RUB

RUHR-UNIVERSITÄT BOCHUM

Security under Selective Opening Attacks

UbiCrypt Research Retreat, October 5th, 2015

Felix Heuer, Chair for Cryptography
Horst Görtz Institute for IT Security
Ruhr University Bochum

hgi
Horst Görtz Institut
für IT-Sicherheit

Selective Opening Attacks

Selective Opening Attacks

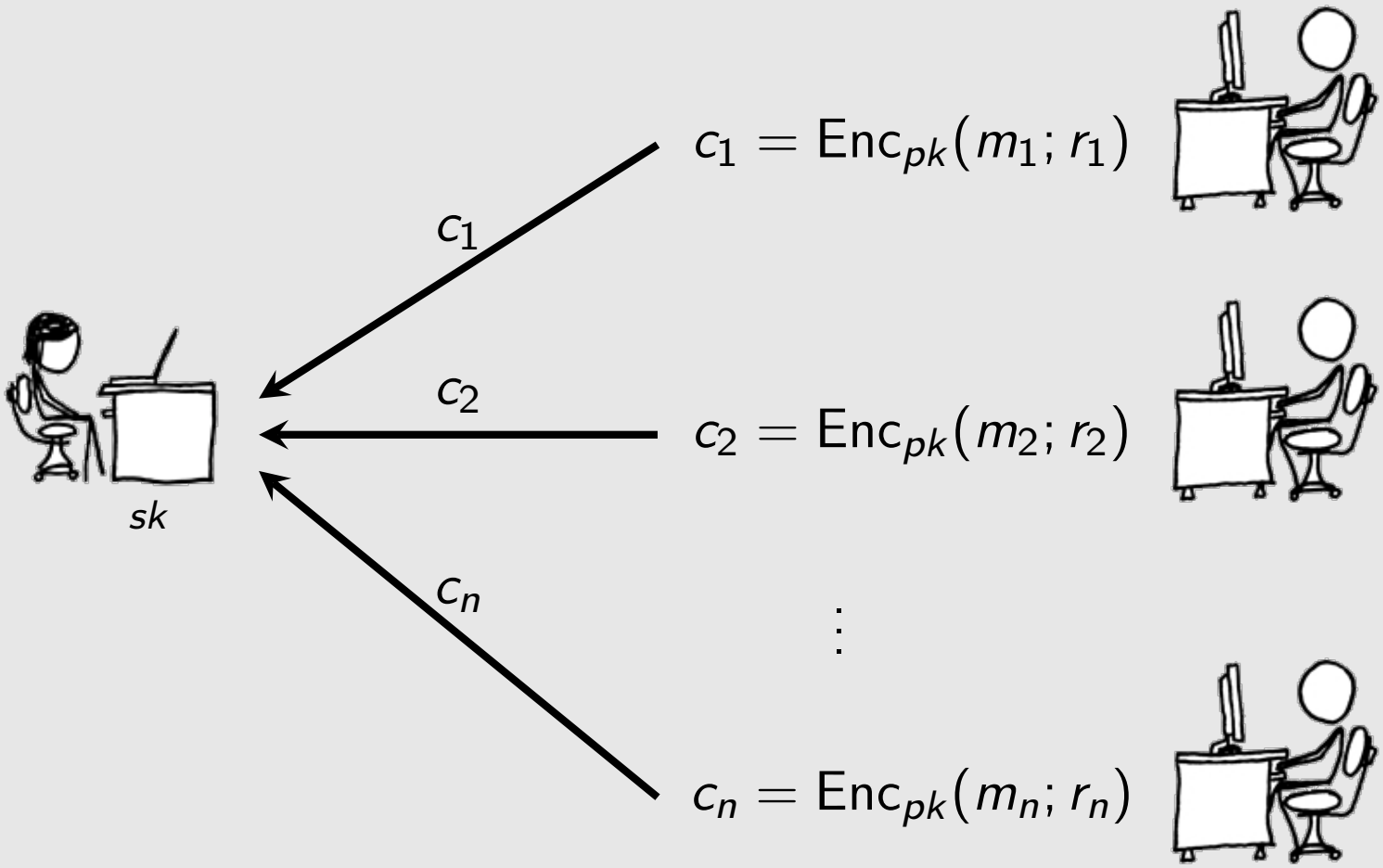


Image source: xkcd.com

Selective Opening Attacks

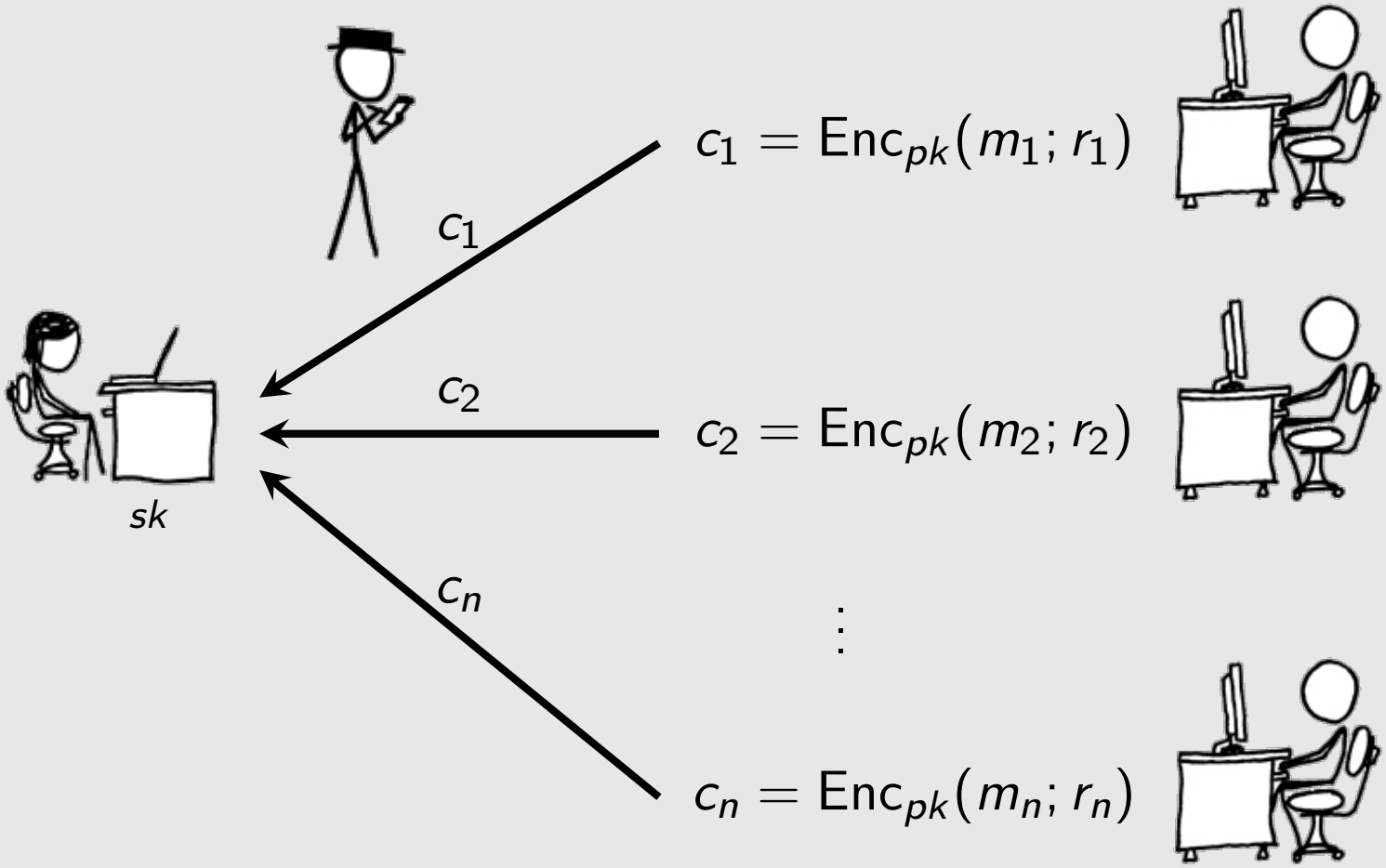


Image source: xkcd.com

Selective Opening Attacks

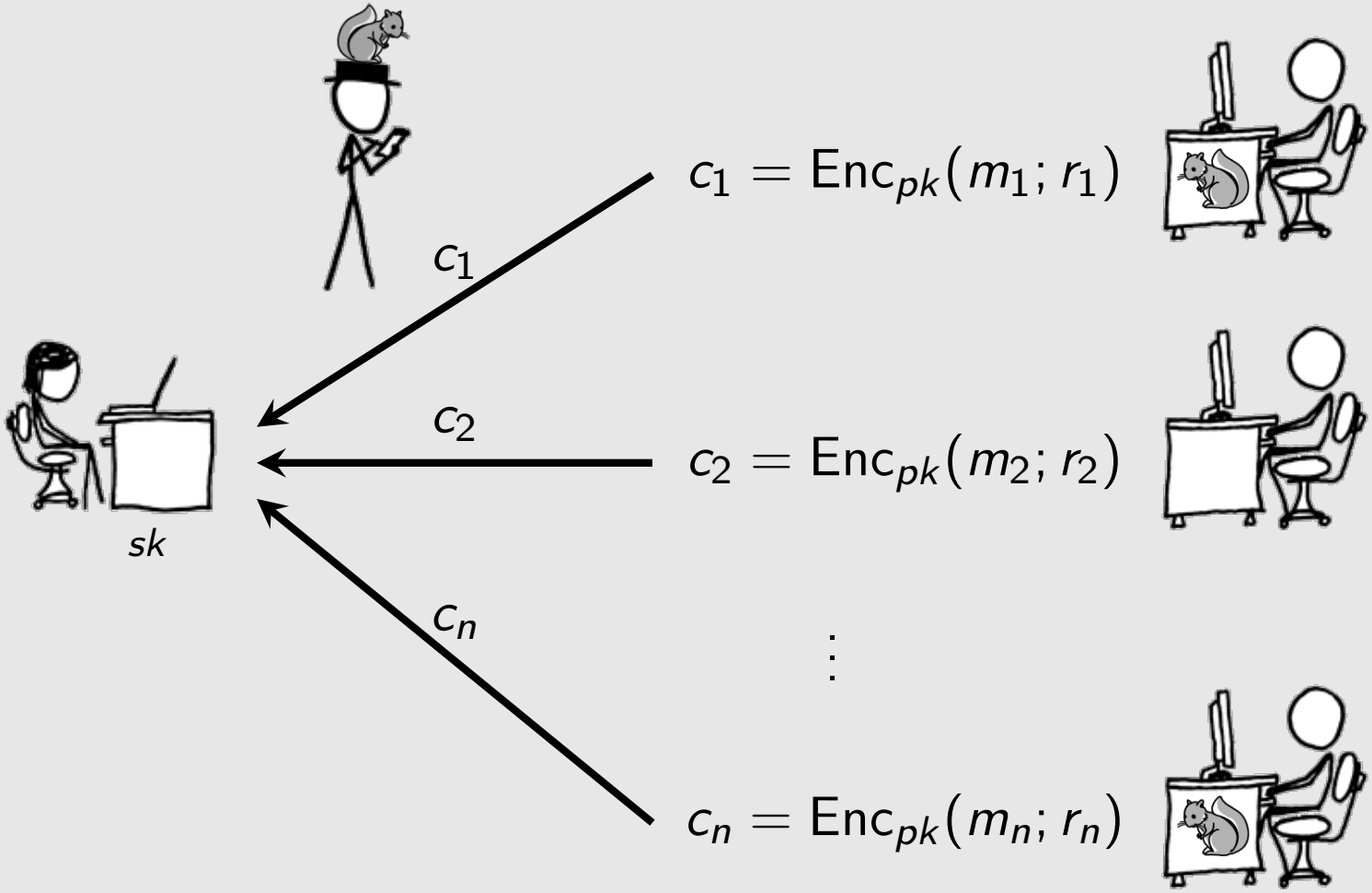


Image source: xkcd.com

Selective Opening Attacks

Do the messages of uncorrupted parties remain confidential?

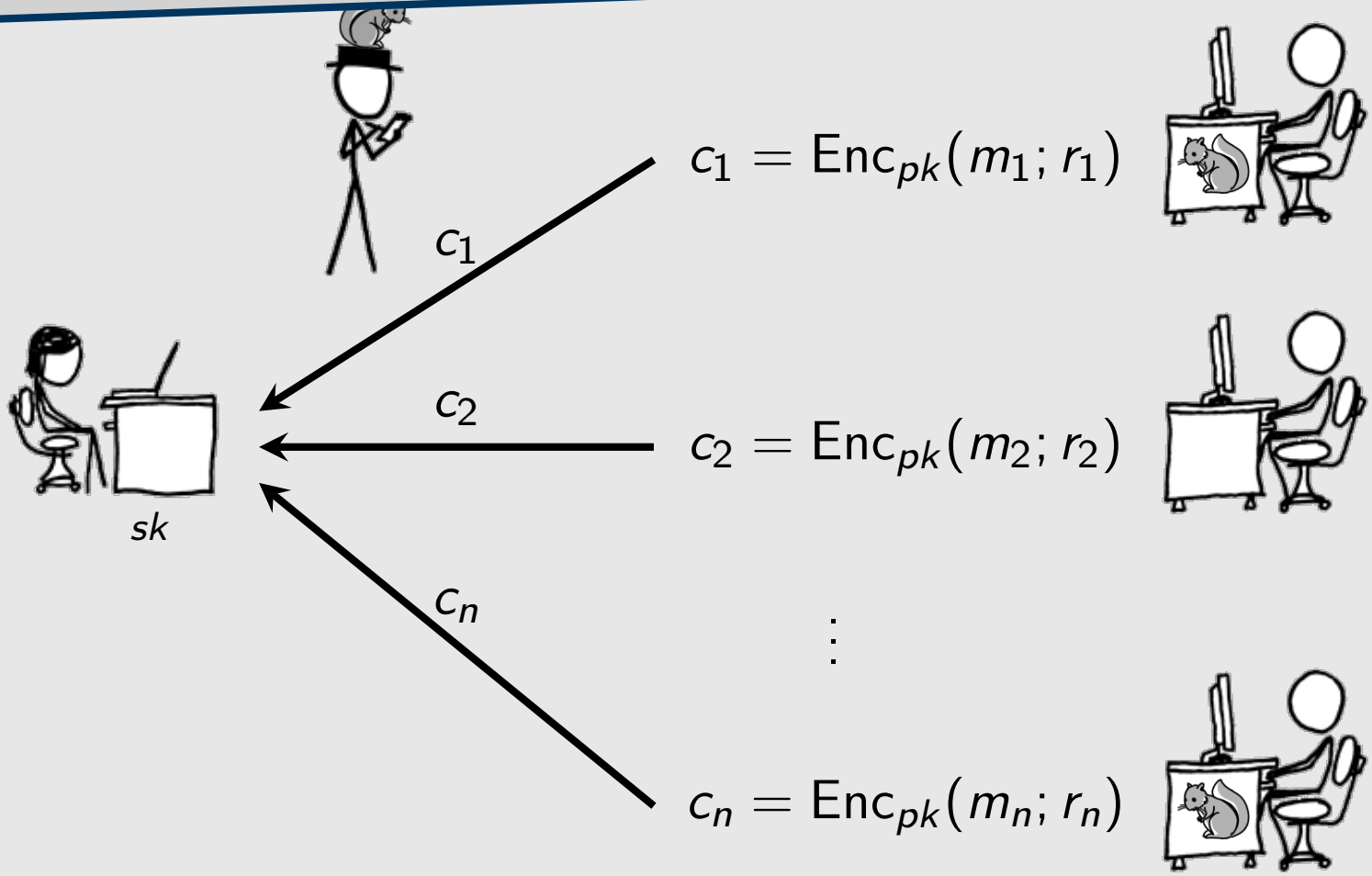
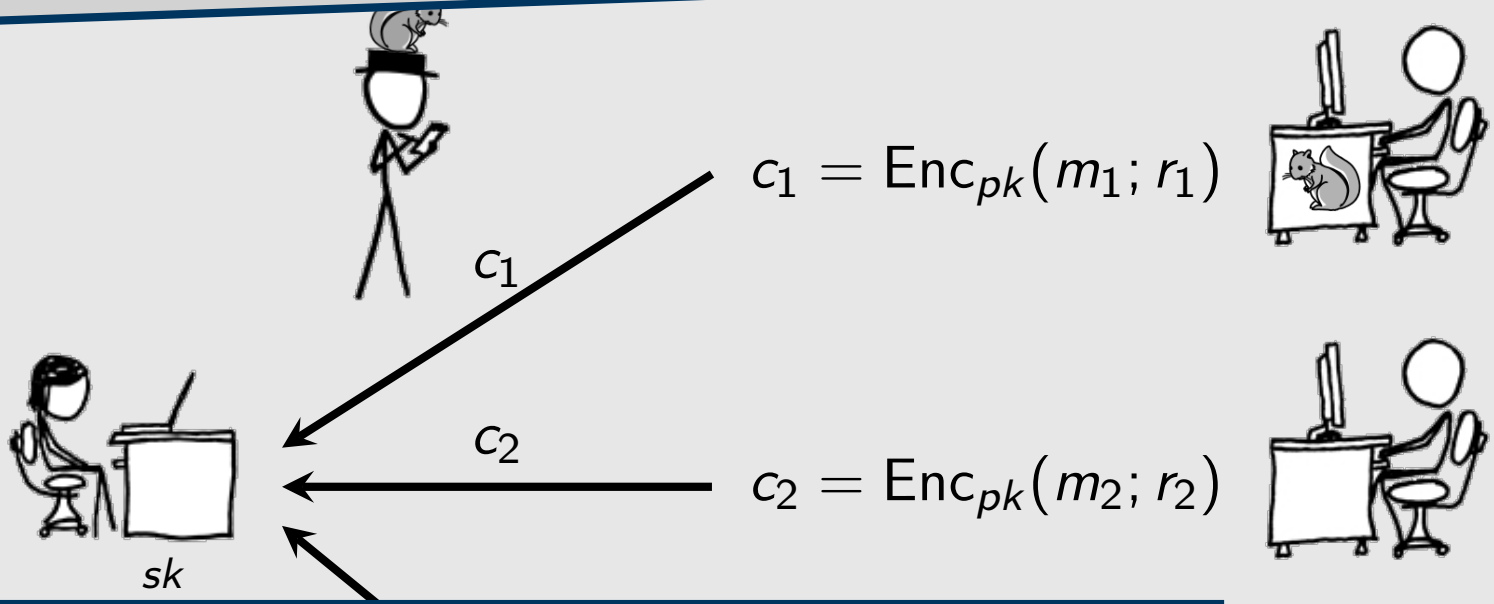


Image source: xkcd.com

Selective Opening Attacks

Do the messages of uncorrupted parties remain confidential?

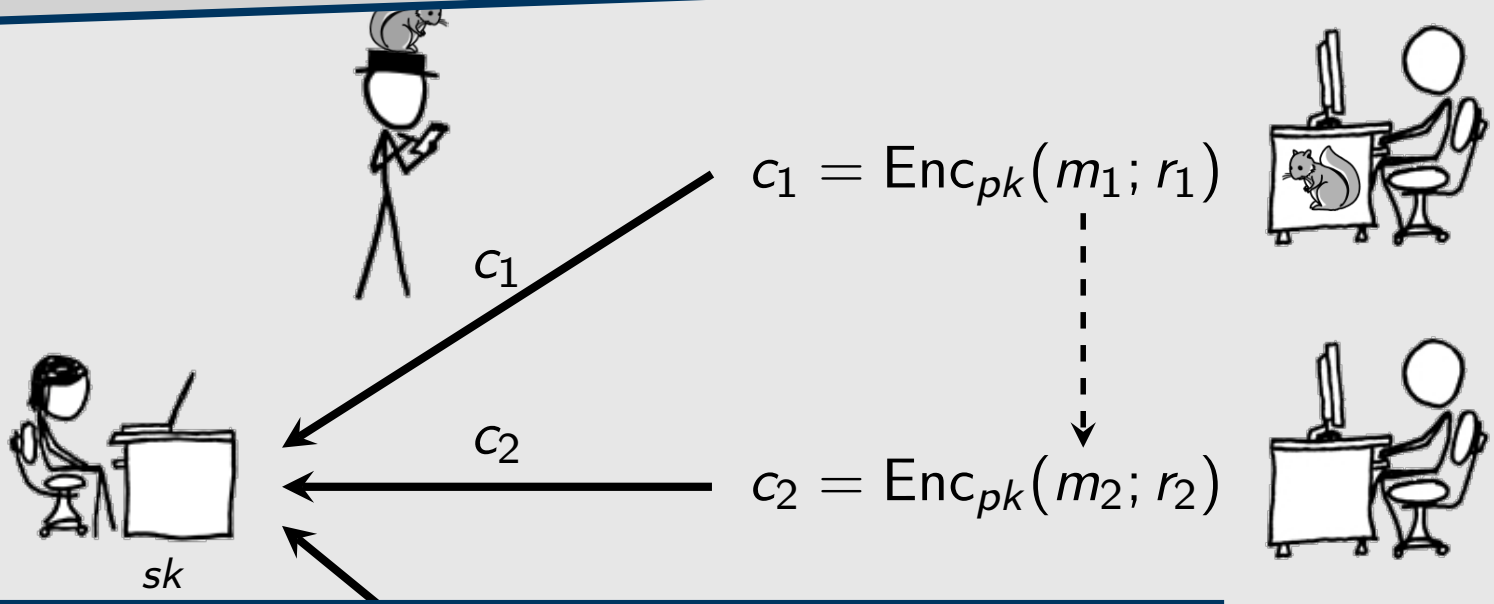


- Naturally arises in secure MPC

Image source: xkcd.com

Selective Opening Attacks

Do the messages of uncorrupted parties remain confidential?

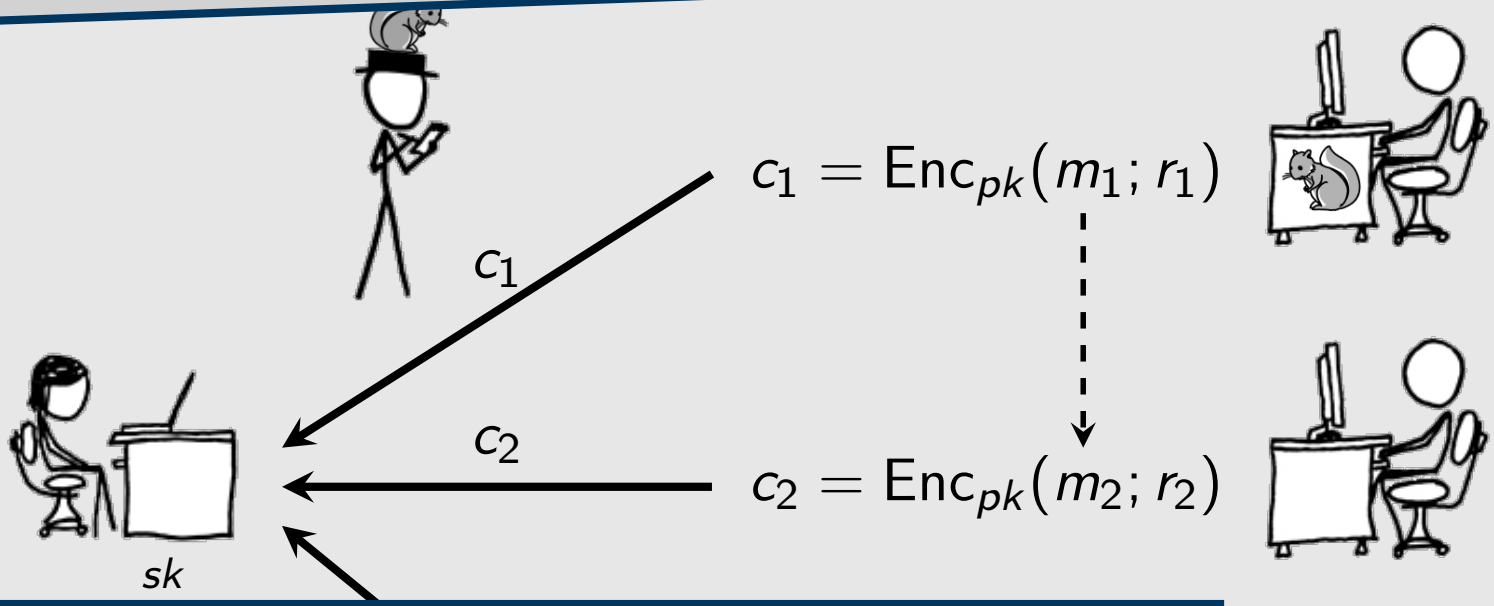


- Naturally arises in secure MPC
- Messages may depend on another

Image source: xkcd.com

Selective Opening Attacks

Do the messages of uncorrupted parties remain confidential?

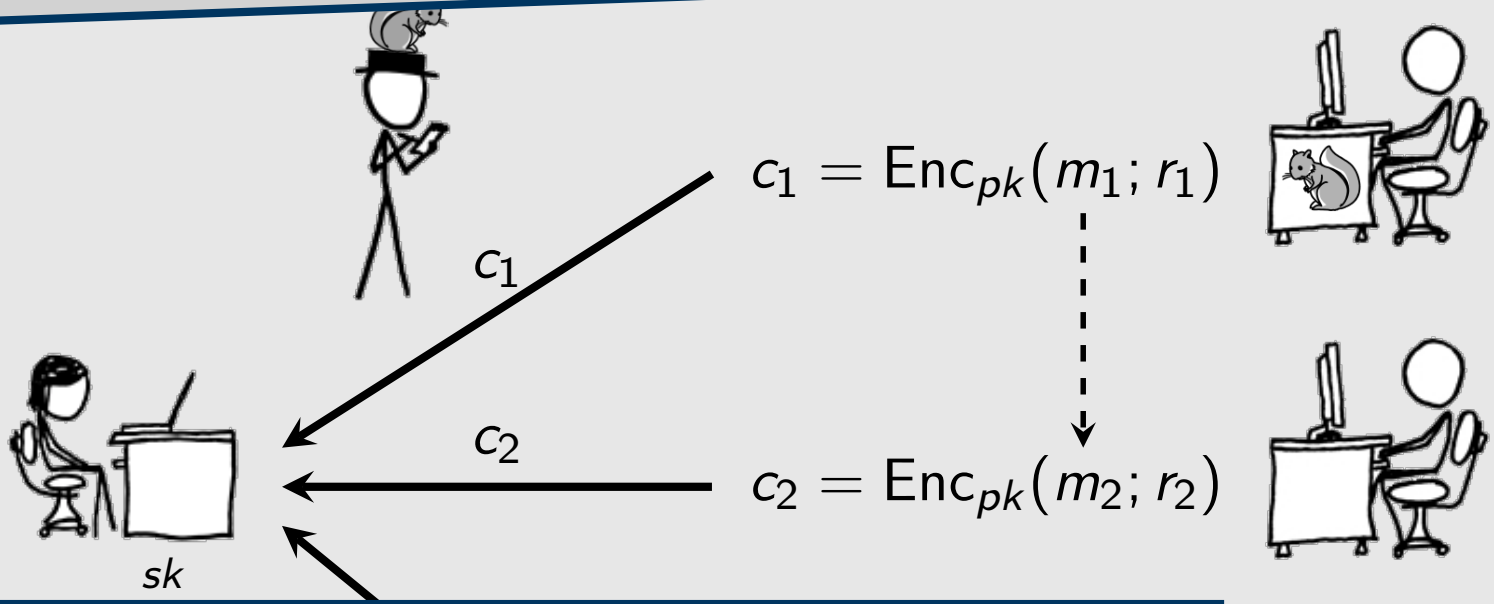


- Naturally arises in secure MPC
- Messages may depend on another
- Three definitions of passive security under SO

Image source: xkcd.com

Selective Opening Attacks

Do the messages of uncorrupted parties remain confidential?

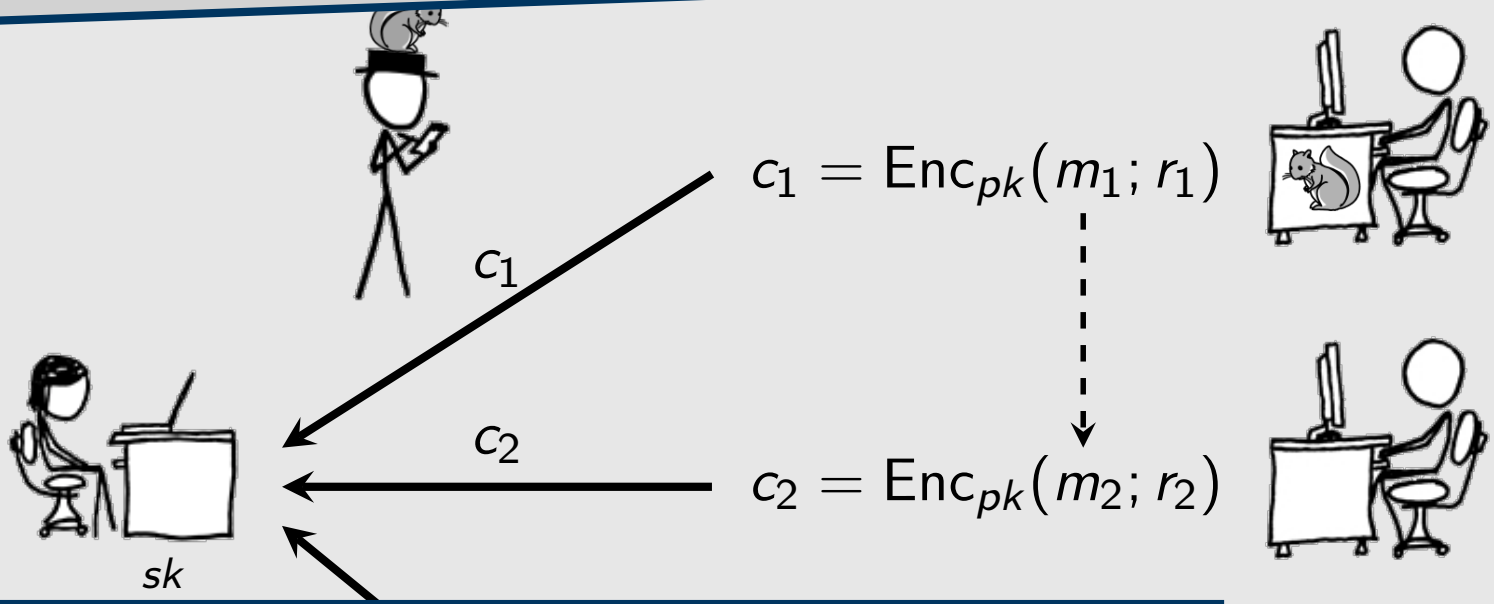


- Naturally arises in secure MPC
- Messages may depend on another
- Three definitions of passive security under SO
- **Not** implied by CPA security! [HRW15]

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
- Three definitions of passive security under SO
- **Not** implied by CPA security! [HRW15]
- 14 papers on IACR conferences since 2009

Image source: xkcd.com

Selective Opening Attacks

Joined the chair for Cryptography in 2014

Selective Opening Attacks

Joined the chair for Cryptography in 2014

- **PKC 2015**: Existing schemes obtain SO security for free
  DHIES, RSA-OAEP are SO secure in a strongest sense [HJKS15]

Selective Opening Attacks

Joined the chair for Cryptography in 2014

- **PKC 2015**: Existing schemes obtain SO security for free
  DHIES, RSA-OAEP are SO secure in a strongest sense [HJKS15]
- **TCC 2016-A**: When does CPA entail SO-CPA for *any* scheme?
  Holds for low-dependency message distributions [HKP16]

Defining SO-CPA Security

Adversary obtains pk and submits a distribution $\mathcal{M}(pk)$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathcal{M}$

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

Image source: xkcd.com

Defining SO-CPA Security

Adversary obtains pk and submits a distribution $\mathcal{M}(pk)$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathcal{M}$

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

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

Image source: xkcd.com

Defining SO-CPA Security

Adversary obtains pk and submits a distribution $\mathcal{M}(pk)$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathcal{M}$

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

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

Image source: xkcd.com

Defining SO-CPA Security

Adversary obtains pk and submits a distribution $\mathcal{M}(pk)$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathcal{M}$

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

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

Image source: xkcd.com

Defining SO-CPA Security

Adversary obtains pk and submits a distribution $\mathcal{M}(pk)$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathcal{M}$

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

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

Image source: xkcd.com

Defining SO-CPA Security

Adversary obtains pk and submits a distribution $\mathcal{M}(pk)$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathcal{M}$

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

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

Image source: xkcd.com

Defining SO-CPA Security

Adversary obtains pk and submits a distribution $\mathcal{M}(pk)$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathcal{M}$

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

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

Challenge:

$$(\, m_1 \qquad m_2 \qquad m_3 \qquad m_4 \qquad \cdots \qquad m_n \,)$$

Image source: xkcd.com

Defining SO-CPA Security

Adversary obtains pk and submits a distribution $\mathcal{M}(pk)$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathcal{M}$

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

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

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 SO-CPA Security

Adversary obtains pk and submits a distribution $\mathcal{M}(pk)$ of its choice.

$(m_1, \ldots, m_n) \leftarrow \mathcal{M}$

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

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

Challenge:

or

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

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

Image source: xkcd.com

Defining SO-CPA Security

Stepping stone in showing 'CPA ⇒ SO-CPA'

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

Challenge:

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

or $\approx$

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

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

Image source: xkcd.com

Defining SO-CPA Security

Stepping stone in showing 'CPA ⇒ SO-CPA'

The reduction has to know $m_3, m_4, \ldots$

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

Challenge:

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

or $\approx$

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

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

Image source: xkcd.com

Defining SO-CPA Security

Stepping stone in showing 'CPA ⇒ SO-CPA'

The reduction has to know $m_3, m_4, \ldots$
before $\mathcal{A}$ announced the first ciphertext it would like to open.

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

Challenge:

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

or $\approx$

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

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

Image source: xkcd.com

Defining SO-CPA Security

Stepping stone in showing 'CPA ⇒ SO-CPA'

The reduction has to know $m_3, m_4, \ldots$
before $\mathcal{A}$ announced the first ciphertext it would like to open.
$\rightsquigarrow$ exponential loss due to guessing of opening queries.

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

Challenge:

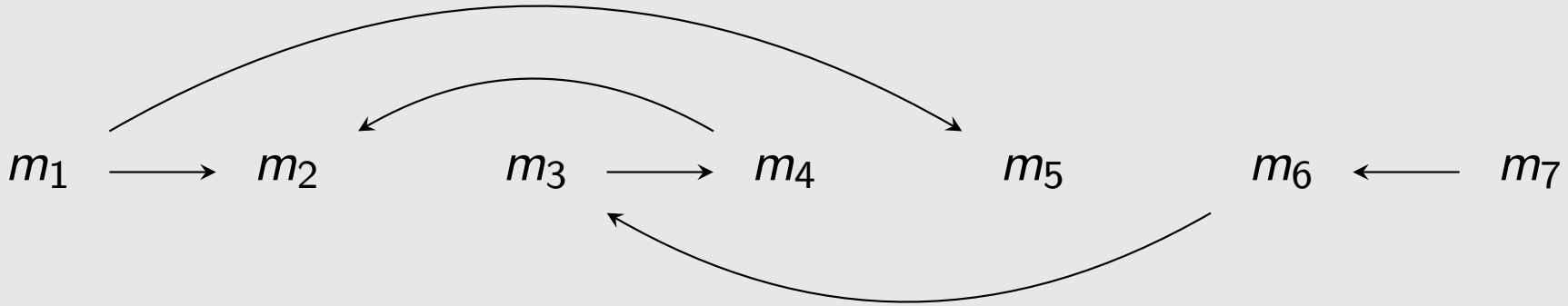
or

$$\begin{array}{ccccccc} (m_1 & m_2 & m_3 & & m_4 & \ldots & m_n) \\ & & & \approx & & & \\ (m_1 & m_2 & m_3 & & m_4 & \ldots & m_n) \end{array}$$

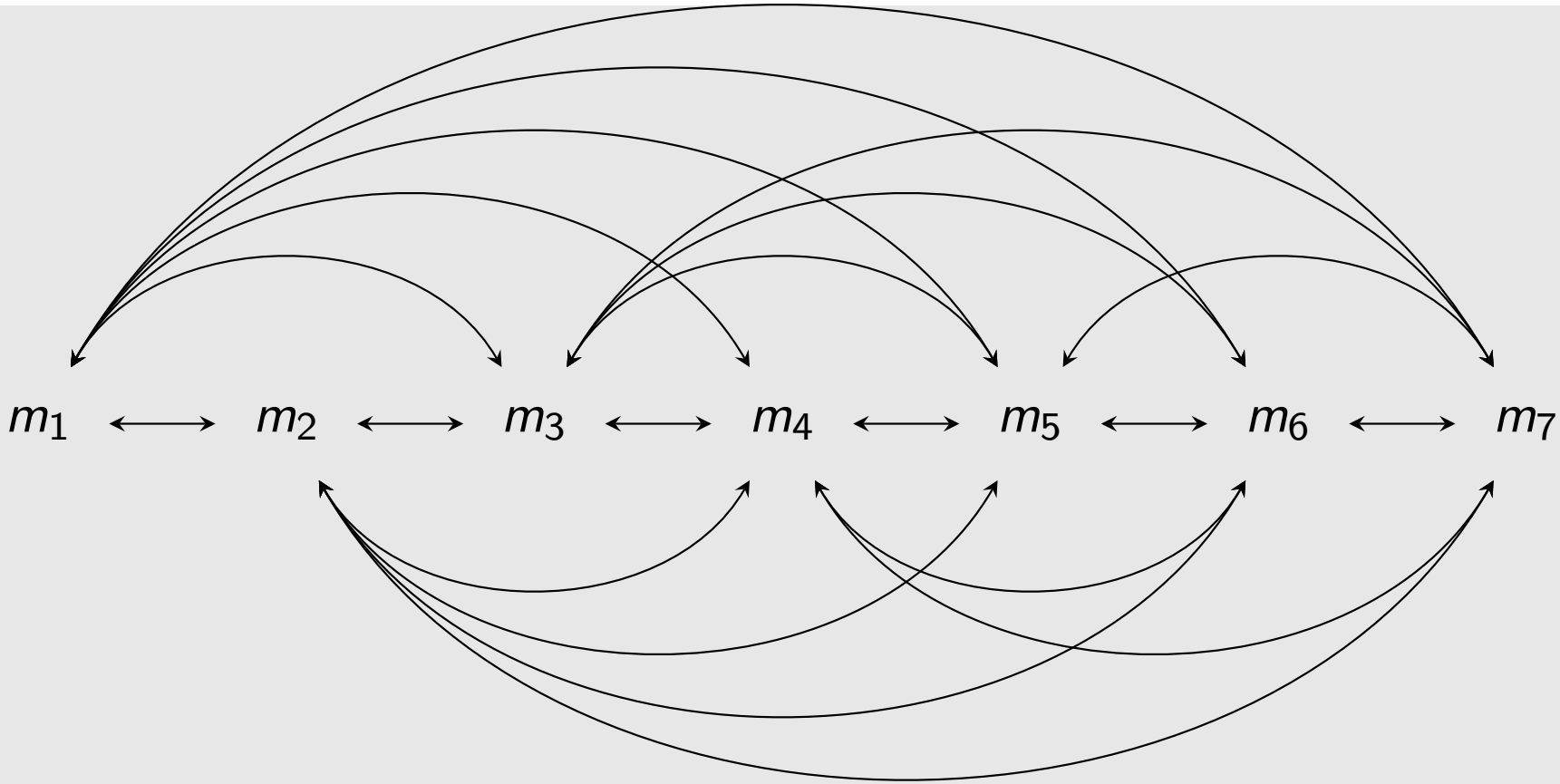
where $m_3, m_4, \ldots$ are resampled conditioned on *every* opened ciphertext.

Image source: xkcd.com

When does 'CPA ⇒ SO-CPA' hold?



When does 'CPA ⇒ SO-CPA' hold?

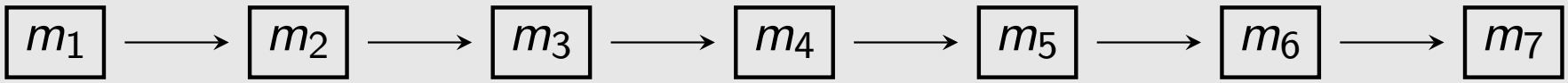


Wishful thinking

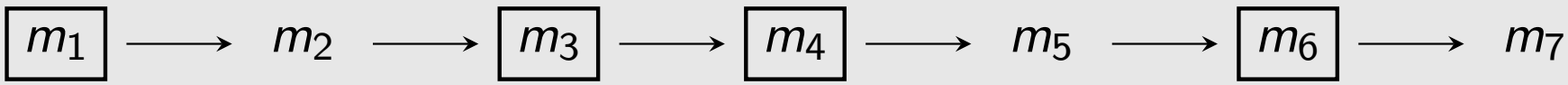
When does 'CPA ⇒ SO-CPA' hold?

m_1 m_2 m_3 m_4 m_5 m_6 m_7

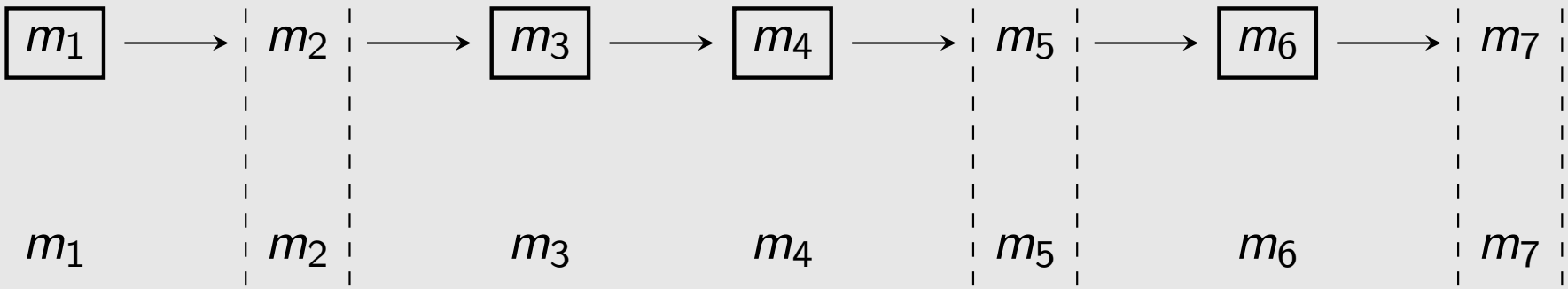
When does 'CPA ⇒ SO-CPA' hold?



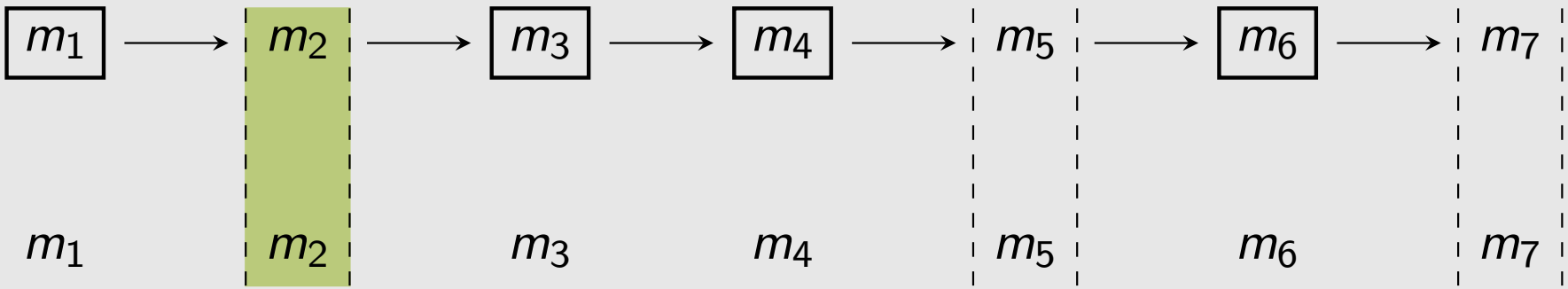
When does 'CPA ⇒ SO-CPA' hold?



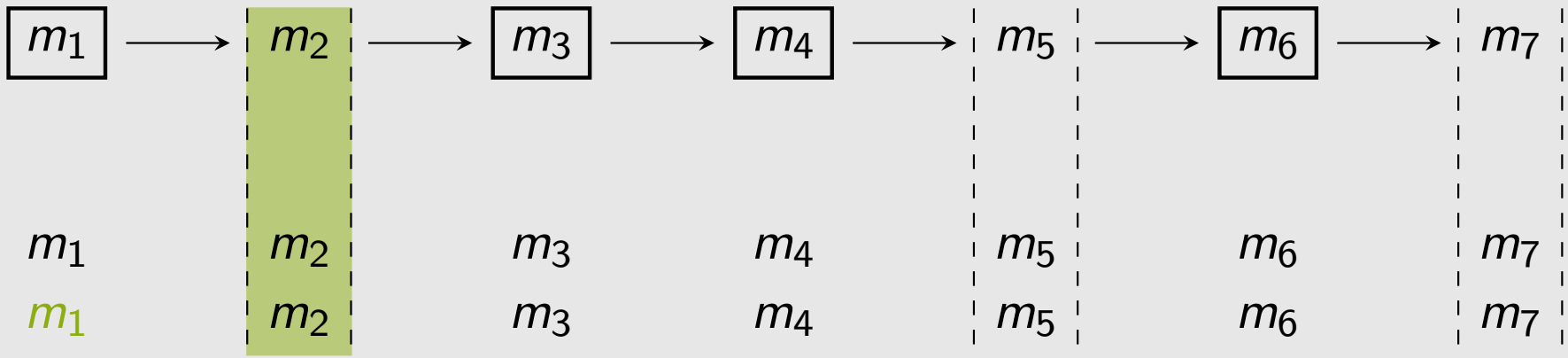
When does 'CPA ⇒ SO-CPA' hold?



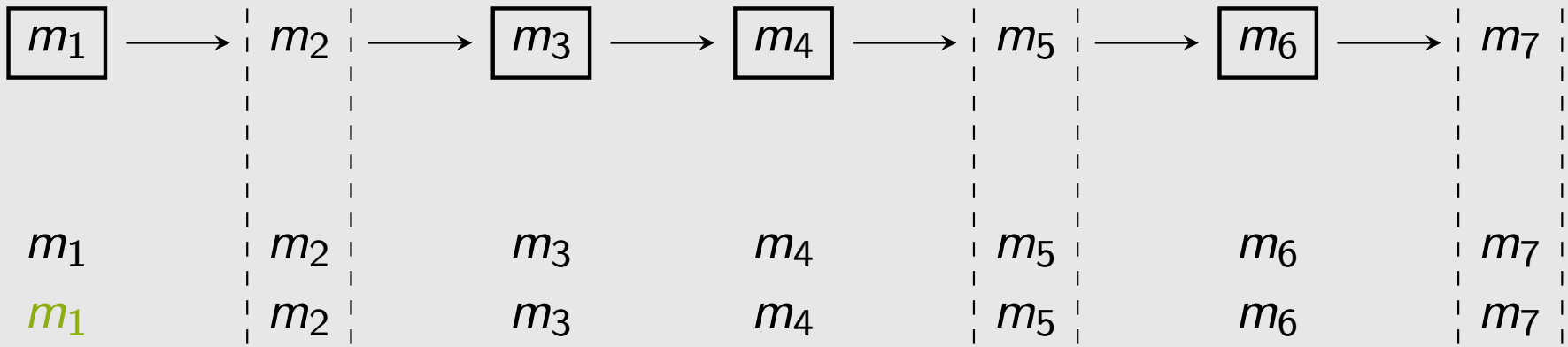
When does 'CPA ⇒ SO-CPA' hold?



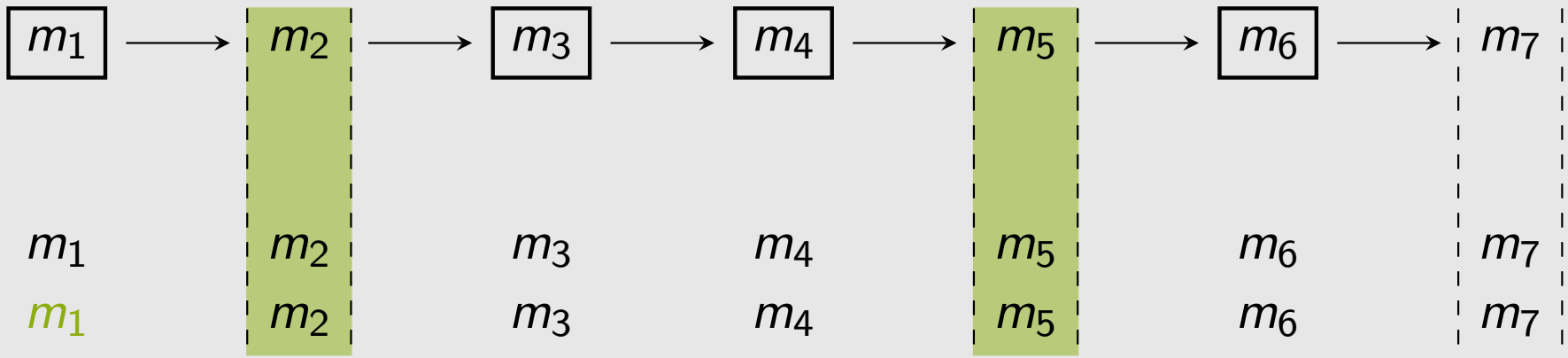
When does 'CPA ⇒ SO-CPA' hold?



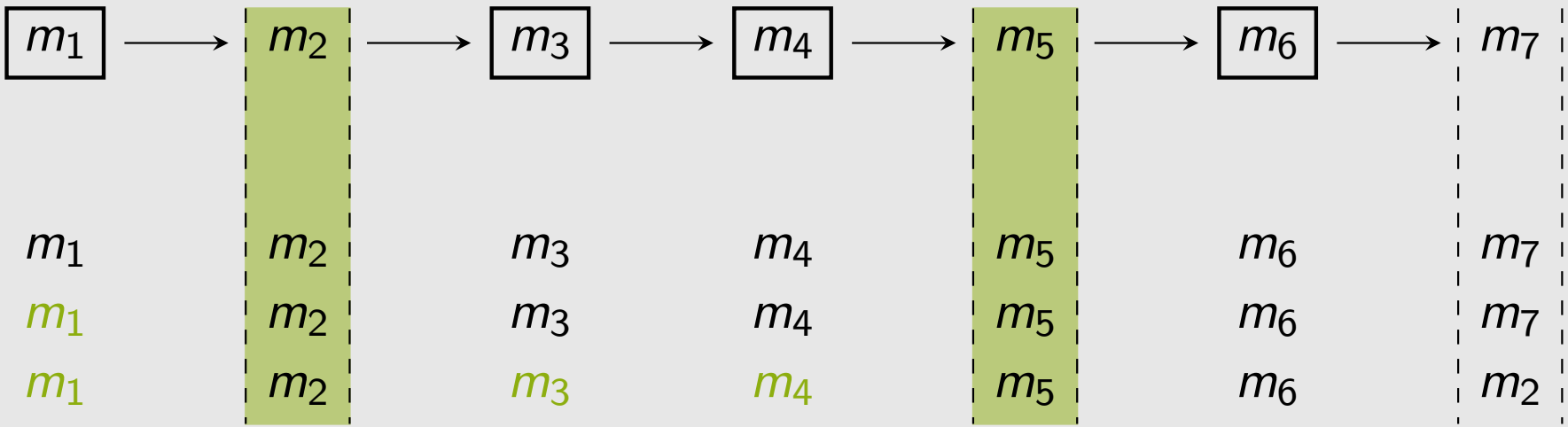
When does 'CPA ⇒ SO-CPA' hold?



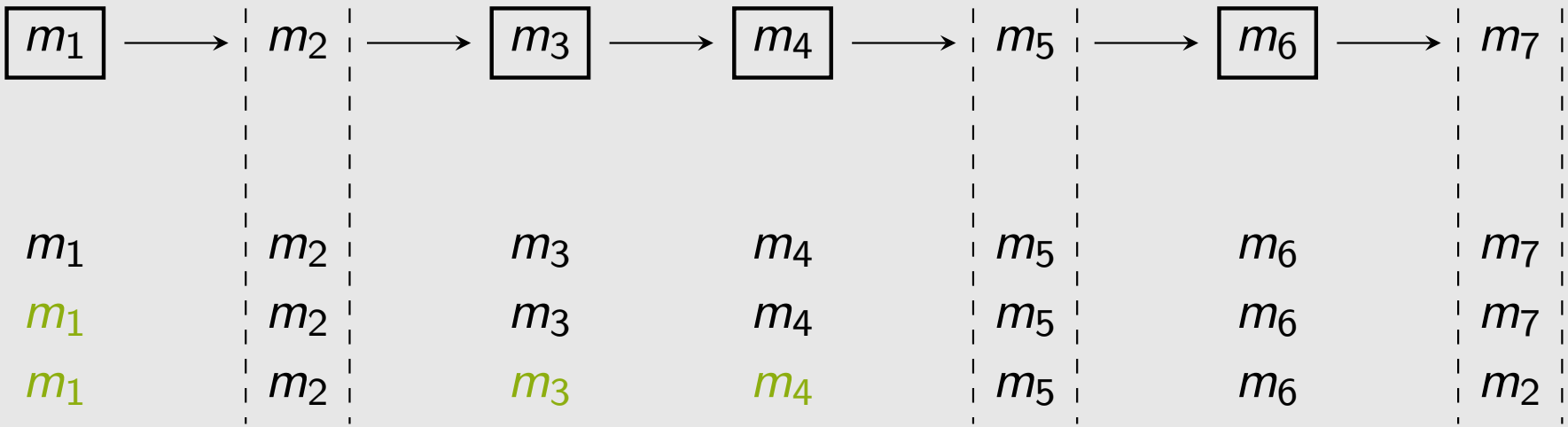
When does 'CPA ⇒ SO-CPA' hold?



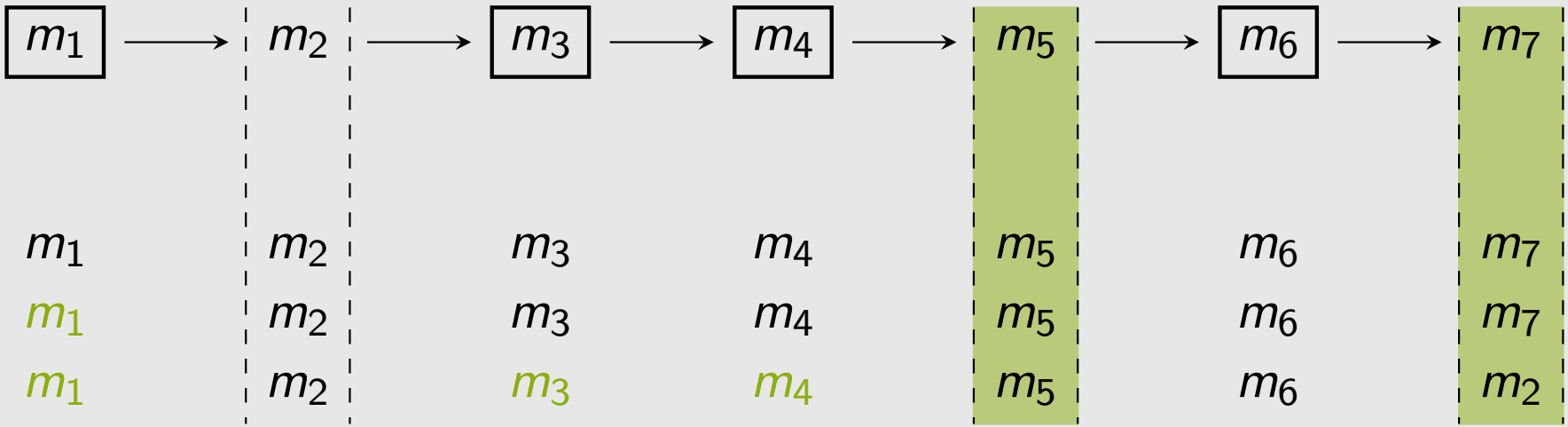
When does 'CPA ⇒ SO-CPA' hold?



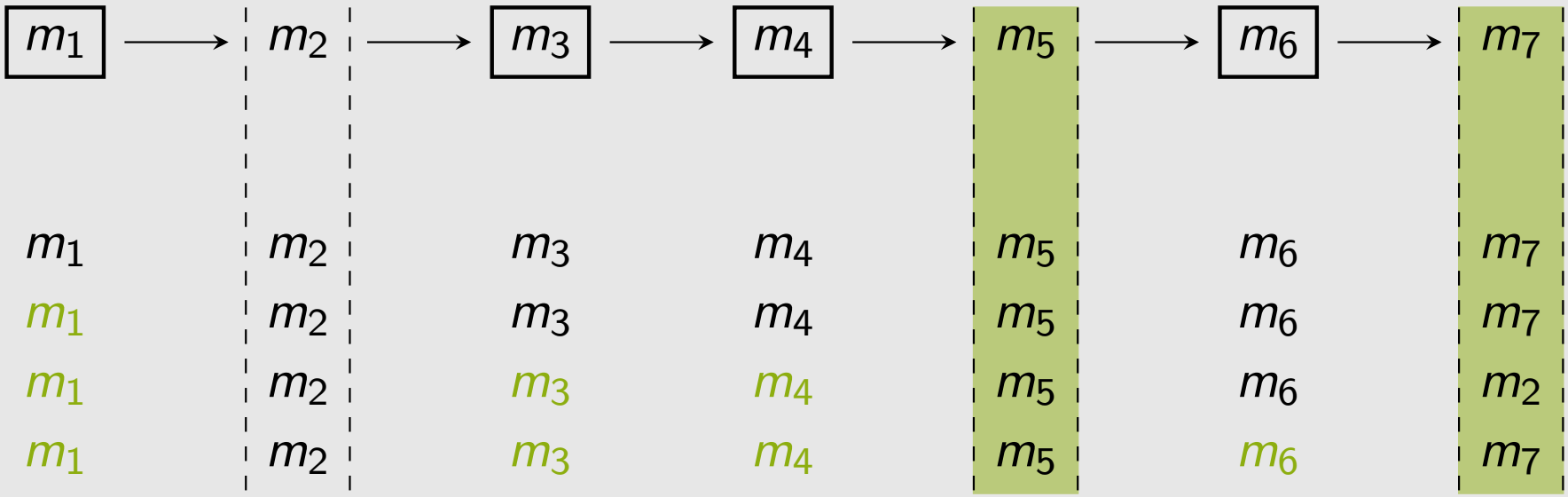
When does 'CPA ⇒ SO-CPA' hold?



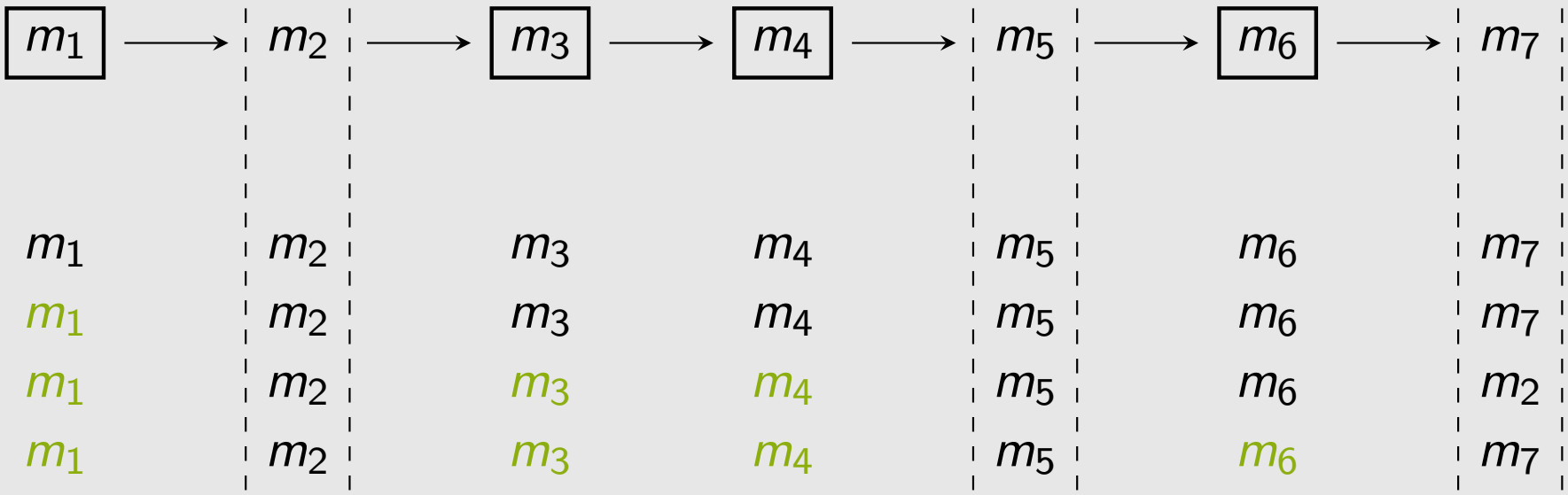
When does 'CPA ⇒ SO-CPA' hold?



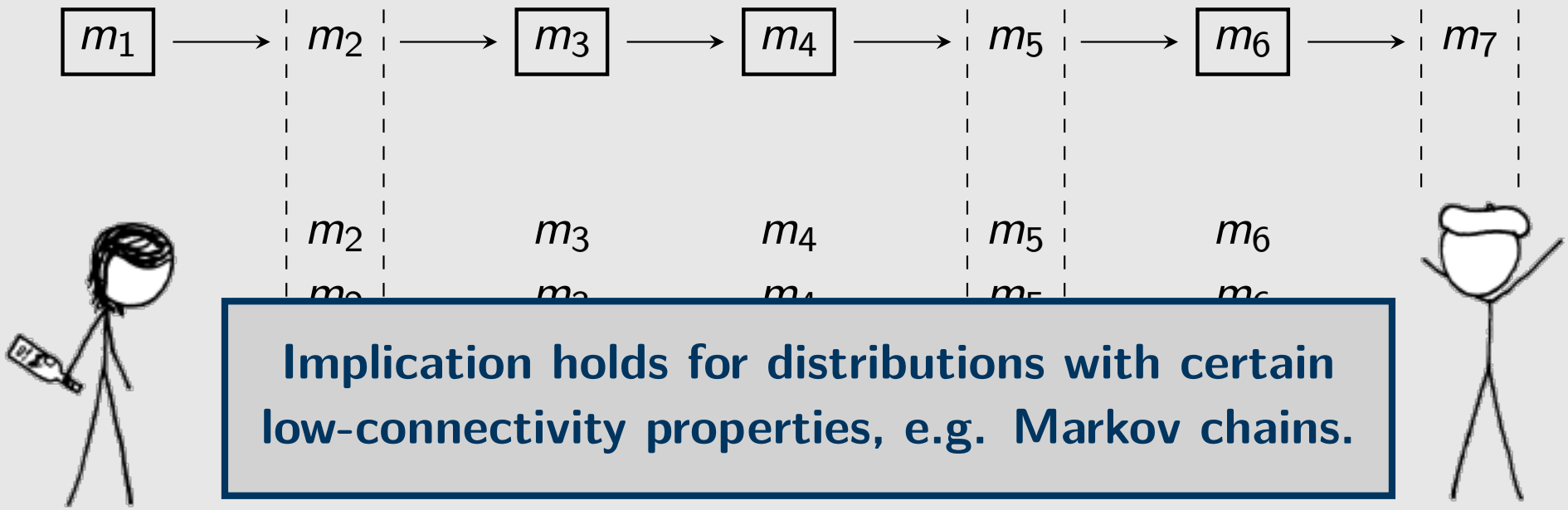
When does 'CPA ⇒ SO-CPA' hold?



When does 'CPA ⇒ SO-CPA' hold?



When does 'CPA ⇒ SO-CPA' hold?



Implication holds for distributions with certain low-connectivity properties, e.g. Markov chains.

Image source: xkcd.com