RUB

RUHR-UNIVERSITÄT BOCHUM

Standard Security Does Imply Security Against Selective Opening for Markov Distributions

TCC 2016-A, Tel Aviv, January 11th, 2016

Georg Fuchsbauer, **Felix Heuer**, Eike Kiltz and Krzysztof Pietrzak

HGI - Ruhr University Bochum, IST Austria

hgi
Horst Görtz Institut für IT-Sicherheit

Selective Opening Attacks

Selective Opening Attacks

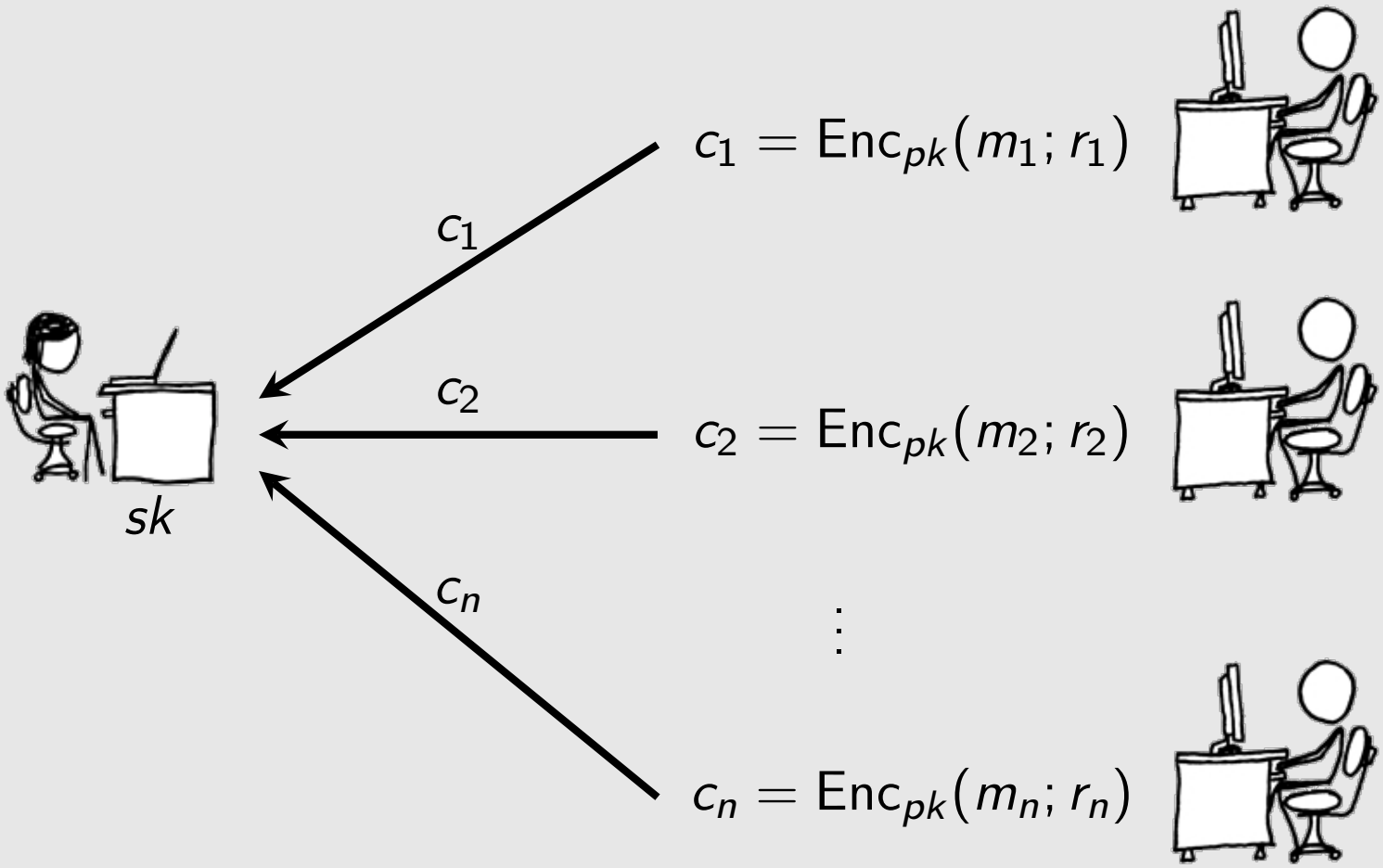


Image source: xkcd.com

Selective Opening Attacks

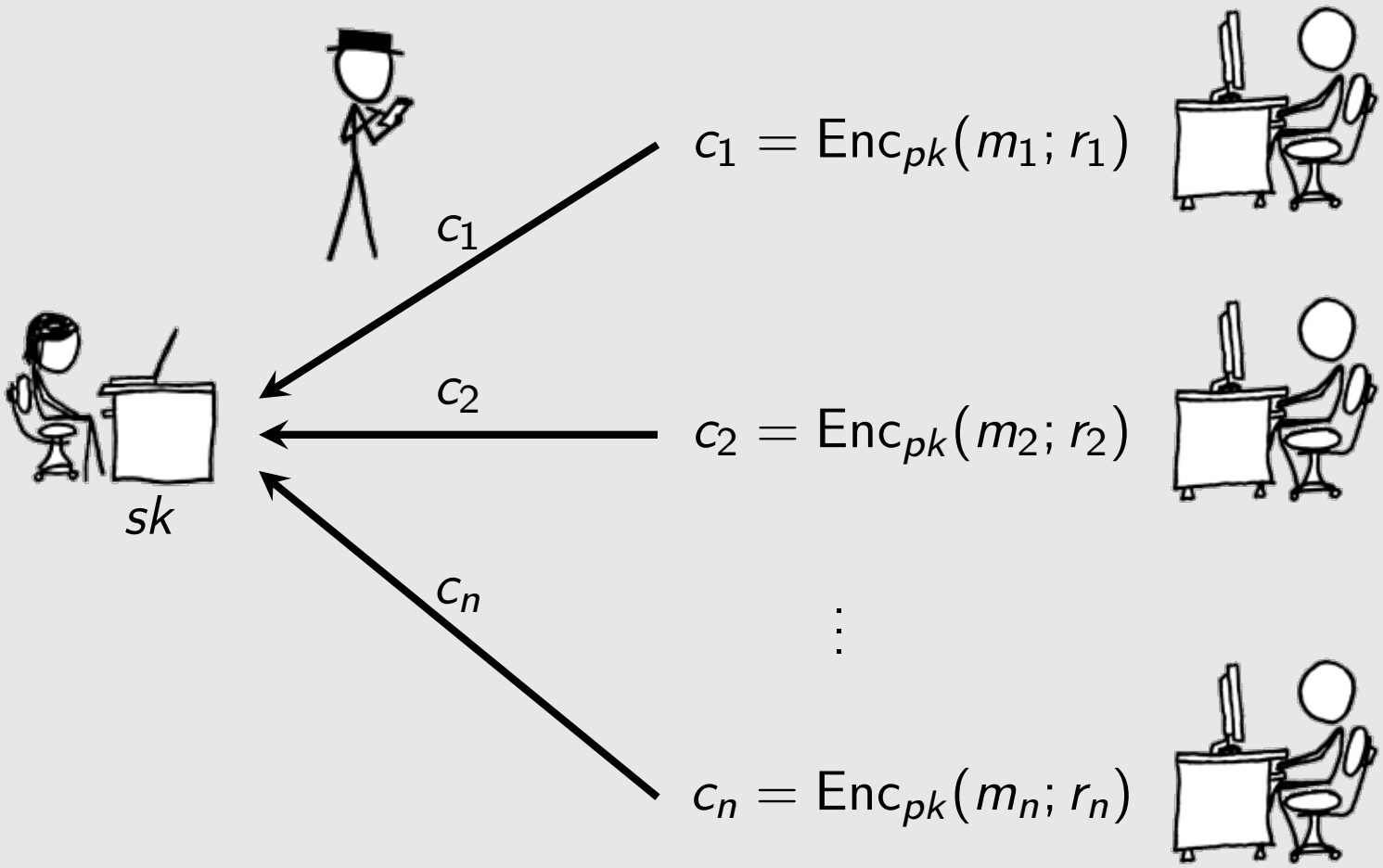


Image source: xkcd.com

Selective Opening Attacks

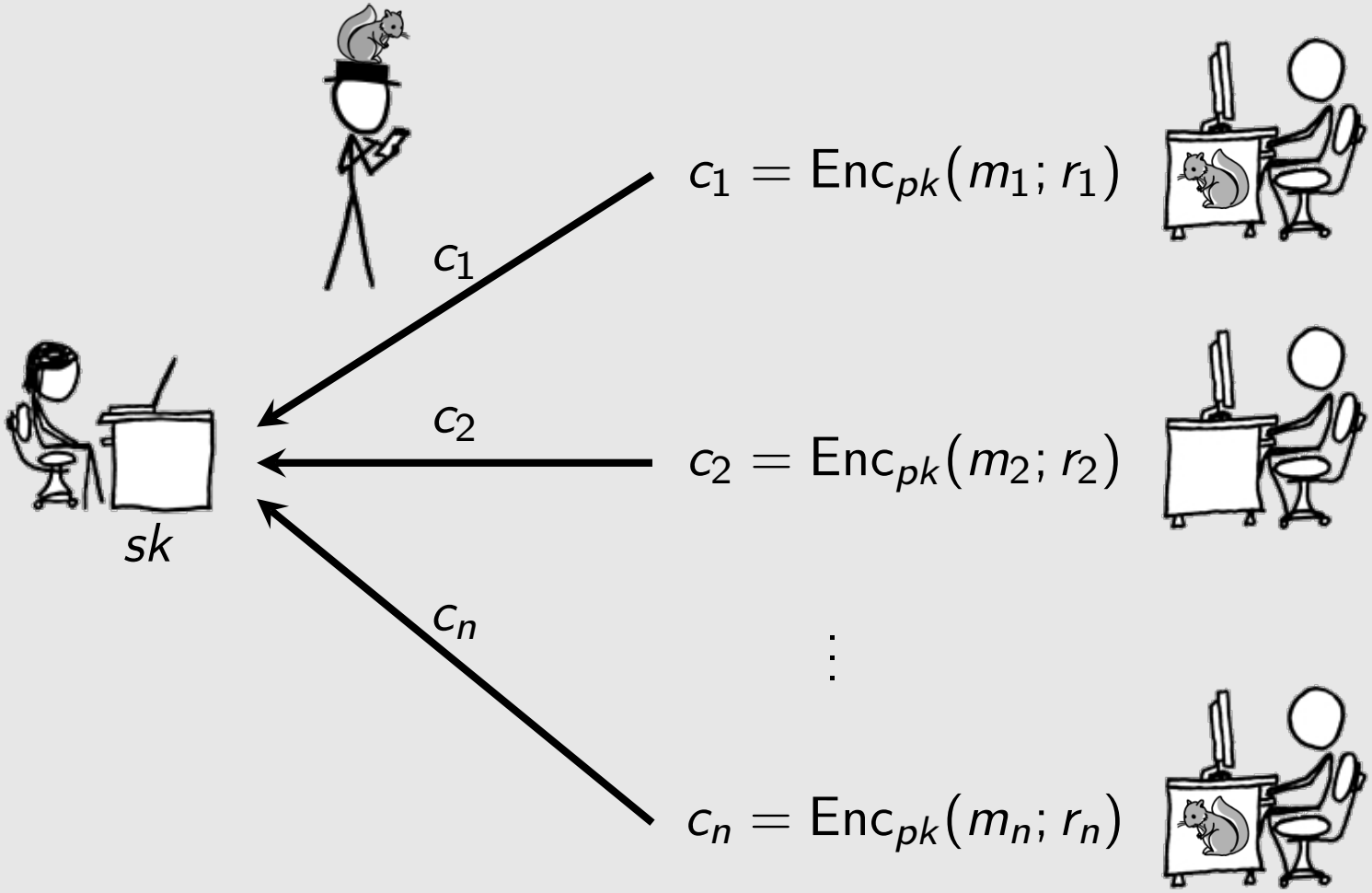


Image source: xkcd.com

Selective Opening Attacks

Do the messages of uncorrupted parties remain confidential?

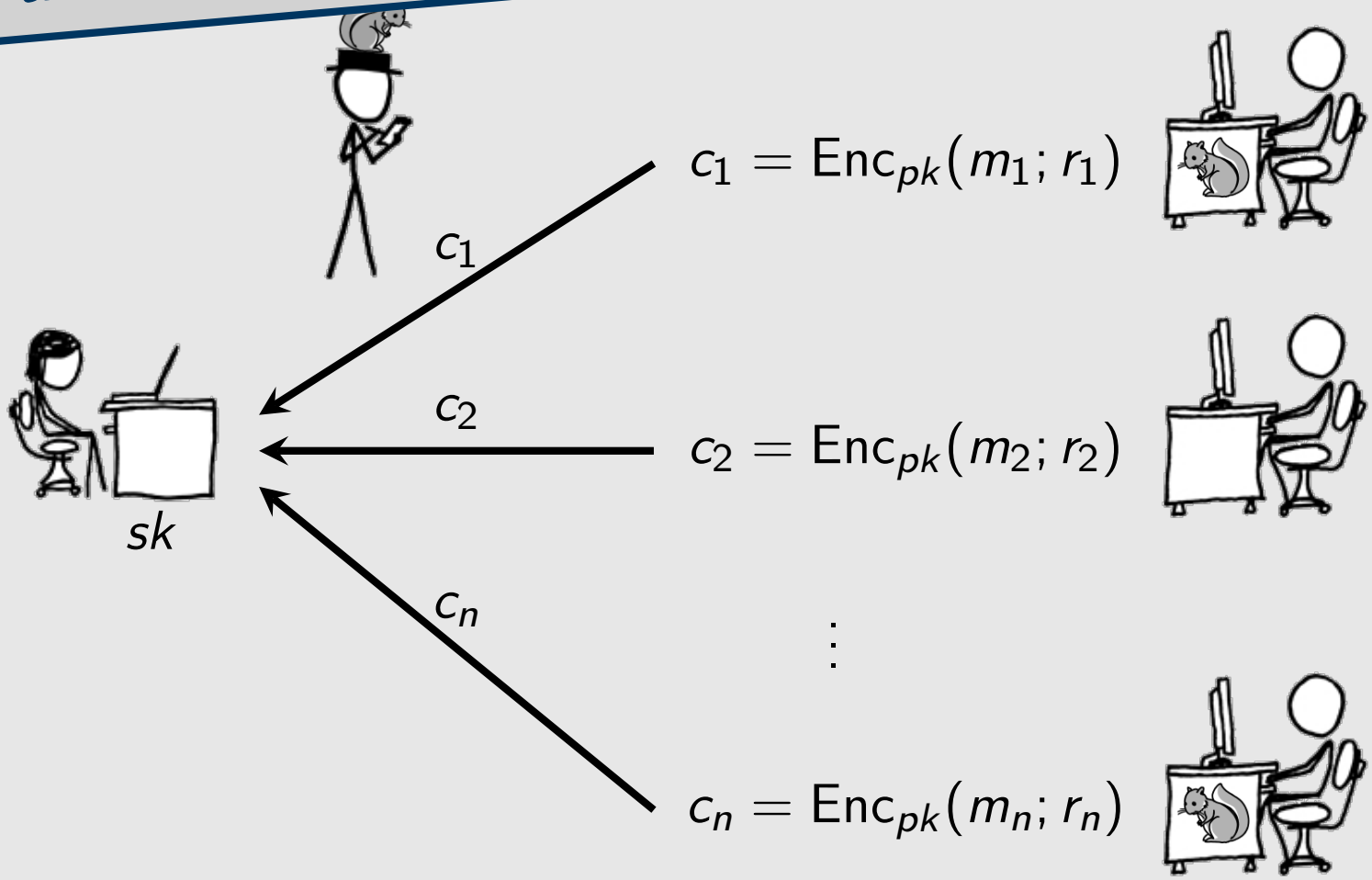
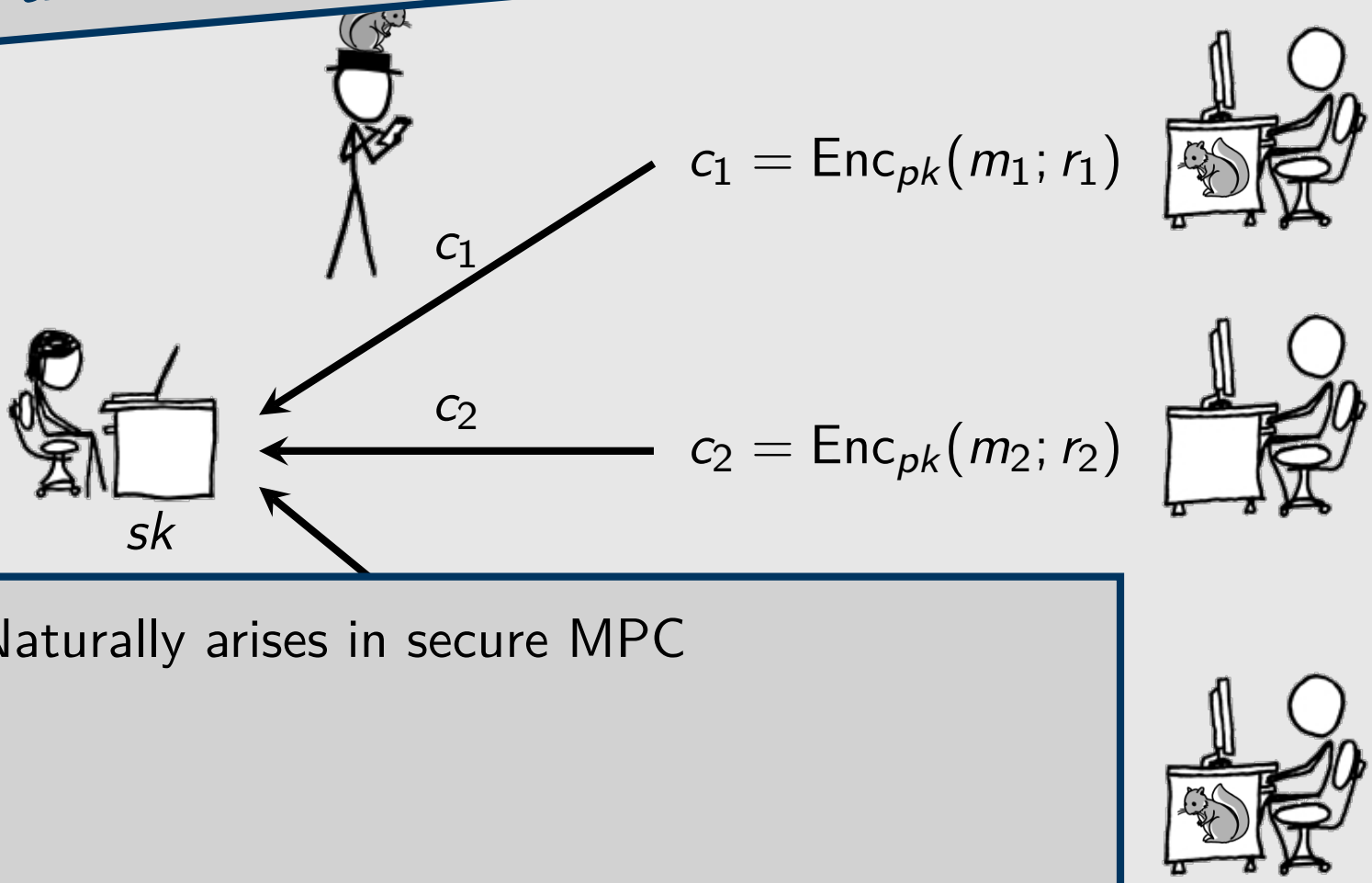


Image source: xkcd.com

Selective Opening Attacks

Do the messages of uncorrupted parties remain confidential?

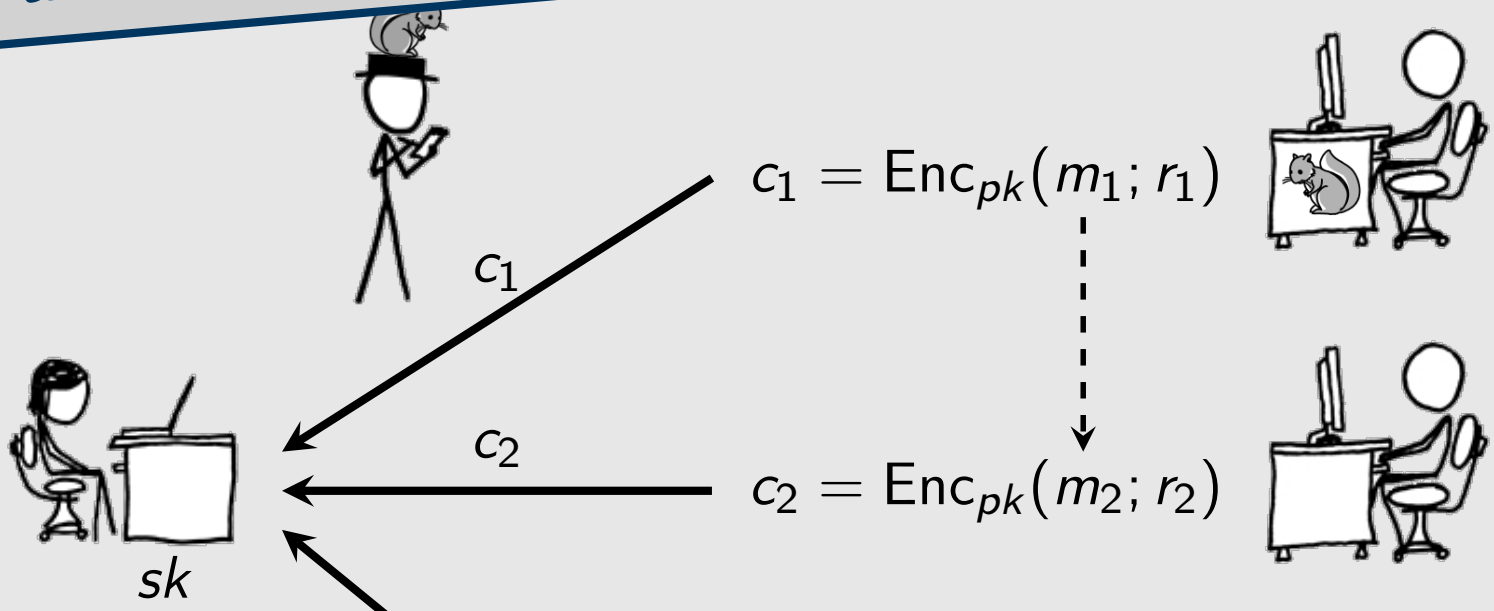


- Naturally arises in secure MPC

Image source: xkcd.com

Selective Opening Attacks

Do the messages of uncorrupted parties remain confidential?

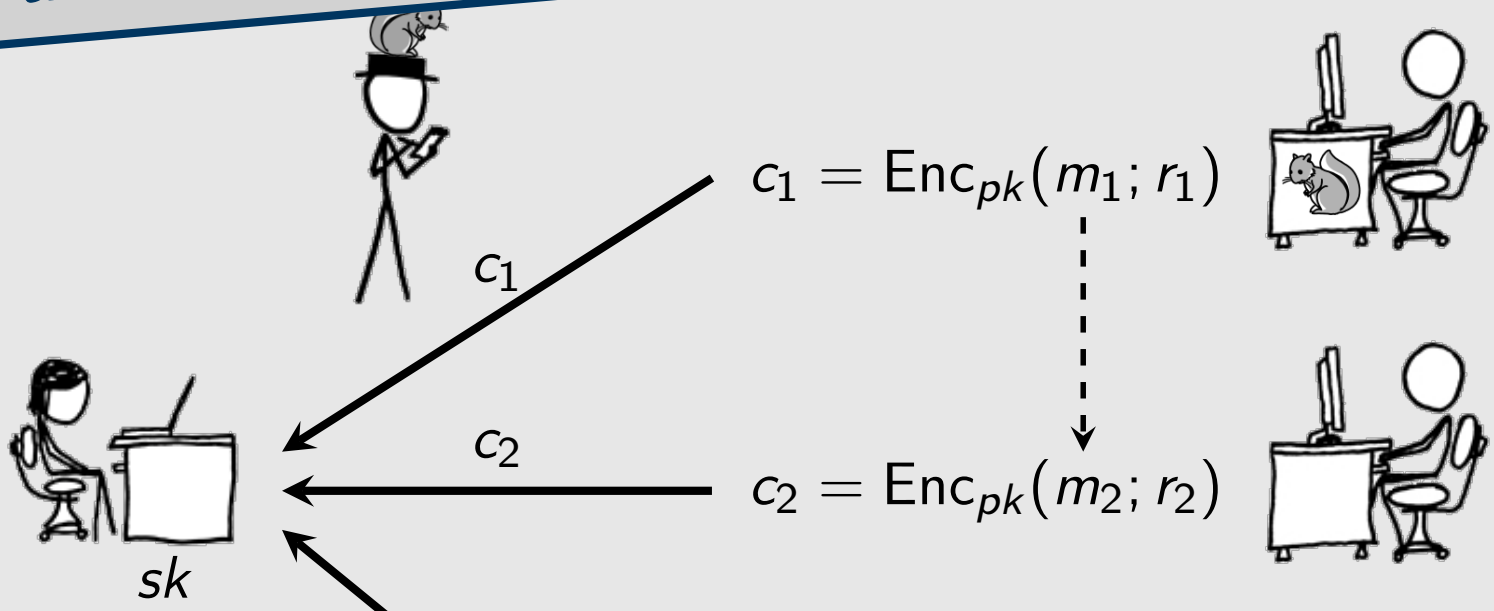


- Naturally arises in secure MPC
- Messages may depend on another

Image source: xkcd.com

Selective Opening Attacks

Do the messages of uncorrupted parties remain confidential?

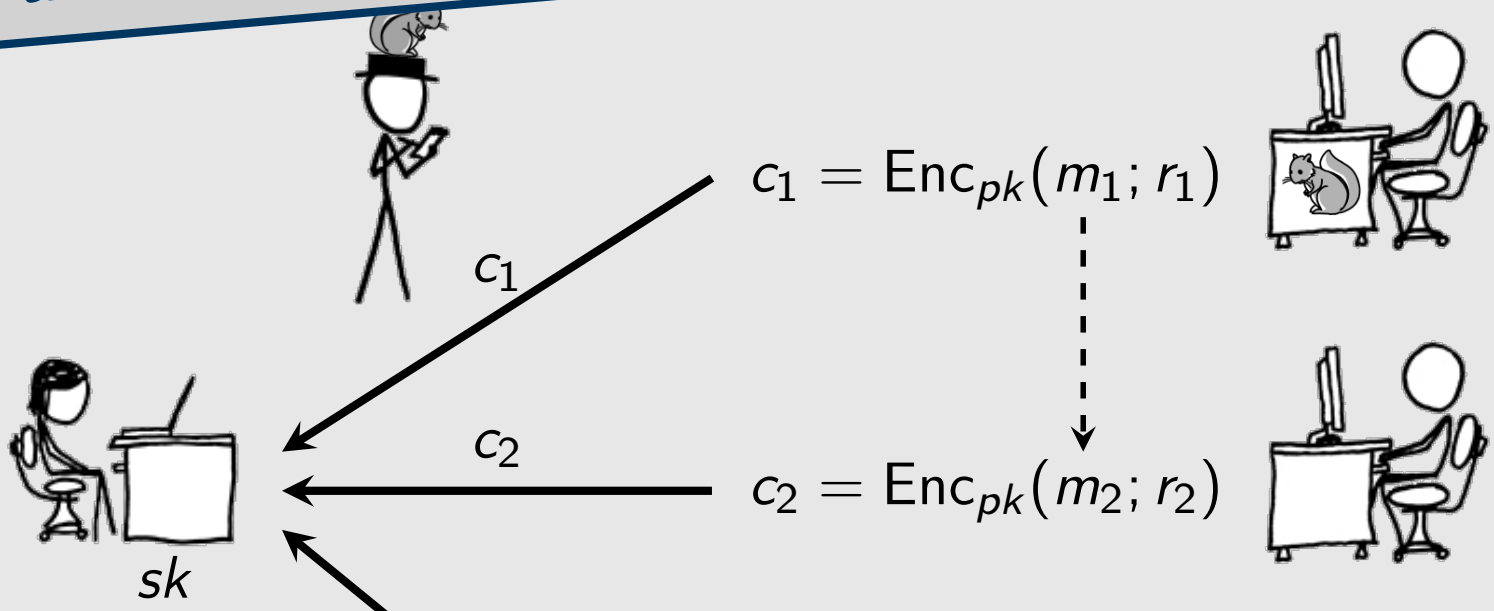


- Naturally arises in secure MPC
- Messages may depend on another
- **Not** implied by (standard) IND-CPA [HRW15]

Image source: xkcd.com

Selective Opening Attacks

Do the messages of uncorrupted parties remain confidential?



- Naturally arises in secure MPC
- Messages may depend on another
- **Not** implied by (standard) IND-CPA [HRW15]
- Dates back to [DNRS99]

Image source: xkcd.com

Defining IND-SO-CPA Security

Adversary obtains pk and submits a distribution $\mathfrak{D}$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$

$\boxed{m_i} := Enc_{pk}(m_i; r_i)$

Image source: xkcd.com

Defining IND-SO-CPA Security

Adversary obtains pk and submits a distribution $\mathfrak{D}$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$

$\boxed{m_i} := Enc_{pk}(m_i; r_i)$

$\boxed{m_1}$ $\boxed{m_2}$ $\boxed{m_3}$ $\boxed{m_4}$ $\cdots$ $\boxed{m_n}$

Image source: xkcd.com

Defining IND-SO-CPA Security

Adversary obtains pk and submits a distribution $\mathfrak{D}$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$

$\boxed{m_i} := Enc_{pk}(m_i; r_i)$

$\boxed{m_1}$ m_2 $\boxed{m_3}$ $\boxed{m_4}$ $\cdots$ $\boxed{m_n}$

Image source: xkcd.com

Defining IND-SO-CPA Security

Adversary obtains pk and submits a distribution $\mathfrak{D}$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$

$\boxed{m_i} := Enc_{pk}(m_i; r_i)$

$\boxed{m_1}$ m_2, r_2 $\boxed{m_3}$ $\boxed{m_4}$ $\cdots$ $\boxed{m_n}$

Image source: xkcd.com

Defining IND-SO-CPA Security

Adversary obtains pk and submits a distribution $\mathfrak{D}$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$

$\boxed{m_i} := Enc_{pk}(m_i; r_i)$

$m_1, r_1 \quad m_2, r_2 \quad \boxed{m_3} \quad \boxed{m_4} \quad \cdots \quad \boxed{m_n}$

Image source: xkcd.com

Defining IND-SO-CPA Security

Adversary obtains pk and submits a distribution $\mathfrak{D}$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$

$\boxed{m_i} := Enc_{pk}(m_i; r_i)$

$$m_1, r_1 \quad m_2, r_2 \quad \boxed{m_3} \quad \boxed{m_4} \quad \cdots \quad m_n, r_n$$

Image source: xkcd.com

Defining IND-SO-CPA Security

Adversary obtains pk and submits a distribution $\mathfrak{D}$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$

$\boxed{m_i} := Enc_{pk}(m_i; r_i)$

$$m_1, r_1 \quad m_2, r_2 \quad \boxed{m_3} \quad \boxed{m_4} \quad \cdots \quad m_n, r_n$$

Challenge:

$$(m_1 \quad m_2 \quad m_3 \quad m_4 \quad \cdots \quad m_n)$$

Image source: xkcd.com

Defining IND-SO-CPA Security

Adversary obtains pk and submits a distribution $\mathfrak{D}$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$

$\boxed{m_i} := Enc_{pk}(m_i; r_i)$

$$m_1, r_1 \quad m_2, r_2 \quad \boxed{m_3} \quad \boxed{m_4} \quad \cdots \quad m_n, r_n$$

Challenge:

$$(m_1 \quad m_2 \quad m_3 \quad m_4 \quad \cdots \quad m_n)$$

or

$$(m_1 \quad m_2 \quad m_3 \quad m_4 \quad \cdots \quad m_n)$$

where $m_3, m_4, \ldots$ are resampled conditioned on *every* opened ciphertext.

Image source: xkcd.com

Defining IND-SO-CPA Security

Adversary obtains pk and submits a distribution $\mathfrak{D}$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$

$\boxed{m_i} := Enc_{pk}(m_i; r_i)$

$$m_1, r_1 \quad m_2, r_2 \quad \boxed{m_3} \quad \boxed{m_4} \quad \cdots \quad m_n, r_n$$

Challenge:

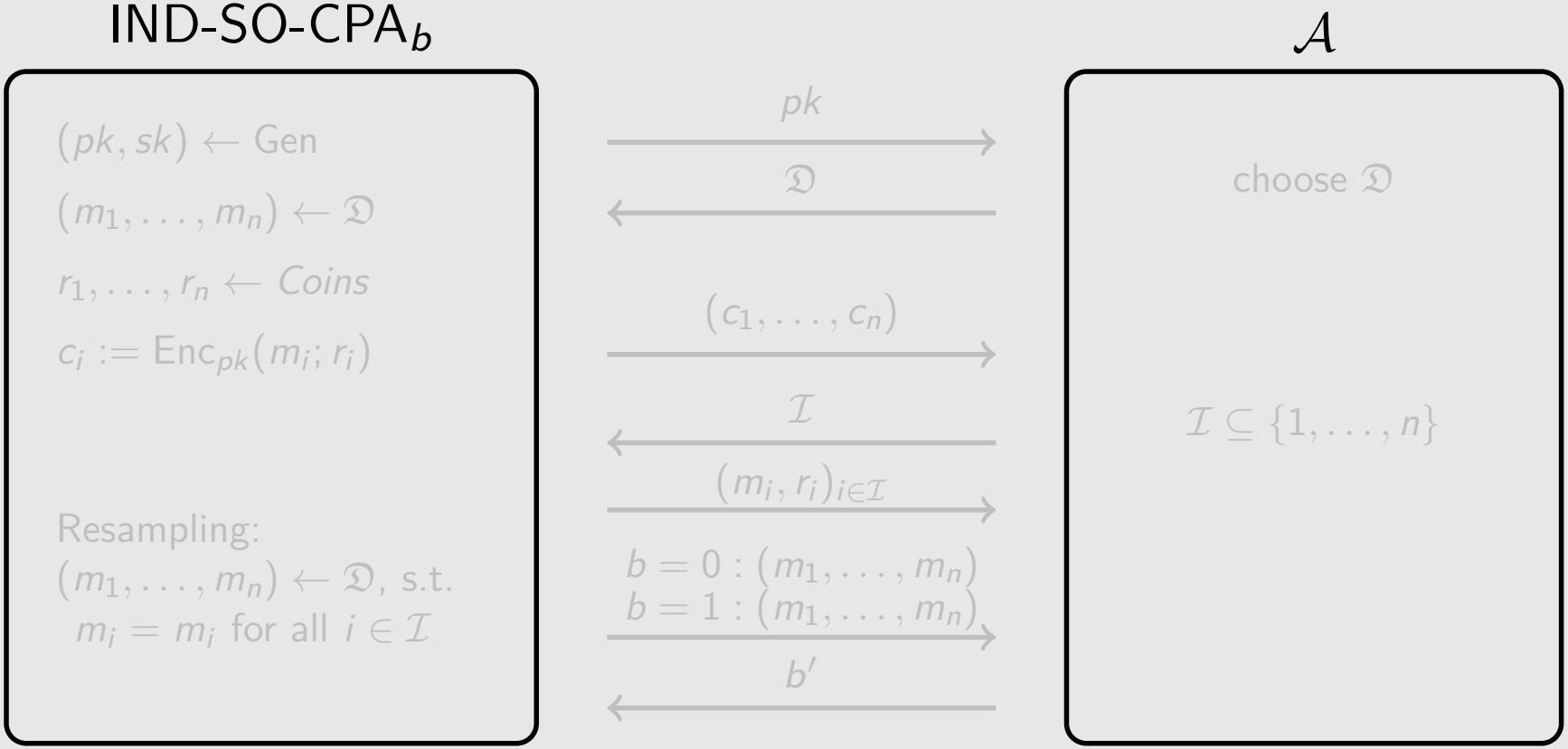
or

$$\begin{array}{cccccc} (m_1 & m_2 & m_3 & m_4 & \cdots & m_n) \\ & & \approx_c & & & \\ (m_1 & m_2 & m_3 & m_4 & \cdots & m_n) \end{array}$$

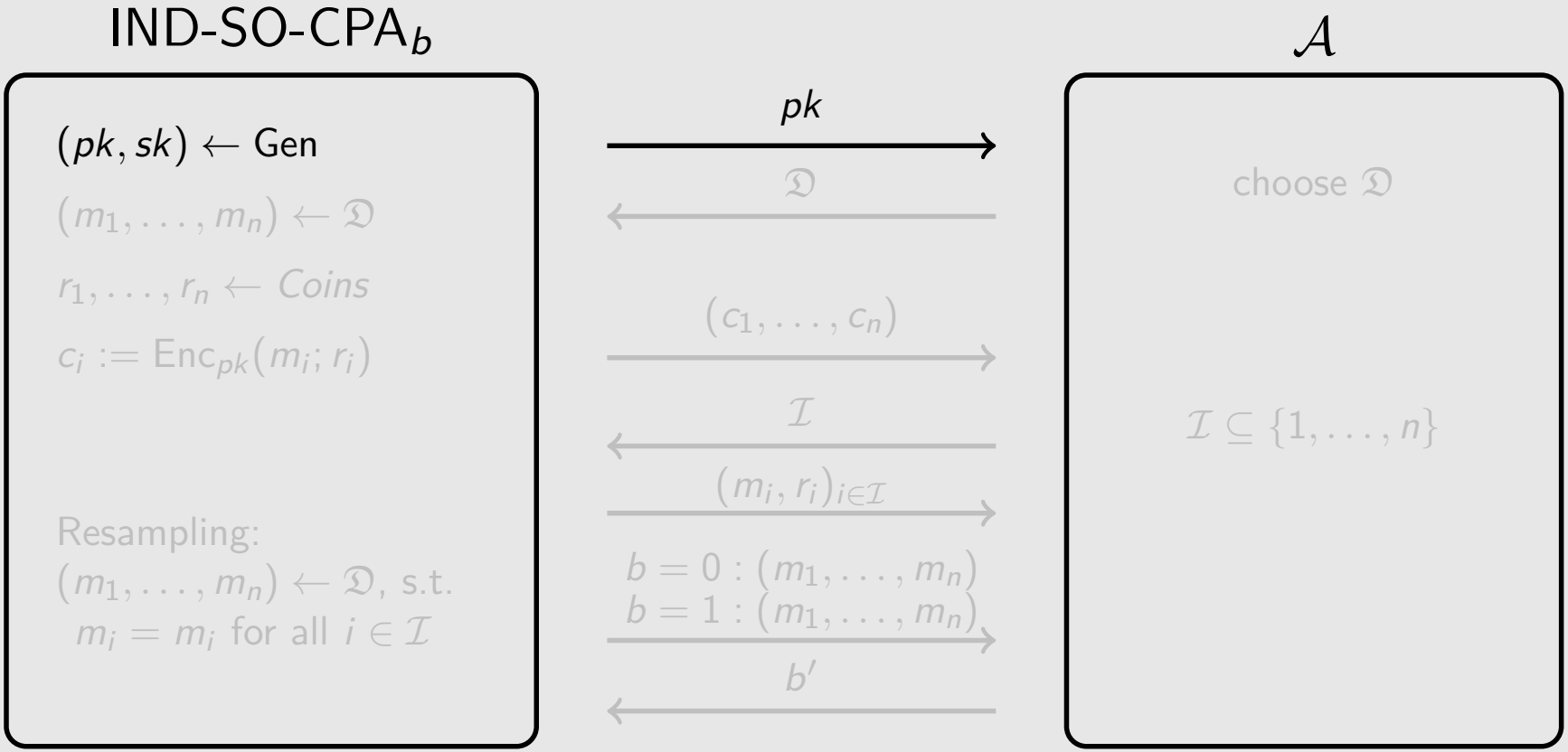
where $m_3, m_4, \ldots$ are resampled conditioned on *every* opened ciphertext.

Image source: xkcd.com

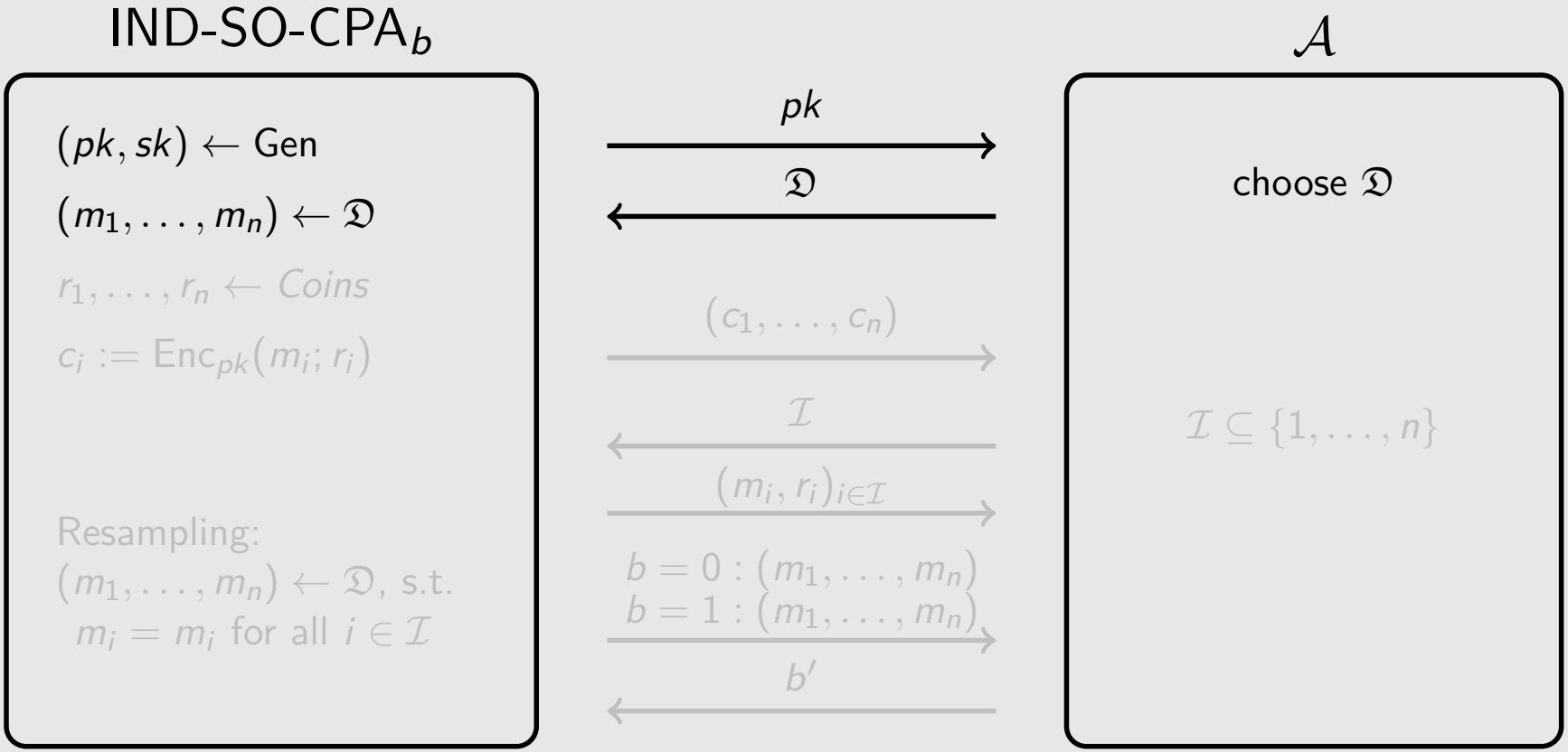
Defining IND-SO-CPA Security



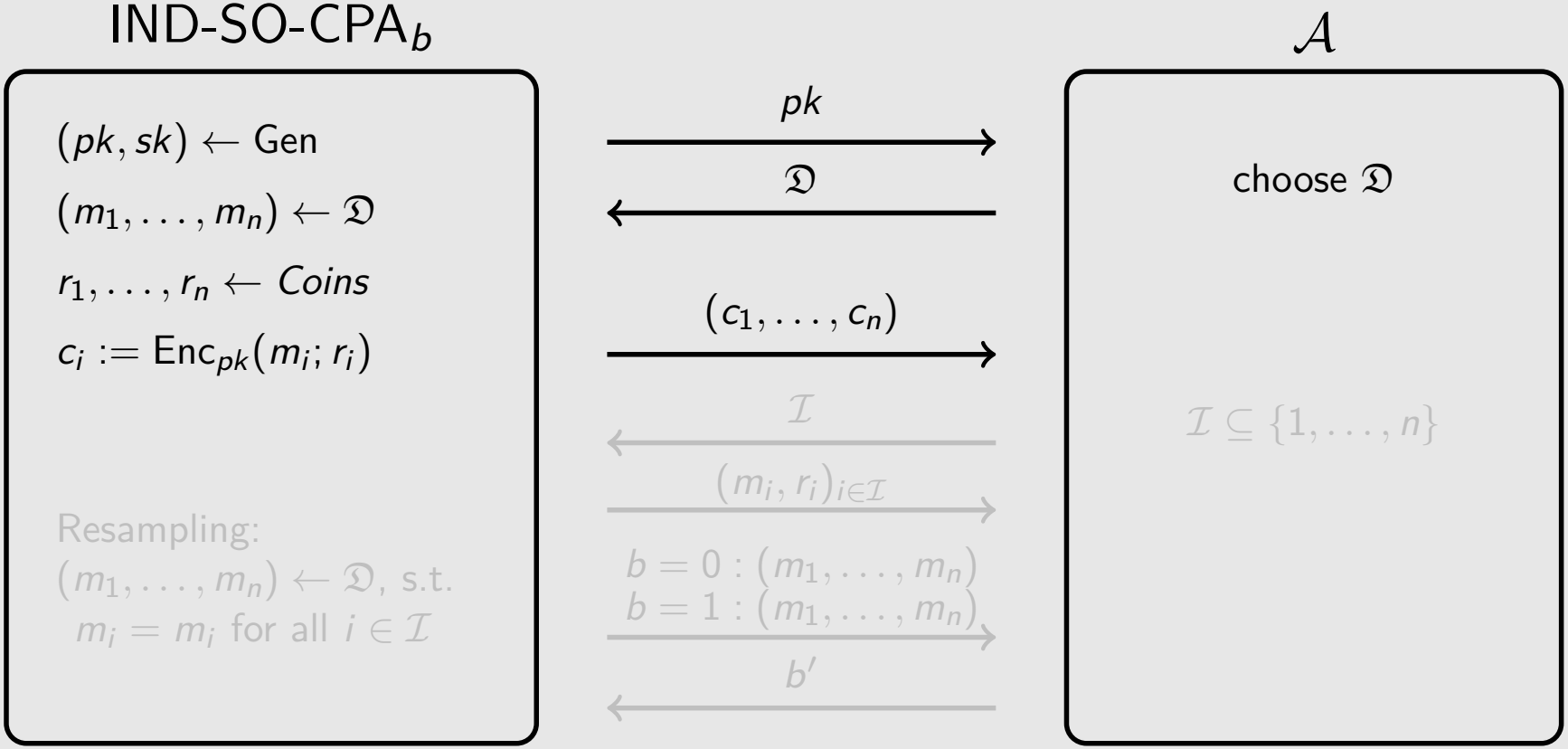
Defining IND-SO-CPA Security



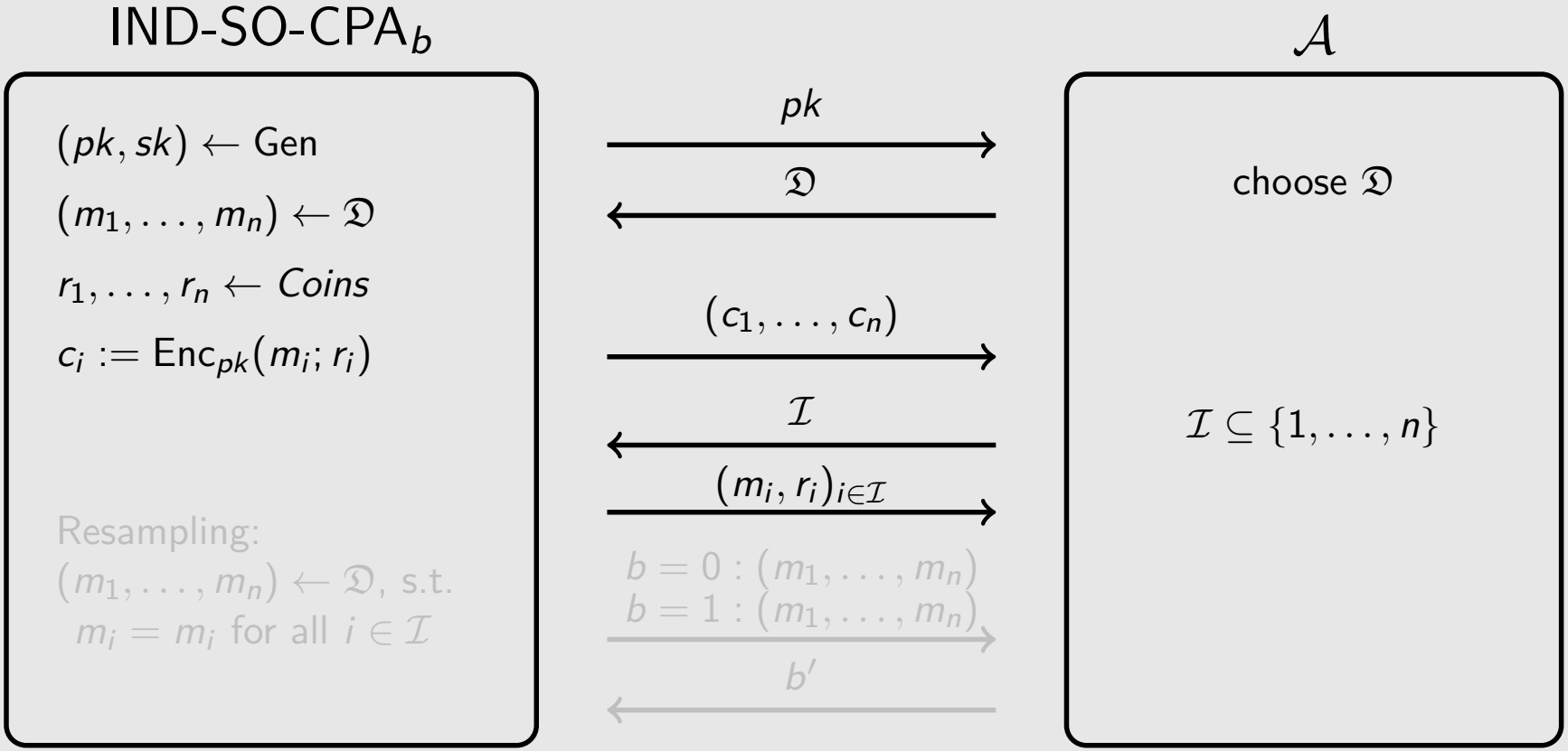
Defining IND-SO-CPA Security



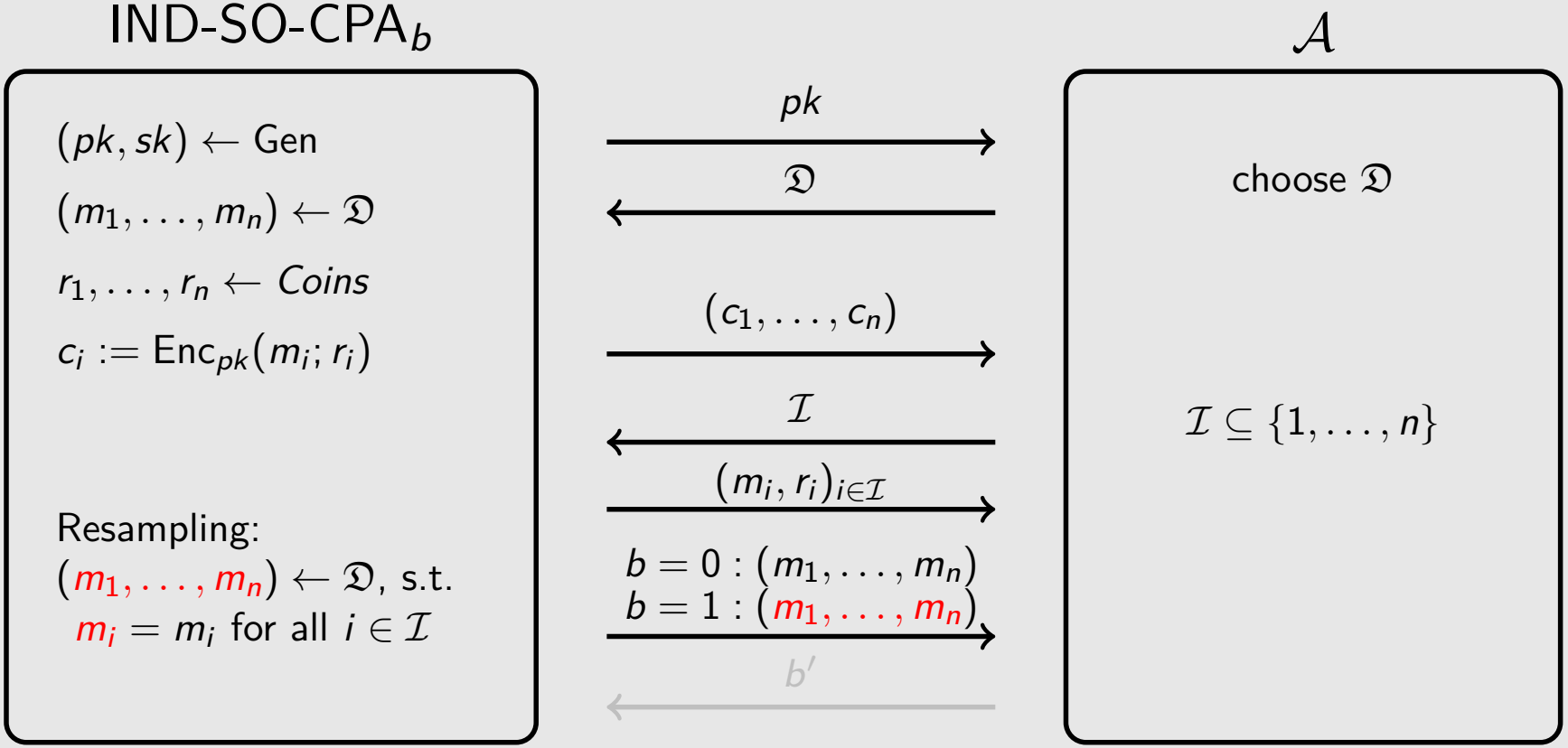
Defining IND-SO-CPA Security



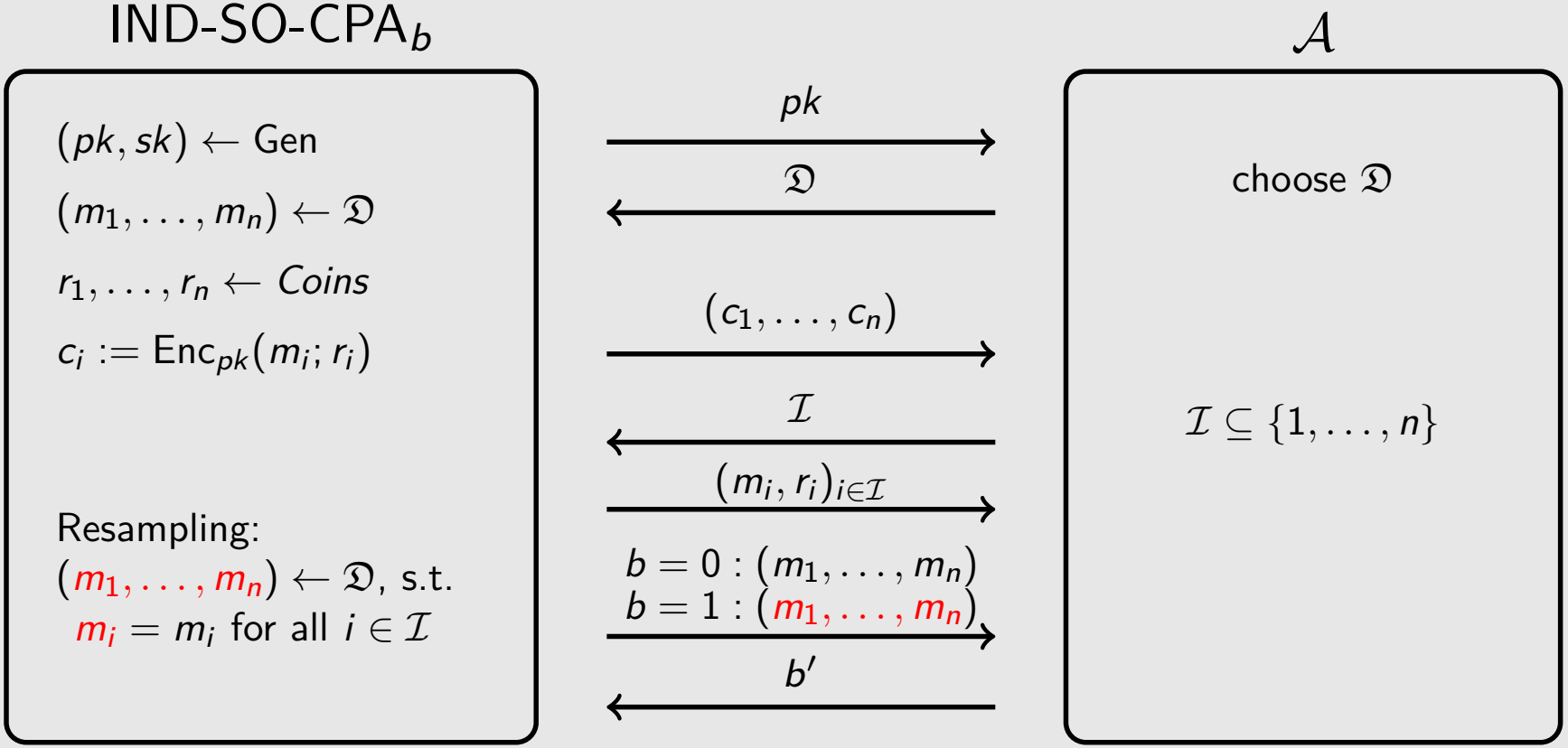
Defining IND-SO-CPA Security



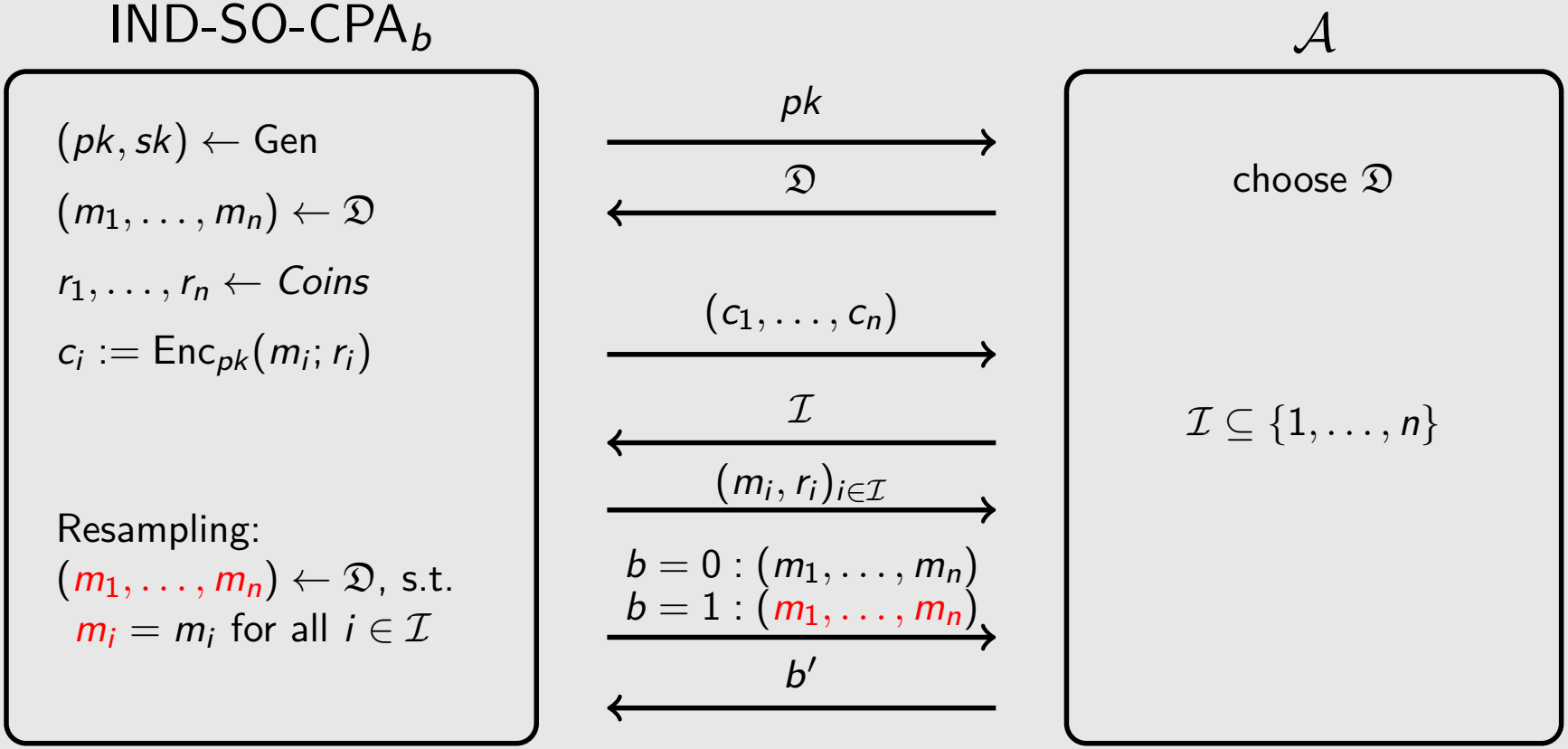
Defining IND-SO-CPA Security



Defining IND-SO-CPA Security



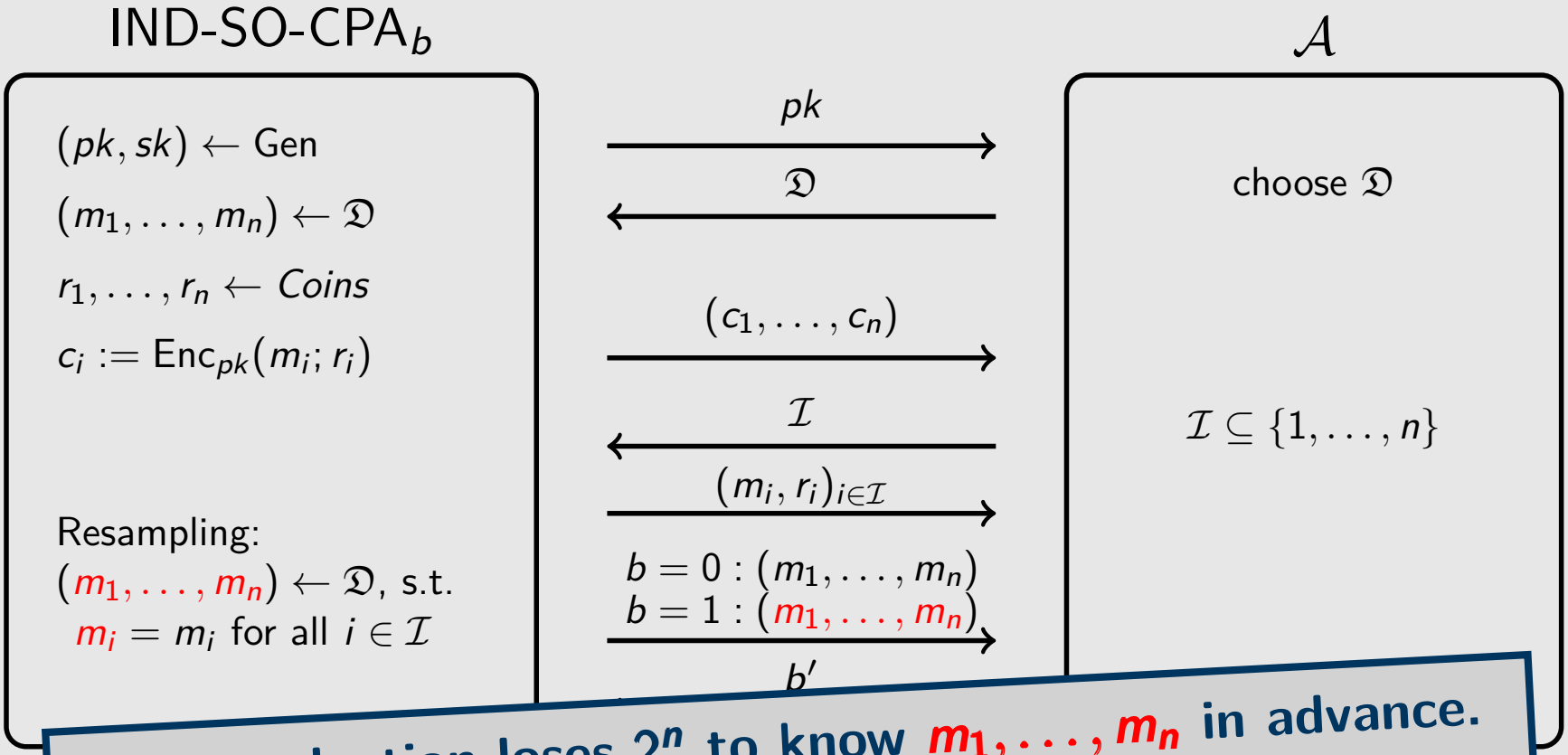
Defining IND-SO-CPA Security



PKE is IND-SO-CPA secure if for all ppt $\mathcal{A}$ and all eff. resamp. $\mathfrak{D}$:

$$\left|\Pr[\text{IND-SO-CPA}_0^{\mathcal{A}} \Rightarrow 1] - \Pr[\text{IND-SO-CPA}_1^{\mathcal{A}} \Rightarrow 1]\right| \leq negl.$$

Defining IND-SO-CPA Security



Naïve reduction loses 2^n to know $m_1, \ldots, m_n$ in advance.

PKE is IND-SO-CPA secure if for all ppt $\mathcal{A}$ and all eff. resamp. $\mathfrak{D}$:

$$\left|\Pr[\text{IND-SO-CPA}_0^{\mathcal{A}} \Rightarrow 1] - \Pr[\text{IND-SO-CPA}_1^{\mathcal{A}} \Rightarrow 1]\right| \leq \mathit{negl}.$$

When does IND-CPA imply IND-SO-CPA?

Theorem 1

Let PKE be any IND-CPA secure scheme. Then PKE is IND-SO-CPA secure w.r.t. to Markov distributions.

When does IND-CPA imply IND-SO-CPA?

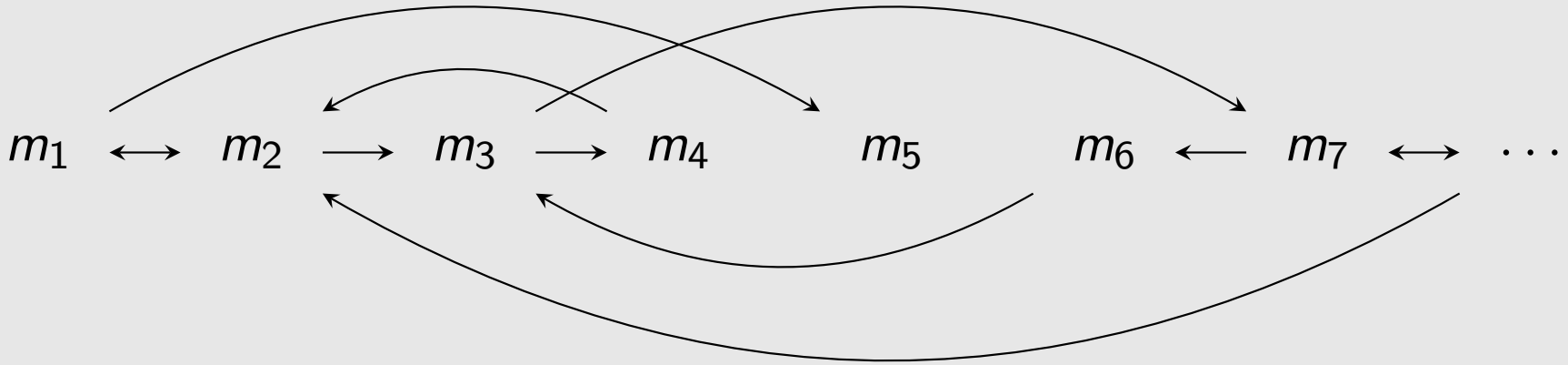
Theorem 1

Let PKE be any IND-CPA secure scheme. Then PKE is IND-SO-CPA secure w.r.t. to Markov distributions.

- First positive result for non-trivial distributions
- Loss of n^3 (see paper)
- Result extends to *low-dependency* distributions (see paper)

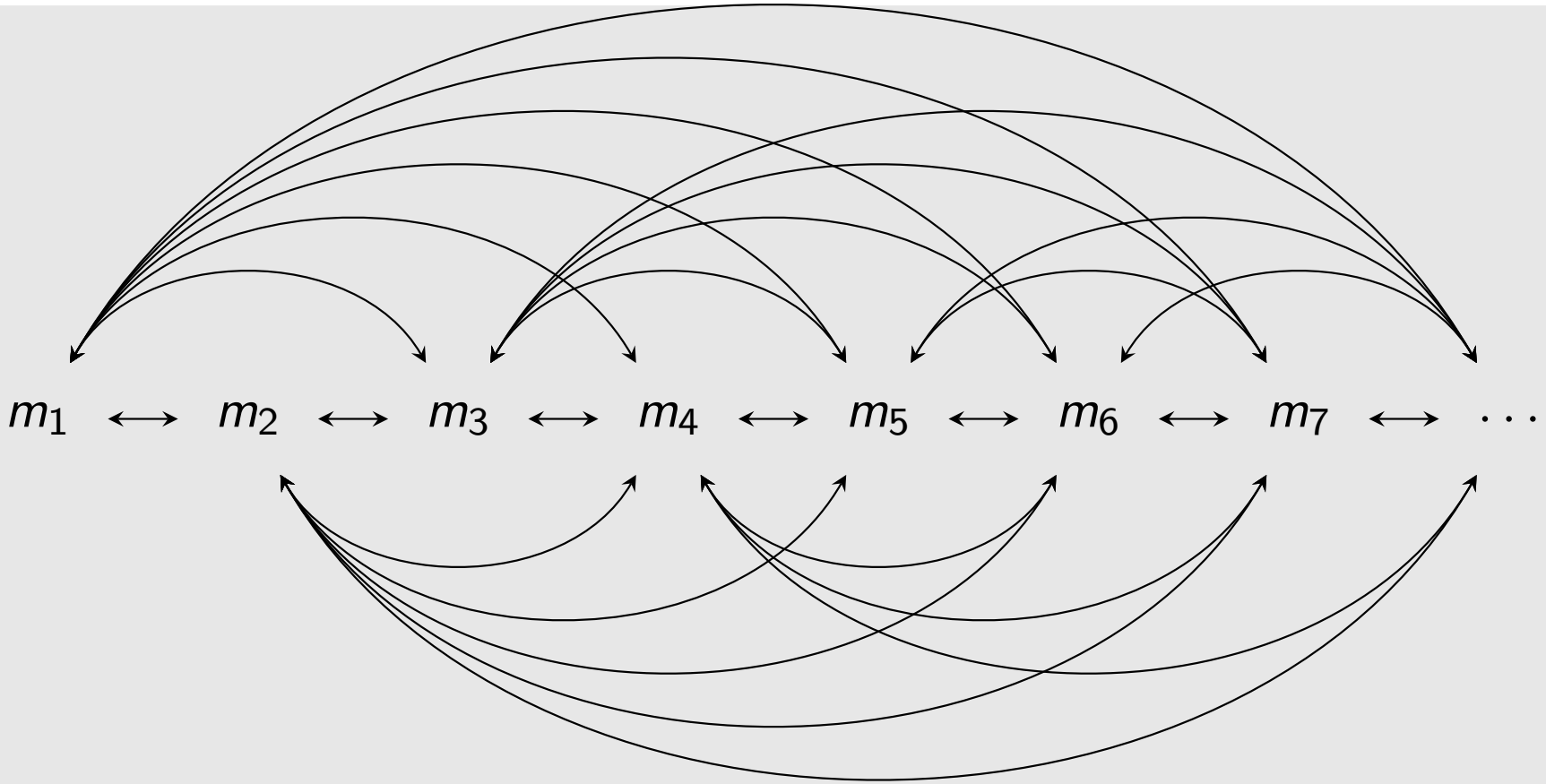
ePrint: 2015/853

When does IND-CPA imply IND-SO-CPA?



Distribution of a message m_i is a function of its immediate predecessors only.

When does IND-CPA imply IND-SO-CPA?



Wishful thinking

When does IND-CPA imply IND-SO-CPA?

m_1 m_2 m_3 m_4 m_5 m_6 m_7 $\cdots$

[DNRS99,BY09]

When does IND-CPA imply IND-SO-CPA?

$$m_1 \longrightarrow m_2 \longrightarrow m_3 \longrightarrow m_4 \longrightarrow m_5 \longrightarrow m_6 \longrightarrow m_7 \longrightarrow \cdots$$

When does IND-CPA imply IND-SO-CPA?

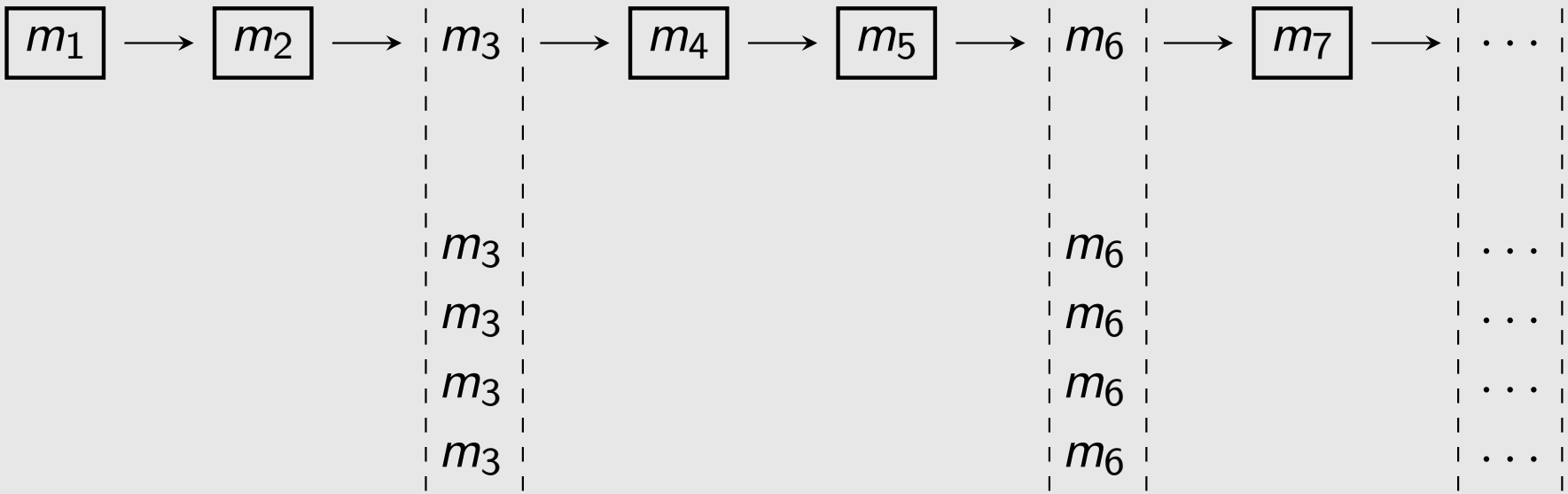
When does IND-CPA imply IND-SO-CPA?

Assume that $\mathcal{A}$ opens $\boxed{m_3}$, $\boxed{m_6}$ and $\boxed{m_8}$, . . . , $\boxed{m_n}$

$$\boxed{m_1} \longrightarrow \boxed{m_2} \longrightarrow m_3 \longrightarrow \boxed{m_4} \longrightarrow \boxed{m_5} \longrightarrow m_6 \longrightarrow \boxed{m_7} \longrightarrow \cdots$$

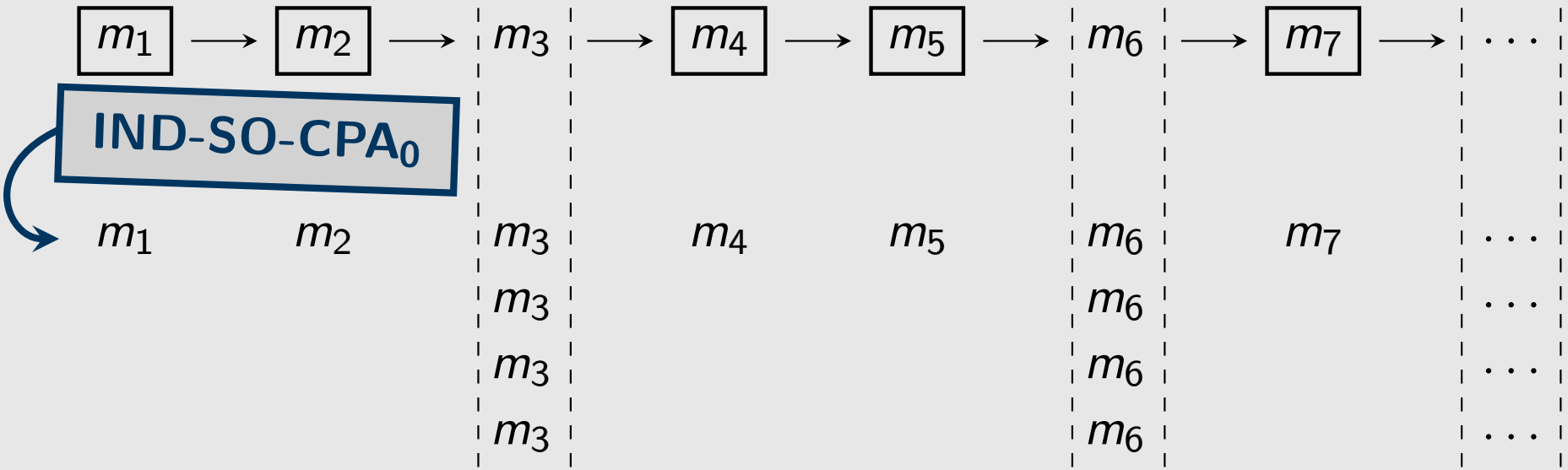
When does IND-CPA imply IND-SO-CPA?

Assume that $\mathcal{A}$ opens $\boxed{m_3}$, $\boxed{m_6}$ and $\boxed{m_8}$, . . . , $\boxed{m_n}$



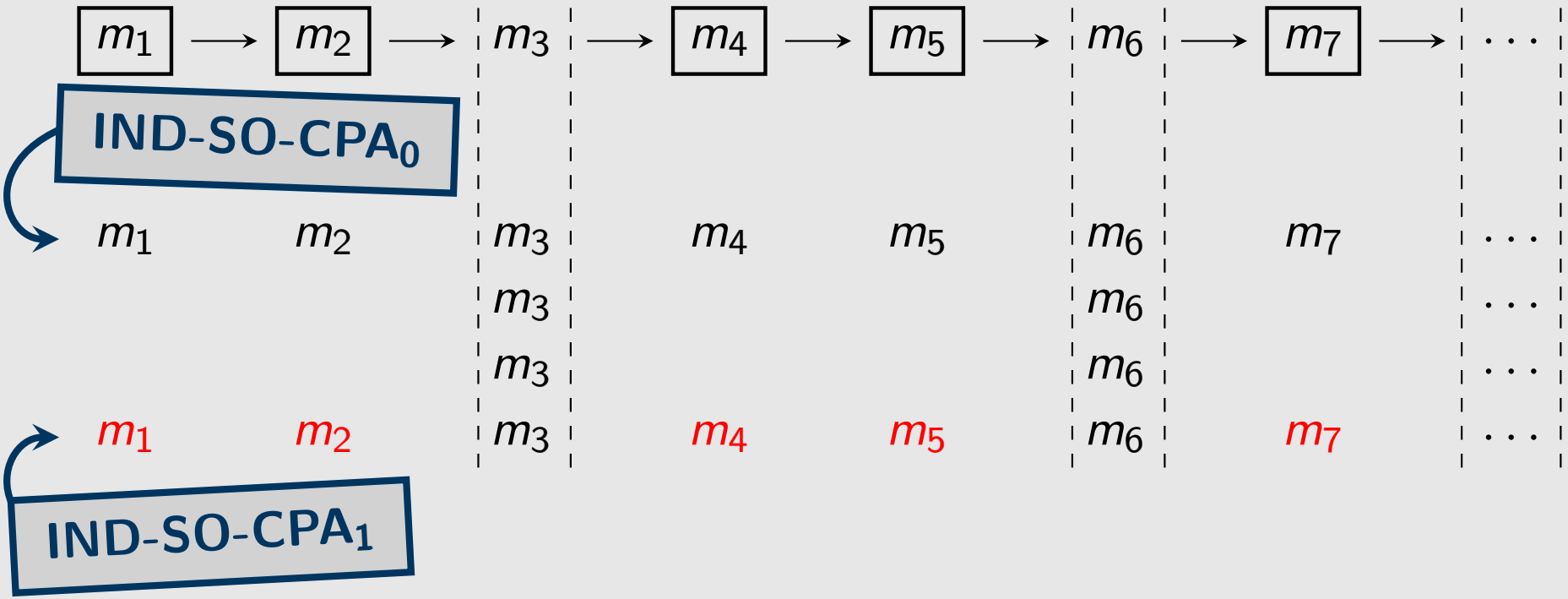
When does IND-CPA imply IND-SO-CPA?

Assume that $\mathcal{A}$ opens $\boxed{m_3}$, $\boxed{m_6}$ and $\boxed{m_8}$, . . . , $\boxed{m_n}$



When does IND-CPA imply IND-SO-CPA?

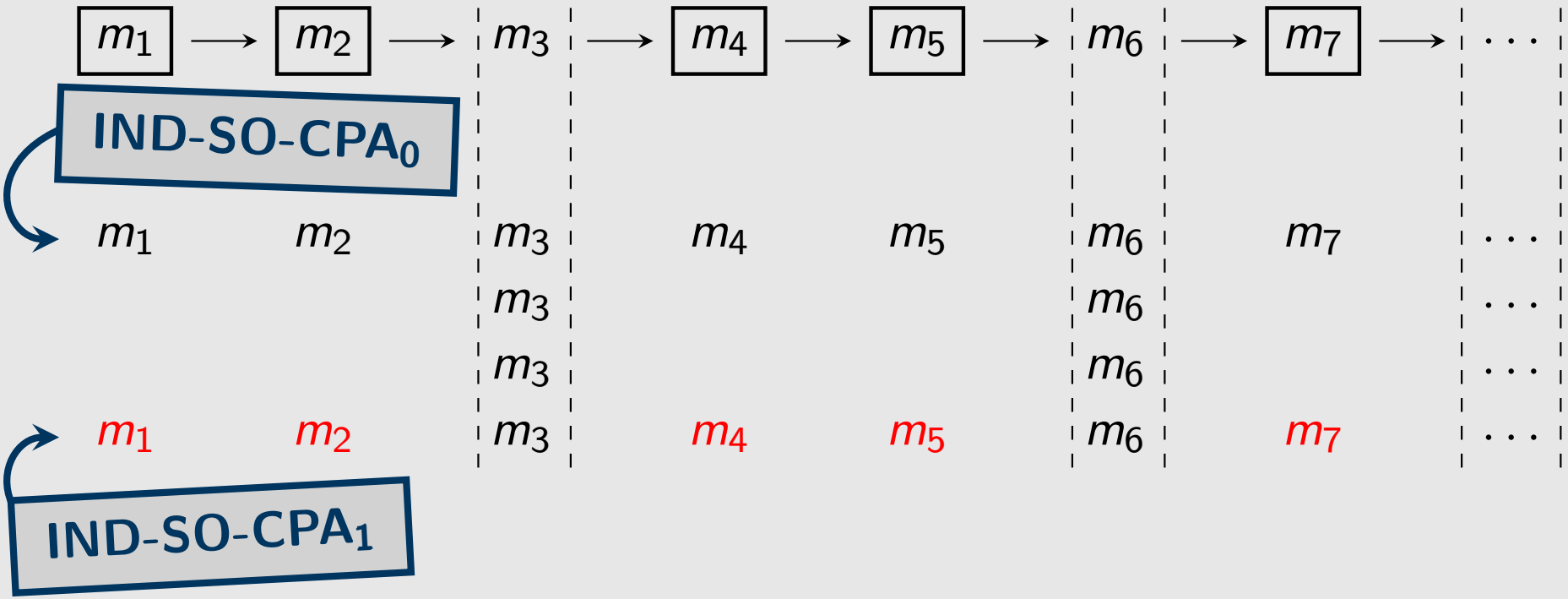
Assume that $\mathcal{A}$ opens $\boxed{m_3}$, $\boxed{m_6}$ and $\boxed{m_8}$, . . . , $\boxed{m_n}$



When does IND-CPA imply IND-SO-CPA?

Assume that $\mathcal{A}$ opens $\boxed{m_3}$, $\boxed{m_6}$ and $\boxed{m_8}$, . . . , $\boxed{m_n}$

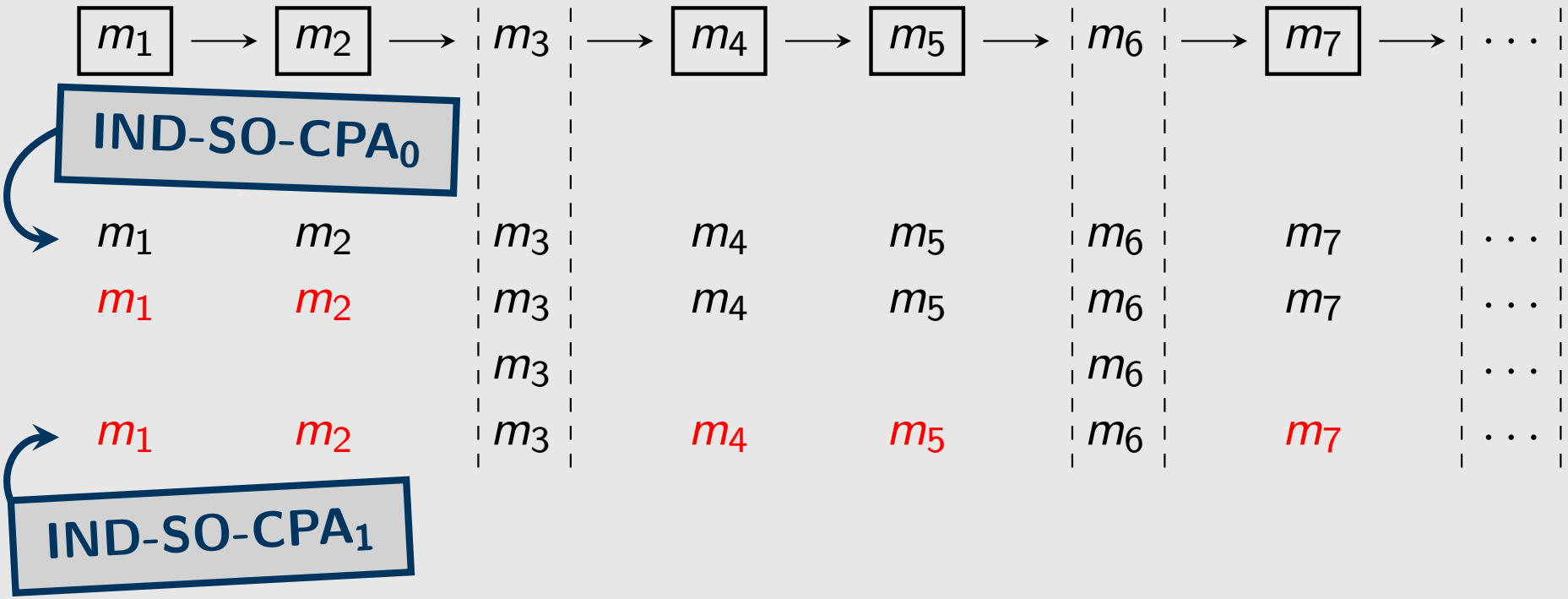
Hybrid i: Return resampled messages up to the i^{th} opening query.



When does IND-CPA imply IND-SO-CPA?

Assume that $\mathcal{A}$ opens $\boxed{m_3}$, $\boxed{m_6}$ and $\boxed{m_8}$, . . . , $\boxed{m_n}$

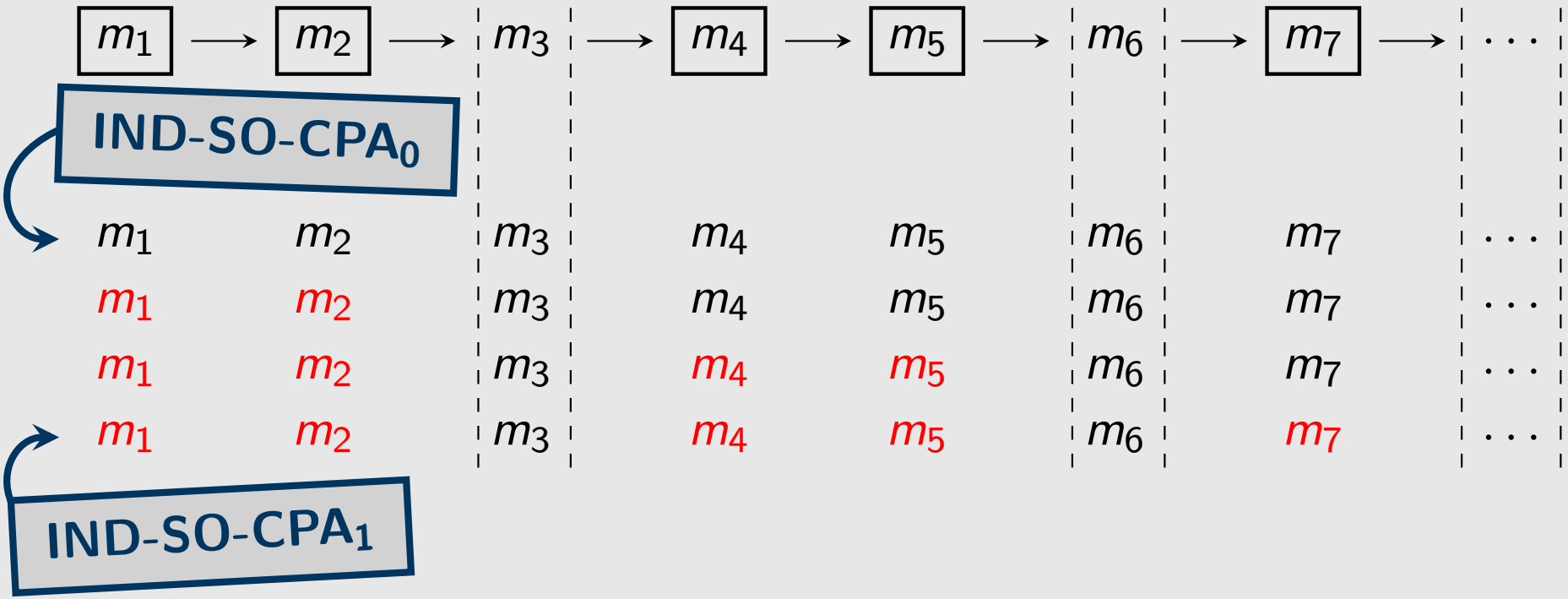
Hybrid i: Return resampled messages up to the i^{th} opening query.



When does IND-CPA imply IND-SO-CPA?

Assume that $\mathcal{A}$ opens $\boxed{m_3}$, $\boxed{m_6}$ and $\boxed{m_8}$, . . . , $\boxed{m_n}$

Hybrid i: Return resampled messages up to the i^{th} opening query.



When does IND-CPA imply IND-SO-CPA?

m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$
m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$

When does IND-CPA imply IND-SO-CPA?

Guess interval $[m_4, m_5]$ confined by consecutive opening queries.

m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$
m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$

When does IND-CPA imply IND-SO-CPA?

Guess interval $[m_4, m_5]$ confined by consecutive opening queries.

Resample $(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$ conditioned on $m_3 = m_3$ and $m_6 = m_6$.

m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$
m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$

When does IND-CPA imply IND-SO-CPA?

Guess interval $[m_4, m_5]$ confined by consecutive opening queries.

Resample $(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$ conditioned on $m_3 = m_3$ and $m_6 = m_6$.

Submit $[m_4, m_5]$ and $[m_4, m_5]$ to (vectorial) IND-CPA challenger.

m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$
m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$

When does IND-CPA imply IND-SO-CPA?

Guess interval $[m_4, m_5]$ confined by consecutive opening queries.

Resample $(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$ conditioned on $m_3 = m_3$ and $m_6 = m_6$.

Submit $[m_4, m_5]$ and $[m_4, m_5]$ to (vectorial) IND-CPA challenger.

Reduction encrypts $m_1, \ldots, m_3$ and $m_6, \ldots, m_n$ on its own.

m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$
m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$

When does IND-CPA imply IND-SO-CPA?

Guess interval $[m_4, m_5]$ confined by consecutive opening queries.

Resample $(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$ conditioned on $m_3 = m_3$ and $m_6 = m_6$.

Submit $[m_4, m_5]$ and $[m_4, m_5]$ to (vectorial) IND-CPA challenger.

Reduction encrypts $m_1, \ldots, m_3$ and $m_6, \ldots, m_n$ on its own.

Open queries might happen on the left of m_3.

m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$
m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$

When does IND-CPA imply IND-SO-CPA?

Guess interval $[m_4, m_5]$ confined by consecutive opening queries.

Resample $(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$ conditioned on $m_3 = m_3$ and $m_6 = m_6$.

Submit $[m_4, m_5]$ and $[m_4, m_5]$ to (vectorial) IND-CPA challenger.

Reduction encrypts $m_1, \ldots, m_3$ and $m_6, \ldots, m_n$ on its own.

Open queries might happen on the left of m_3.

Resample $(\widetilde{m_1}, \ldots, \widetilde{m_n}) \leftarrow \mathfrak{D}$ conditioned on every opened ciphertext.

m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$
m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$

When does IND-CPA imply IND-SO-CPA?

Guess interval $[m_4, m_5]$ confined by consecutive opening queries.

Resample $(m_1, \ldots, m_n) \leftarrow \mathfrak{D}$ conditioned on $m_3 = m_3$ and $m_6 = m_6$.

Submit $[m_4, m_5]$ and $[m_4, m_5]$ to (vectorial) IND-CPA challenger.

Reduction encrypts $m_1, \ldots, m_3$ and $m_6, \ldots, m_n$ on its own.

Open queries might happen on the left of m_3.

Resample $(\widetilde{m_1}, \ldots, \widetilde{m_n}) \leftarrow \mathfrak{D}$ conditioned on every opened ciphertext.

Use m_3 to glue resampled and sampled partial vectors together.

m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$
m_1	m_2	m_3	m_4	m_5	m_6	m_7	$\cdots$

Summing up

- IND-CPA implies IND-SO-CPA for Markov Distributions.

Summing up

- IND-CPA implies IND-SO-CPA for Markov Distributions.
- Our approach extends to *low-dependency* distributions.

Summing up

- IND-CPA implies IND-SO-CPA for Markov Distributions.
- Our approach extends to *low-dependency* distributions.
- However, there's a gap to distributions used in [HRW15].

Summing up

- IND-CPA implies IND-SO-CPA for Markov Distributions.
- Our approach extends to *low-dependency* distributions.
- However, there's a gap to distributions used in [HRW15].
- Can we apply similar techniques to more general distributions?

Summing up

- IND-CPA implies IND-SO-CPA for Markov Distributions.
- Our approach extends to *low-dependency* distributions.
- However, there's a gap to distributions used in [HRW15].
- Can we apply similar techniques to more general distributions?