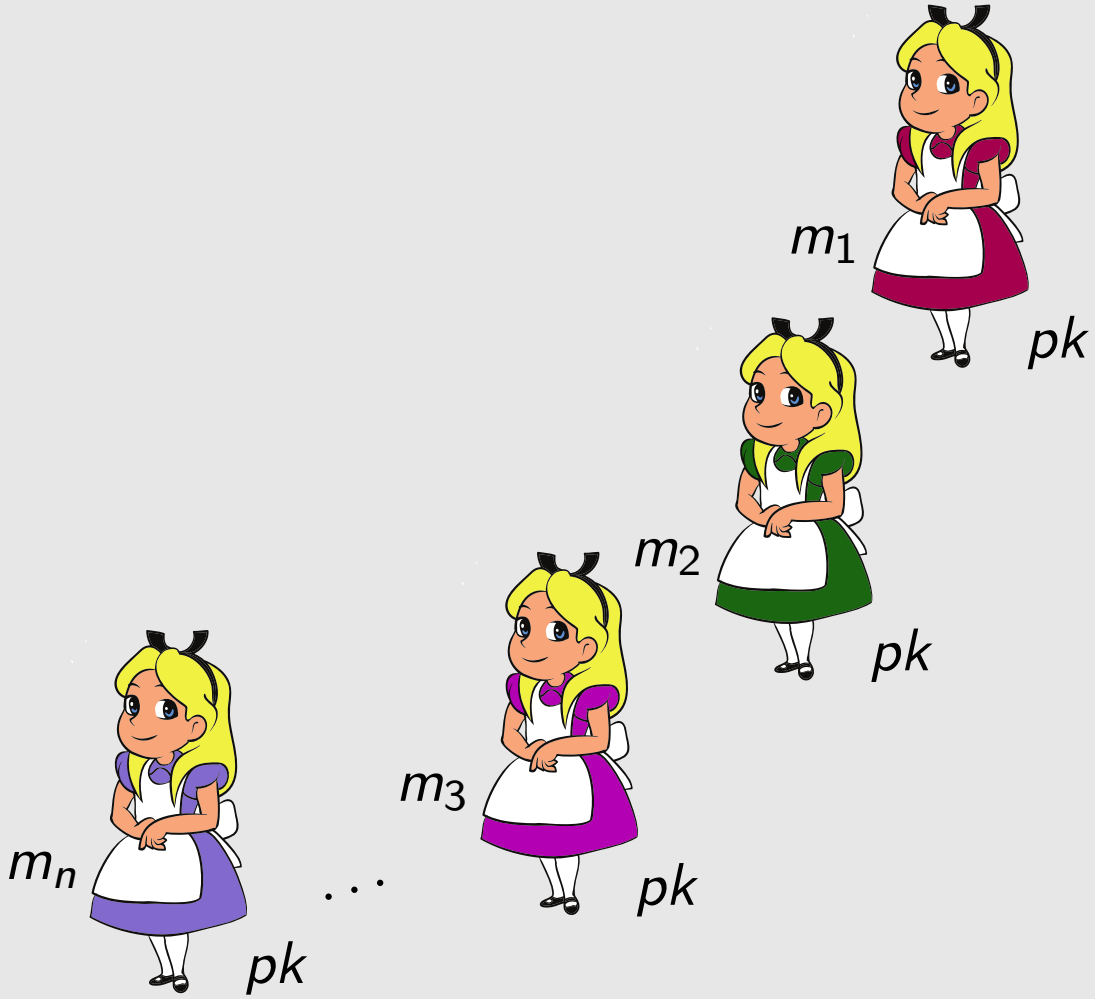
Receiver

Senders

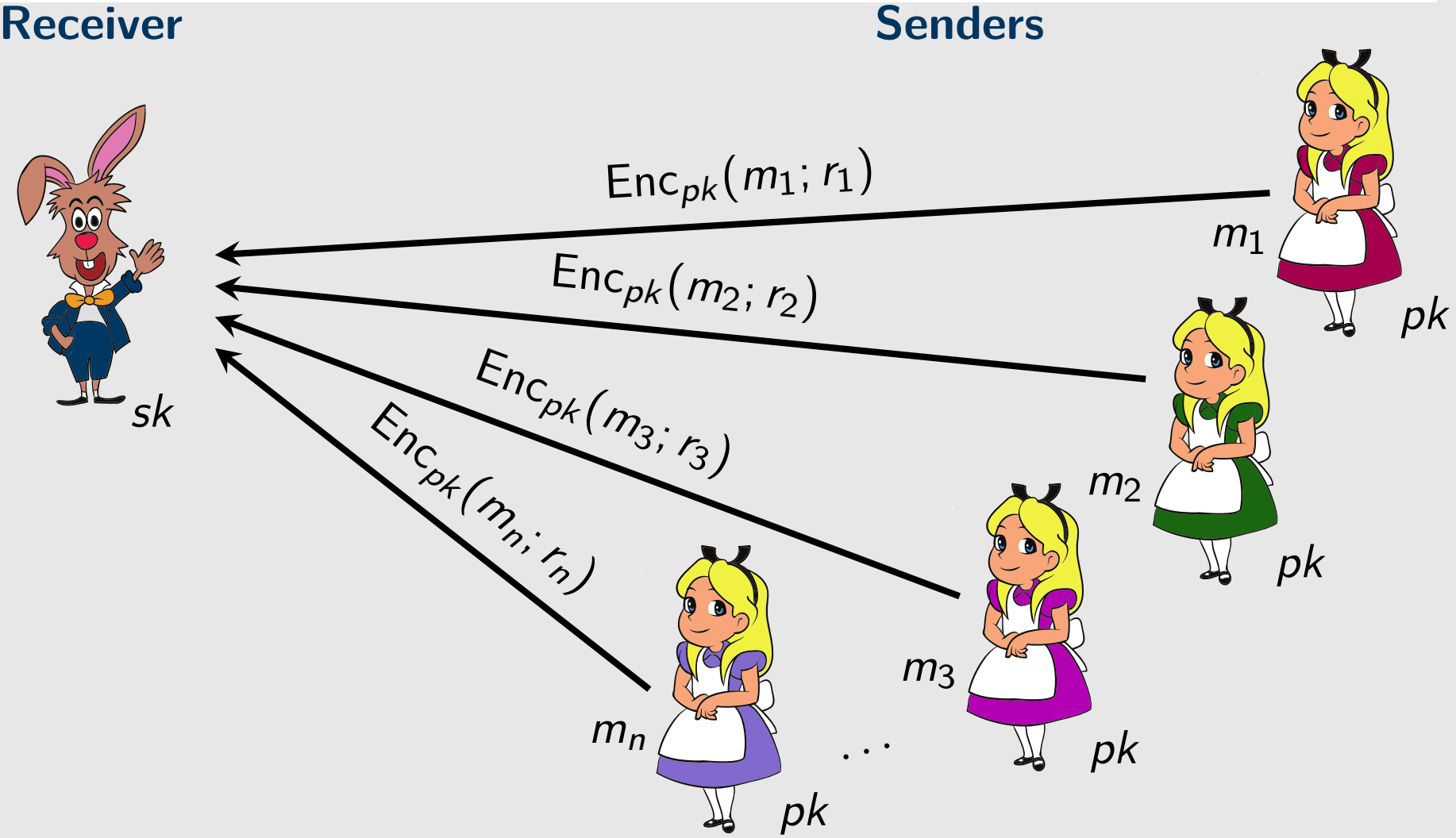
Selective Opening Attacks

Receiver

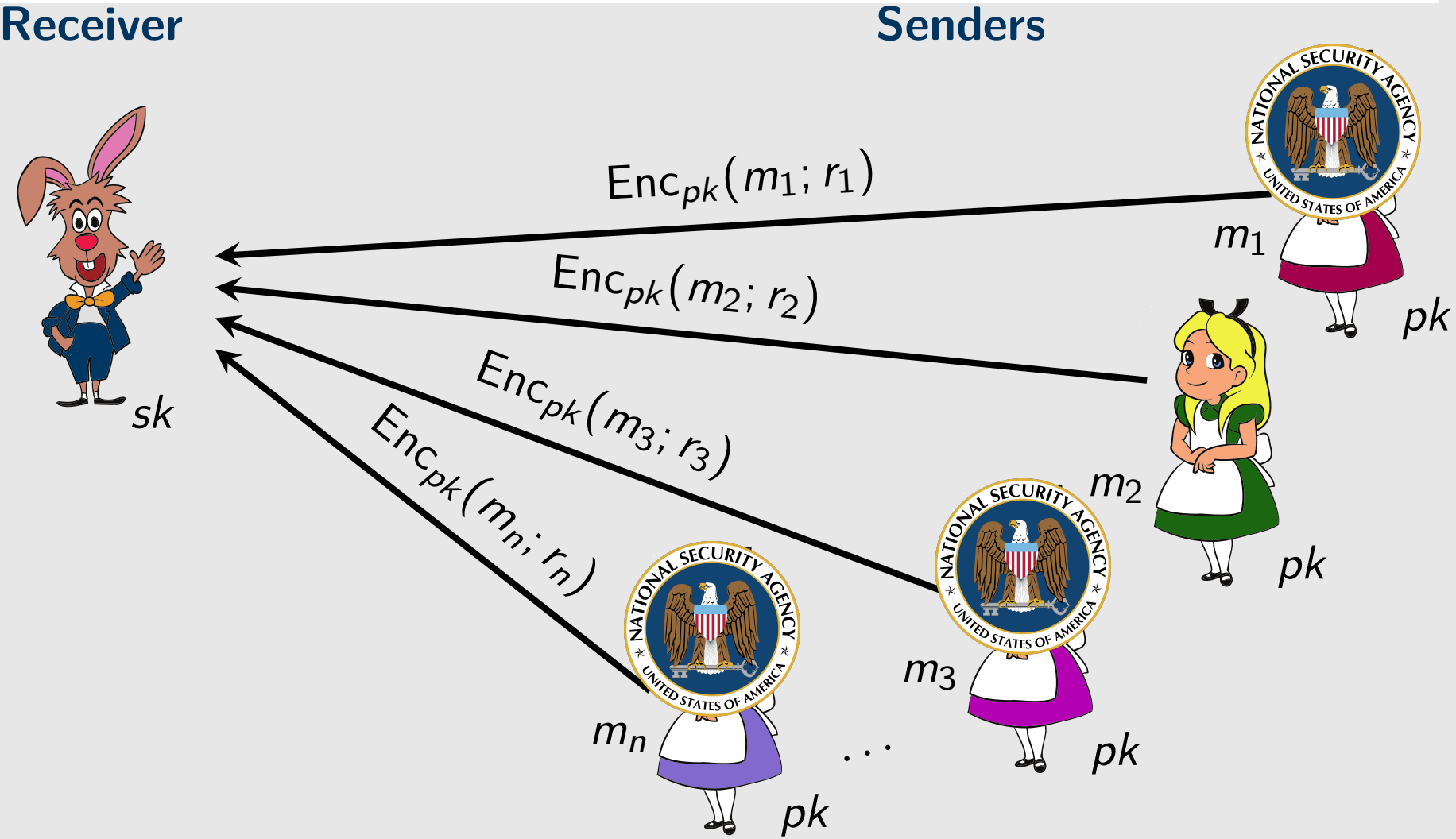
Senders



Selective Opening Attacks



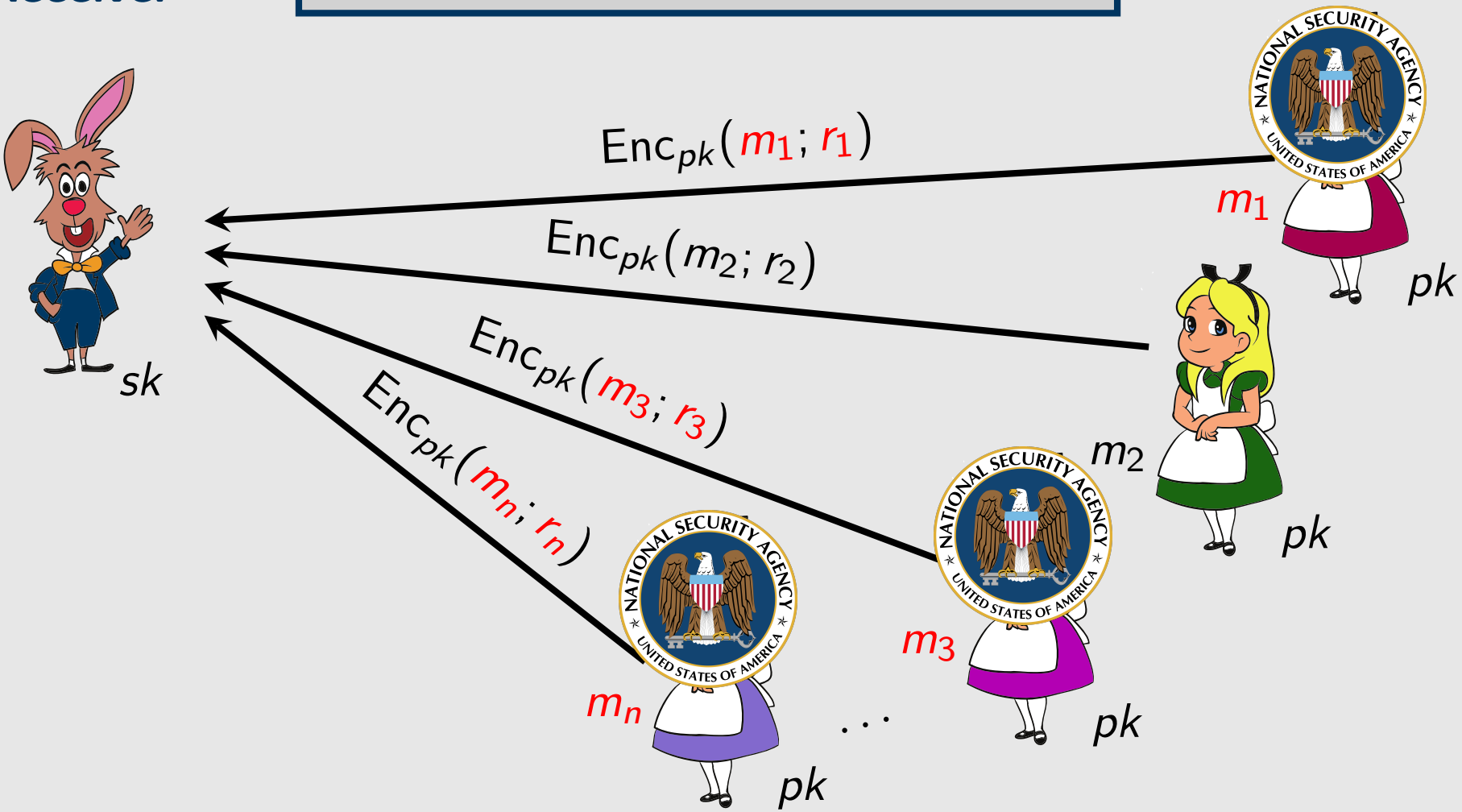
Selective Opening Attacks



Selective Opening Attacks

Receiver

Corrupting senders reveals m and r.



Selective Opening Attacks

Corrupting senders reveals m and r.

Receiver

sk

$\mathrm{Enc}_{pk}(m_1; r_1)$

$\mathrm{Enc}_{pk}(m_2; r_2)$

$\mathrm{Enc}_{pk}(m_3; r_3)$

$\mathrm{Enc}_{pk}(m_n; r_n)$

m_1 pk

m_2 pk

m_3 pk

m_n pk

$\ldots$

Do messages of uncorrupted parties remain confidential?

Selective Opening Attacks

Corrupting senders reveals m and r.

Receiver

sk

$\mathrm{Enc}_{pk}(m_1; r_1)$

$\mathrm{Enc}_{pk}(m_2; r_2)$

$\mathrm{Enc}_{pk}(m_3; r_3)$

$\mathrm{Enc}_{pk}($

m_1 pk

m_2 pk

m_3 pk

$\ldots$

- Dates back to [DNRS99]

Do messages of uncorrupted parties remain confidential?

Selective Opening Attacks

Receiver

Corrupting senders reveals m and r.

sk

$\mathsf{Enc}_{pk}(m_1; r_1)$

$\mathsf{Enc}_{pk}(m_2; r_2)$

$\mathsf{Enc}_{pk}(m_3; r_3)$

$\mathsf{Enc}_{pk}(\ldots)$

m_1

pk

m_2

pk

m_3

pk

- Dates back to [DNRS99]
- Messages may depend on another

Do messages of uncorrupted parties remain confidential?

Selective Opening Attacks

Corrupting senders reveals m and r.

Receiver

sk

$\mathrm{Enc}_{pk}(m_1; r_1)$

$\mathrm{Enc}_{pk}(m_2; r_2)$

$\mathrm{Enc}_{pk}(m_3; r_3)$

$\mathrm{Enc}_{pk}($

$\ldots$

m_1

pk

m_2

pk

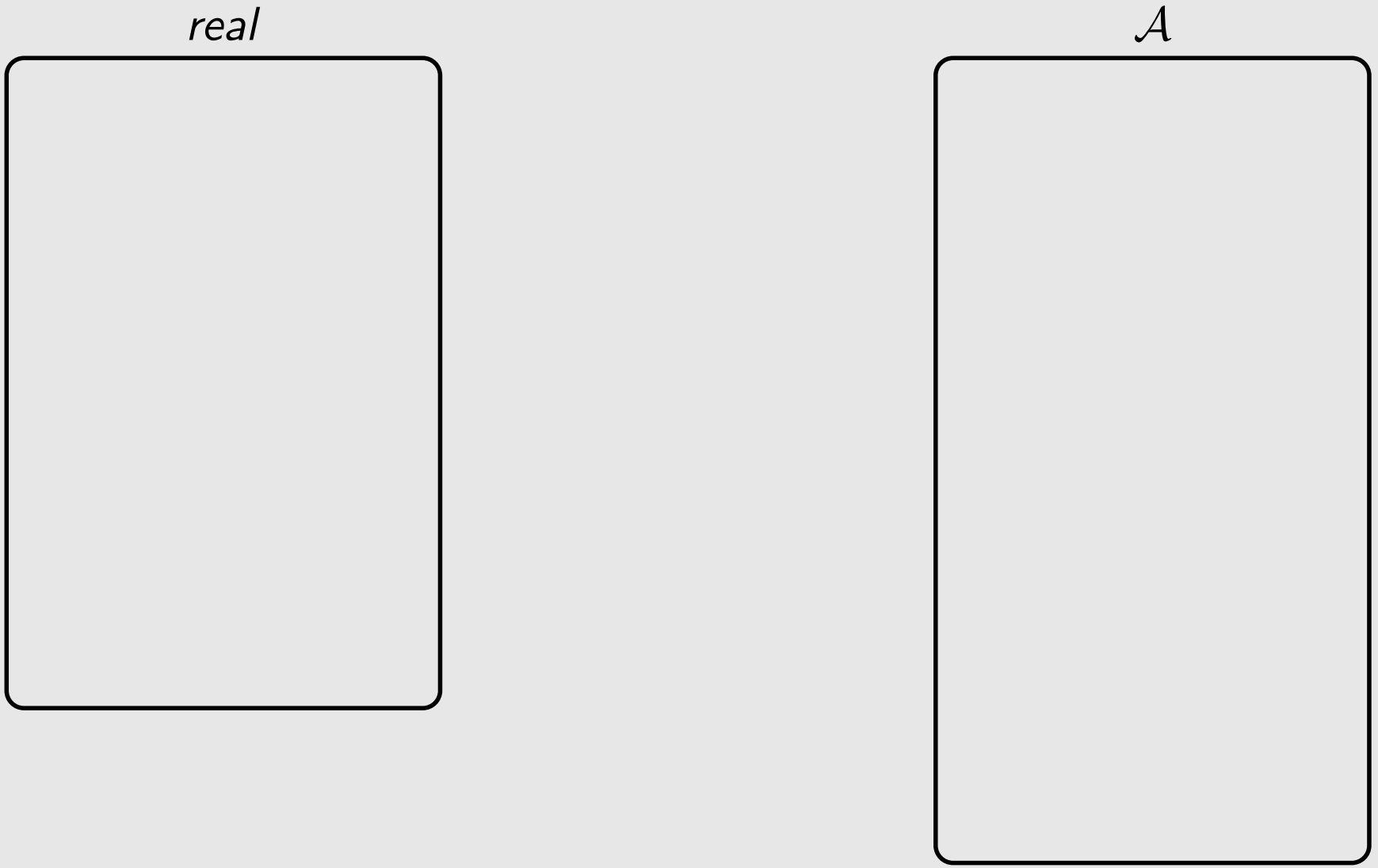
m_3

pk

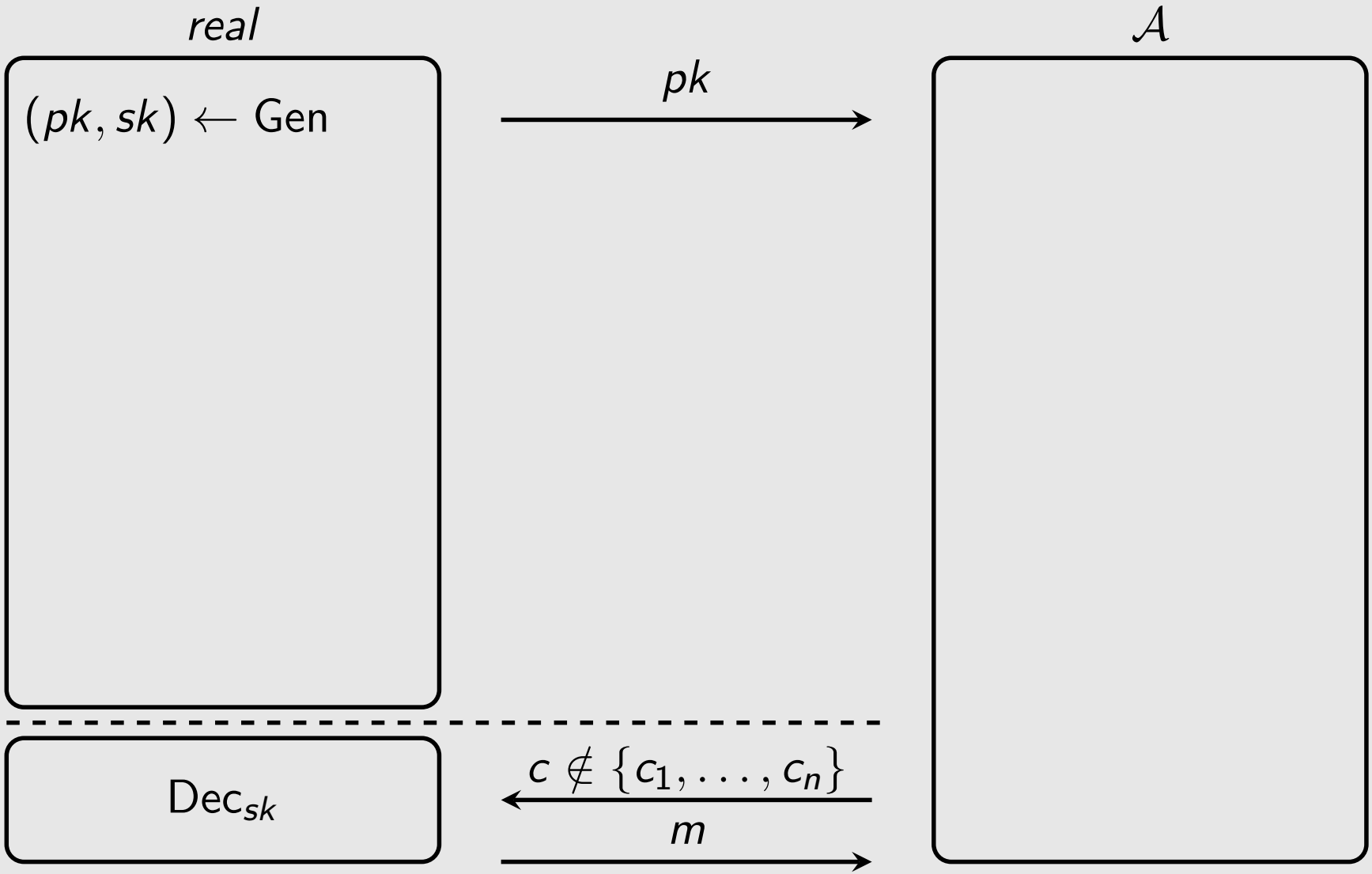
- Dates back to [DNRS99]
- Messages may depend on another
- SO security strictly stronger than standard security [HR14,HRW15]

Do messages of uncorrupted parties remain confidential?

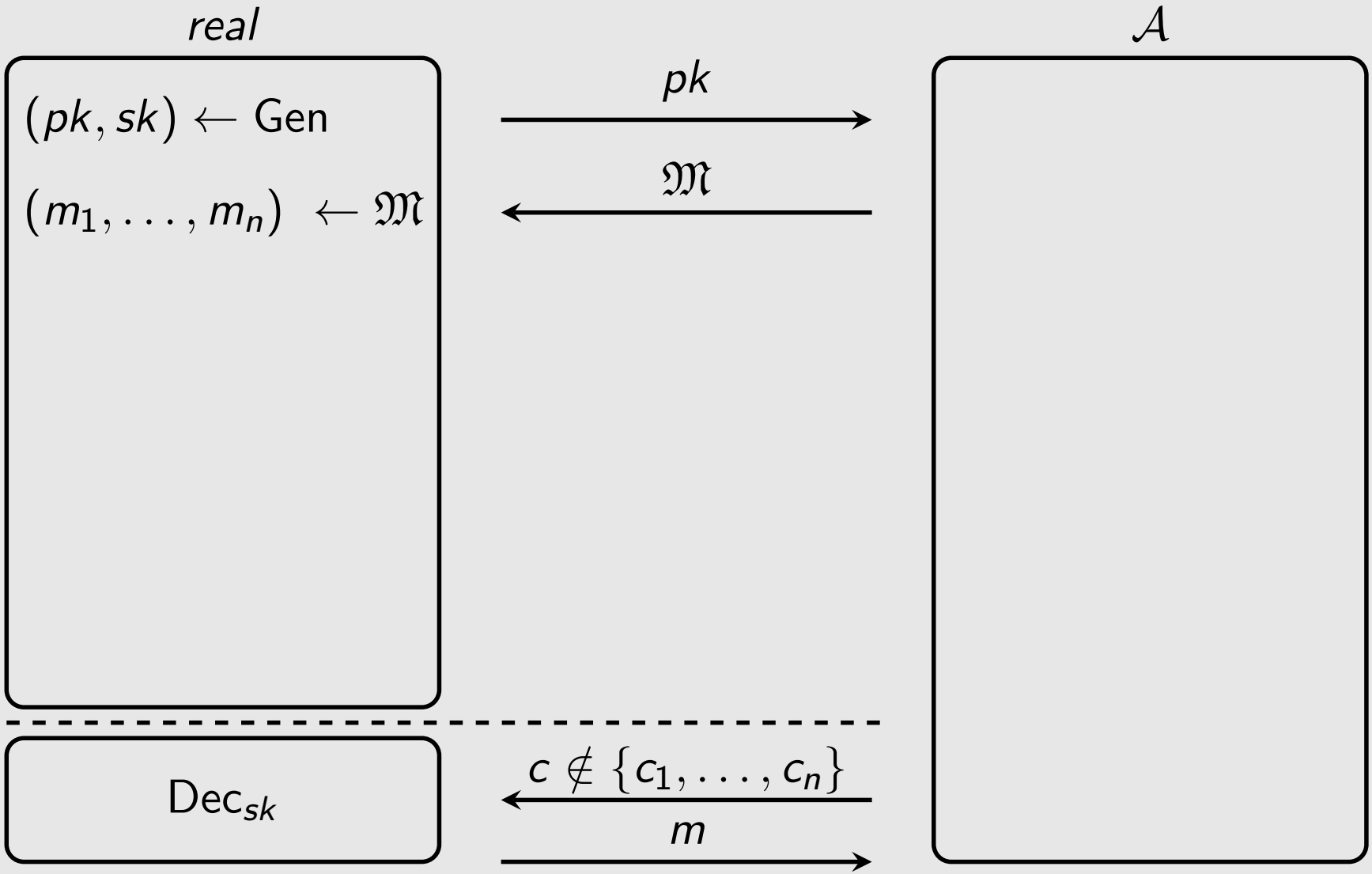
Defining SIM-SO-CCA Security [BHK12]



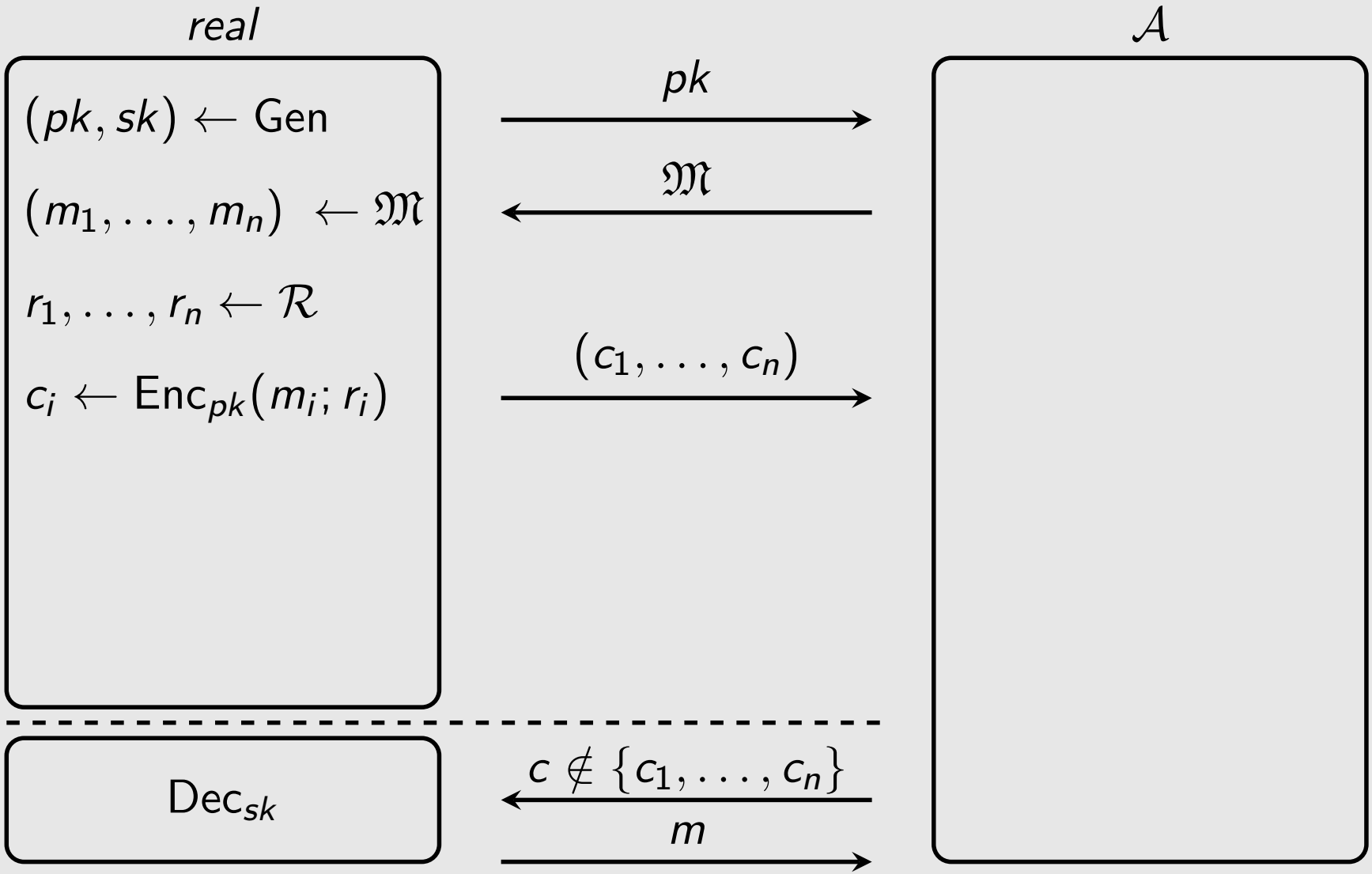
Defining SIM-SO-CCA Security [BHK12]



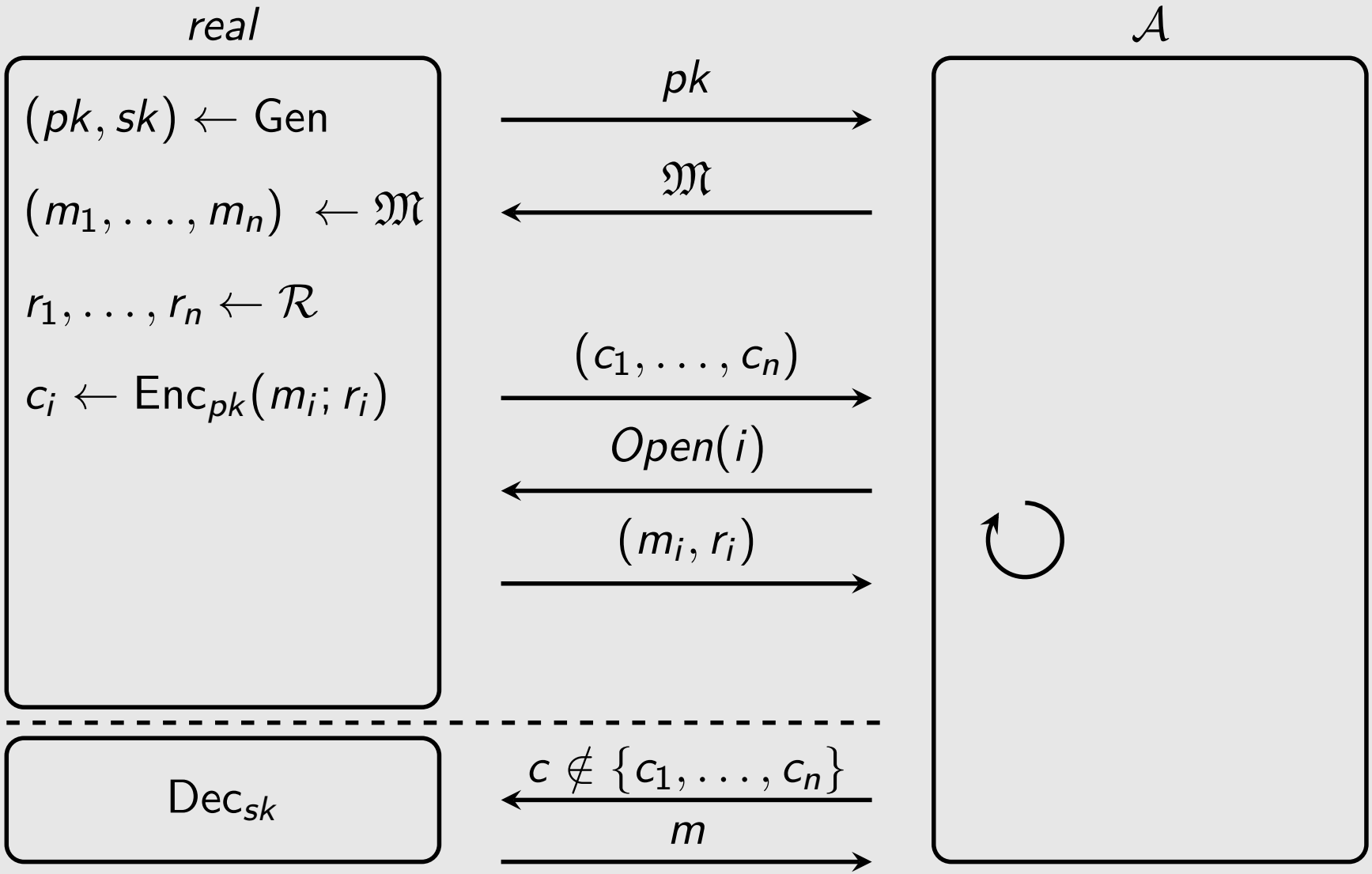
Defining SIM-SO-CCA Security [BHK12]



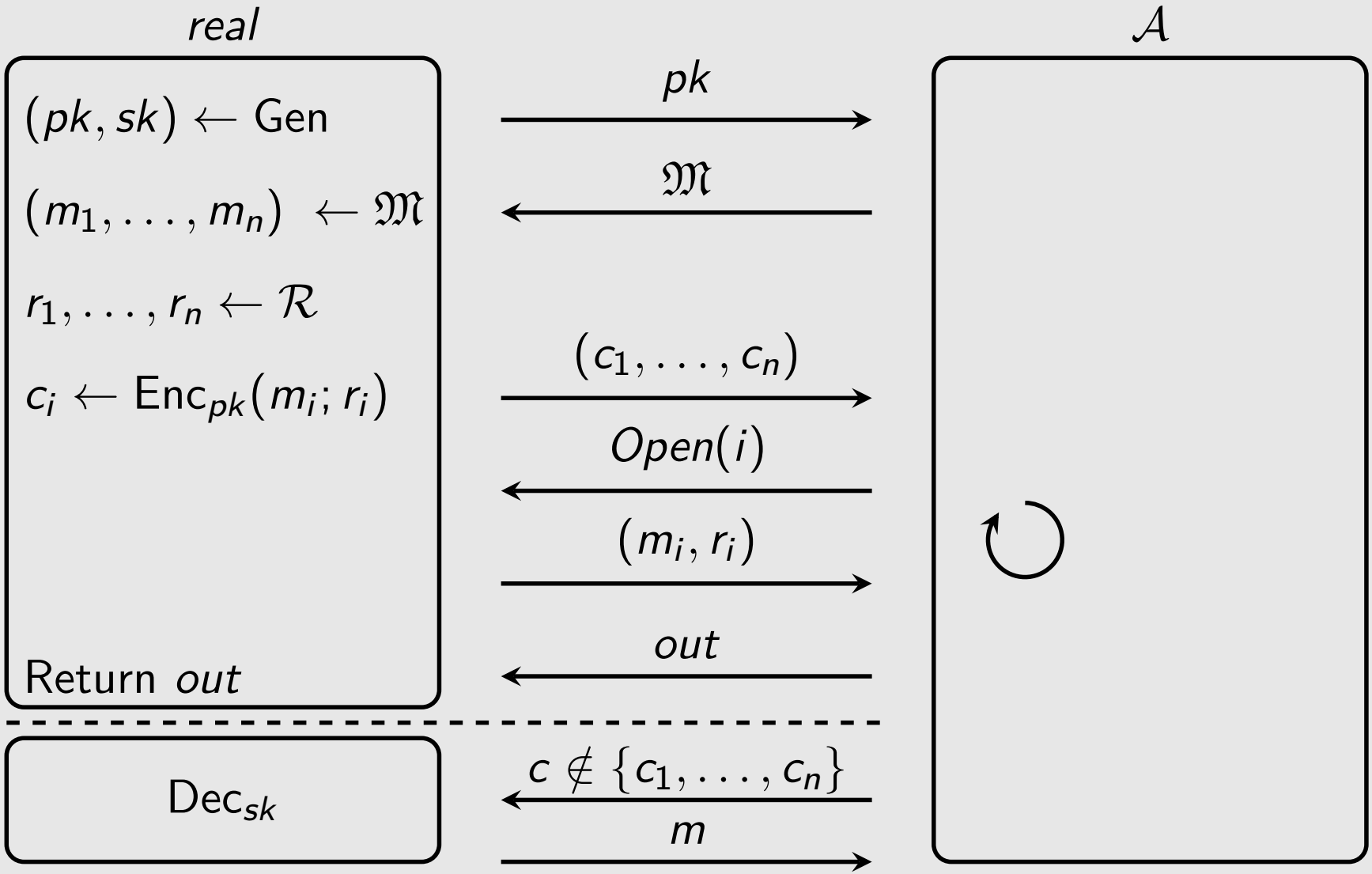
Defining SIM-SO-CCA Security [BHK12]



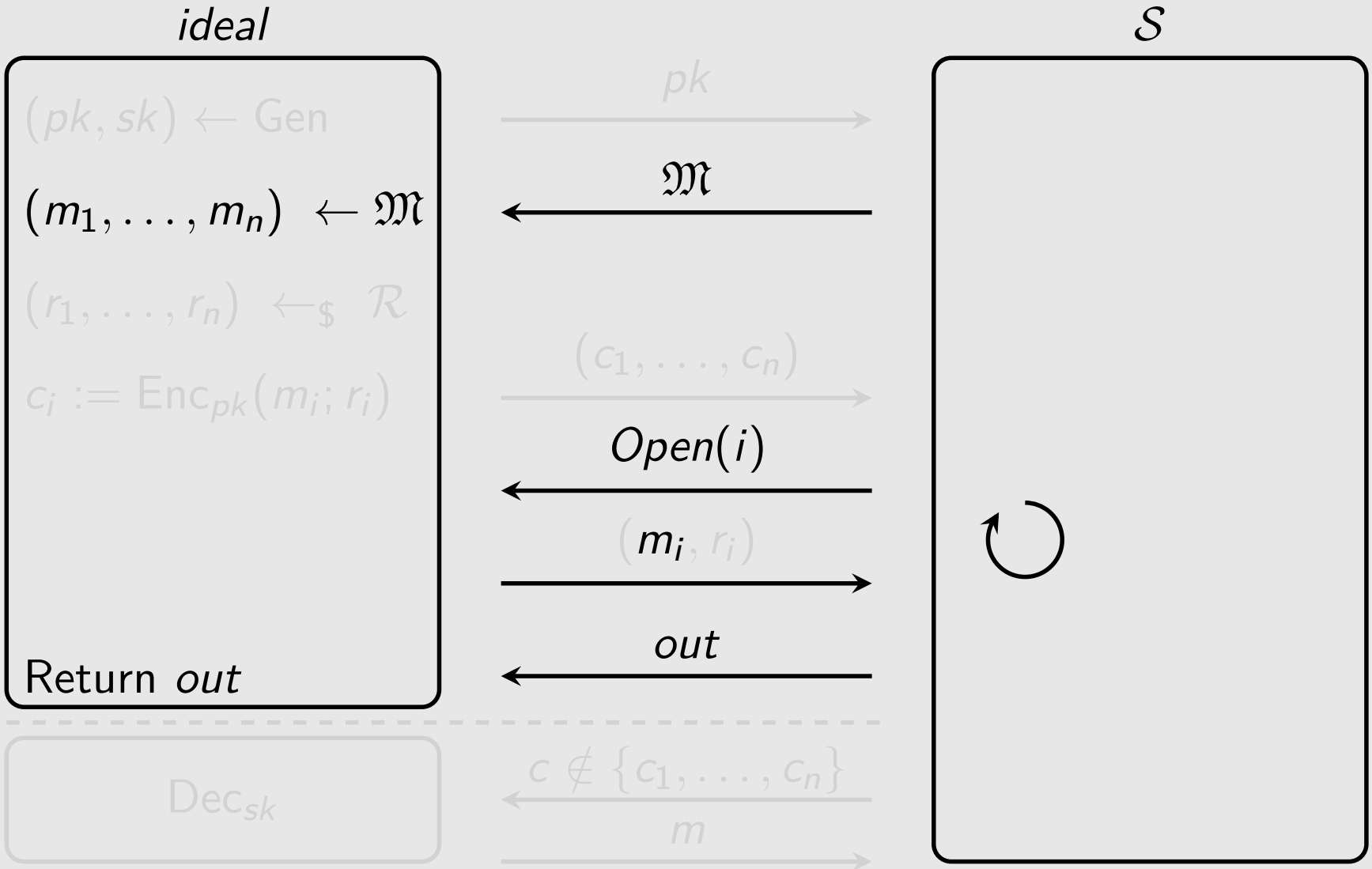
Defining SIM-SO-CCA Security [BHK12]



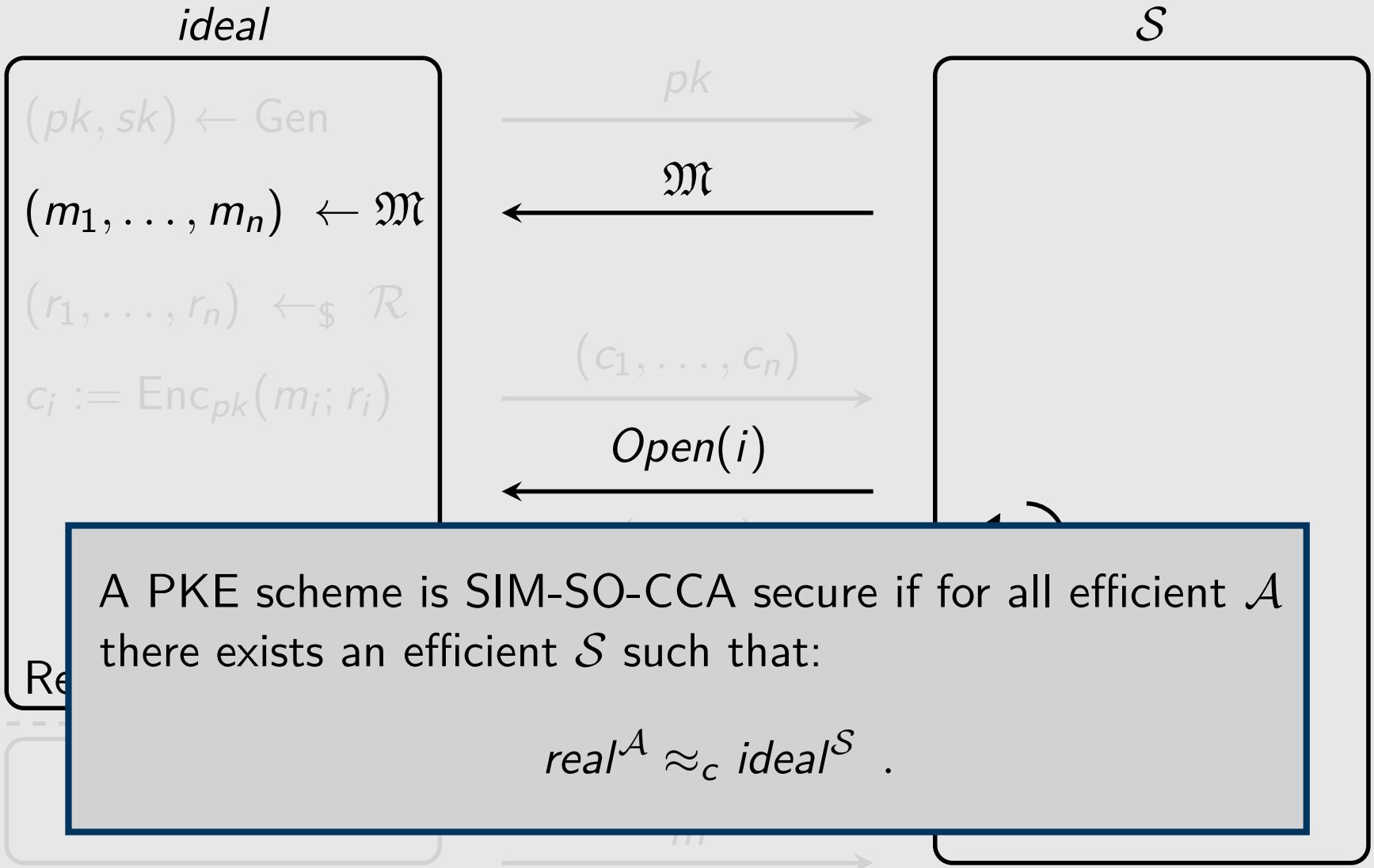
Defining SIM-SO-CCA Security [BHK12]



Defining SIM-SO-CCA Security [BHK12]



Defining SIM-SO-CCA Security [BHK12]



A PKE scheme is SIM-SO-CCA secure if for all efficient $\mathcal{A}$ there exists an efficient $\mathcal{S}$ such that:

$$real^{\mathcal{A}} \approx_c ideal^{\mathcal{S}} \ .$$

PKE in Practice and Previous Results

Hybrid Encryption – KEM/DEM paradigm

PKE in Practice and Previous Results

Hybrid Encryption – KEM/DEM paradigm

- Asymmetric primitive to establish key (KEM)

PKE in Practice and Previous Results

Hybrid Encryption – KEM/DEM paradigm

- Asymmetric primitive to establish key (KEM)
- Symmetric primitive to encrypt the message (DEM)
  e.g. CTR, CBC, CCM, GCM blockcipher modes

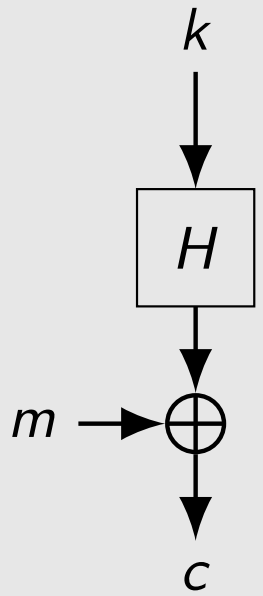
PKE in Practice and Previous Results

Hybrid Encryption – KEM/DEM paradigm

- Asymmetric primitive to establish key (KEM)
- Symmetric primitive to encrypt the message (DEM)
  e.g. CTR, CBC, CCM, GCM blockcipher modes

Previous Results

- DHIES, RSA-OAEP are SIM-SO-CCA secure [HJKS15]
- DEM: xor with the output of a random oracle



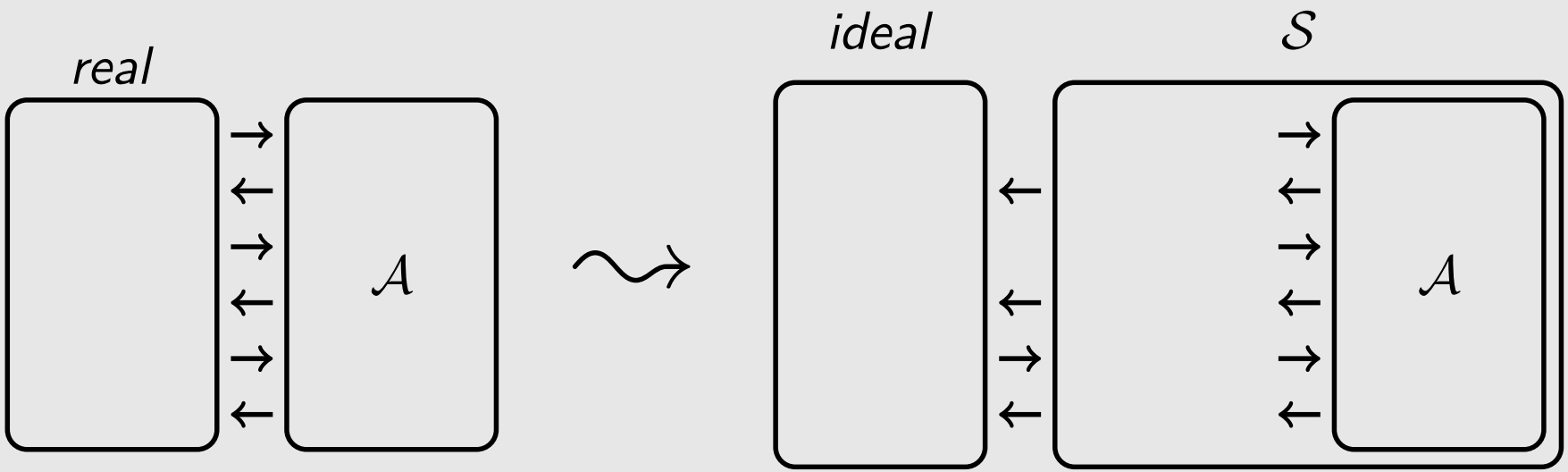
A Strategy for Proving SIM-SO-CCA Security

Given any adversary $\mathcal{A}$, construct a simulator $\mathcal{S}$.

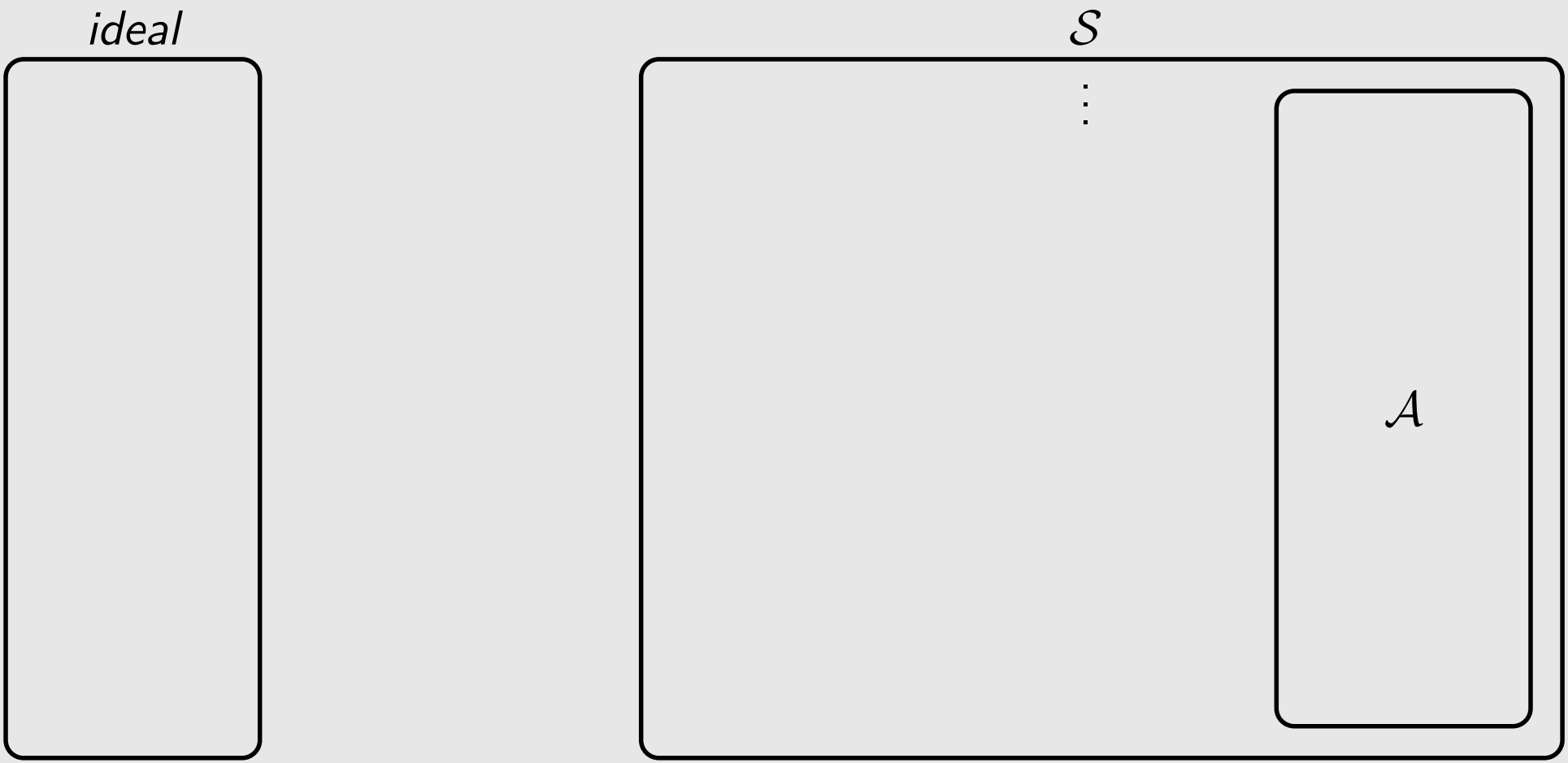
A Strategy for Proving SIM-SO-CCA Security

Given any adversary $\mathcal{A}$, construct a simulator $\mathcal{S}$.

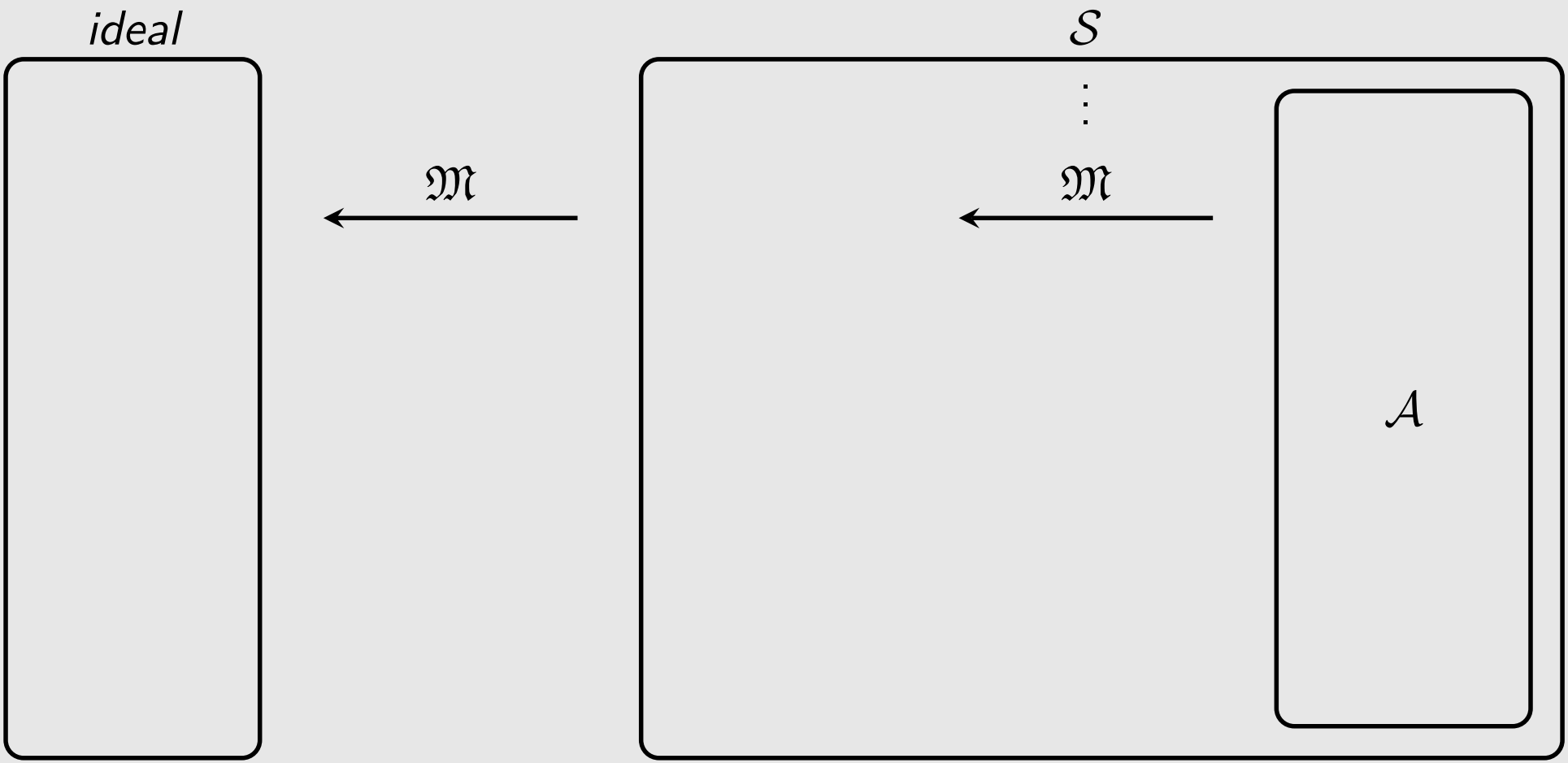
$\mathcal{S}$ (internally) runs $\mathcal{A}$ to draw the same conclusions as $\mathcal{A}$.



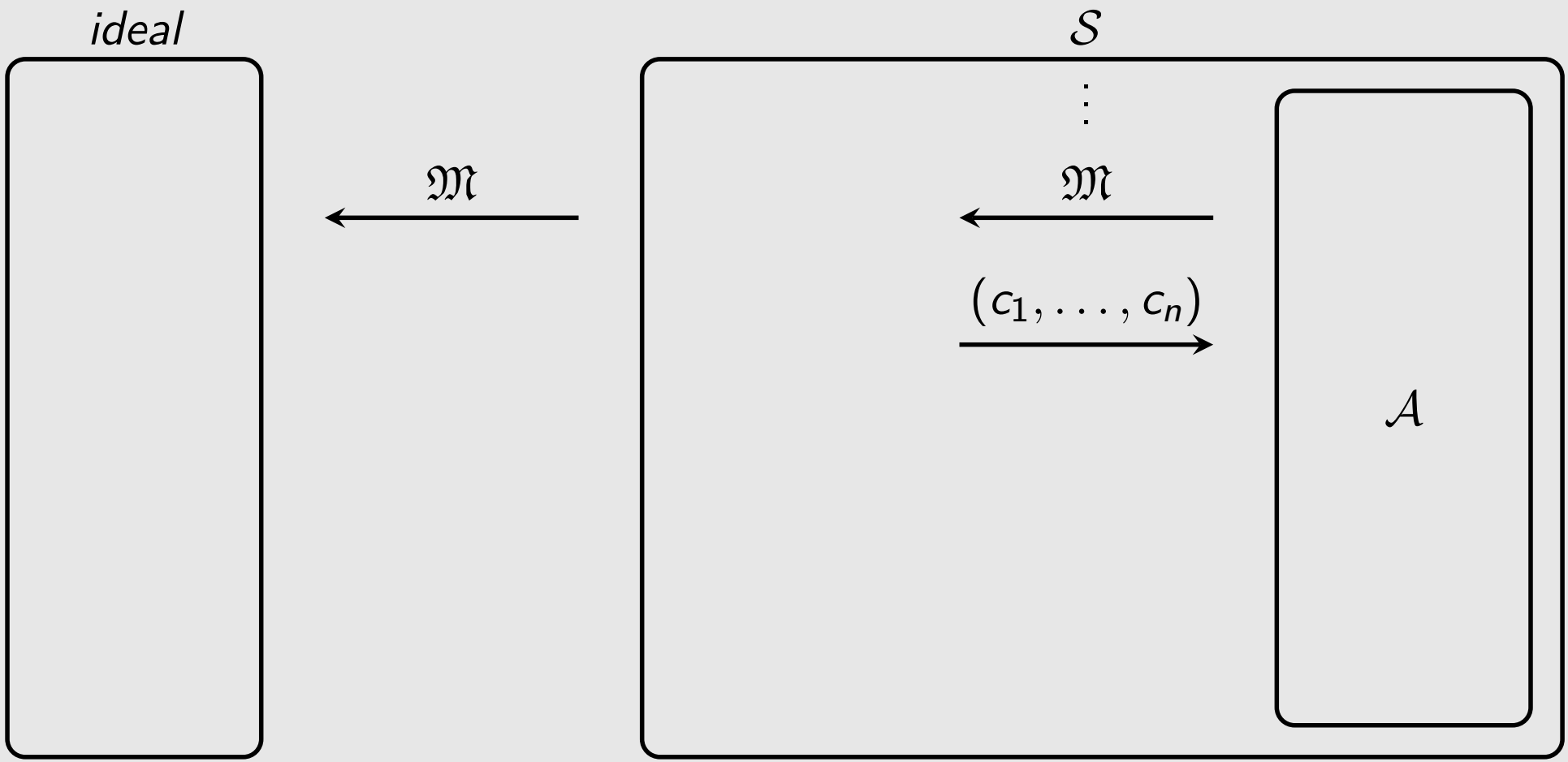
A Strategy for Proving SIM-SO-CCA Security



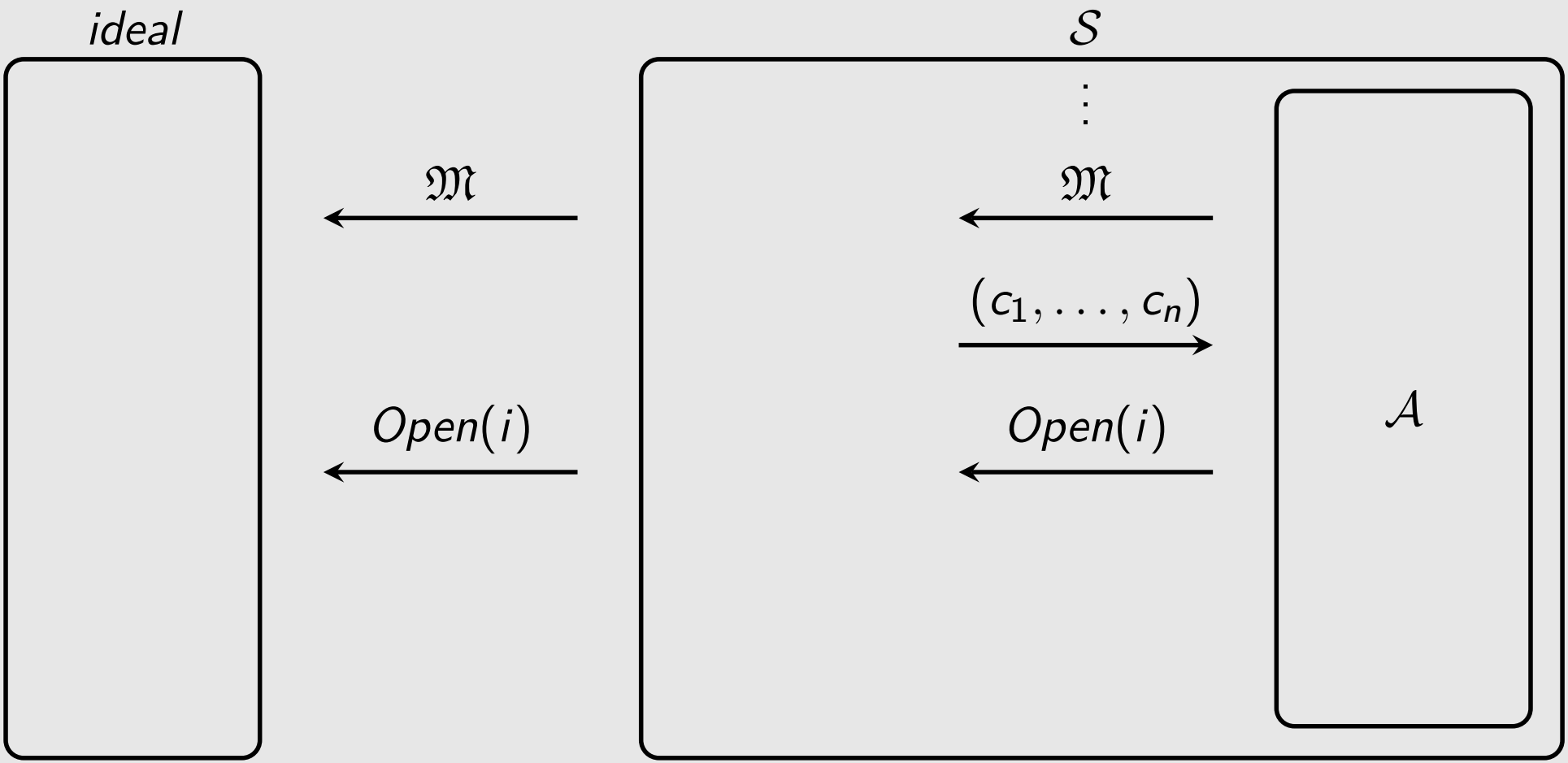
A Strategy for Proving SIM-SO-CCA Security



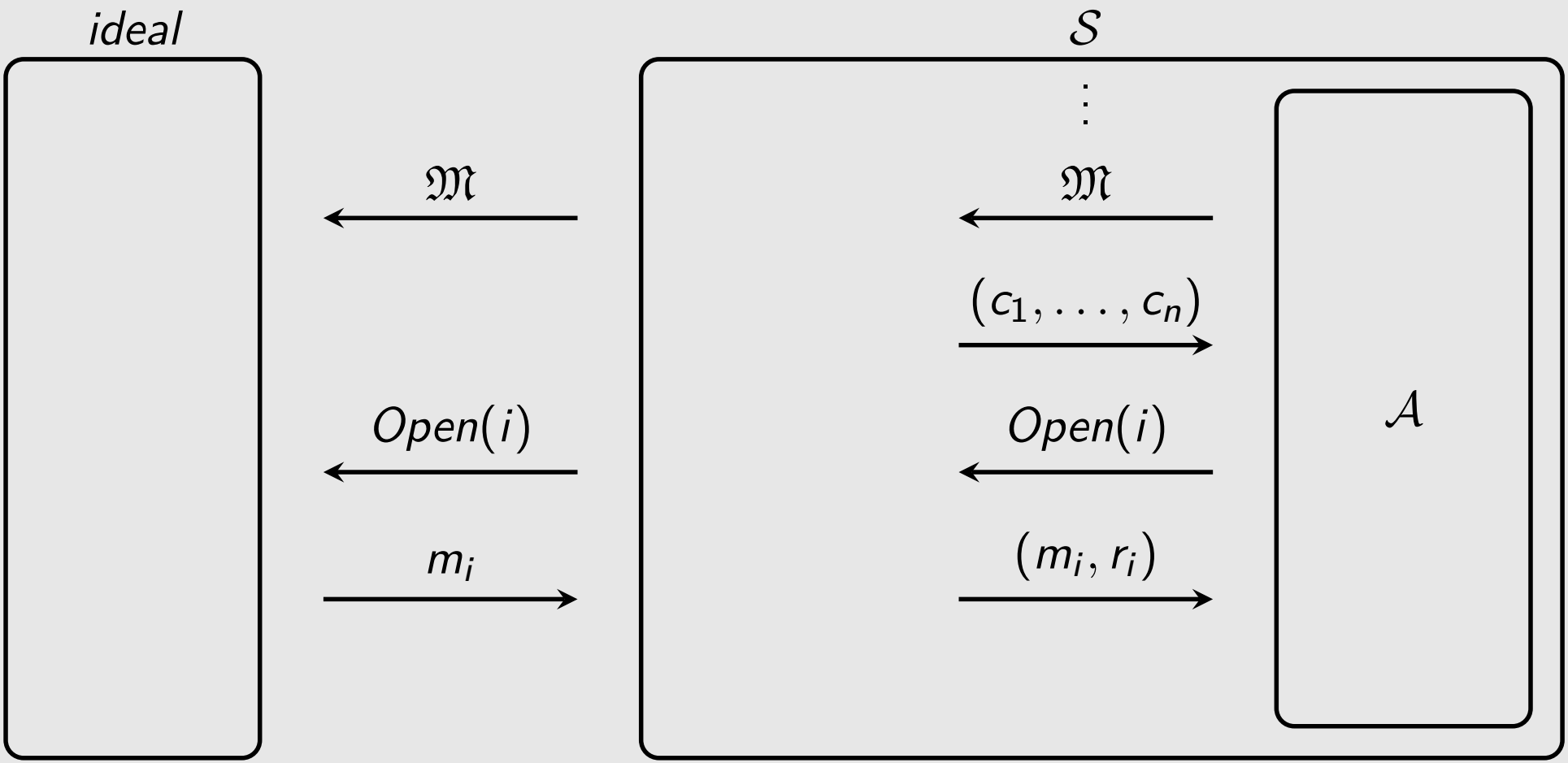
A Strategy for Proving SIM-SO-CCA Security



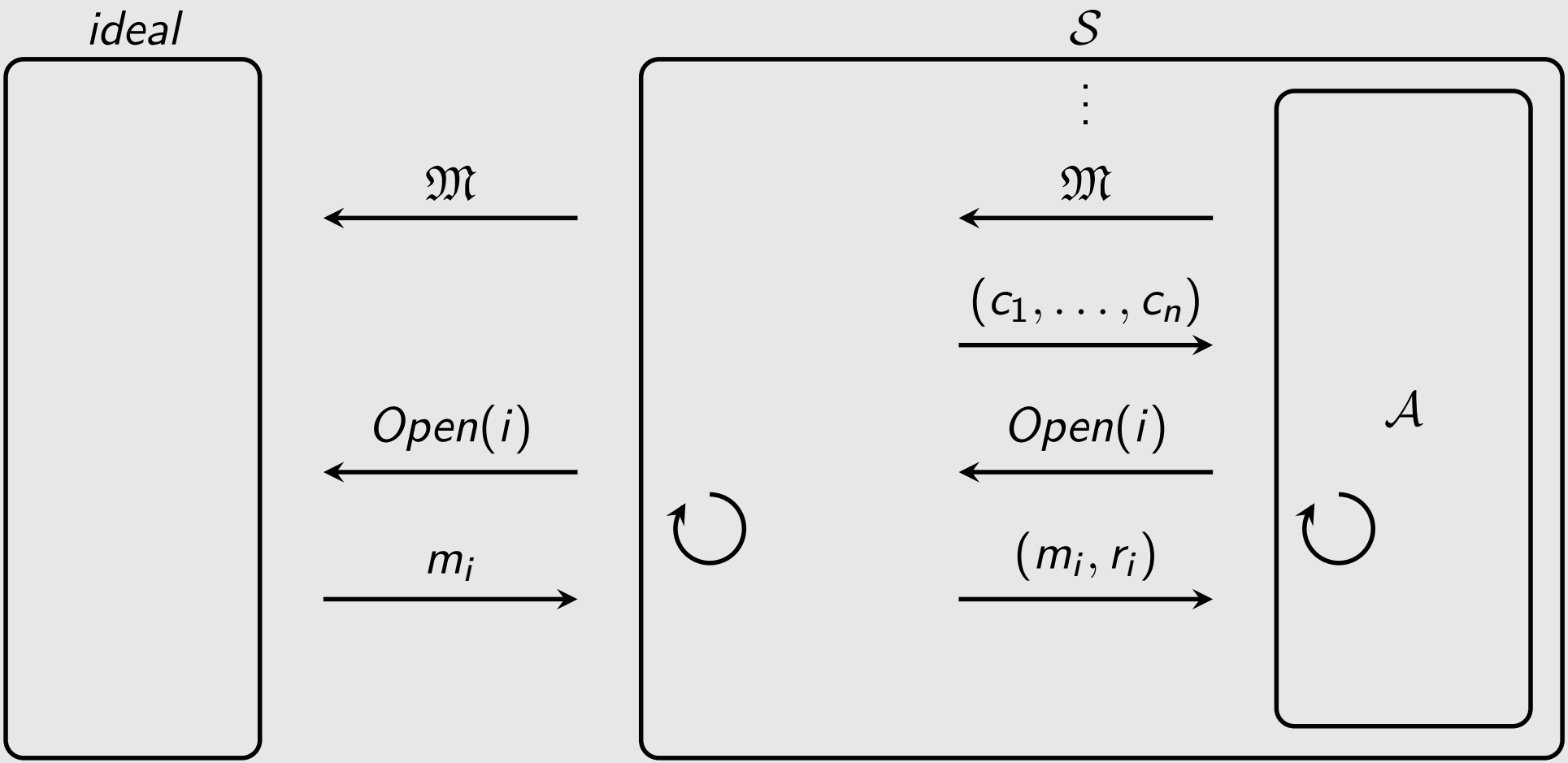
A Strategy for Proving SIM-SO-CCA Security



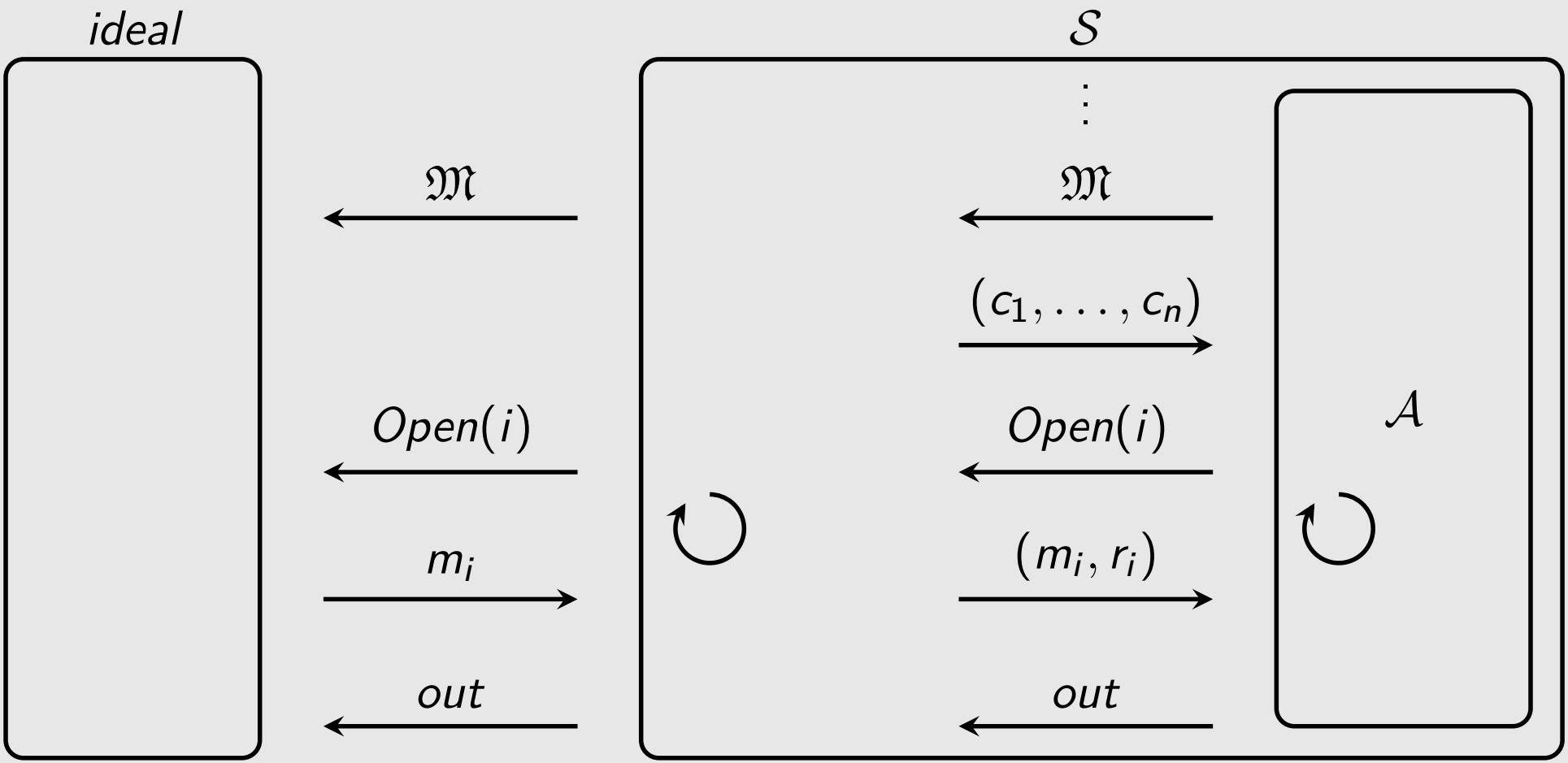
A Strategy for Proving SIM-SO-CCA Security



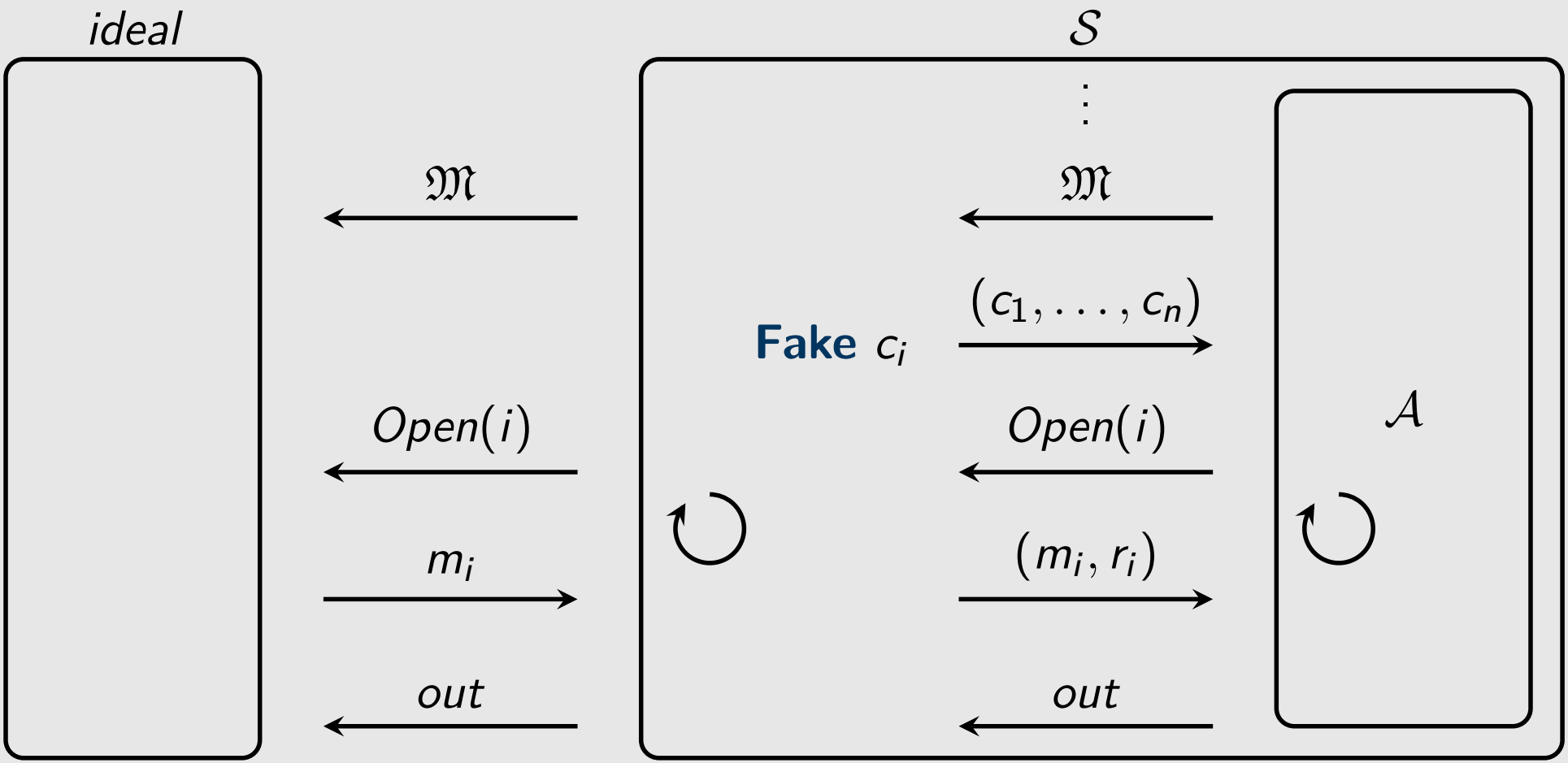
A Strategy for Proving SIM-SO-CCA Security



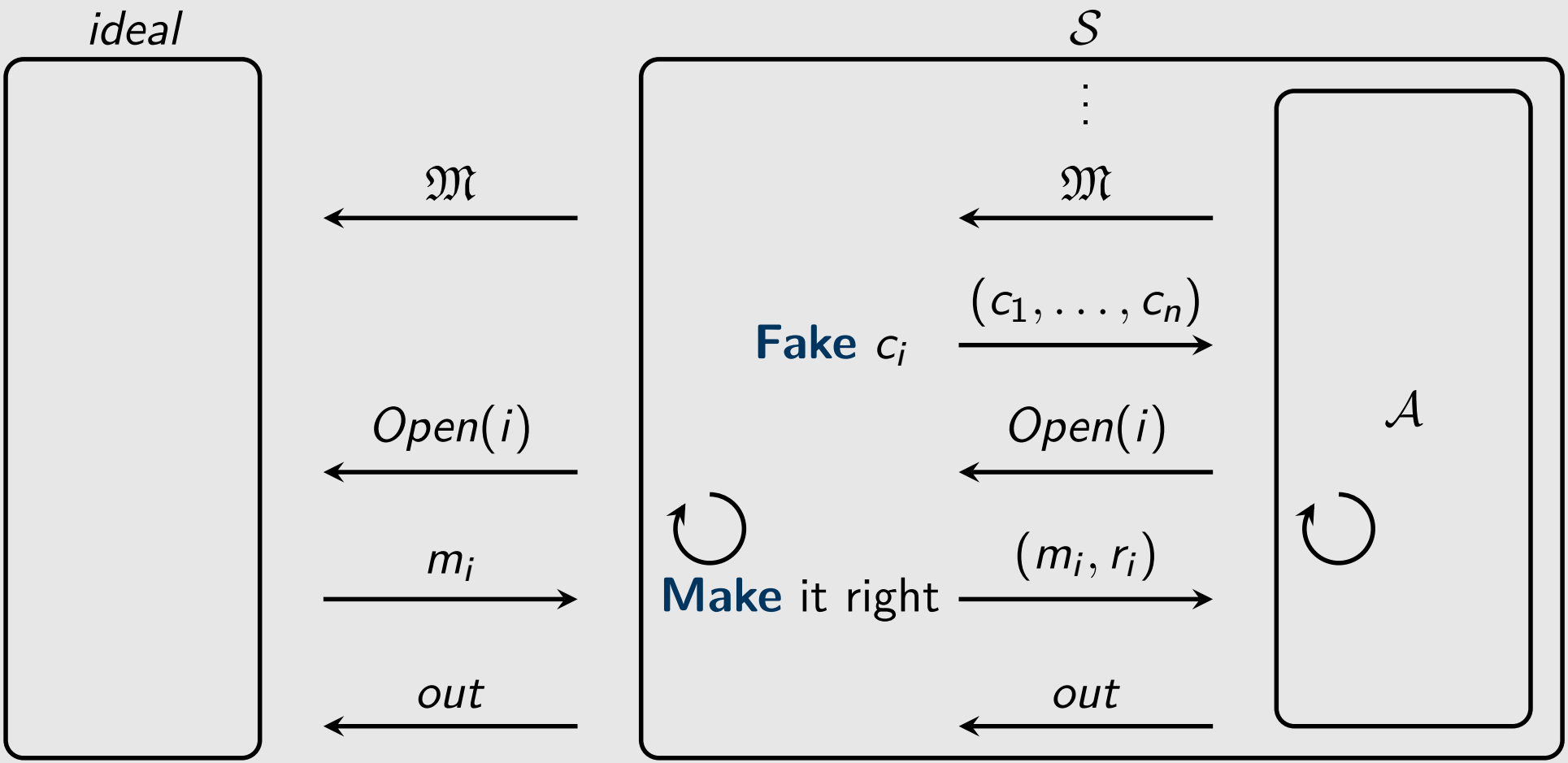
A Strategy for Proving SIM-SO-CCA Security



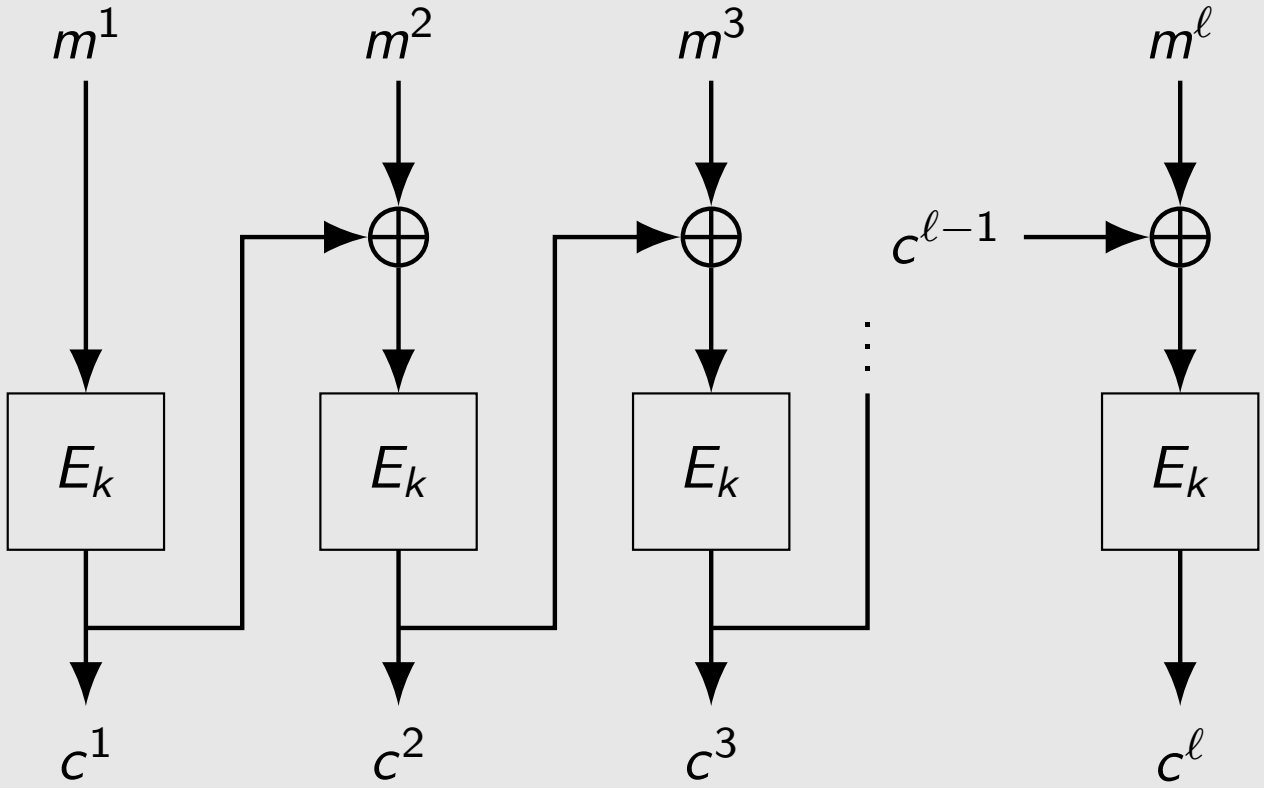
A Strategy for Proving SIM-SO-CCA Security



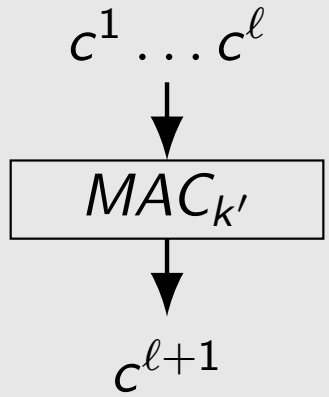
A Strategy for Proving SIM-SO-CCA Security



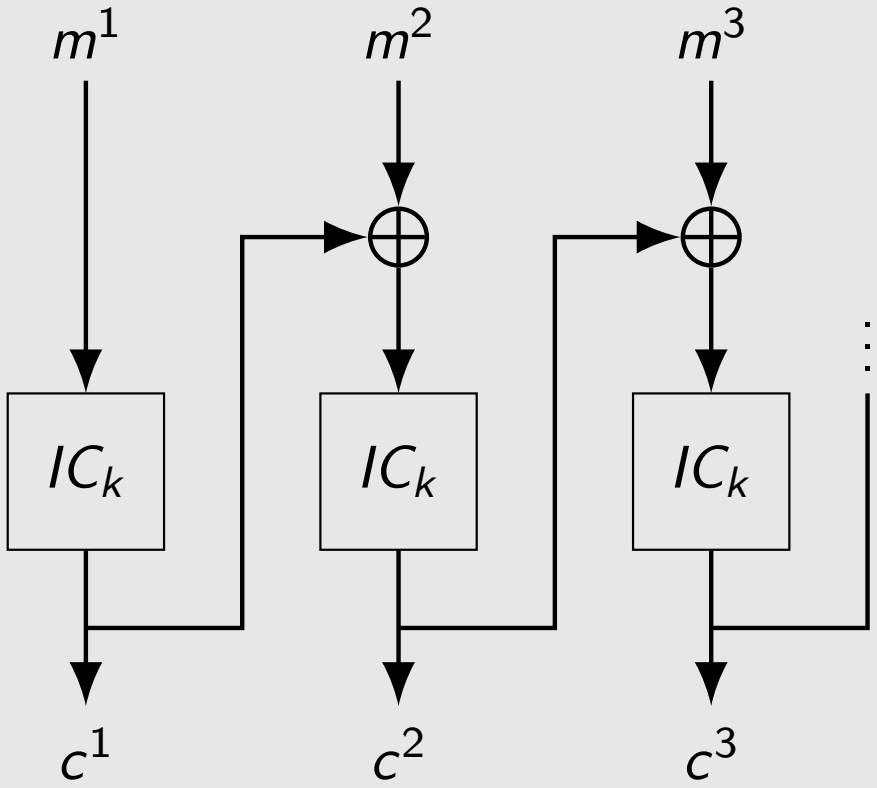
CBC Mode + MAC



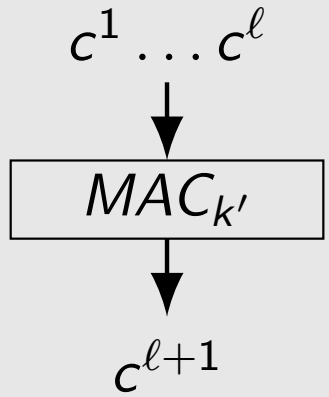
k : **blockcipher key**
k': **additional key material**



CBC Mode + MAC



k : **blockcipher key**
k': **additional key material**



Simulatable oracle DEMs

Definition 1 (Simulatable DEM)

A 'DEM' $(\mathsf{Enc}, \mathsf{Dec})$ with oracle access to a permutation π where

$$\mathsf{Enc}^{\pi} : \mathcal{K}' \times \mathcal{M} \to \mathcal{C}$$

Simulatable oracle DEMs

Definition 1 (Simulatable DEM)

A 'DEM' $(\mathsf{Enc}, \mathsf{Dec})$ with oracle access to a permutation π where

$$\mathsf{Enc}^{\pi} : \mathcal{K}' \times \mathcal{M} \to \mathcal{C}$$

is *simulatable* if there exist stateful algorithms **Fake**, **Make** where

$$\textbf{Fake} : \mathcal{K}' \to \mathcal{C} \qquad \textbf{Make} : \mathcal{M} \to \mathsf{Perm}$$

such that:

Simulatable oracle DEMs

Definition 1 (Simulatable DEM)

A 'DEM' $(\mathsf{Enc}, \mathsf{Dec})$ with oracle access to a permutation π where

$$\mathsf{Enc}^{\pi} : \mathcal{K}' \times \mathcal{M} \to \mathcal{C}$$

is *simulatable* if there exist stateful algorithms **Fake**, **Make** where

$$\textbf{Fake} : \mathcal{K}' \to \mathcal{C} \qquad \textbf{Make} : \mathcal{M} \to \mathsf{Perm}$$

such that:

1. If $(c \leftarrow \textbf{Fake}(k'); \tilde{\pi} \leftarrow \textbf{Make}(m))$ then $c = \mathsf{Enc}^{\tilde{\pi}}(k', m)$.

Simulatable oracle DEMs

Definition 1 (Simulatable DEM)

A 'DEM' $(\mathsf{Enc}, \mathsf{Dec})$ with oracle access to a permutation π where

$$\mathsf{Enc}^{\pi} : \mathcal{K}' \times \mathcal{M} \to \mathcal{C}$$

is *simulatable* if there exist stateful algorithms **Fake**, **Make** where

$$\textbf{Fake} : \mathcal{K}' \to \mathcal{C} \qquad \textbf{Make} : \mathcal{M} \to \mathsf{Perm}$$

such that:

1. If $(c \leftarrow \textbf{Fake}(k'); \tilde{\pi} \leftarrow \textbf{Make}(m))$ then $c = \mathsf{Enc}^{\tilde{\pi}}(k', m)$.
2. Running (**Fake**,**Make**) yields a uniform permutation.

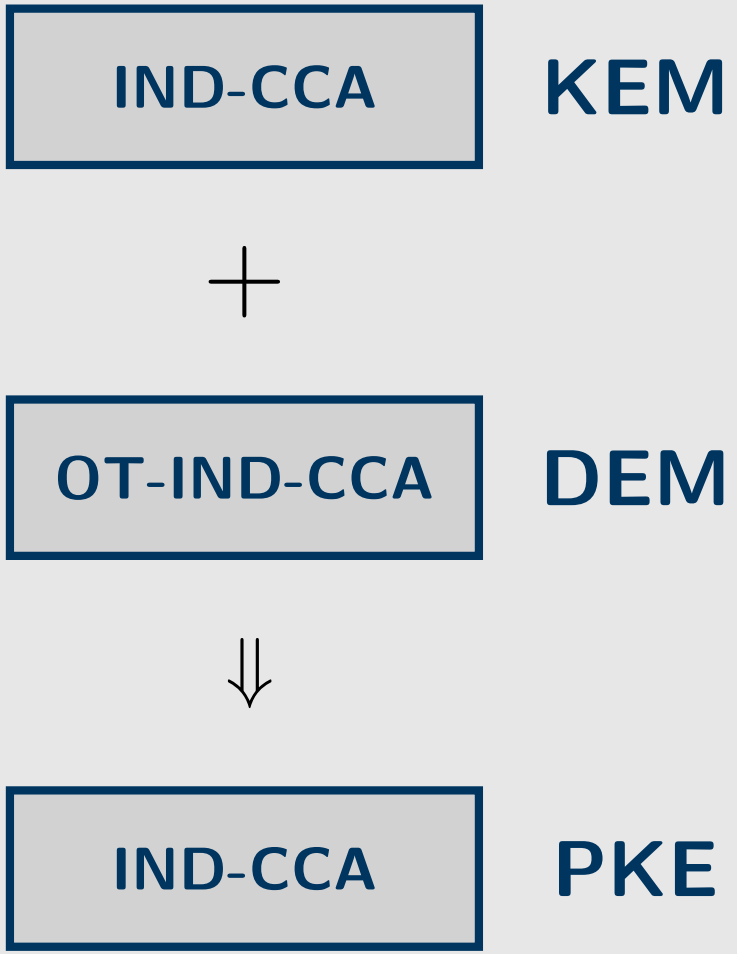
Security of Hybrid Encryption

KEM

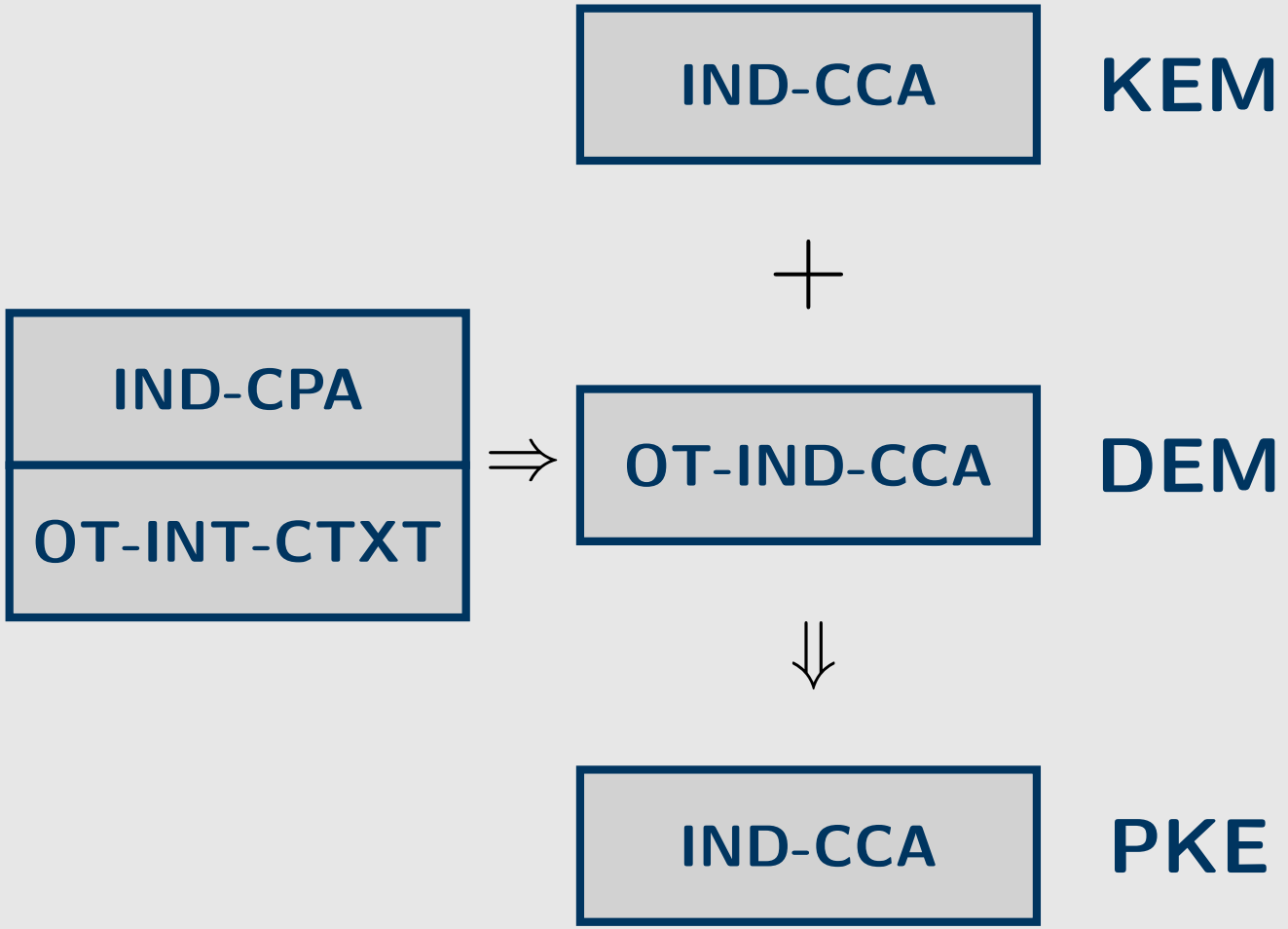
DEM

PKE

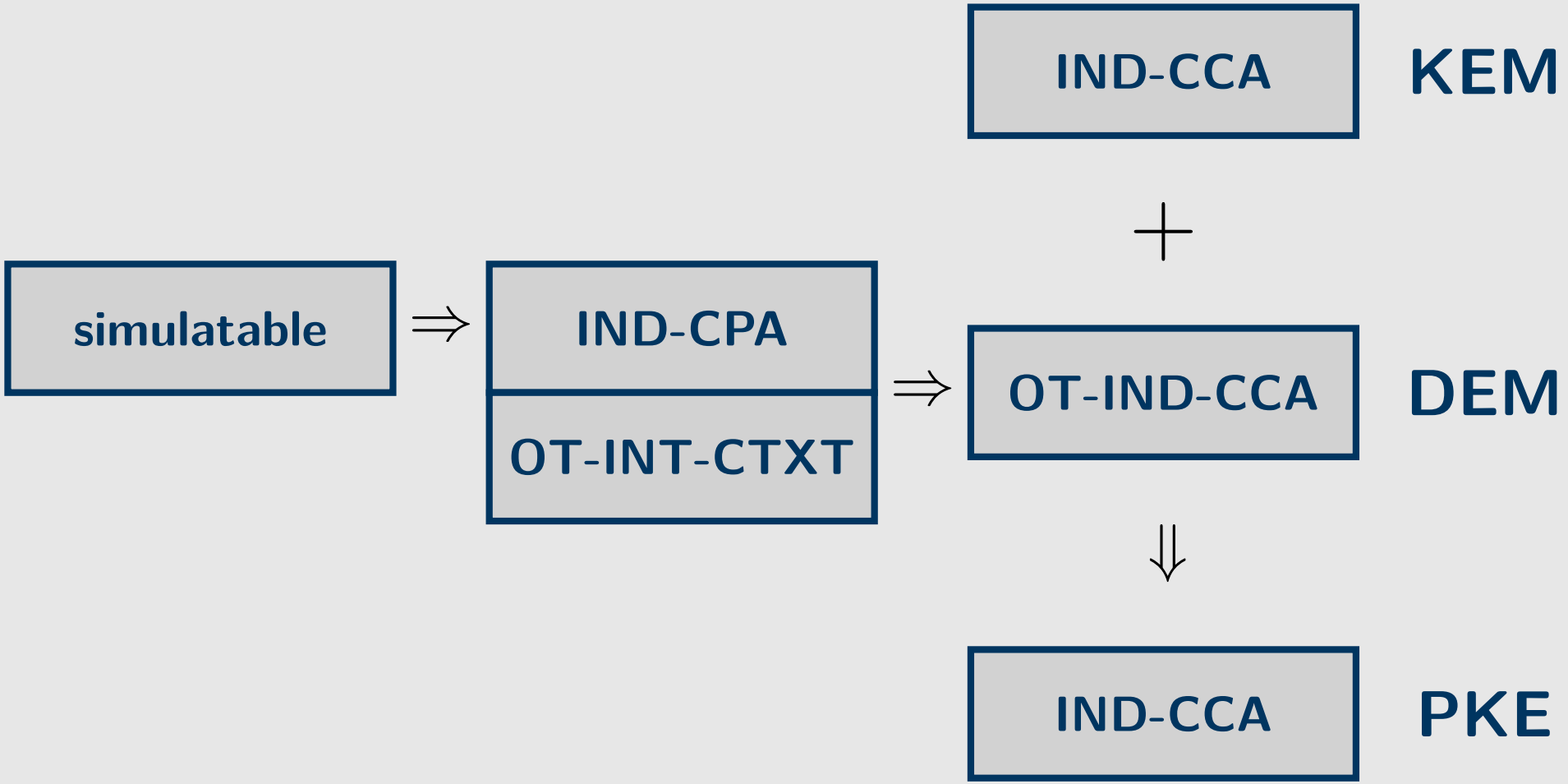
Security of Hybrid Encryption



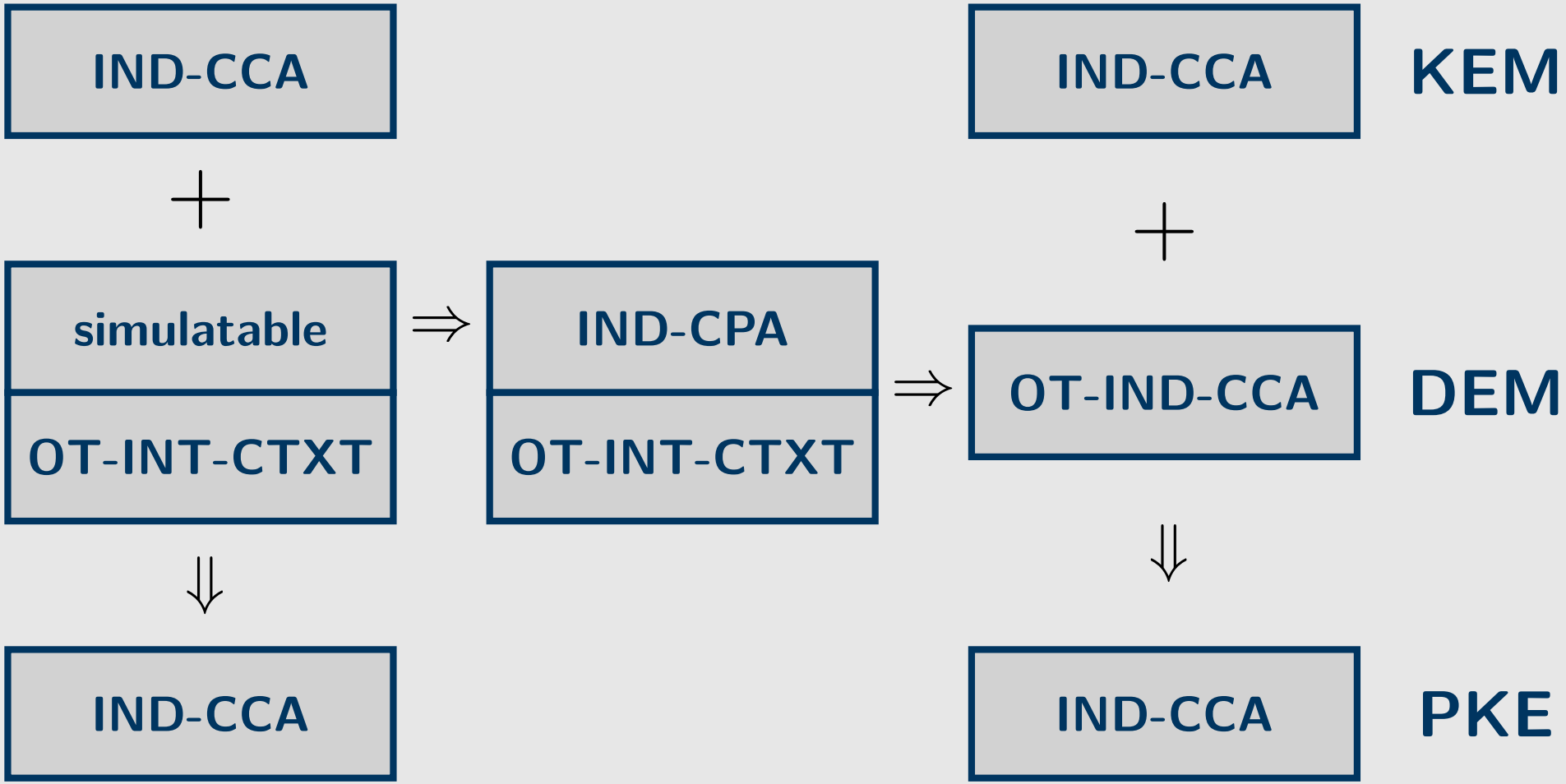
Security of Hybrid Encryption



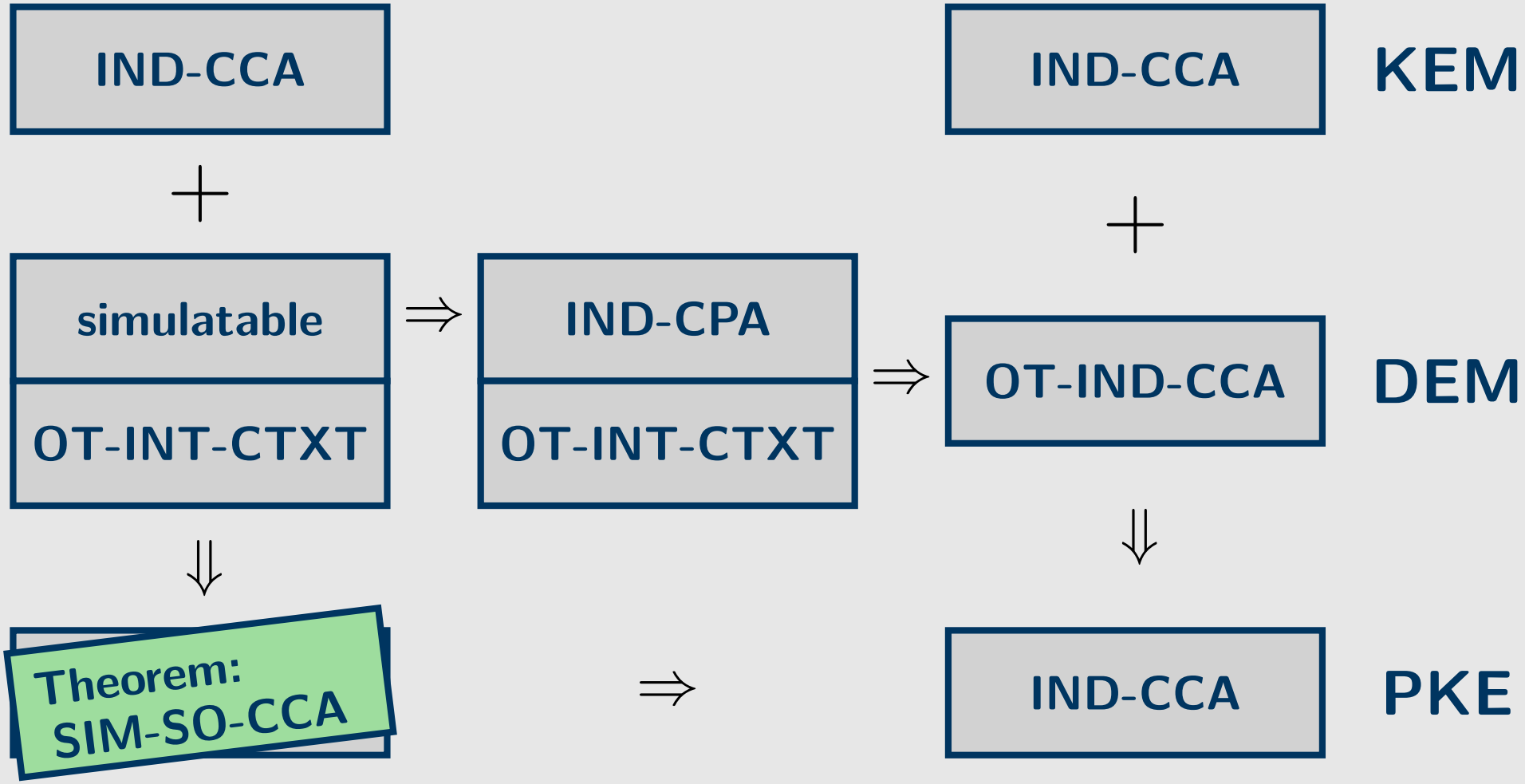
Security of Hybrid Encryption



Security of Hybrid Encryption



Security of Hybrid Encryption



Security of Hybrid Encryption

Theorem:

IND-CCA

KEM

DEM

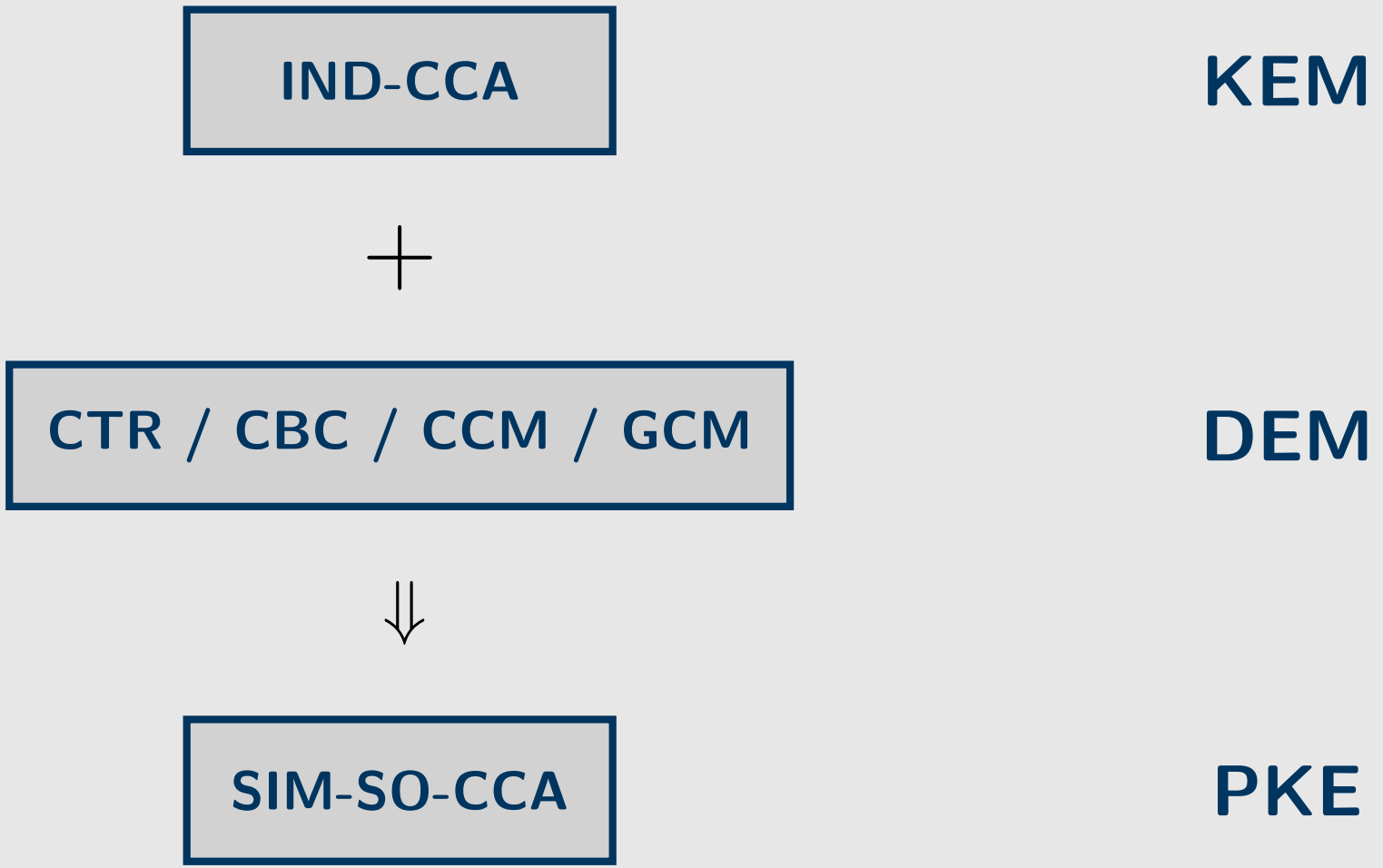
PKE

Security of Hybrid Encryption

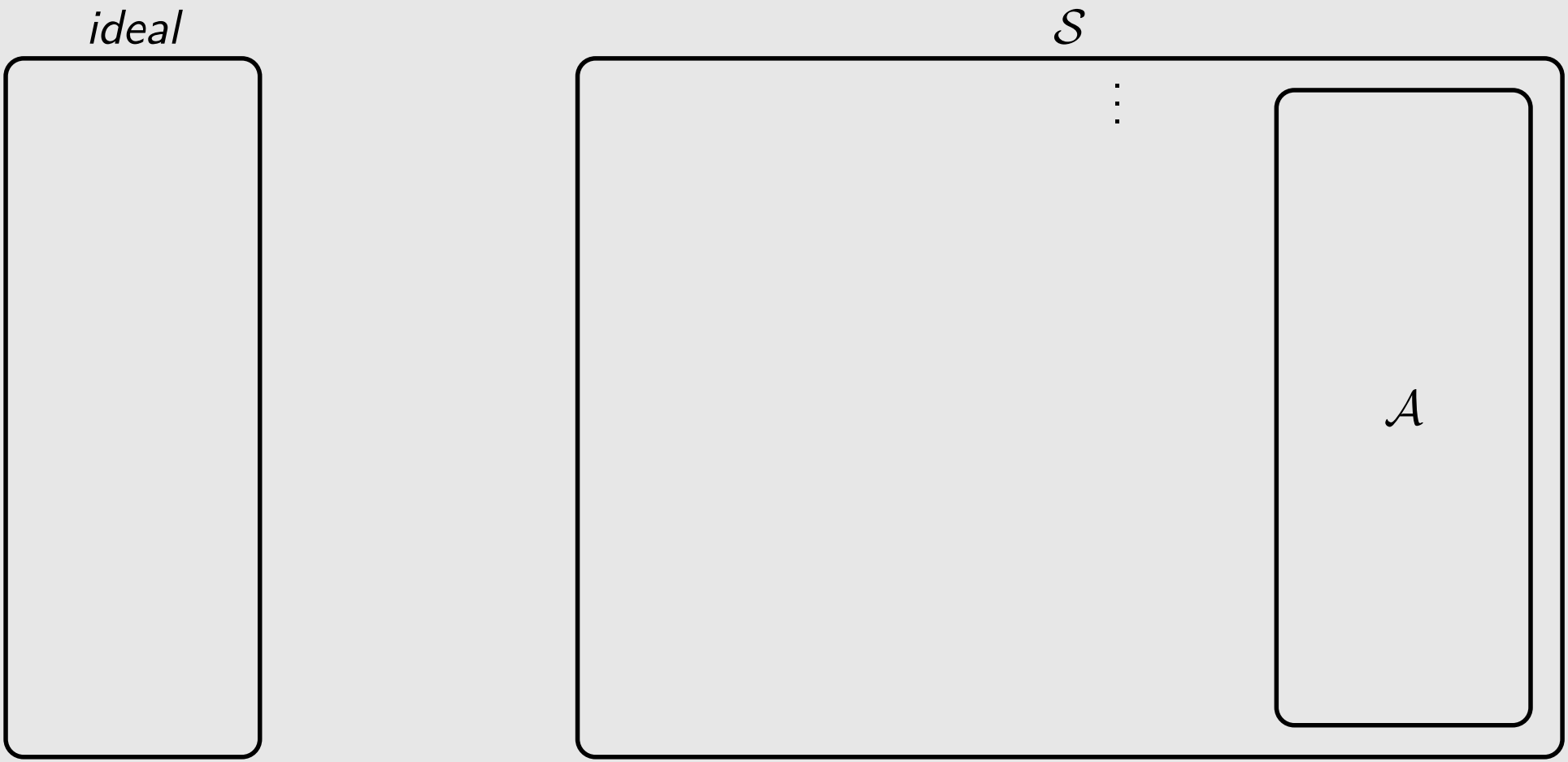
Theorem:

Security of Hybrid Encryption

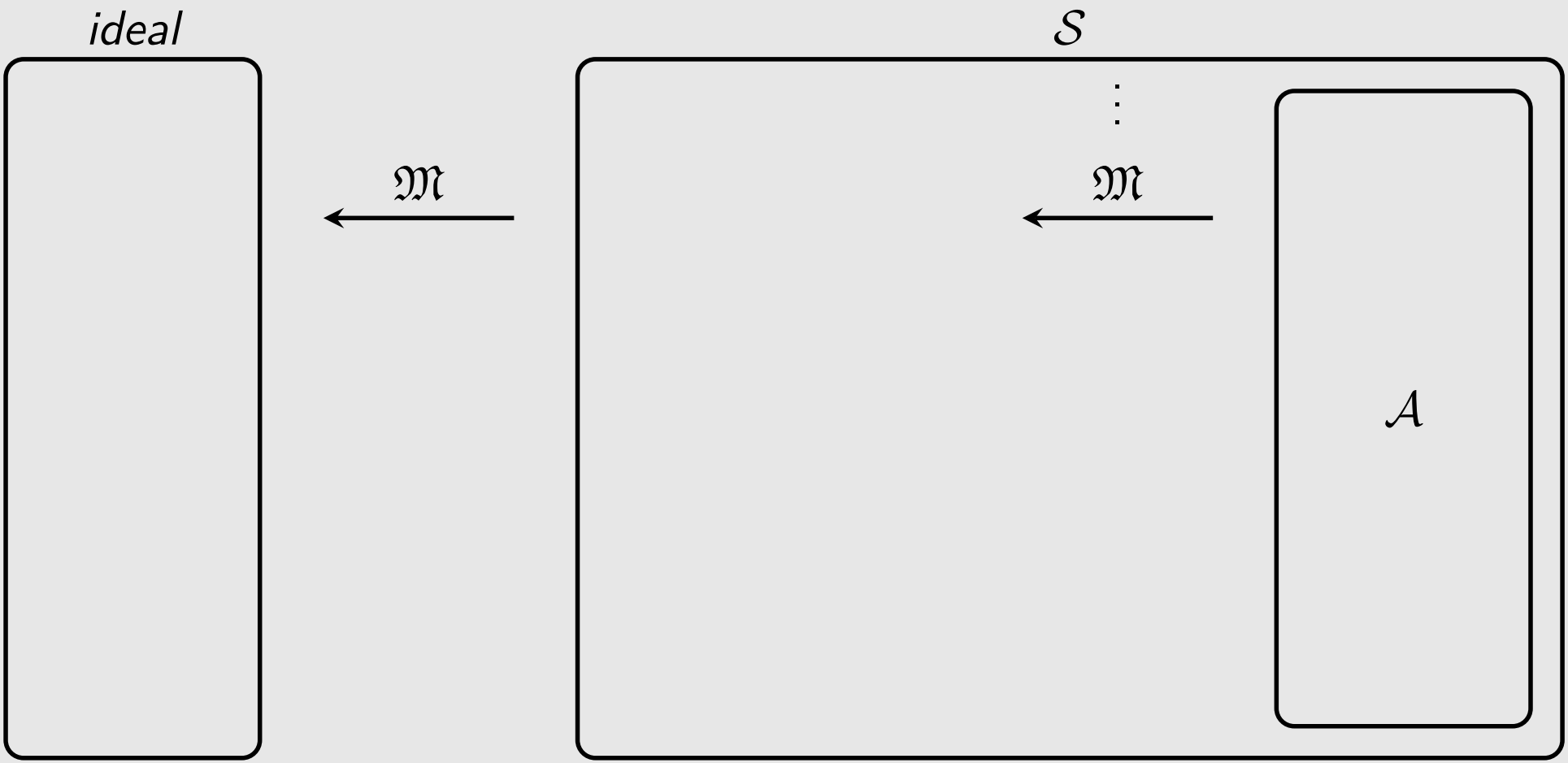
Theorem:



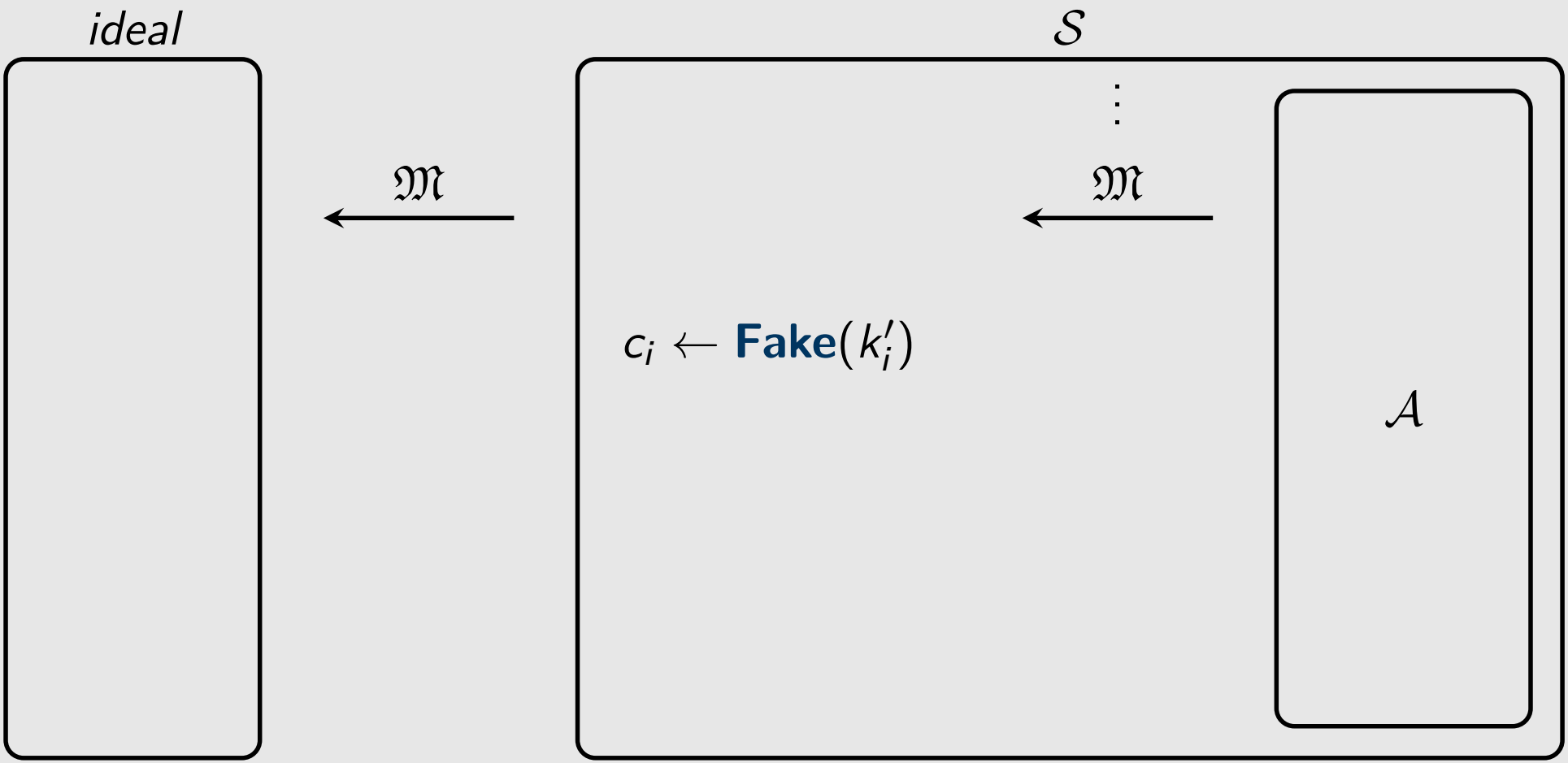
Intuition for the Proof



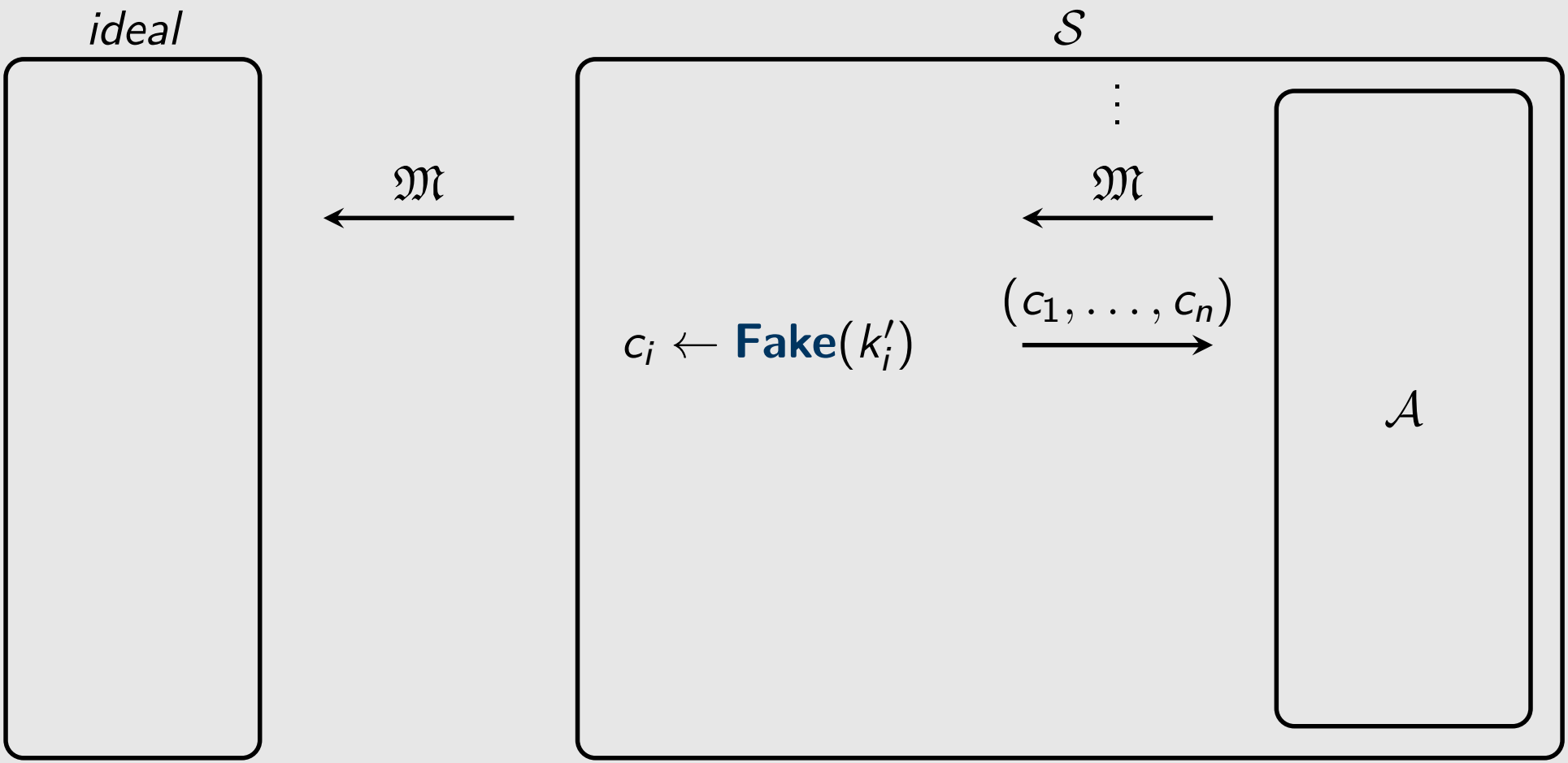
Intuition for the Proof



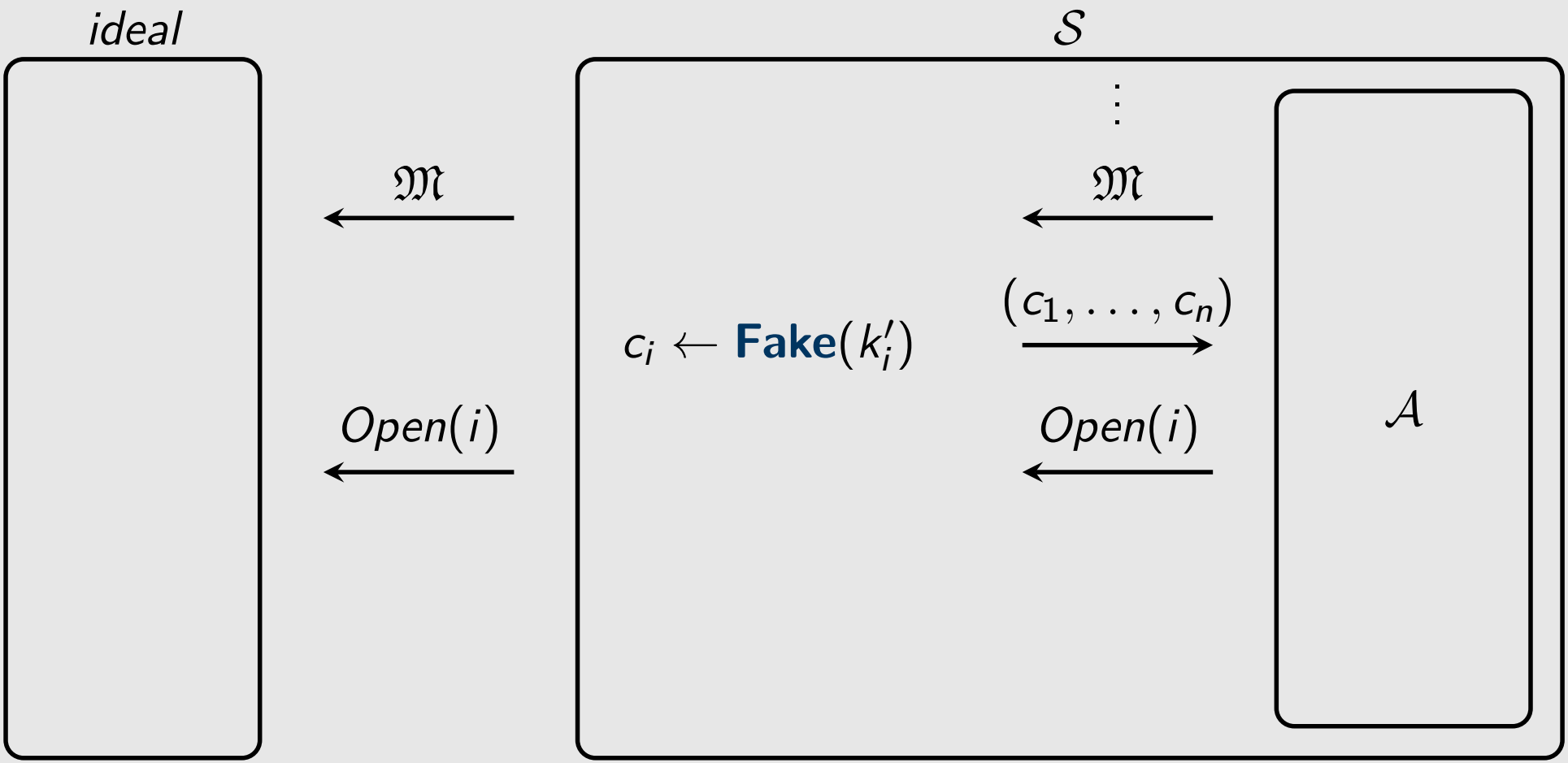
Intuition for the Proof



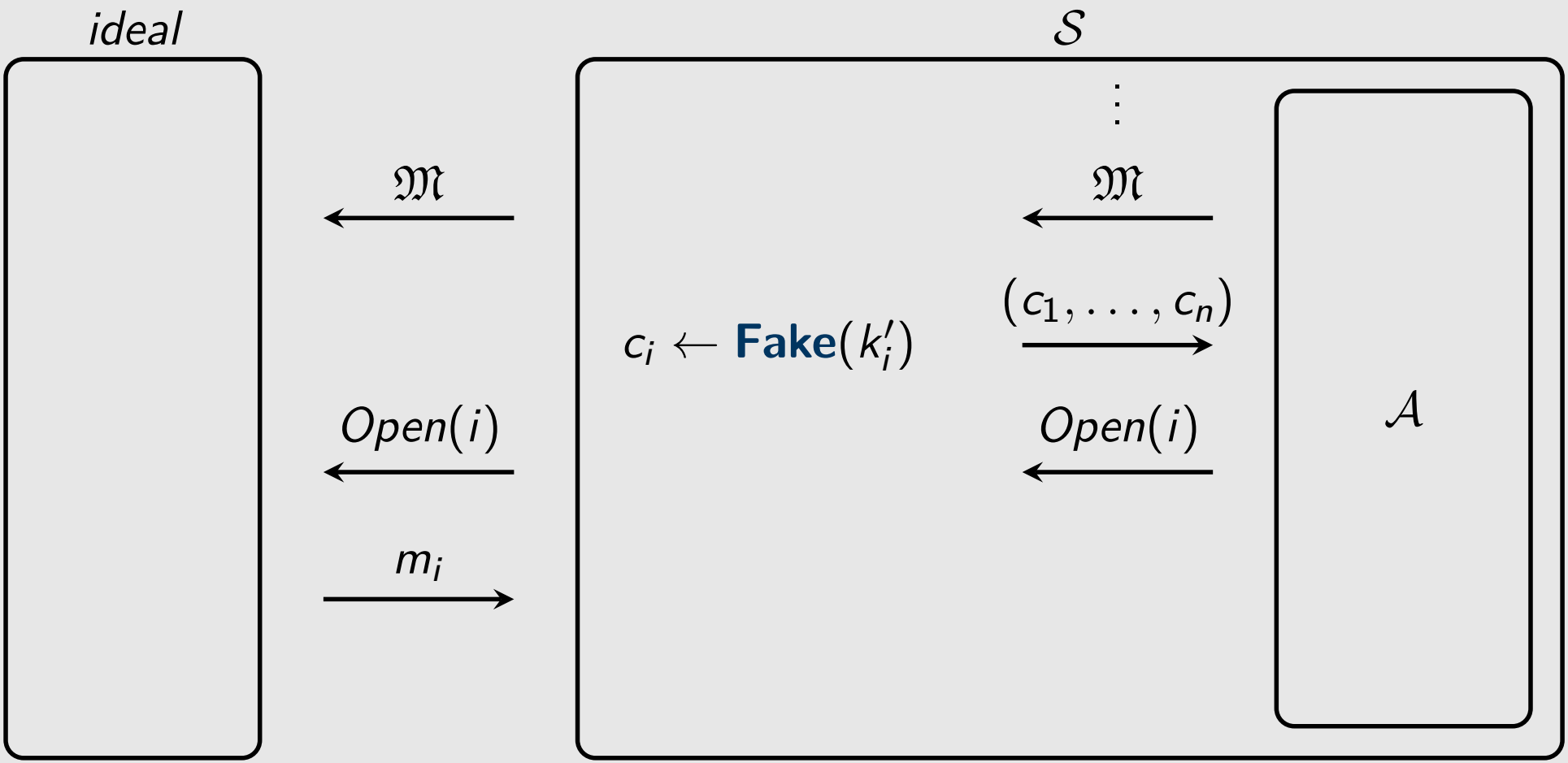
Intuition for the Proof



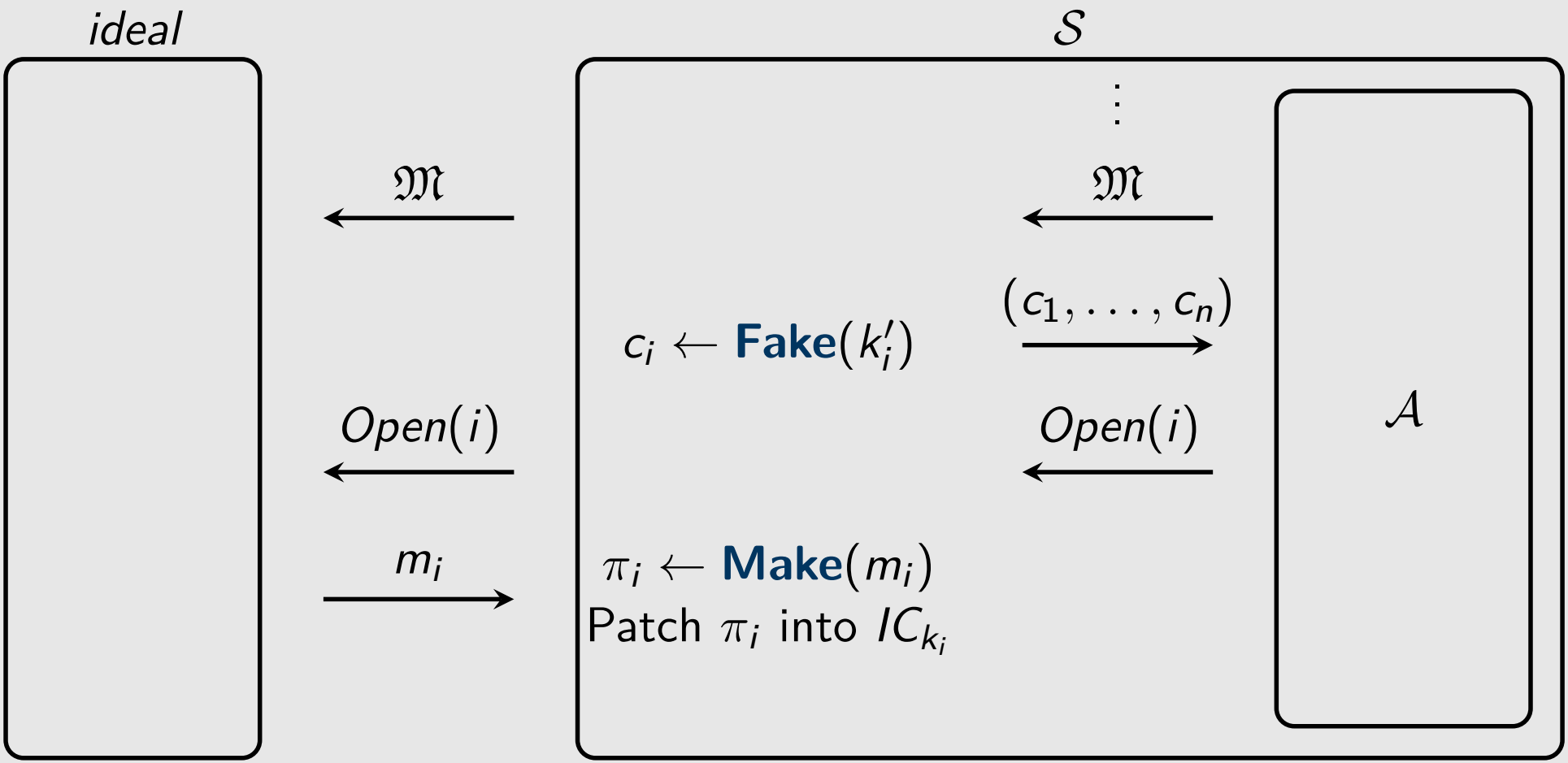
Intuition for the Proof



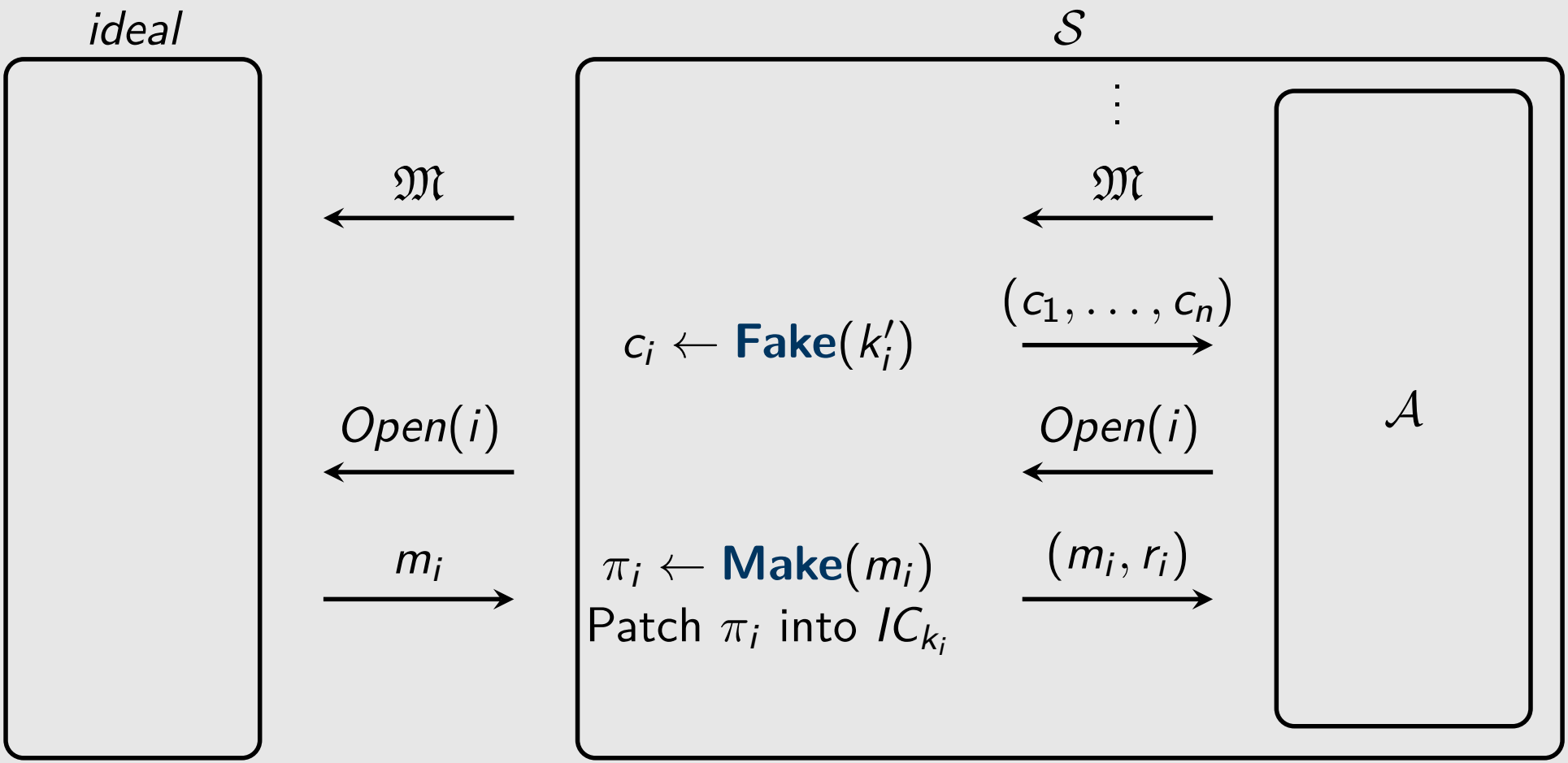
Intuition for the Proof



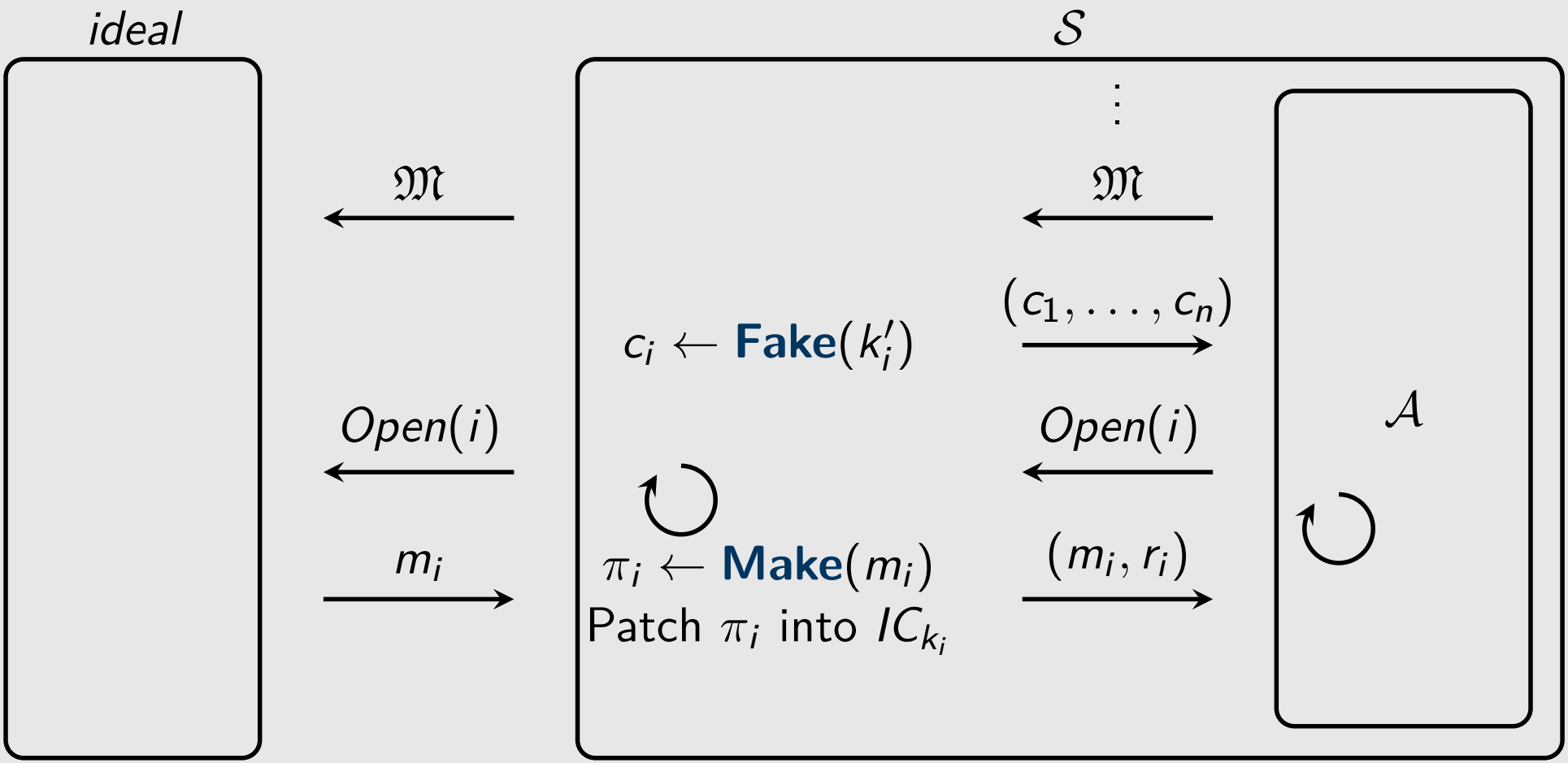
Intuition for the Proof



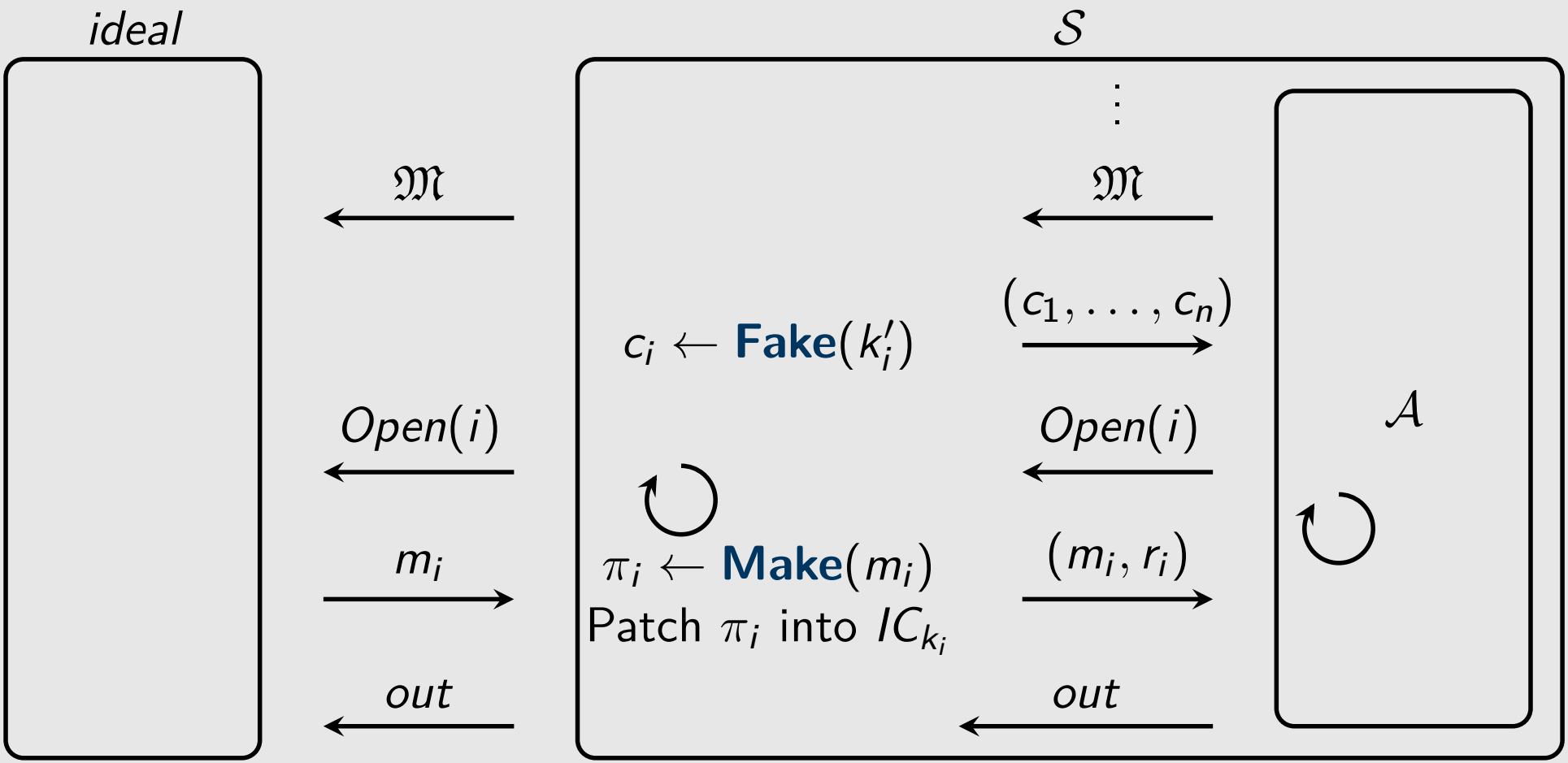
Intuition for the Proof



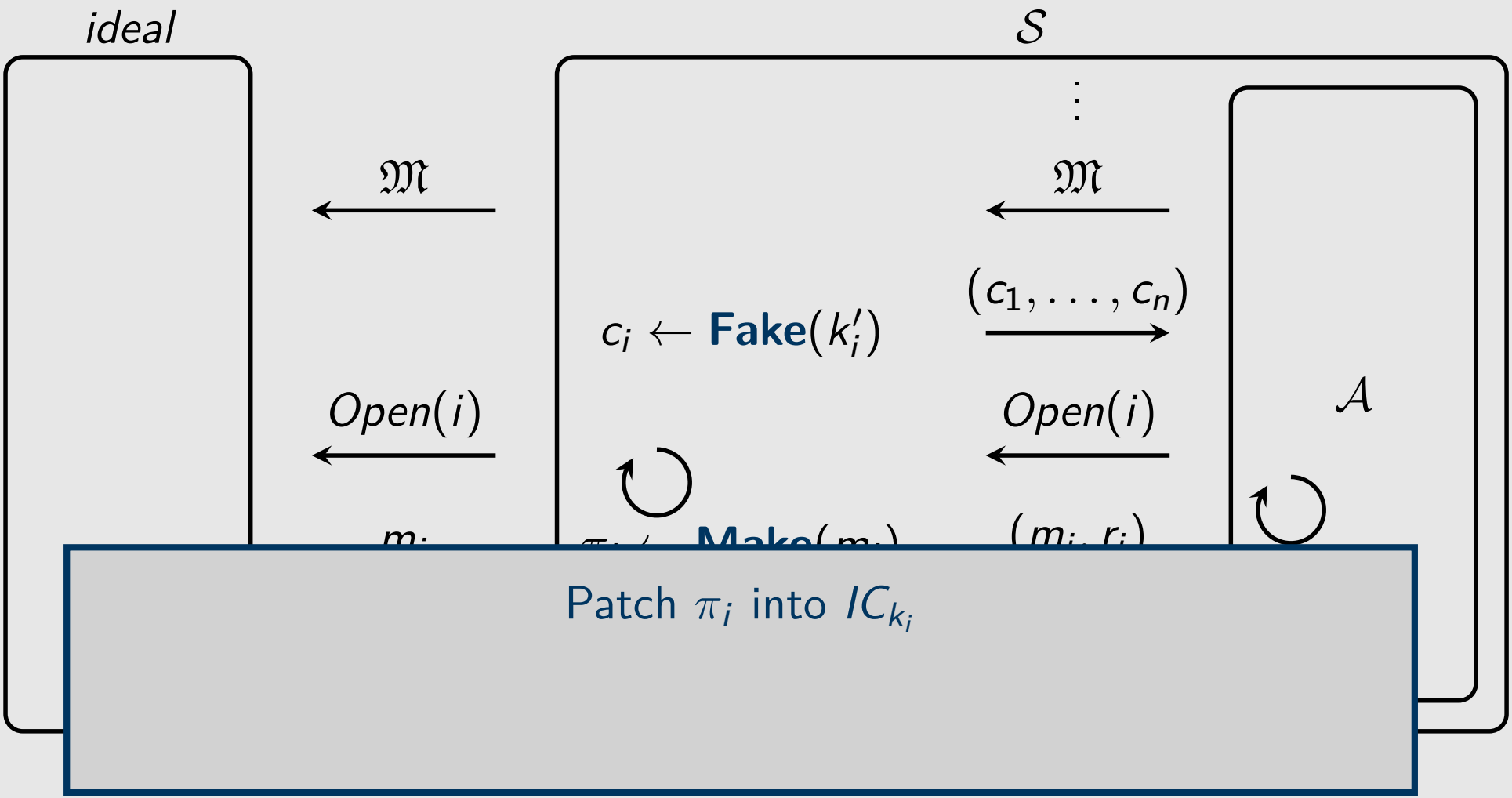
Intuition for the Proof



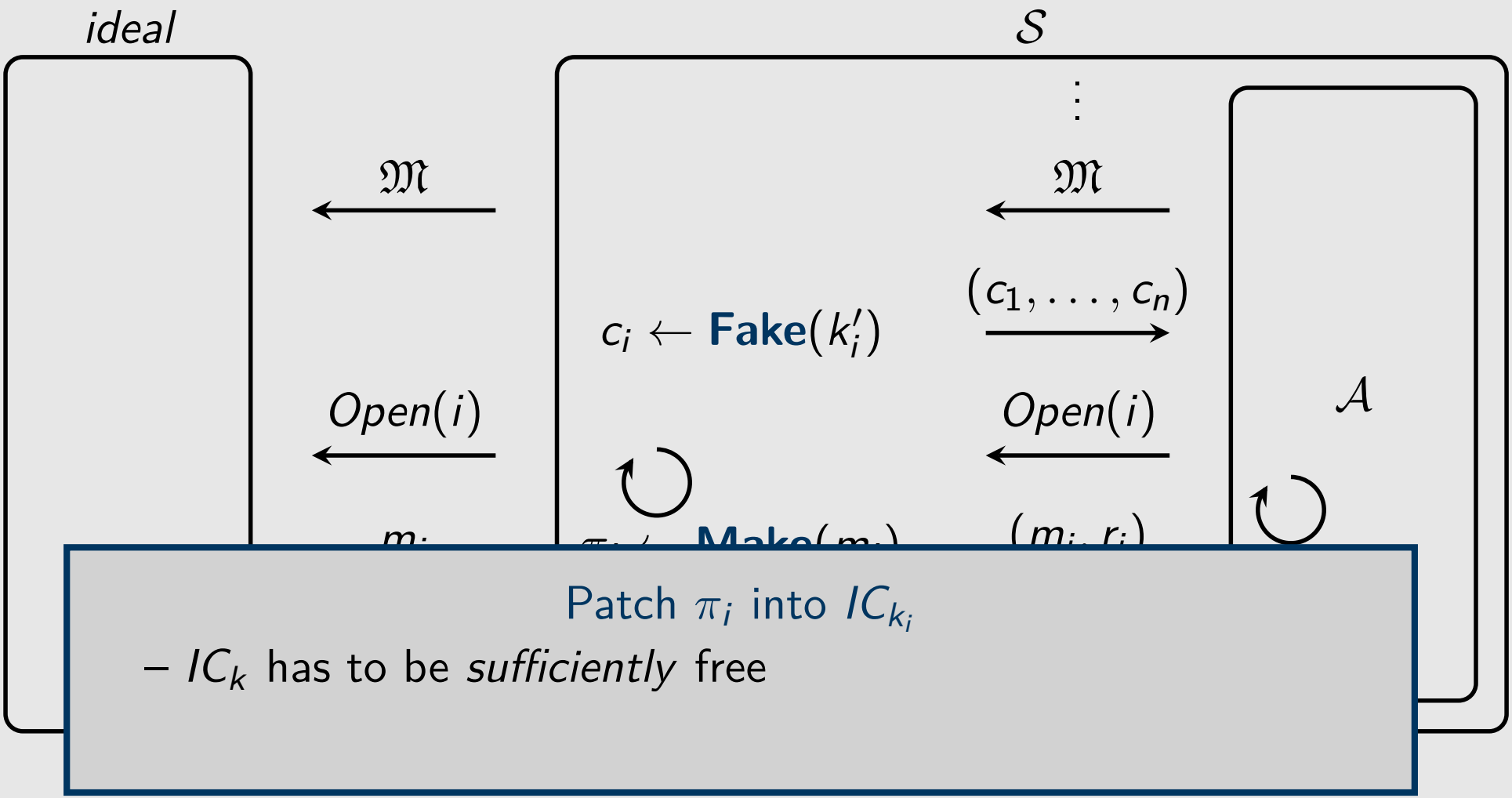
Intuition for the Proof



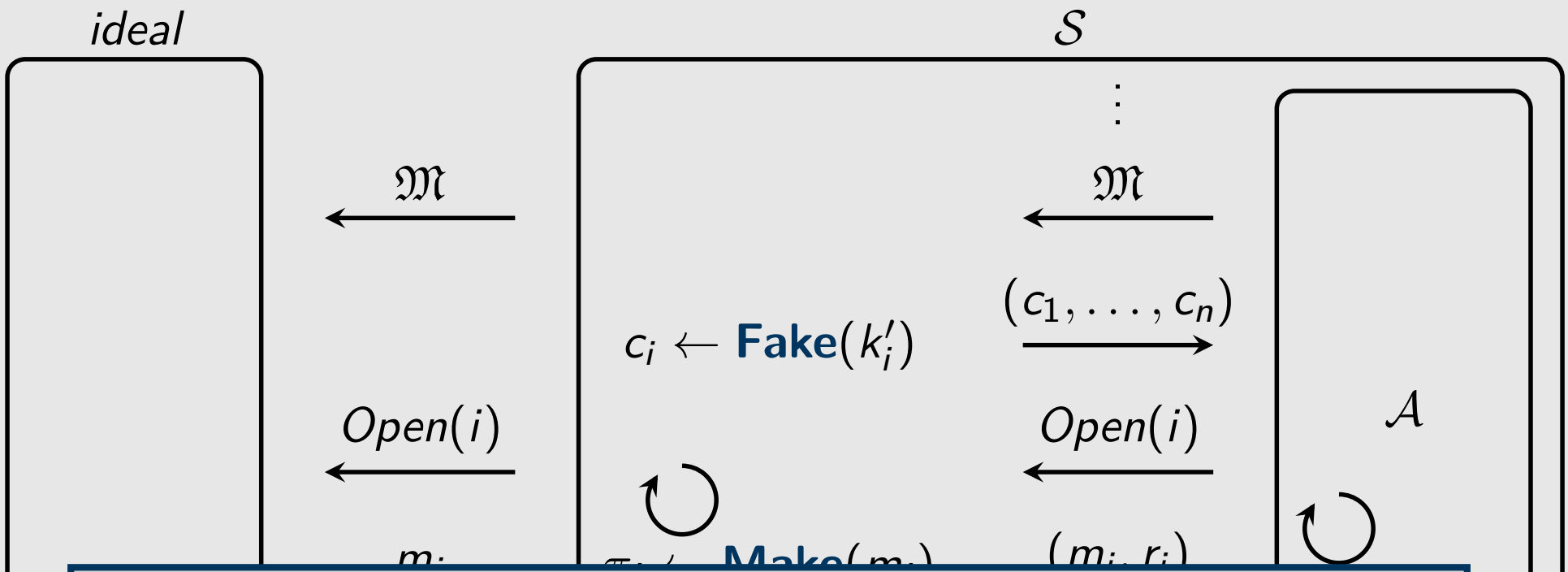
Intuition for the Proof



Intuition for the Proof



Intuition for the Proof



Patch π_i into IC_{k_i}

- IC_k has to be *sufficiently* free
- Ensured by standard security properties of KEM and DEM

In a nutshell

- We define a structural property of DEMs: *Simulatability*.

In a nutshell

- We define a structural property of DEMs: *Simulatability*.
- Simulatability of the DEM lifts security of the hybrid PKE from IND-CCA to SIM-SO-CCA security.

In a nutshell

- We define a structural property of DEMs: *Simulatability*.
- Simulatability of the DEM lifts security of the hybrid PKE from IND-CCA to SIM-SO-CCA security.
- Many practical hybrid PKE schemes are SIM-SO-CCA secure.

In a nutshell

- We define a structural property of DEMs: *Simulatability*.
- Simulatability of the DEM lifts security of the hybrid PKE from IND-CCA to SIM-SO-CCA security.
- Many practical hybrid PKE schemes are SIM-SO-CCA secure.

Proof Sketch

Ideal cipher: $(IC_k)_{k \in \mathcal{K}}$, IC_k random permutation.

Let $\boxed{k, k'}$ denote a key encapsulation of (k, k').

Proof Sketch

Ideal cipher: $(IC_k)_{k\in\mathcal{K}}$, IC_k random permutation.

Let $\boxed{k, k'}$ denote a key encapsulation of (k, k').

Let $(\boxed{k, k'}, \mathrm{Enc}^{IC_k}(k', m))$ be the hybrid encryption of m.

Proof Sketch

Ideal cipher: $(IC_k)_{k \in \mathcal{K}}$, IC_k random permutation.

Let $\boxed{k, k'}$ denote a key encapsulation of (k, k').

Let $(\boxed{k, k'}, \mathrm{Enc}^{IC_k}(k', m))$ be the hybrid encryption of m.

Ensure that IC_k remains unevaluated until $\mathcal{A}$ queries *Open*.

Proof Sketch

Ideal cipher: $(IC_k)_{k\in\mathcal{K}}$, IC_k random permutation.

Let $\boxed{k, k'}$ denote a key encapsulation of (k, k').

Let $(\boxed{k, k'}, \mathrm{Enc}^{IC_k}(k', m))$ be the hybrid encryption of m.

Ensure that IC_k remains unevaluated until $\mathcal{A}$ queries *Open*.

- IND-CCA secure KEM: (k, k') computationally hidden.

Proof Sketch

Ideal cipher: $(IC_k)_{k\in\mathcal{K}}$, IC_k random permutation.

Let $\boxed{k, k'}$ denote a key encapsulation of (k, k').

Let $(\boxed{k, k'}, \mathrm{Enc}^{IC_k}(k', m))$ be the hybrid encryption of m.

Ensure that IC_k remains unevaluated until $\mathcal{A}$ queries *Open*.

- IND-CCA secure KEM: (k, k') computationally hidden.
- OT-INT-CTXT secure DEM: $\mathcal{A}$ cannot force an evaluation of IC_k by querying $\mathrm{Dec}(\boxed{k, k'}, \ldots)$.

In a nutshell

- We define a structural property of DEMs: *Simulatability*.

In a nutshell

- We define a structural property of DEMs: *Simulatability*.
- Simulatability of the DEM lifts security of the hybrid PKE from IND-CCA to SIM-SO-CCA security.

In a nutshell

- We define a structural property of DEMs: *Simulatability*.
- Simulatability of the DEM lifts security of the hybrid PKE from IND-CCA to SIM-SO-CCA security.
- Many practical hybrid PKE schemes are SIM-SO-CCA secure.

In a nutshell

- We define a structural property of DEMs: *Simulatability*.
- Simulatability of the DEM lifts security of the hybrid PKE from IND-CCA to SIM-SO-CCA security.
- Many practical hybrid PKE schemes are SIM-SO-CCA secure.