Unfair Coin Tossing

Grégory Demay and Ueli Maurer

Department of Computer Science
ETH Zürich

ISIT 2013

Outline

Outline

Coin Tossing Protocols

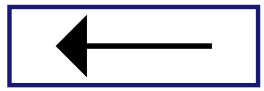
Setting

- 2 distrustful parties: one of them being potentially dishonest
- *Goal*: construct an ideal coin tossing resource

Ideal Coin Tossing Resource

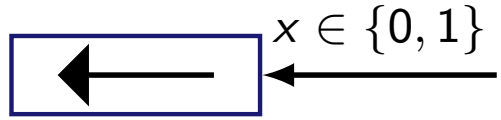
Available Resources

Perfect Communication Channel



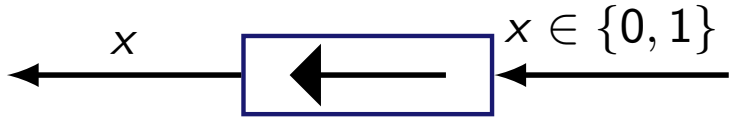
Available Resources

Perfect Communication Channel



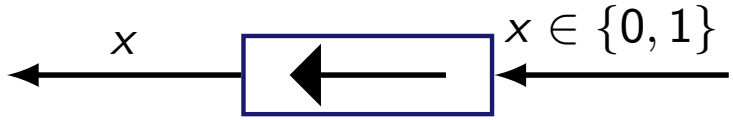
Available Resources

Perfect Communication Channel

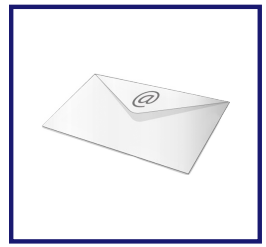


Available Resources

Perfect Communication Channel

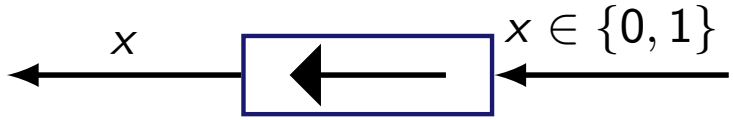


Ideal Bit Commitment Resource

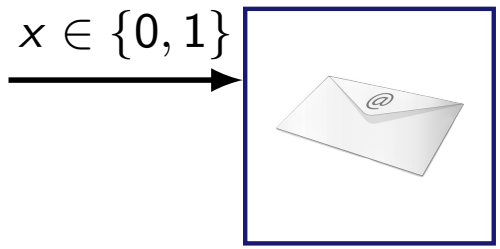


Available Resources

Perfect Communication Channel

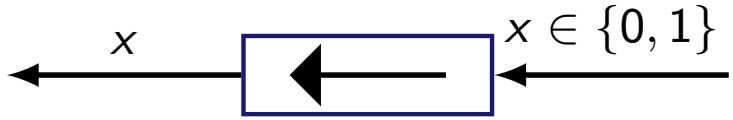


Ideal Bit Commitment Resource

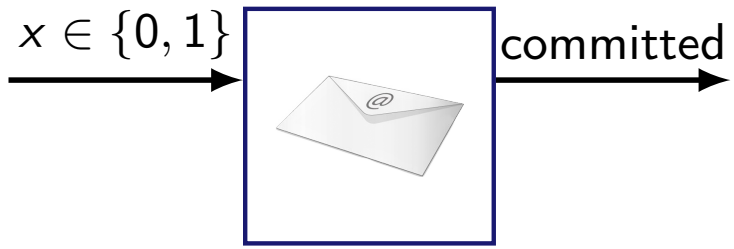


Available Resources

Perfect Communication Channel

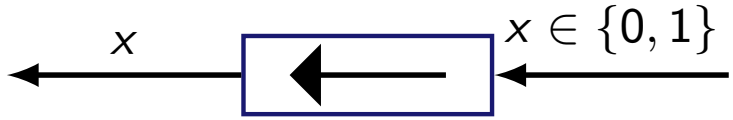


Ideal Bit Commitment Resource

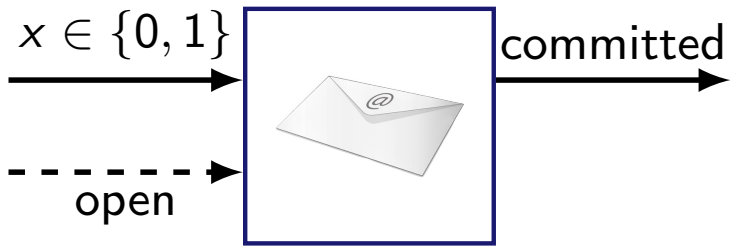


Available Resources

Perfect Communication Channel

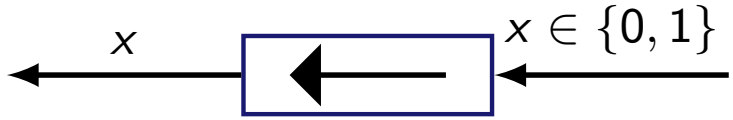


Ideal Bit Commitment Resource

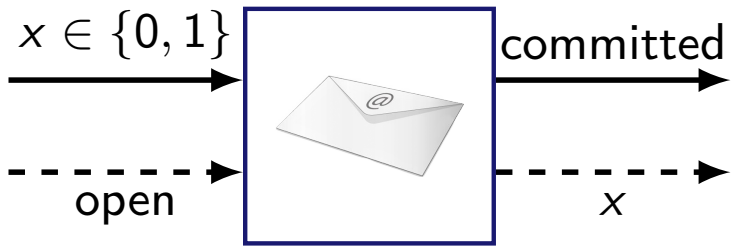


Available Resources

Perfect Communication Channel

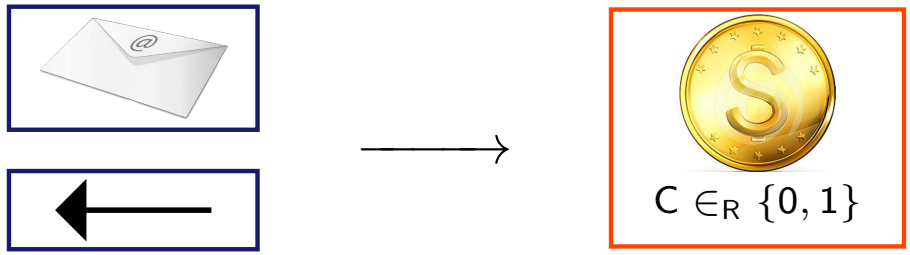


Ideal Bit Commitment Resource



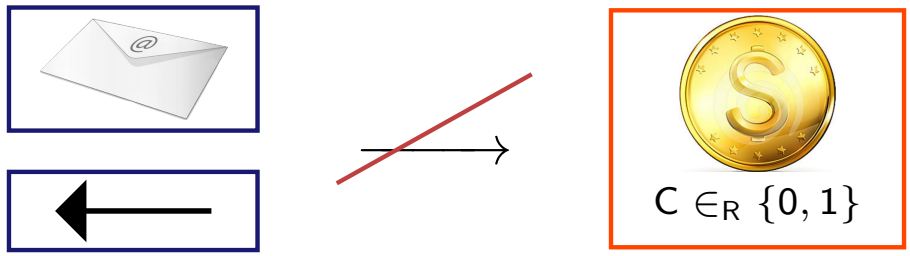
Motivation

Goal



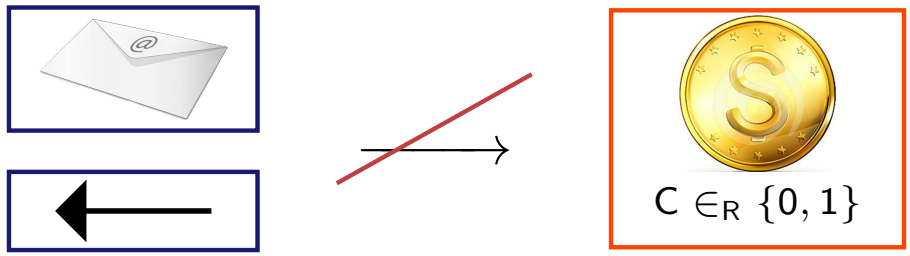
Motivation

(Unachievable) Goal



Motivation

(Unachievable) Goal



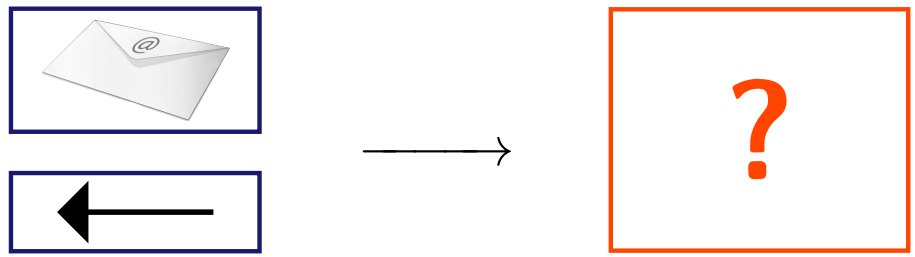
Previous Work

Cl86 : every coin tossing protocol with r rounds has a bias of $\Omega\left(\frac{1}{r}\right)$

- No guarantee in case of abortion
- Notion of optimally fair coin tossing protocol [Katz07], [MNS09], [BOO10] ...

Motivation

This Work



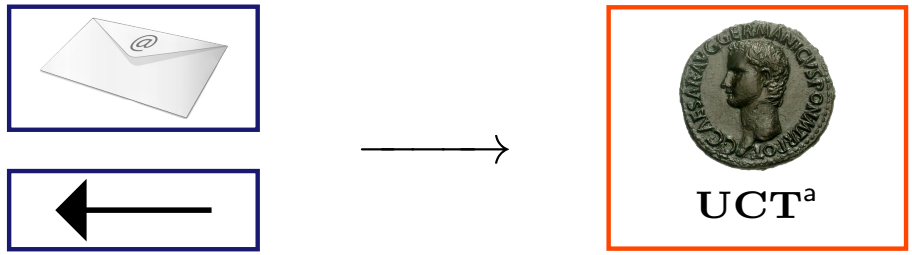
Previous Work

Cl86 : every coin tossing protocol with r rounds has a bias of $\Omega\left(\frac{1}{r}\right)$

- No guarantee in case of abortion
- Notion of optimally fair coin tossing protocol [Katz07], [MNS09], [BOO10] ...

Motivation

This Work



Previous Work

Cl86 : every coin tossing protocol with r rounds has a bias of $\Omega\left(\frac{1}{r}\right)$

- No guarantee in case of abortion
- Notion of optimally fair coin tossing protocol [Katz07], [MNS09], [BOO10] ...

The Construction Paradigm[1]

Construction Concept

real resource **R** $\xrightarrow{(\text{protocol } \pi, \varepsilon)}$ ideal resource **S**

[1] U. Maurer and R. Renner: *Abstract Cryptography*, 2011

The Construction Paradigm[1]

Construction Concept

real resource **R** $\xrightarrow{(\text{protocol } \pi, \varepsilon)}$ ideal resource **S**

Generally Composable Constructions

- Sequential Composability

$$\mathbf{R} \xrightarrow{(\pi_1,\varepsilon_1)} \mathbf{S} \;\wedge\; \mathbf{S} \xrightarrow{(\pi_2,\varepsilon_2)} \mathbf{T} \;\Longrightarrow\; \mathbf{R} \xrightarrow{(\pi_1 \circ \pi_2, \varepsilon_1 + \varepsilon_2)} \mathbf{T}$$

[1] U. Maurer and R. Renner: *Abstract Cryptography*, 2011

The Construction Paradigm[1]

Construction Concept

$$\text{real resource } \mathbf{R} \xrightarrow{(\text{protocol } \pi, \varepsilon)} \text{ideal resource } \mathbf{S}$$

Generally Composable Constructions

- Sequential Composability

$$\mathbf{R} \xrightarrow{(\pi_1,\varepsilon_1)} \mathbf{S} \;\wedge\; \mathbf{S} \xrightarrow{(\pi_2,\varepsilon_2)} \mathbf{T} \;\Longrightarrow\; \mathbf{R} \xrightarrow{(\pi_1 \circ \pi_2, \varepsilon_1+\varepsilon_2)} \mathbf{T}$$

- Parallel Composability

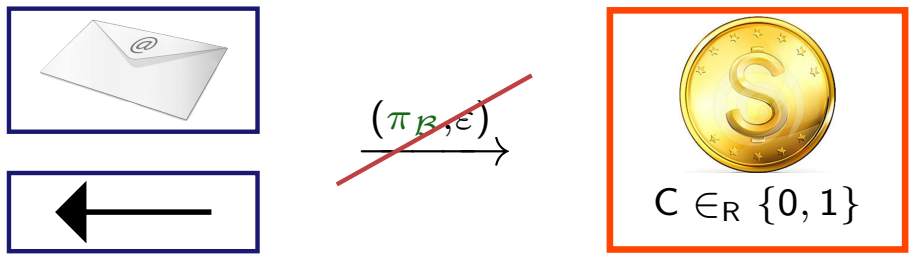
$$\mathbf{R} \xrightarrow{(\pi,\varepsilon)} \mathbf{S} \;\Longrightarrow\; \mathbf{R}\|\mathbf{T} \xrightarrow{(\pi|\mathrm{id},\varepsilon)} \mathbf{S}\|\mathbf{T} \;\wedge\; \mathbf{T}\|\mathbf{R} \xrightarrow{(\mathrm{id}|\pi,\varepsilon)} \mathbf{T}\|\mathbf{S}$$

[1] U. Maurer and R. Renner: *Abstract Cryptography*, 2011

Outline

Blum's Coin Tossing Protocol[2]

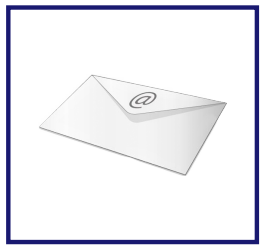
Unachievable Goal



[2] M. Blum: *Coin Flipping By Telephone A Protocol For Solving Impossible Problems*, 1983

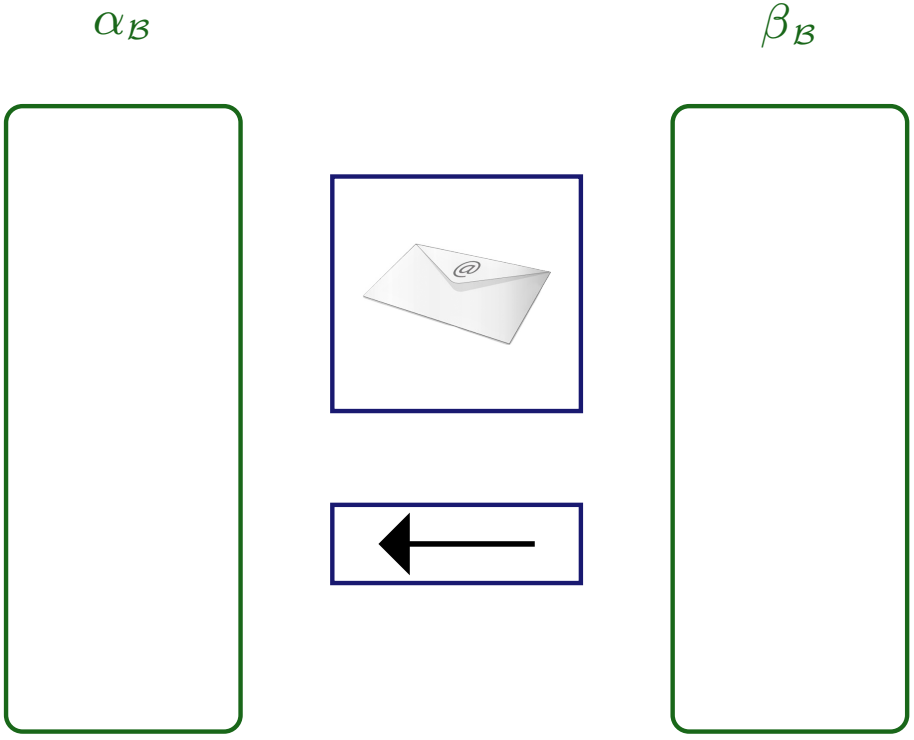
Blum's Coin Tossing Protocol

Honest Execution



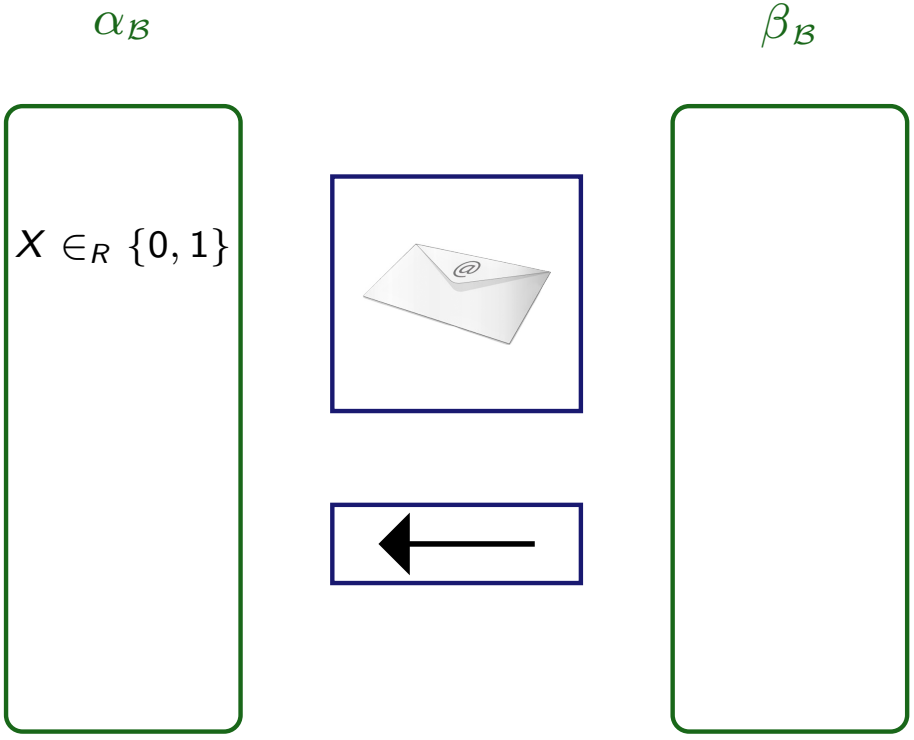
Blum's Coin Tossing Protocol

Honest Execution



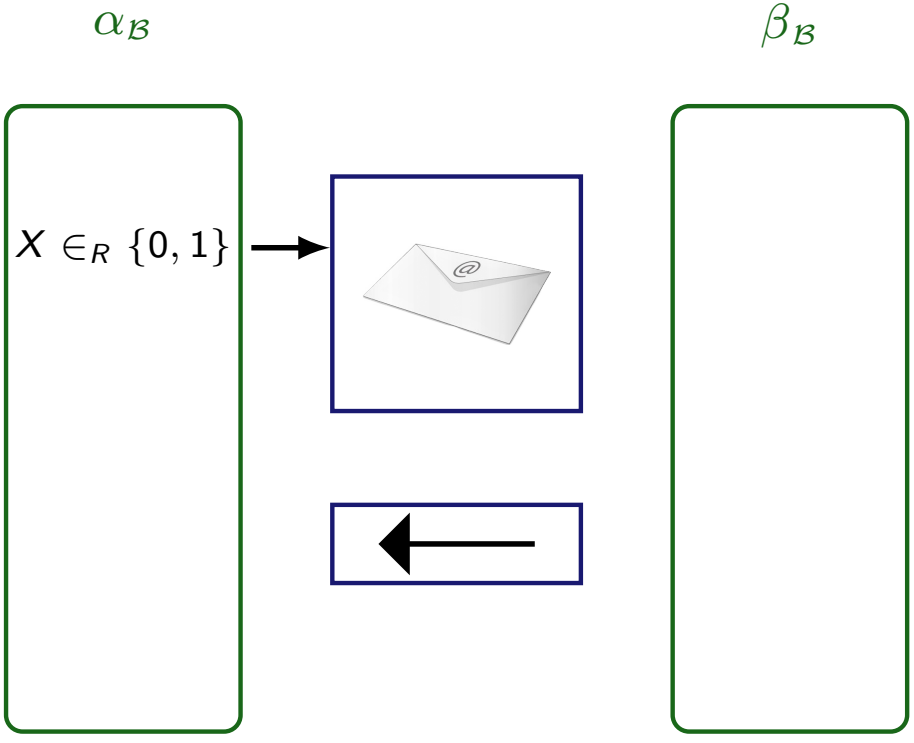
Blum's Coin Tossing Protocol

Honest Execution



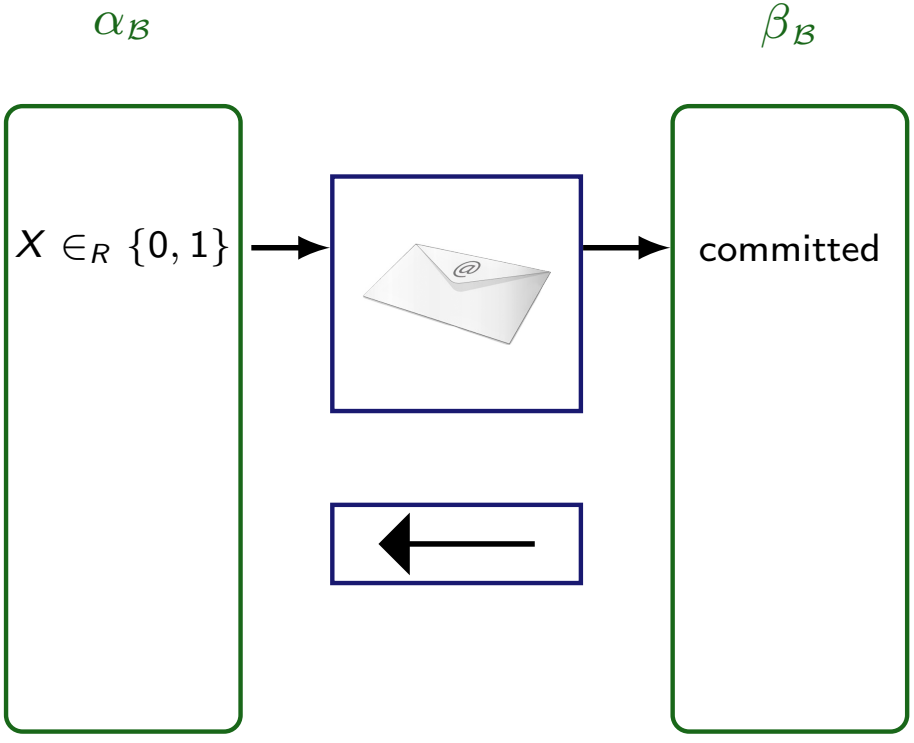
Blum's Coin Tossing Protocol

Honest Execution



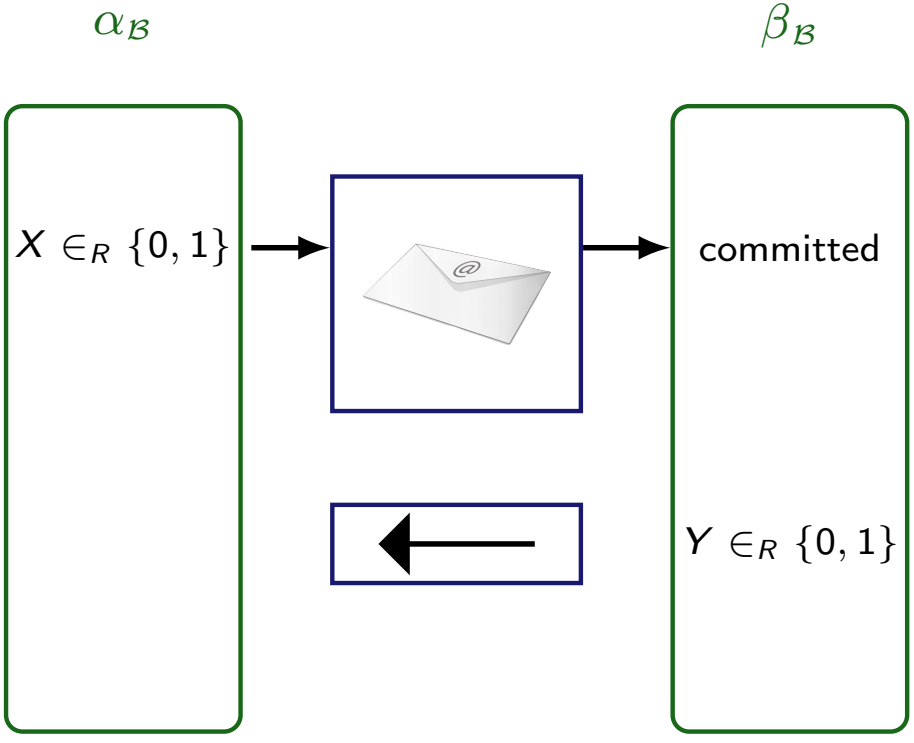
Blum's Coin Tossing Protocol

Honest Execution



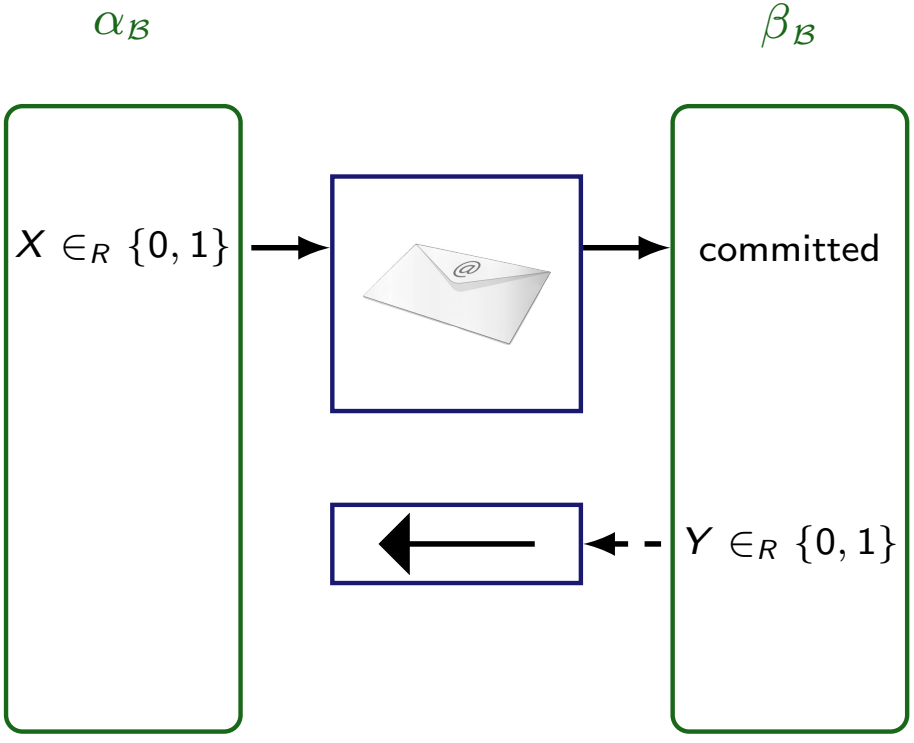
Blum's Coin Tossing Protocol

Honest Execution



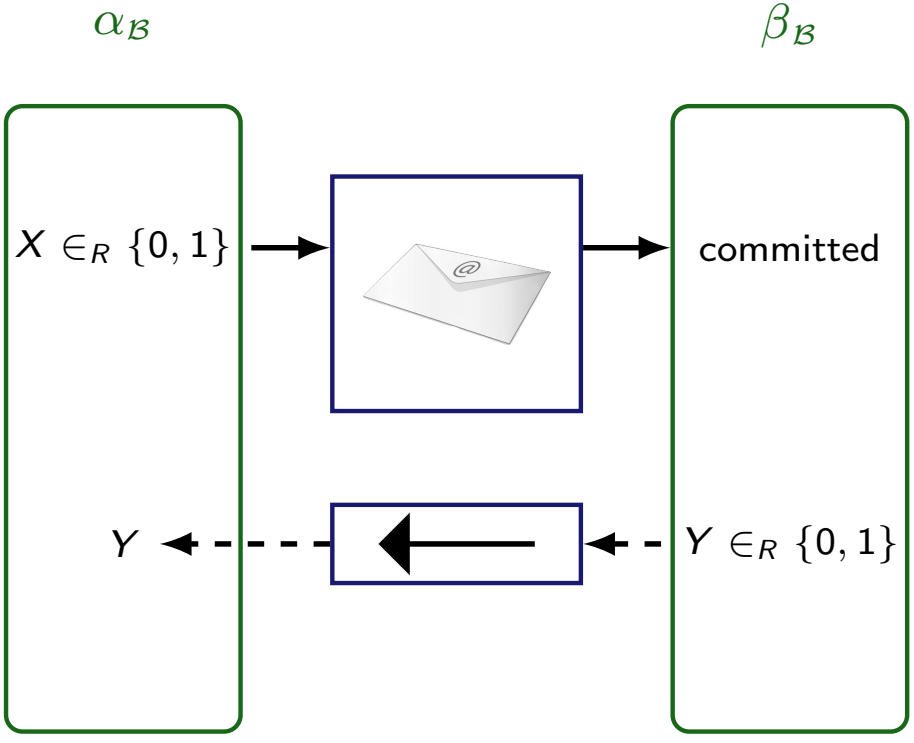
Blum's Coin Tossing Protocol

Honest Execution



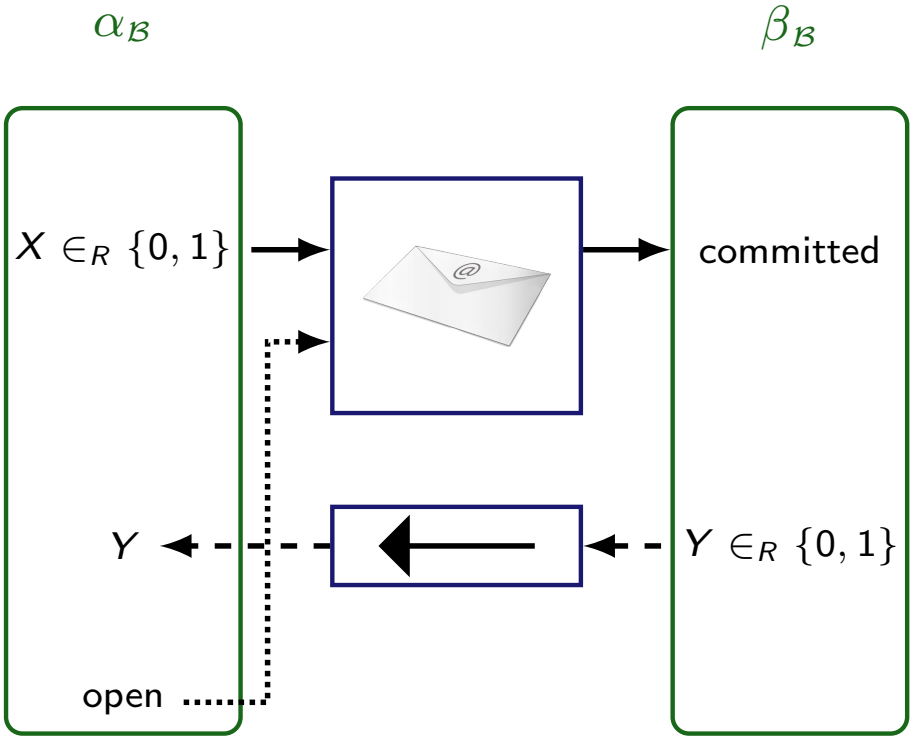
Blum's Coin Tossing Protocol

Honest Execution



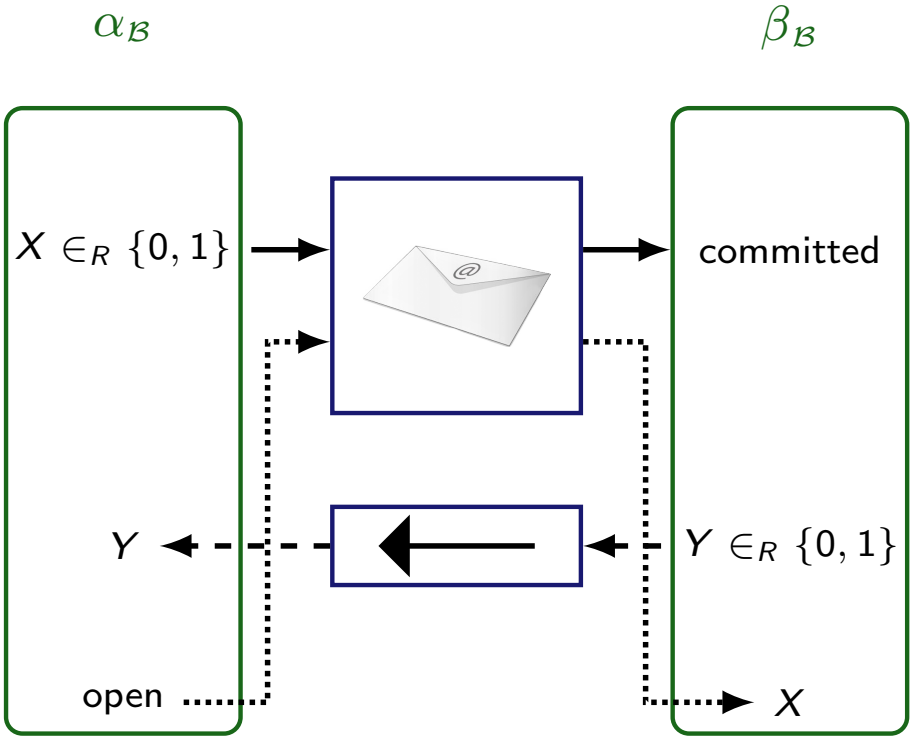
Blum's Coin Tossing Protocol

Honest Execution



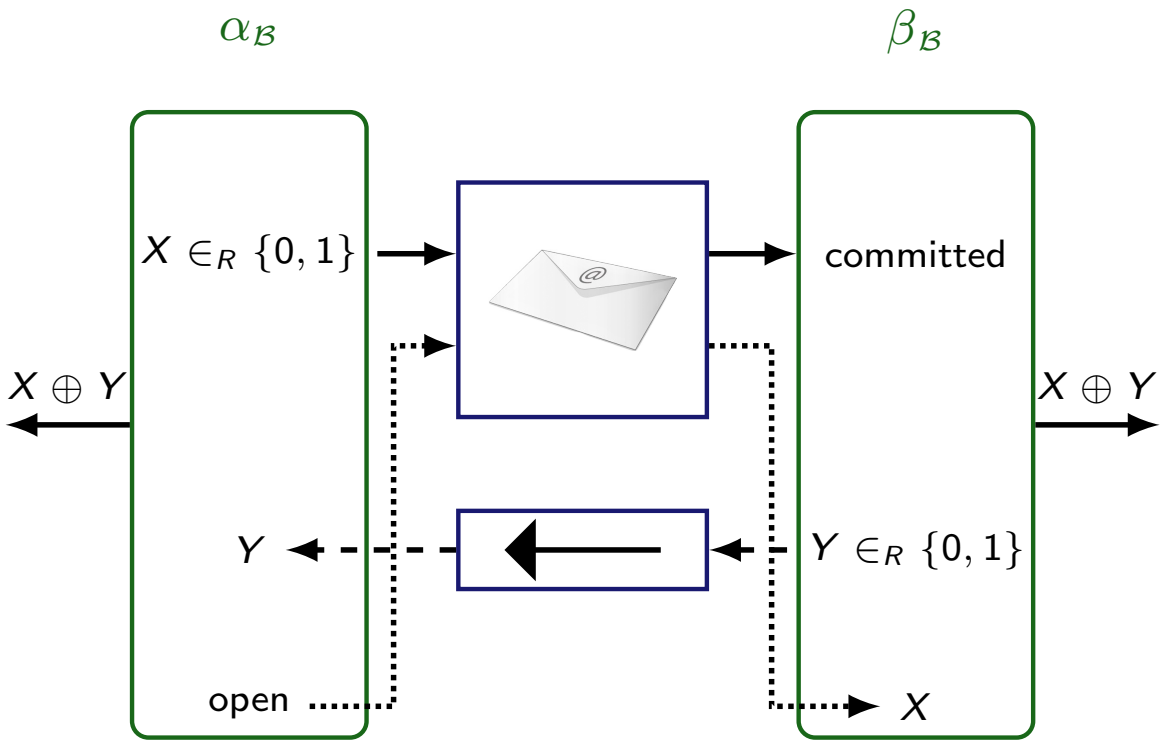
Blum's Coin Tossing Protocol

Honest Execution



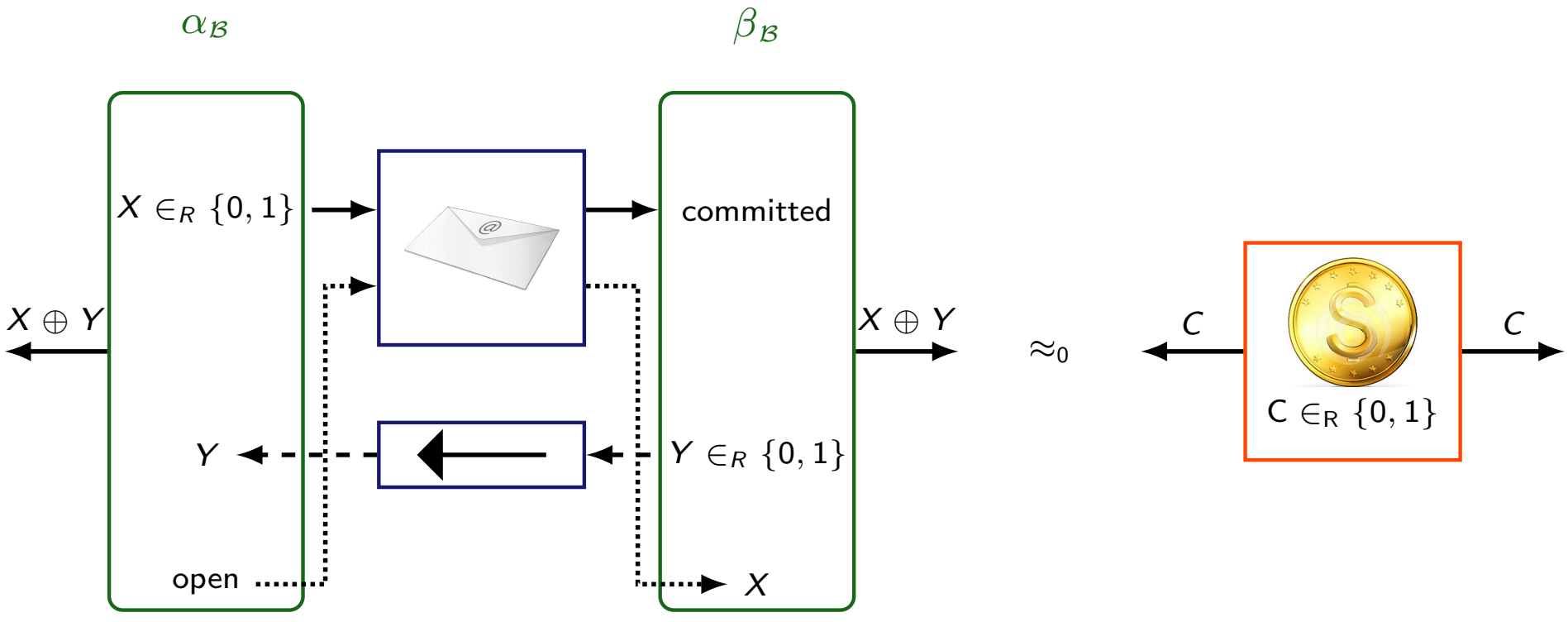
Blum's Coin Tossing Protocol

Honest Execution



Blum's Coin Tossing Protocol

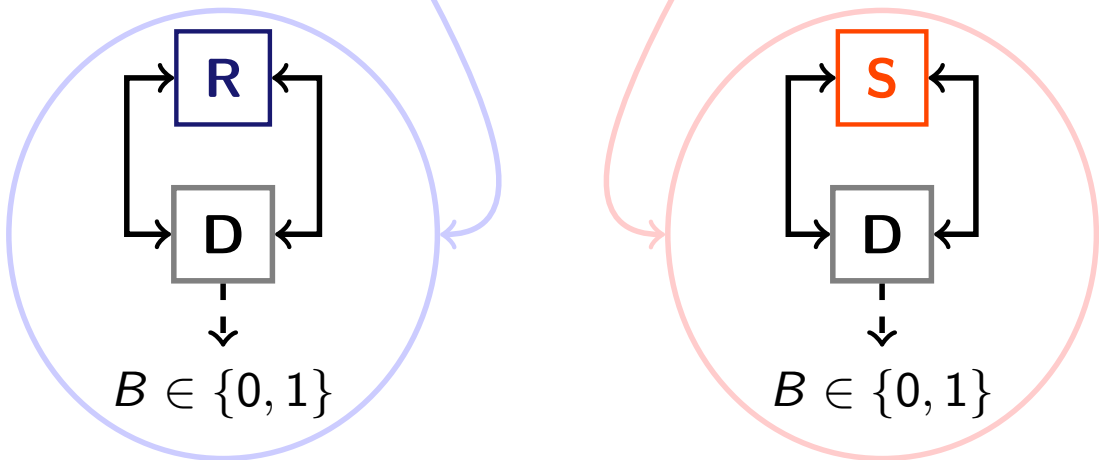
Honest Execution



Comparing Resources

- Distinguishing advantage of a distinguisher **D**

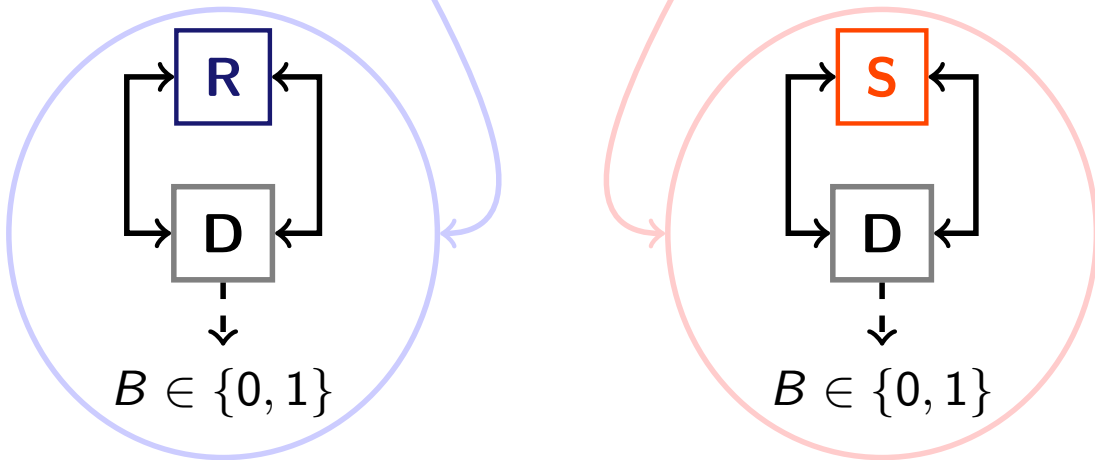
$$\Delta^{\mathbf{D}}(\mathbf{R}, \mathbf{S}) := \left| \mathrm{P}^{\mathbf{D}\mathbf{R}}(B = 1) - \mathrm{P}^{\mathbf{D}\mathbf{S}}(B = 1) \right|$$



Comparing Resources

- Distinguishing advantage of a distinguisher $\mathbf{D}$

$$\Delta^{\mathbf{D}}(\mathbf{R}, \mathbf{S}) := \left| \mathrm{P}^{\mathbf{D}\mathbf{R}}(B = 1) - \mathrm{P}^{\mathbf{D}\mathbf{S}}(B = 1) \right|$$



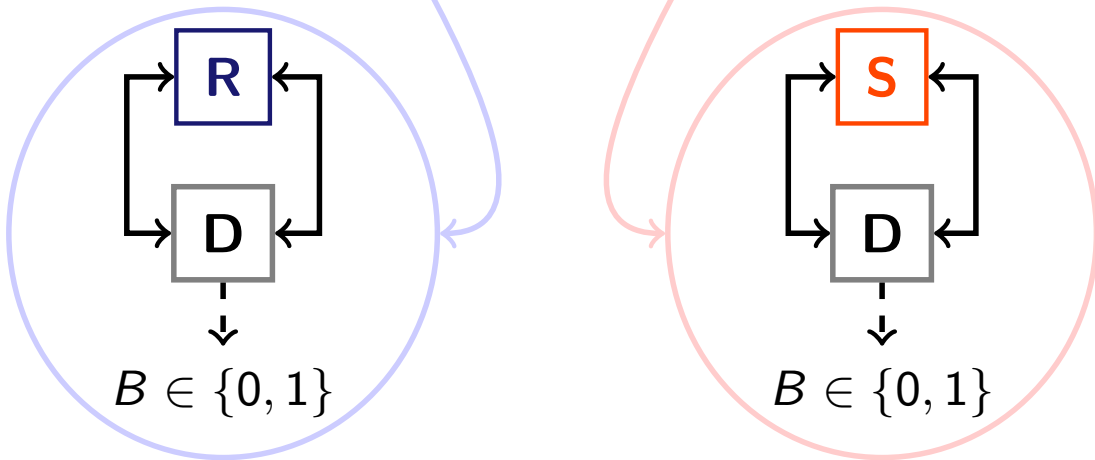
- Pseudo-metric induced

$$\mathbf{R} \approx_{\varepsilon} \mathbf{S} \quad :\Leftrightarrow \quad \forall \mathbf{D} \in \mathcal{D} : \ \Delta^{\mathbf{D}}(\mathbf{R}, \mathbf{S}) \leq \varepsilon.$$

Comparing Resources

- Distinguishing advantage of a distinguisher $\mathbf{D}$

$$\Delta^{\mathbf{D}}(\mathbf{R}, \mathbf{S}) := \left| \mathrm{P}^{\mathbf{D}\mathbf{R}}(B = 1) - \mathrm{P}^{\mathbf{D}\mathbf{S}}(B = 1) \right|$$



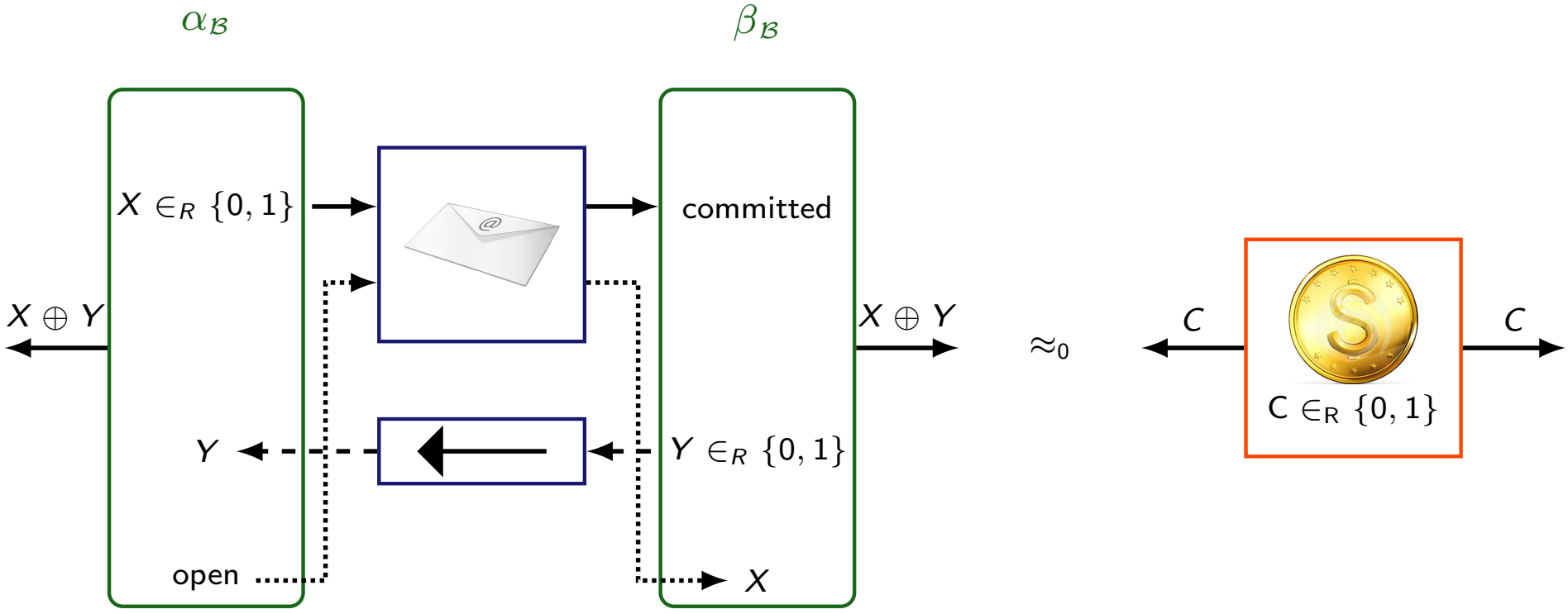
- Pseudo-metric induced

$$\mathbf{R} \approx_{\varepsilon} \mathbf{S} \quad :\Leftrightarrow \quad \forall \mathbf{D} \in \mathcal{D} : \ \Delta^{\mathbf{D}}(\mathbf{R}, \mathbf{S}) \leq \varepsilon.$$

- *Information-theoretic* constructions $\quad \Longrightarrow \quad$ no restriction on $\mathcal{D}$

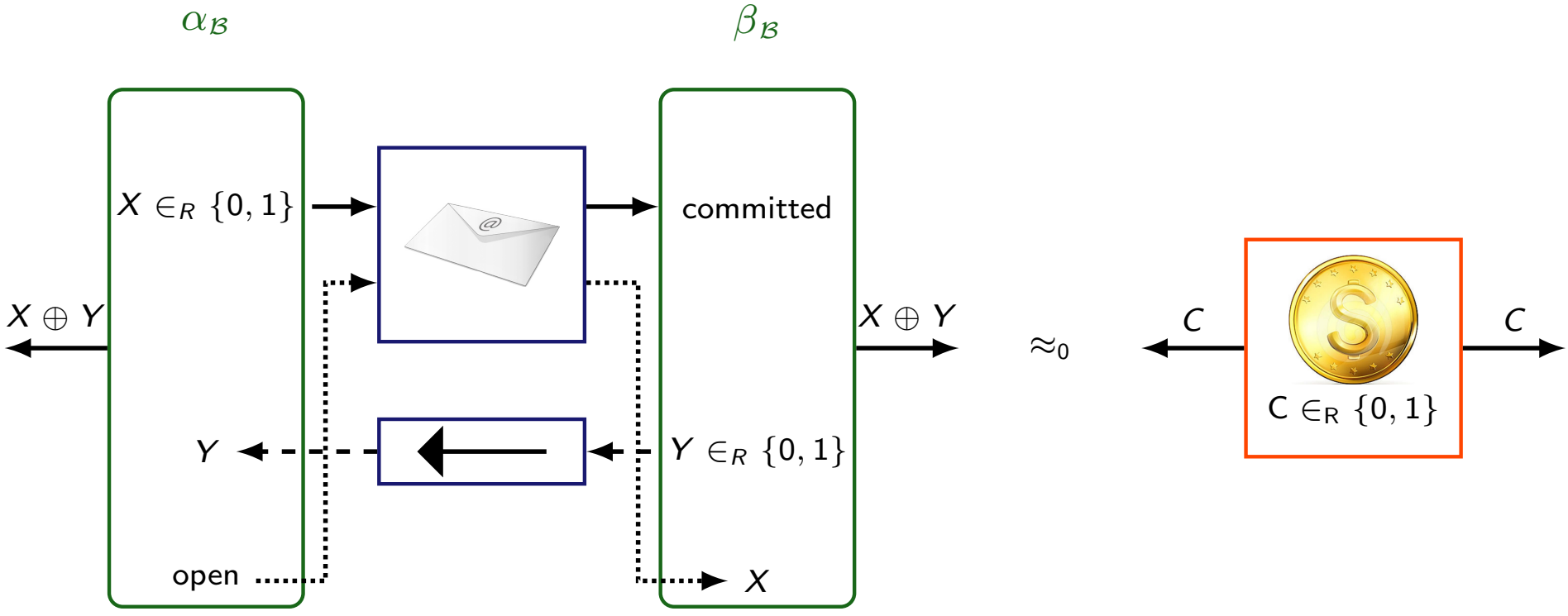
Blum's Coin Tossing Protocol

Honest Execution



Blum's Coin Tossing Protocol

Honest Execution

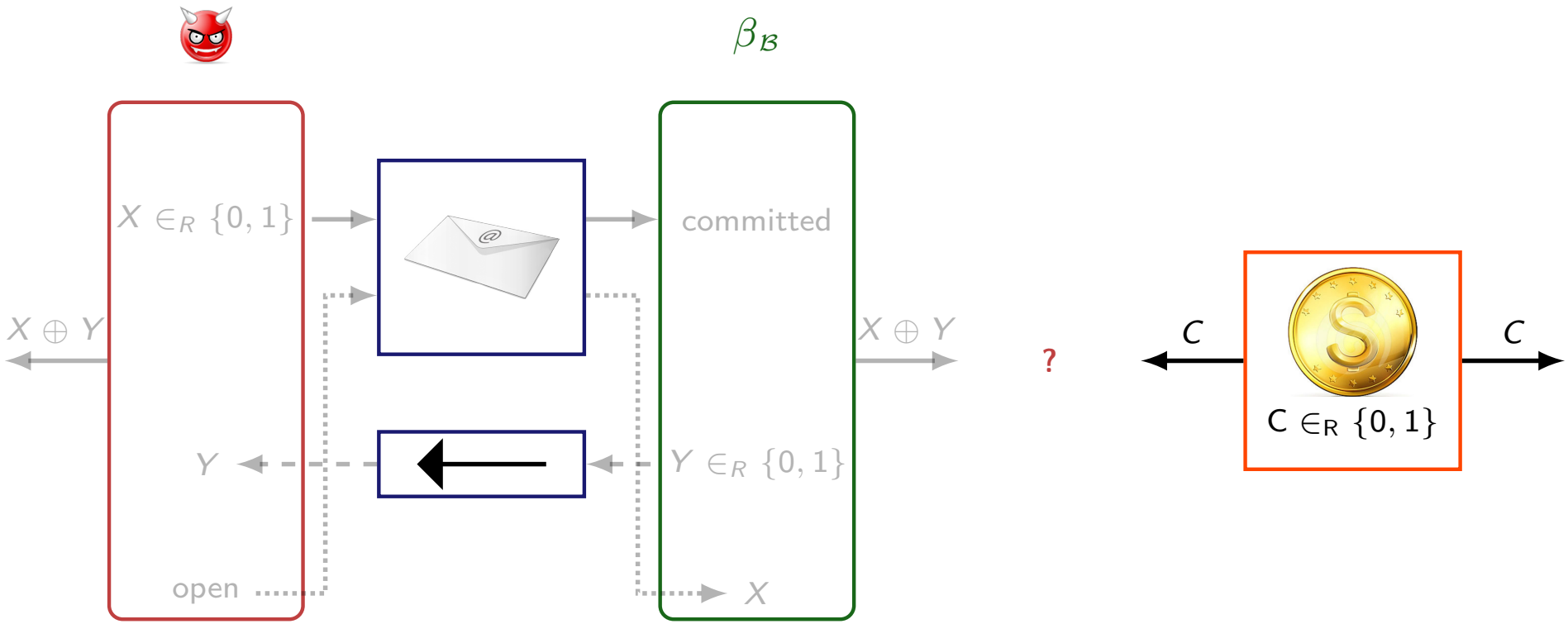


Setting

- 2 distrustful parties: one of them being potentially dishonest
- *Goal*: construct an ideal coin tossing resource

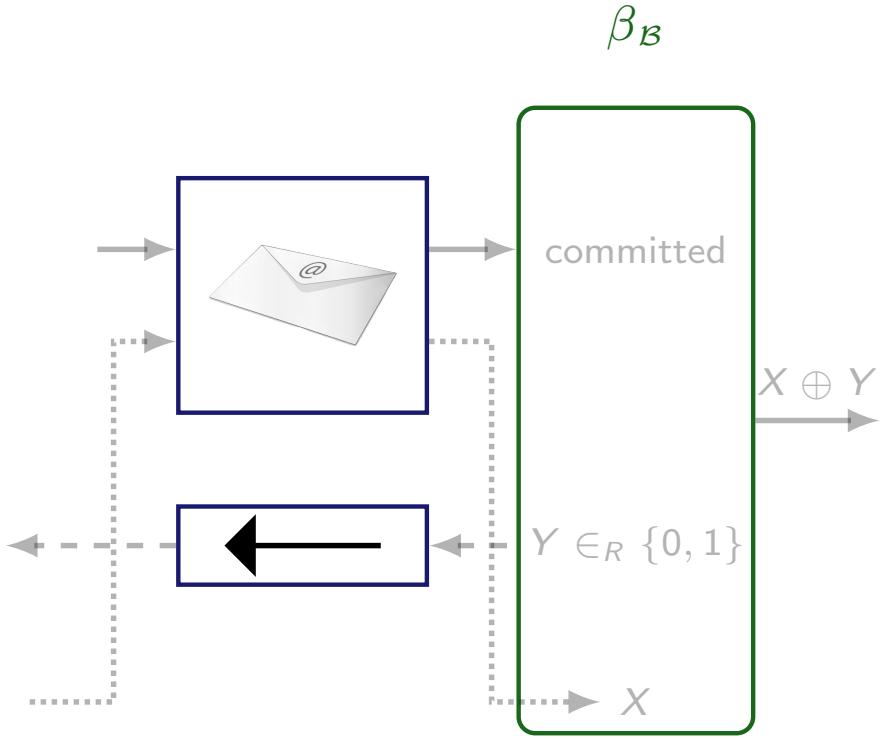
Blum's Coin Tossing Protocol - Security

Malicious Alice



Blum's Coin Tossing Protocol - Security

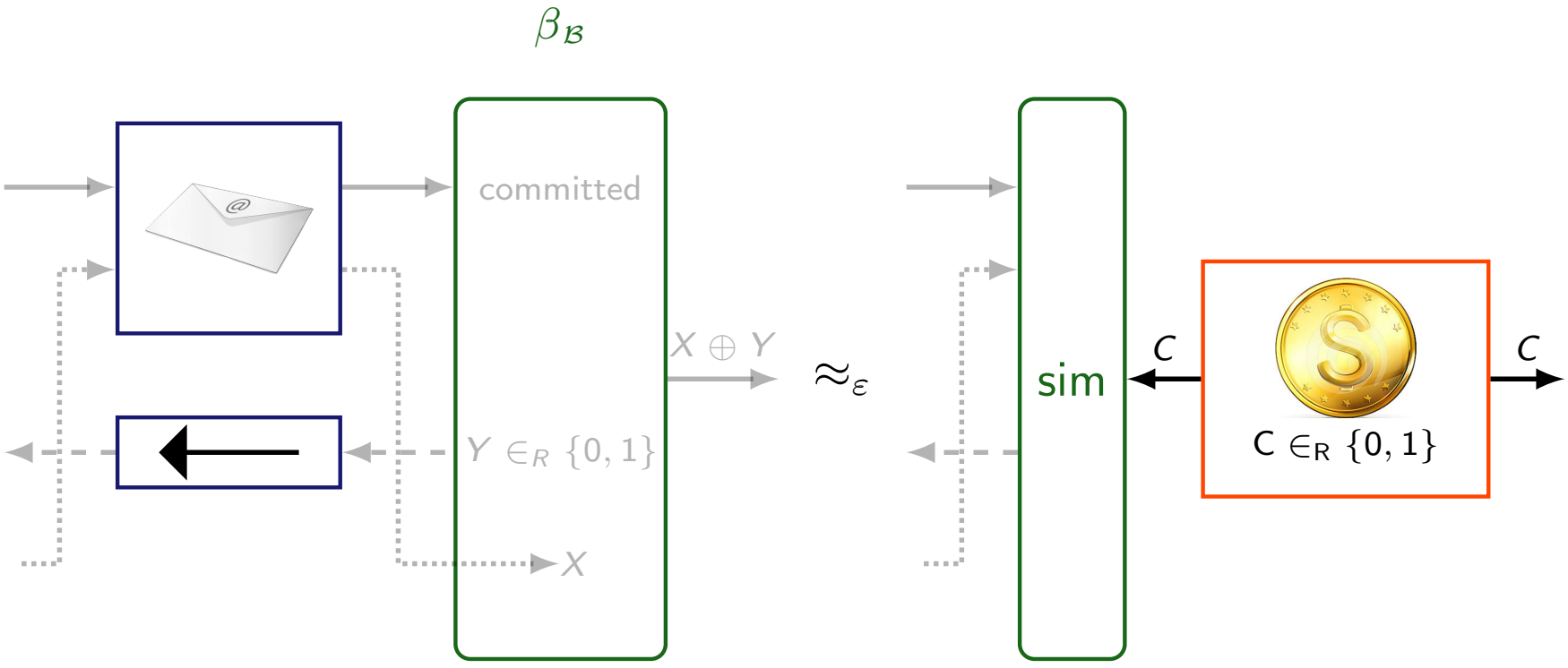
Malicious Alice



?

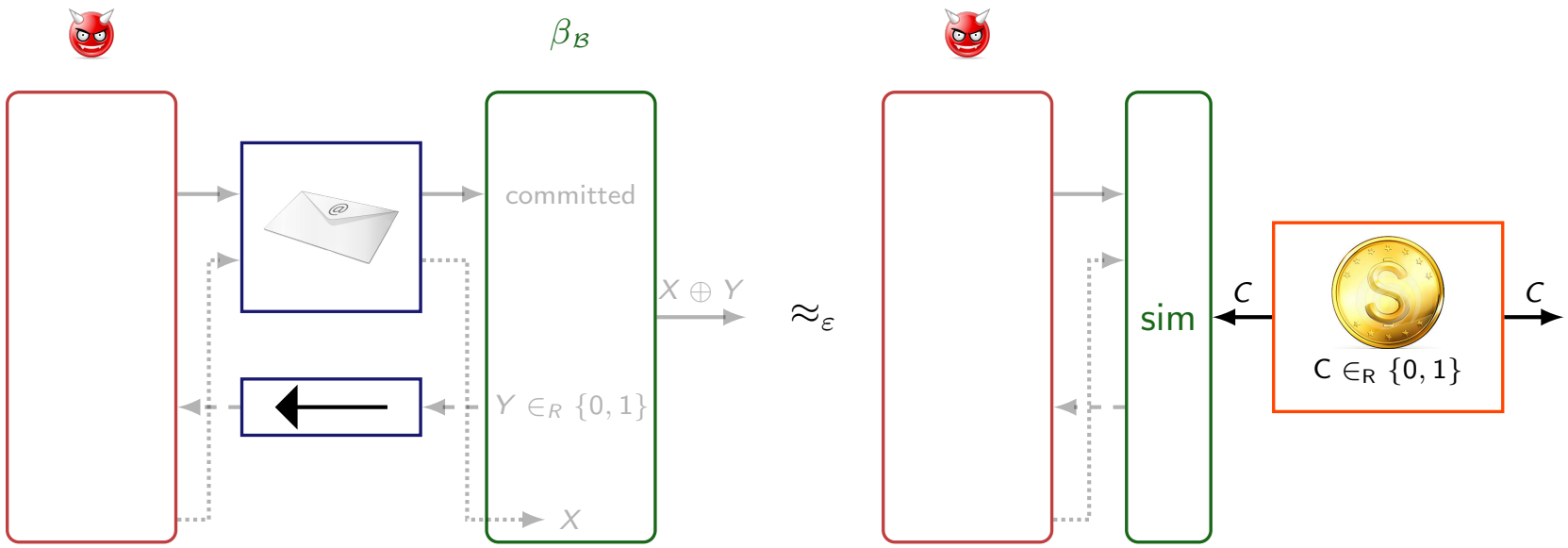
Blum's Coin Tossing Protocol - Security

Simulator



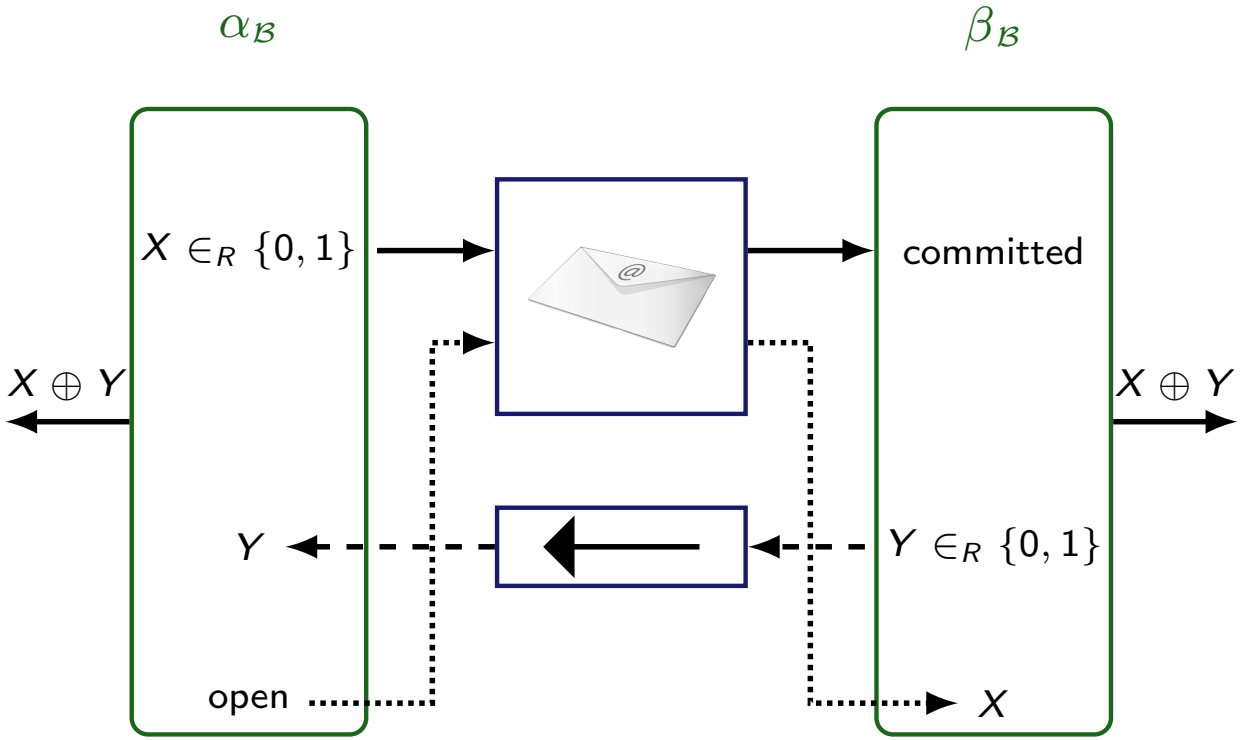
Blum's Coin Tossing Protocol - Security

Simulator



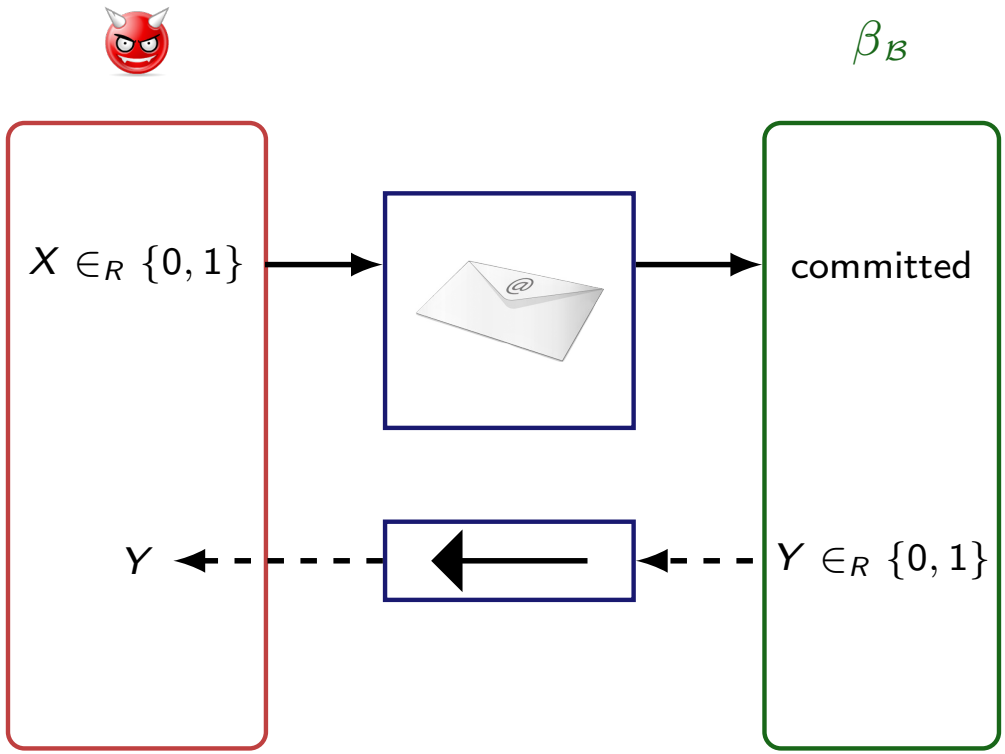
Blum's Coin Tossing Protocol

Malicious Alice - Real World



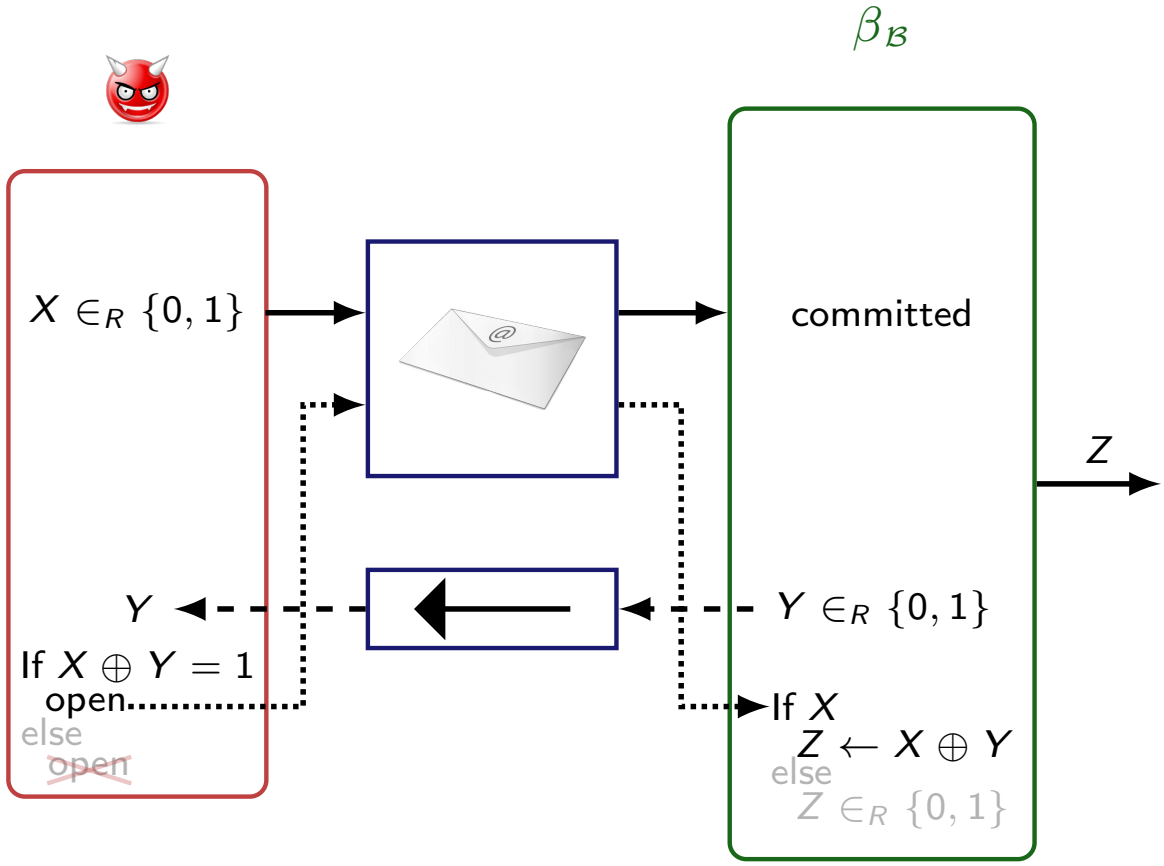
Blum's Coin Tossing Protocol

Malicious Alice - Real World



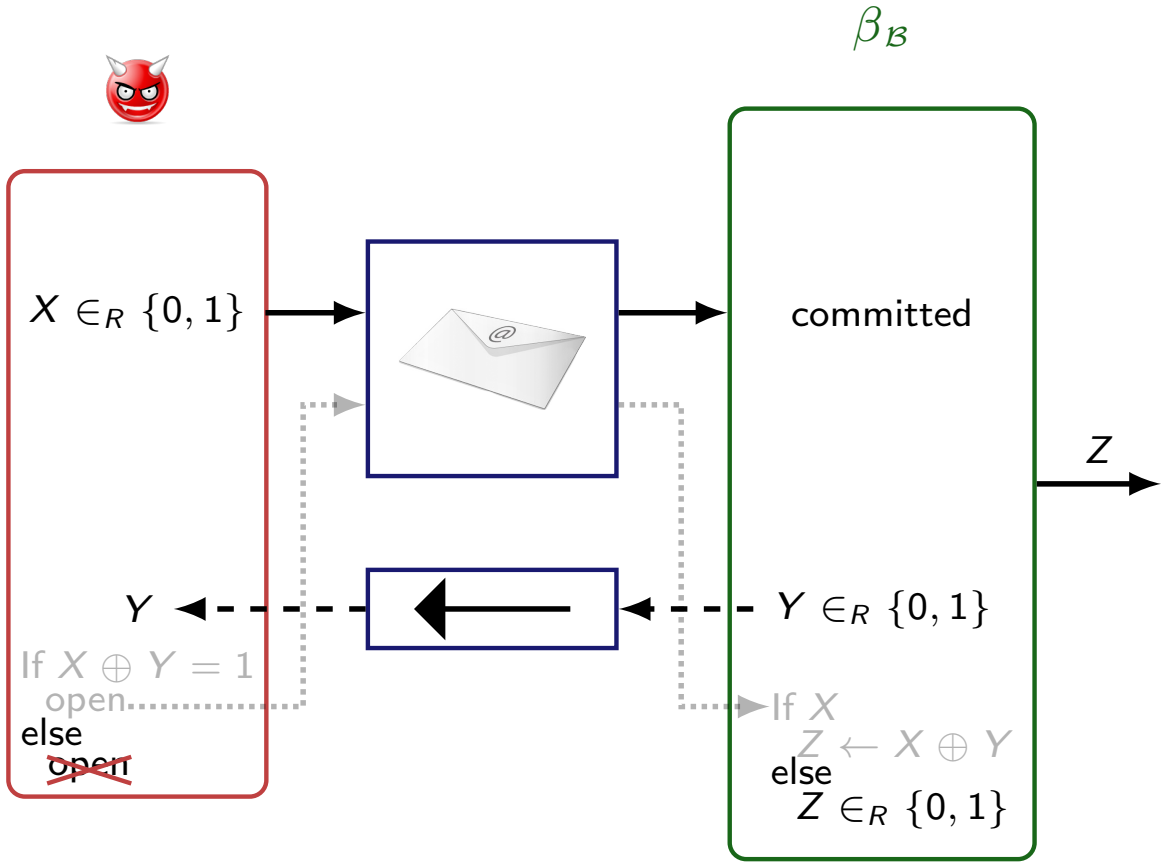
Blum's Coin Tossing Protocol

Malicious Alice - Real World



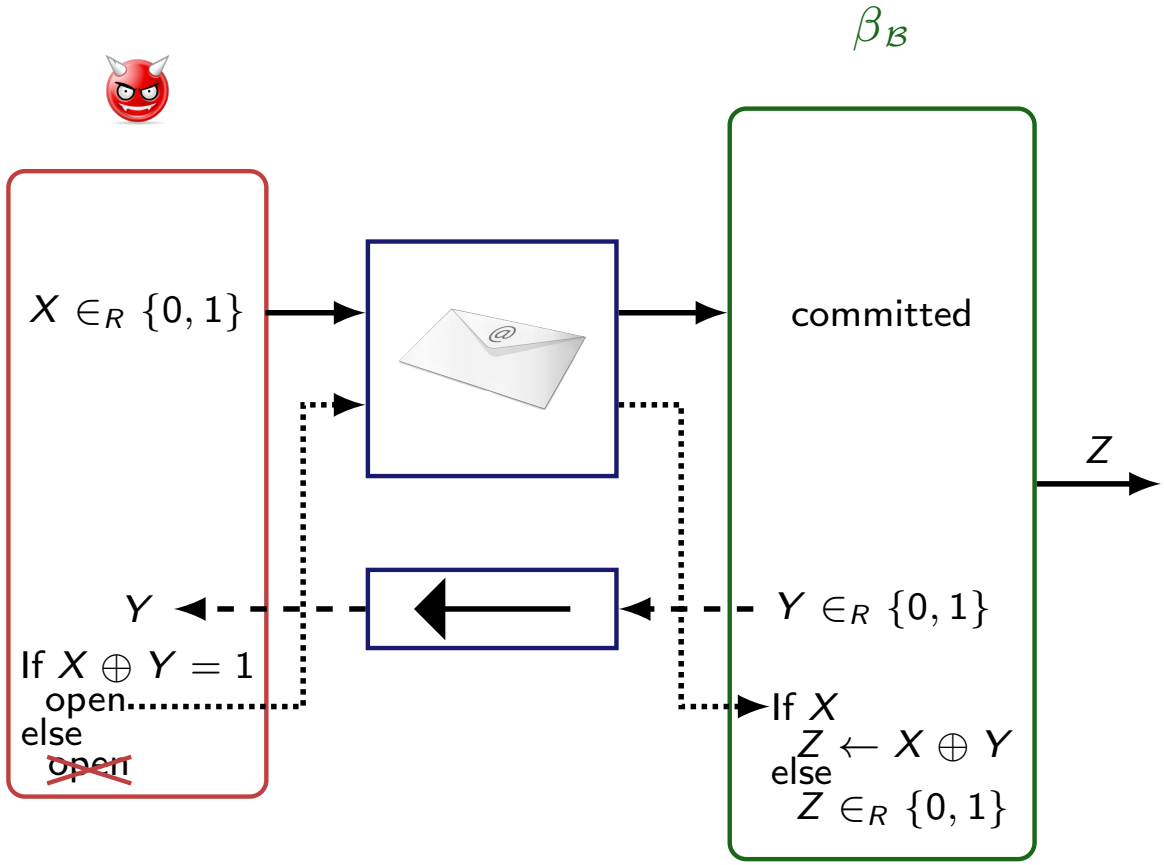
Blum's Coin Tossing Protocol

Malicious Alice - Real World



Blum's Coin Tossing Protocol

Malicious Alice - Real World



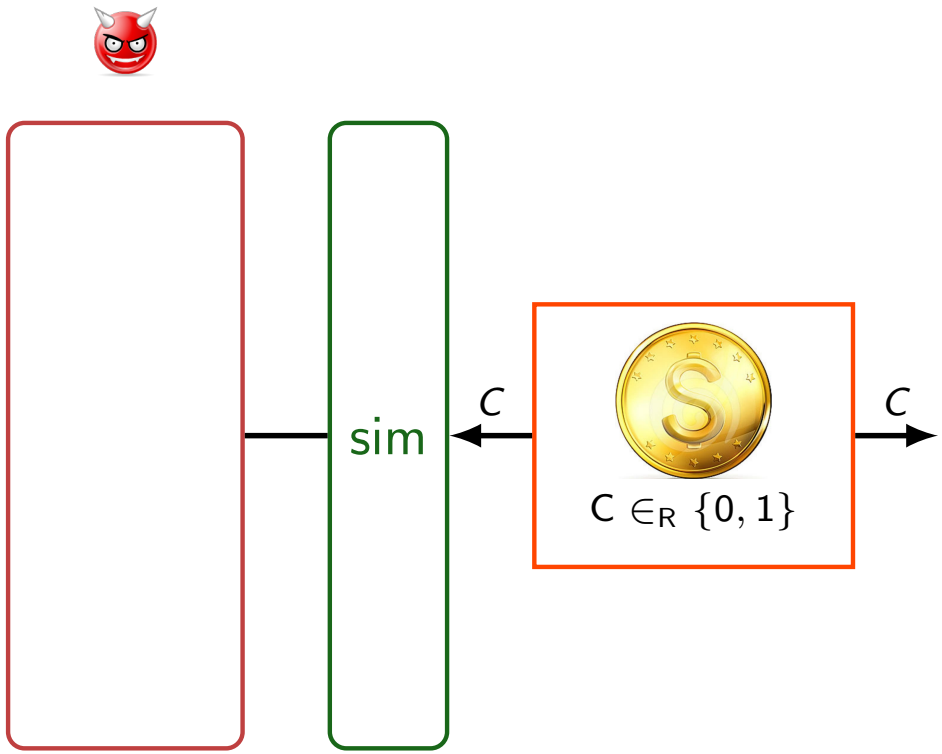
$$\mathrm{P}(Z = 1) = \frac{3}{4}$$

Blum's Coin Tossing Protocol

Malicious Alice - Ideal World

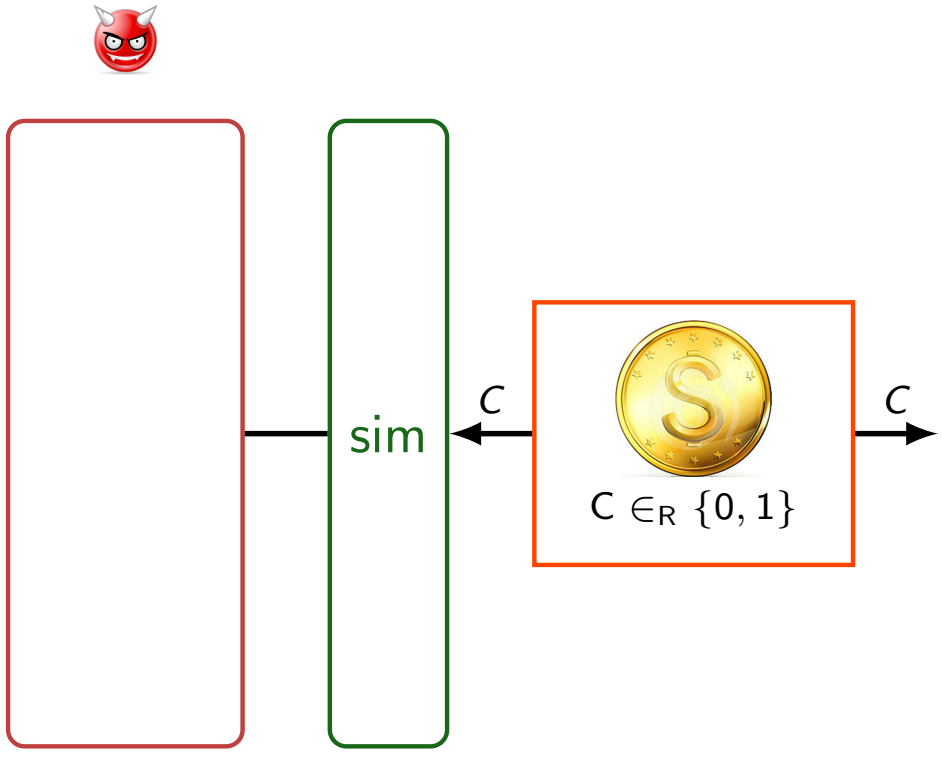
Blum's Coin Tossing Protocol

Malicious Alice - Ideal World



Blum's Coin Tossing Protocol

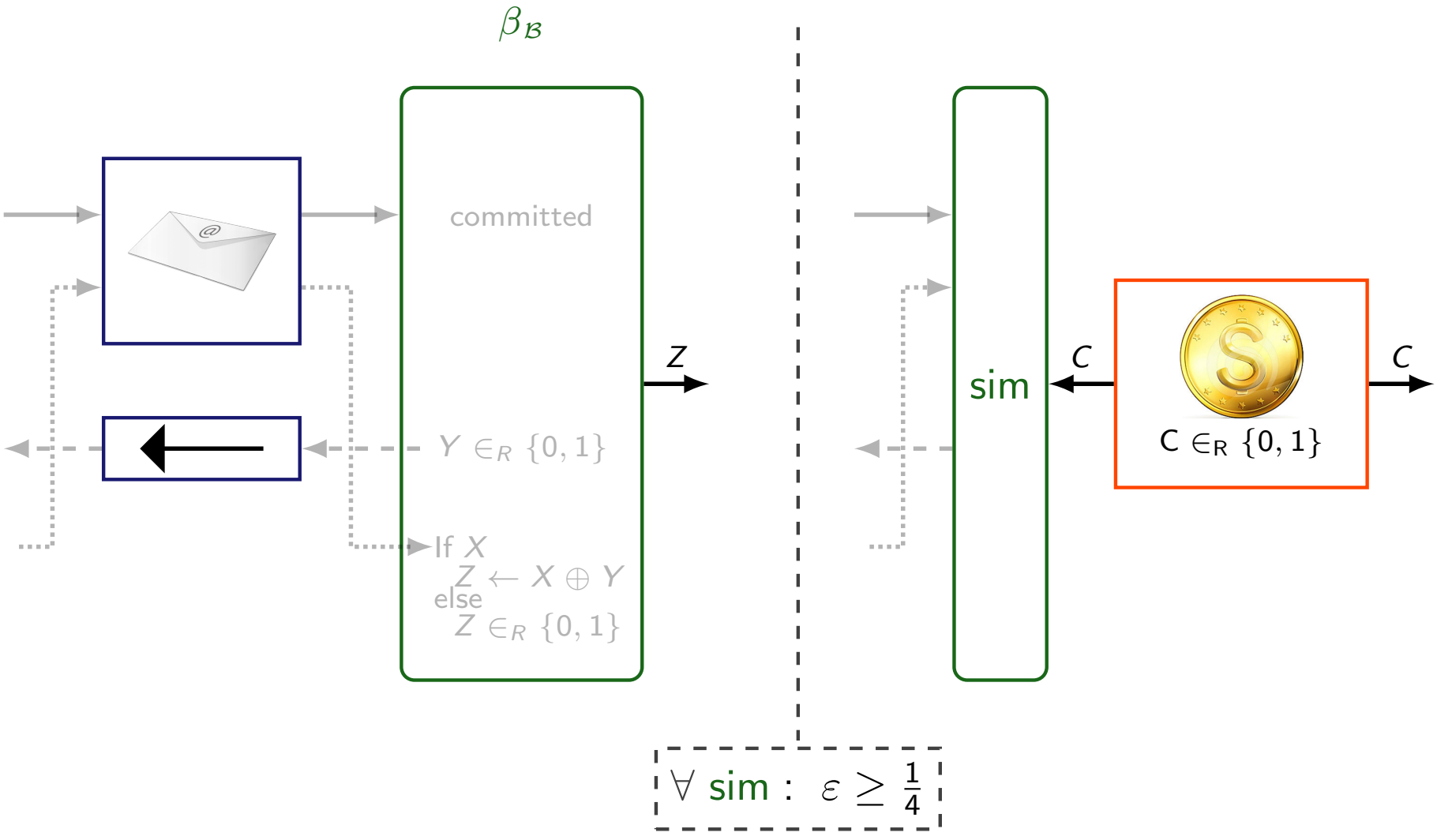
Malicious Alice - Ideal World



$$\forall \text{ } \forall \text{ sim}: \ \mathrm{P}(C = 1) = \frac{1}{2}$$

Blum's Coin Tossing Protocol

Malicious Alice



Outline

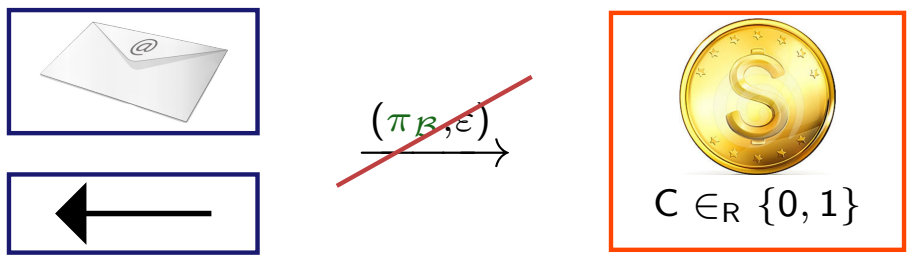
Unfair Coin Tossing

Goal

$\xrightarrow{(\pi_{\mathcal{B}},\varepsilon)}$

Unfair Coin Tossing

(Unachievable) Goal



Unfair Coin Tossing

(Unachievable) Goal

$\xrightarrow{(\pi_{\mathcal{B}},\varepsilon)}$

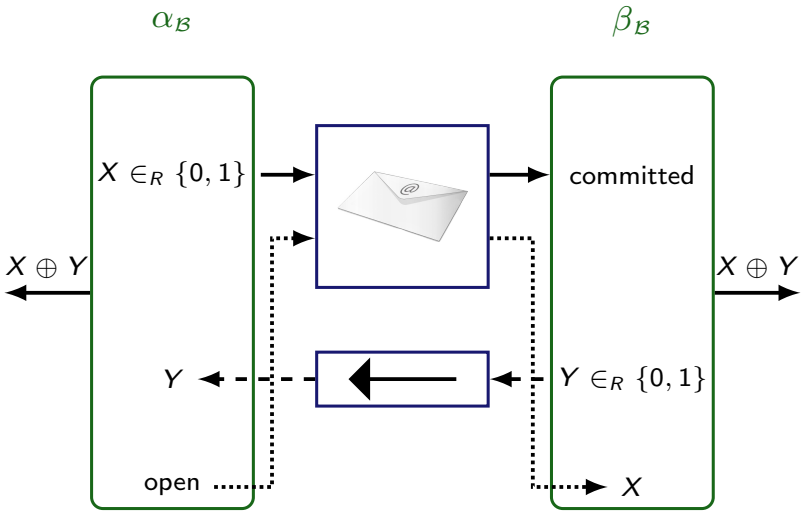
Unfair Coin Tossing

Goal

$\xrightarrow{(\pi_{\mathcal{B}},0)}$

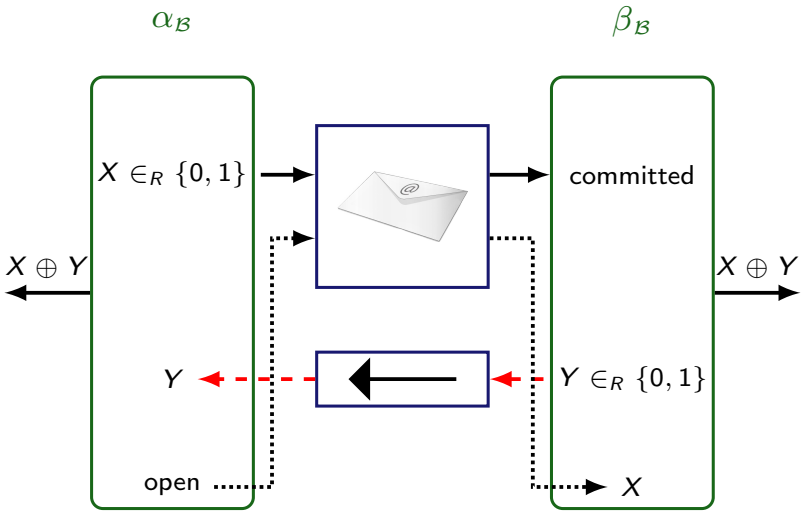
Unfair Coin Tossing Resource

Unfair Coin Tossing Resource



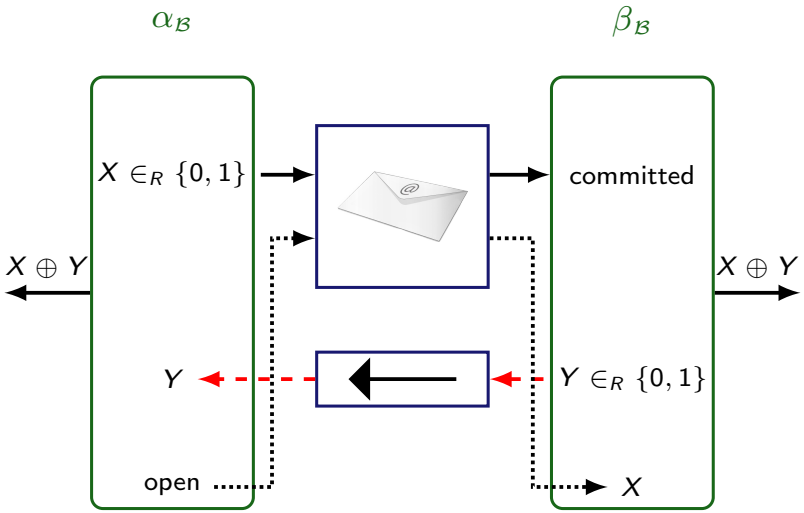
Unfair Coin Tossing Resource

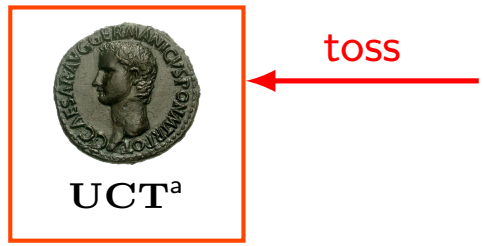
Unfair Coin Tossing Resource



Unfair Coin Tossing Resource

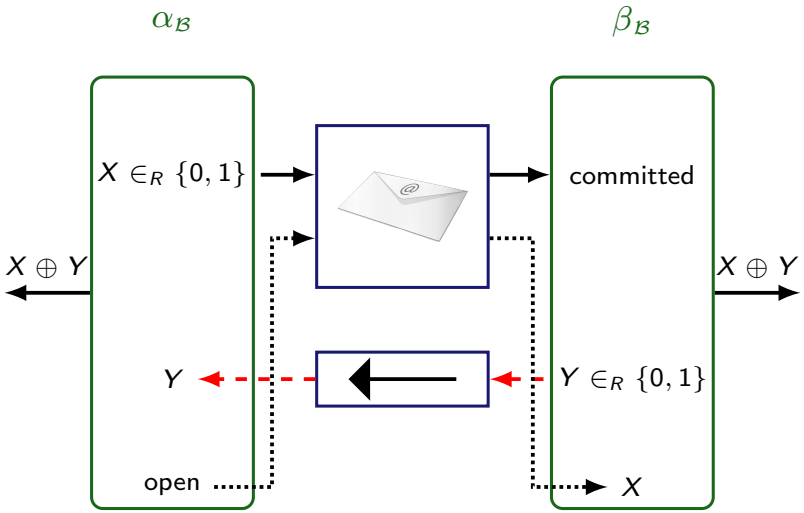
Unfair Coin Tossing Resource





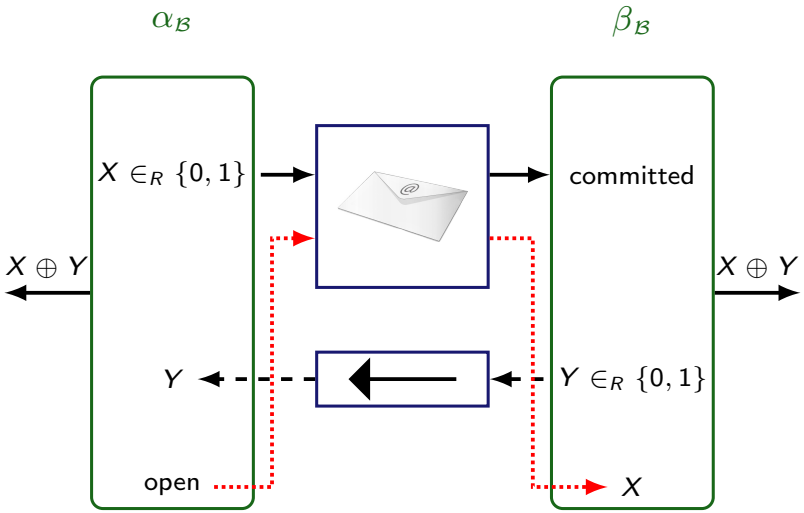
Unfair Coin Tossing Resource

Unfair Coin Tossing Resource



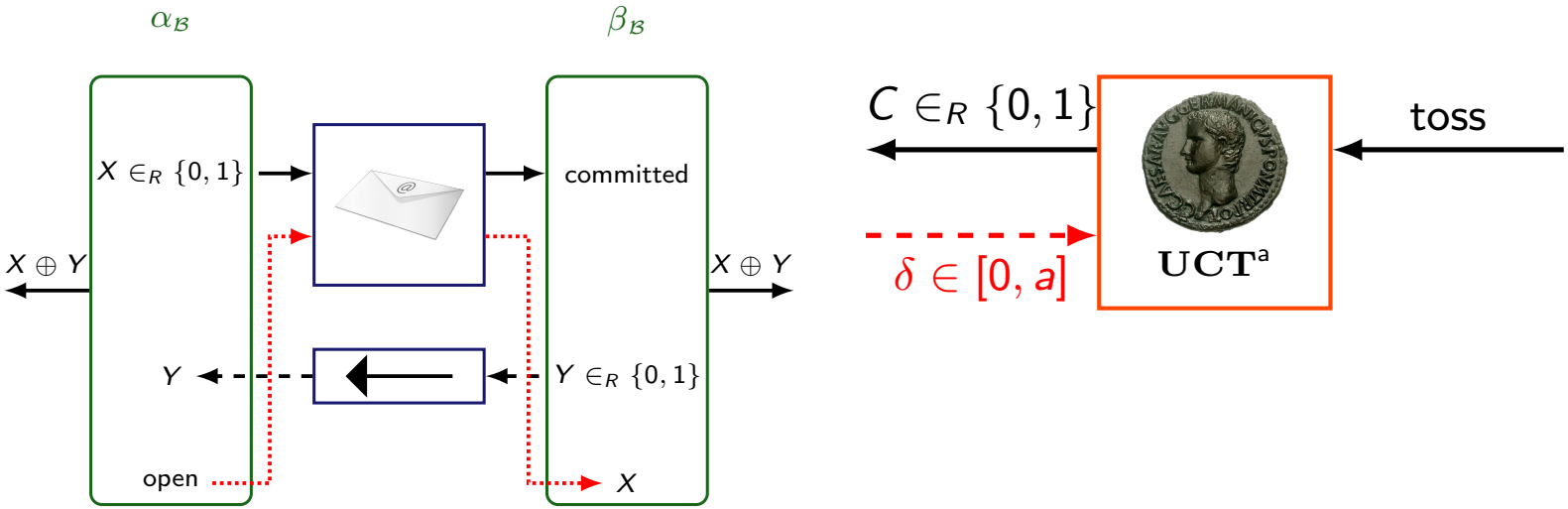
Unfair Coin Tossing Resource

Unfair Coin Tossing Resource



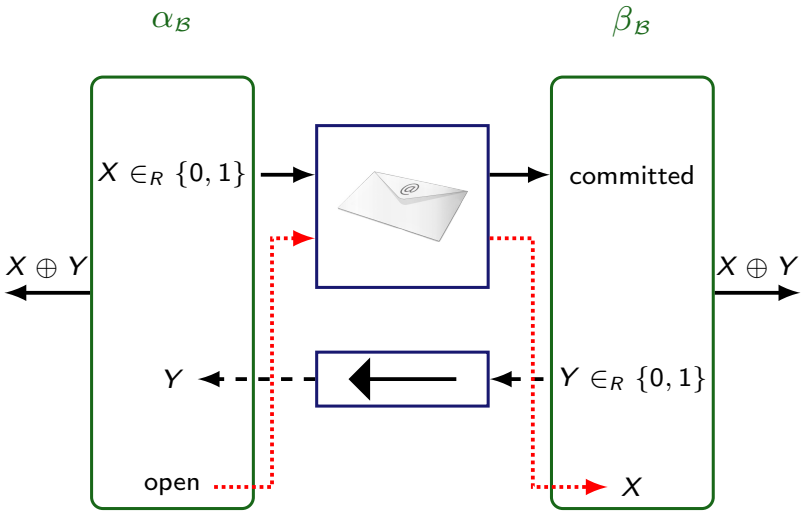
Unfair Coin Tossing Resource

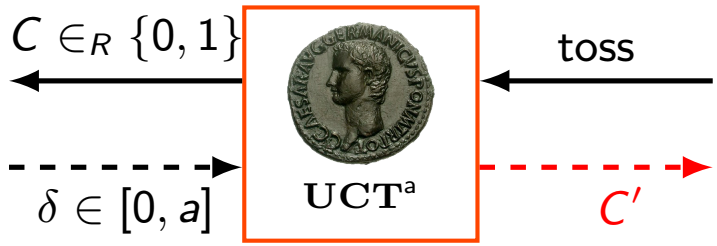
Unfair Coin Tossing Resource



Unfair Coin Tossing Resource

Unfair Coin Tossing Resource

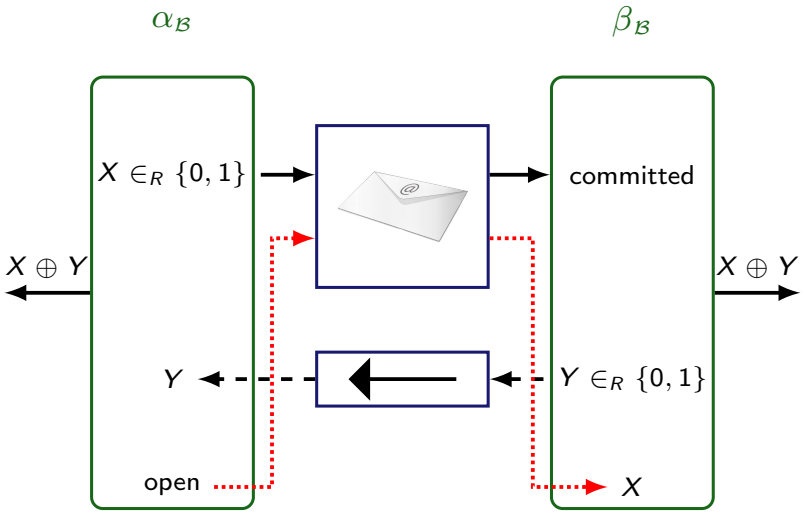


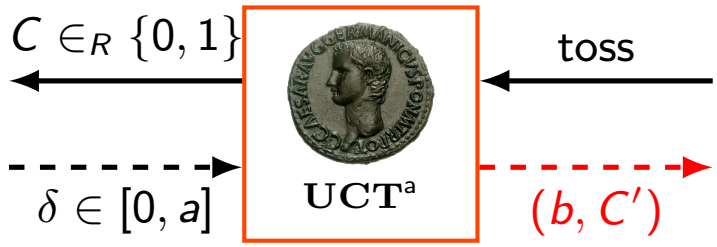


$C' := C \oplus N$, where $N \sim \mathrm{Ber}(\delta)$.

Unfair Coin Tossing Resource

Unfair Coin Tossing Resource





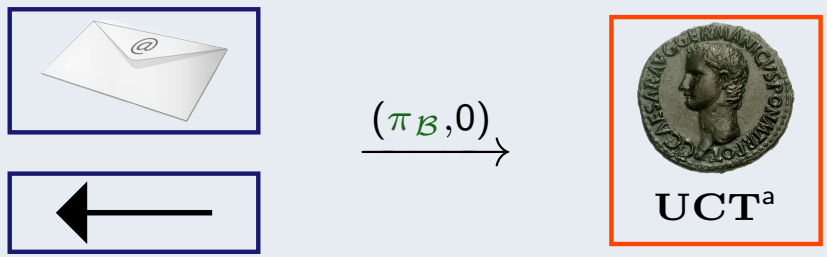
$$b := \mathbb{1}_{\delta \neq 0}$$

$$C' := C \oplus N, \text{ where } N \sim \mathrm{Ber}(\delta).$$

Blum's protocol

Theorem 1

Blum's protocol perfectly constructs a biased unfair coin tossing resource, i.e,

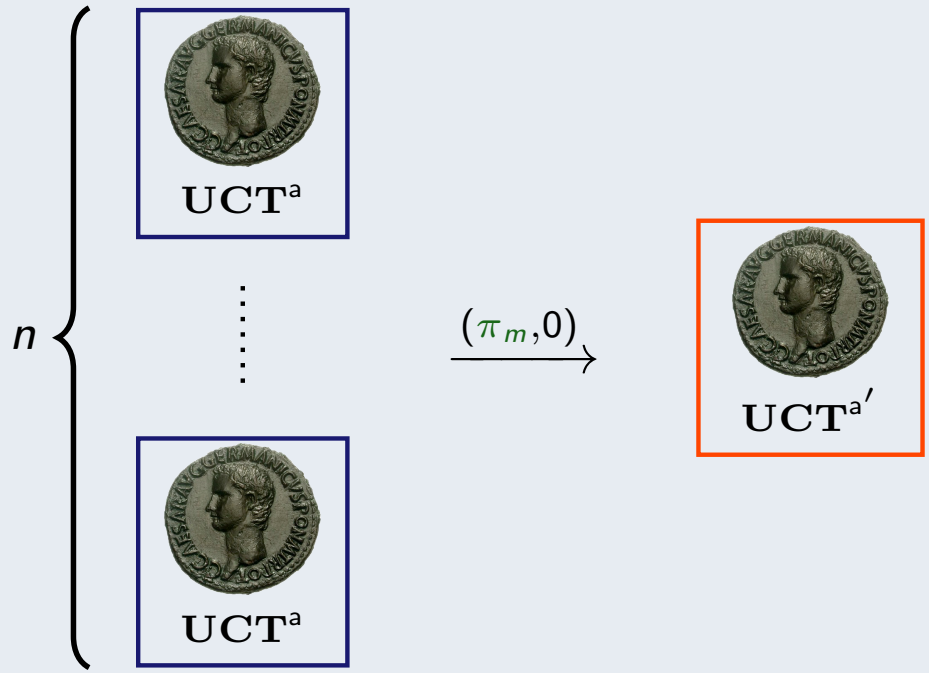


where $a \geq \frac{1}{2}$.

Multiple Unfair Coin Tossing Resources

Theorem 2

There exists a 2-party protocol π_m s.t. for an odd number n of unfair coin tossing resources,



where $a' \approx \frac{2}{\sqrt{2\pi n}} a$.

Outline

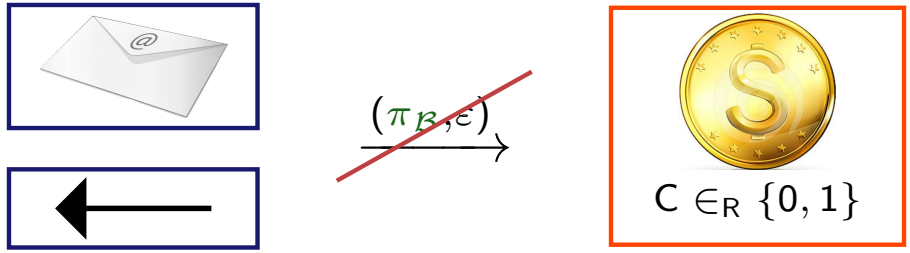
Summary

Unfair Coin Tossing Resource

Summary

Unfair Coin Tossing Resource

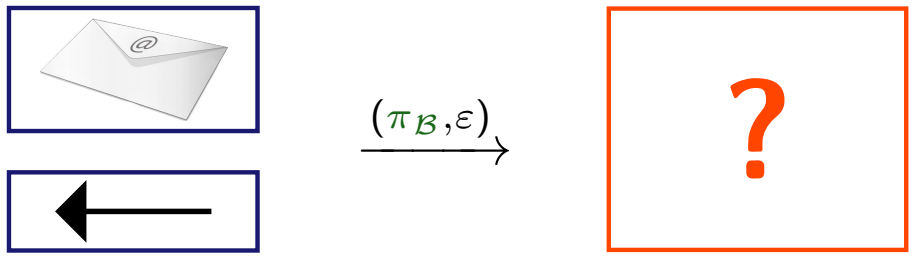
State the Exact Resource Constructed



Summary

Unfair Coin Tossing Resource

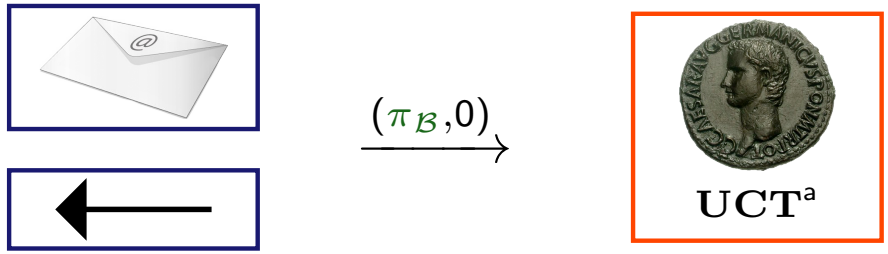
State the Exact Resource Constructed



Summary

Unfair Coin Tossing Resource

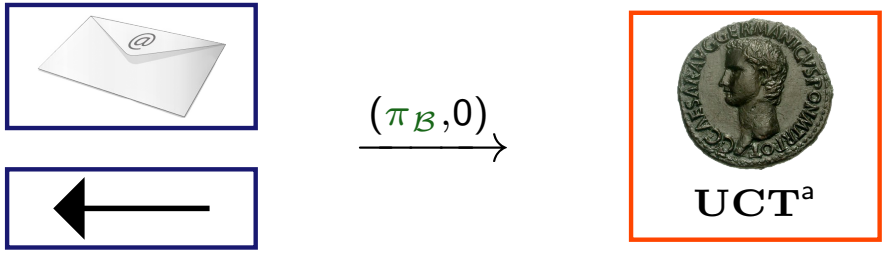
State the Exact Resource Constructed



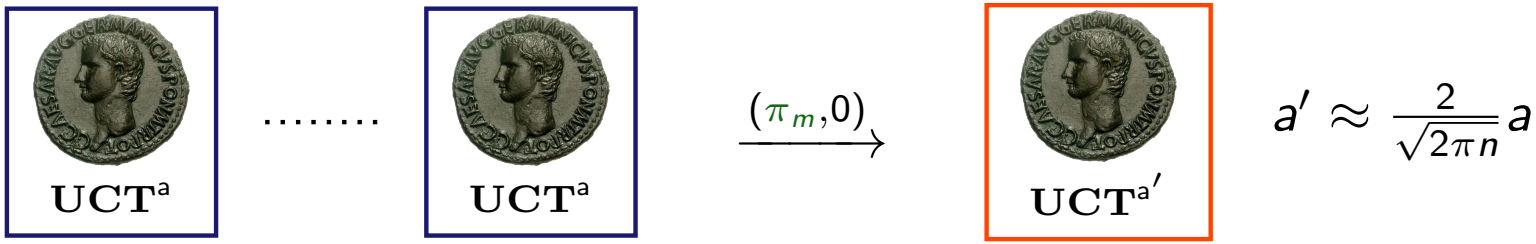
Summary

Unfair Coin Tossing Resource

State the Exact Resource Constructed



Majority Protocol



Thank You!

Construction Notion for 2-Party

Construction in (Alice, Bob)-setting

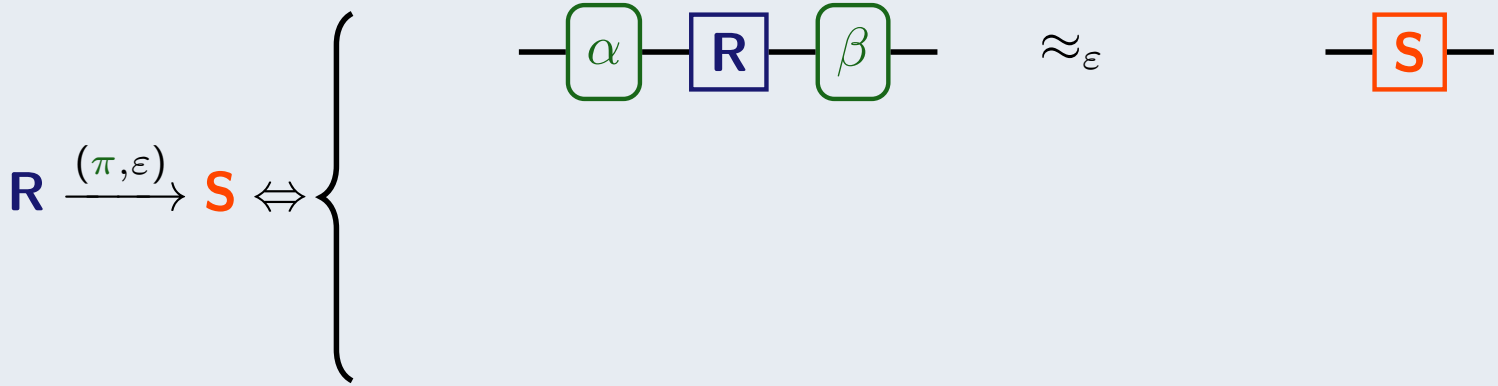
For a 2-party protocol $\pi = (\alpha, \beta)$,

$\mathbf{R} \xrightarrow{(\pi,\varepsilon)} \mathbf{S} \Leftrightarrow$

Construction Notion for 2-Party

Construction in (Alice, Bob)-setting

For a 2-party protocol $\pi = (\alpha, \beta)$,



Construction Notion for 2-Party

Construction in (Alice, Bob)-setting

For a 2-party protocol $\pi = (\alpha, \beta)$,

$$\mathbf{R} \xrightarrow{(\pi,\varepsilon)} \mathbf{S} \Leftrightarrow \begin{cases} \alpha \; \mathbf{R} \; \beta \approx_\varepsilon \mathbf{S} \\ \exists\, \sigma : \; \alpha \; \mathbf{R} \approx_\varepsilon \mathbf{S} \; \sigma \end{cases}$$

Construction Notion for 2-Party

Construction in (Alice, Bob)-setting

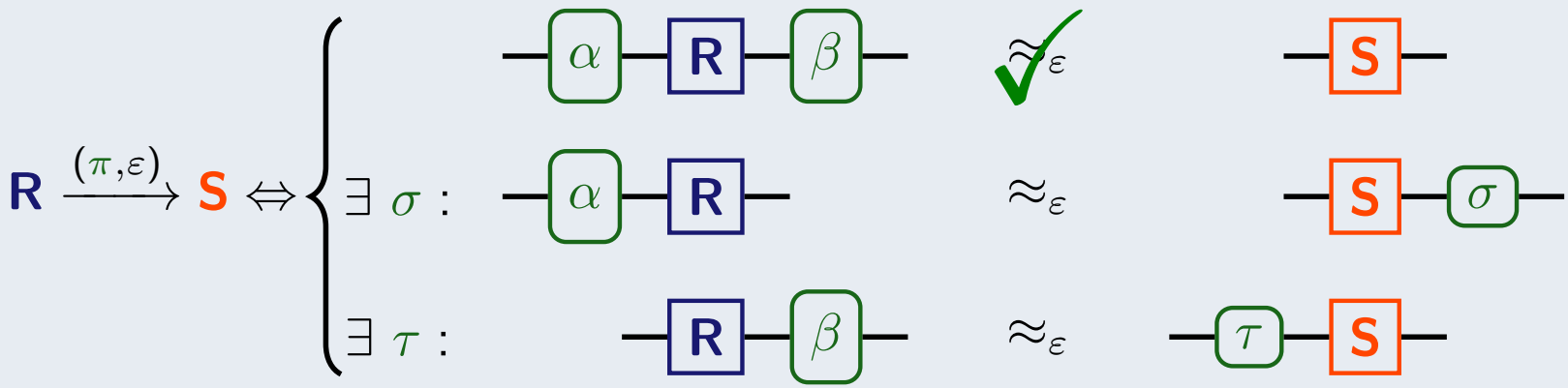
For a 2-party protocol $\pi = (\alpha, \beta)$,

$$\mathbf{R} \xrightarrow{(\pi,\varepsilon)} \mathbf{S} \Leftrightarrow \begin{cases} \alpha \text{—} \mathbf{R} \text{—} \beta & \approx_\varepsilon \quad \mathbf{S} \\ \exists\, \sigma: \ \alpha \text{—} \mathbf{R} & \approx_\varepsilon \quad \mathbf{S} \text{—} \sigma \\ \exists\, \tau: \ \mathbf{R} \text{—} \beta & \approx_\varepsilon \quad \tau \text{—} \mathbf{S} \end{cases}$$

Construction Notion for 2-Party

Construction in (Alice, Bob)-setting

For a 2-party protocol $\pi = (\alpha, \beta)$,



Construction Notion for 2-Party

Construction in (Alice, Bob)-setting

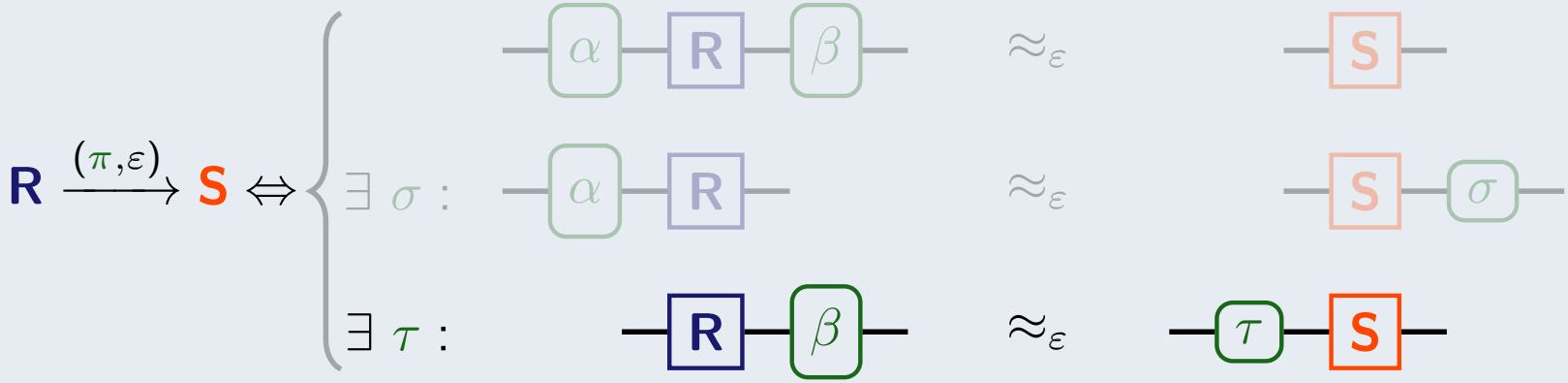
For a 2-party protocol $\pi = (\alpha, \beta)$,

$$\mathbf{R} \xrightarrow{(\pi,\varepsilon)} \mathbf{S} \Leftrightarrow \begin{cases} \alpha \; \mathbf{R} \; \beta \approx_\varepsilon \mathbf{S} \\ \exists\, \sigma: \; \alpha \; \mathbf{R} \approx_\varepsilon \mathbf{S} \; \sigma \\ \exists\, \tau: \; \mathbf{R} \; \beta \approx_\varepsilon \tau \; \mathbf{S} \end{cases}$$

Blum's Coin Tossing Protocol

Construction in (Alice, Bob)-setting

For a 2-party protocol $\pi = (\alpha, \beta)$,



Blum's Coin Tossing Protocol

Construction in (Alice, Bob)-setting

For a 2-party protocol $\pi = (\alpha, \beta)$,