Abstraction in Cryptography

Ueli Maurer

ETH Zurich

CRYPTO 2009, August 19, 2009

Abstraction in Cryptography

> "I can only understand simple things."
>
> JAMES MASSEY

Ueli Maurer

ETH Zurich

CRYPTO 2009, August 19, 2009

Abstraction

Abstraction: eliminate irrelevant details from consideration

Examples: group, field, vector space, relation, graph, ...

Goals of abstraction:

- simpler definitions
- generality of results
- simpler proofs
- elegance
- didactic suitability

Abstraction

Abstraction: eliminate irrelevant details from consideration

Examples: group, field, vector space, relation, graph, ...

Goals of abstraction:

- simpler definitions
- generality of results
- simpler proofs
- elegance
- didactic suitability
- understanding

Abstraction

Abstraction: eliminate irrelevant details from consideration

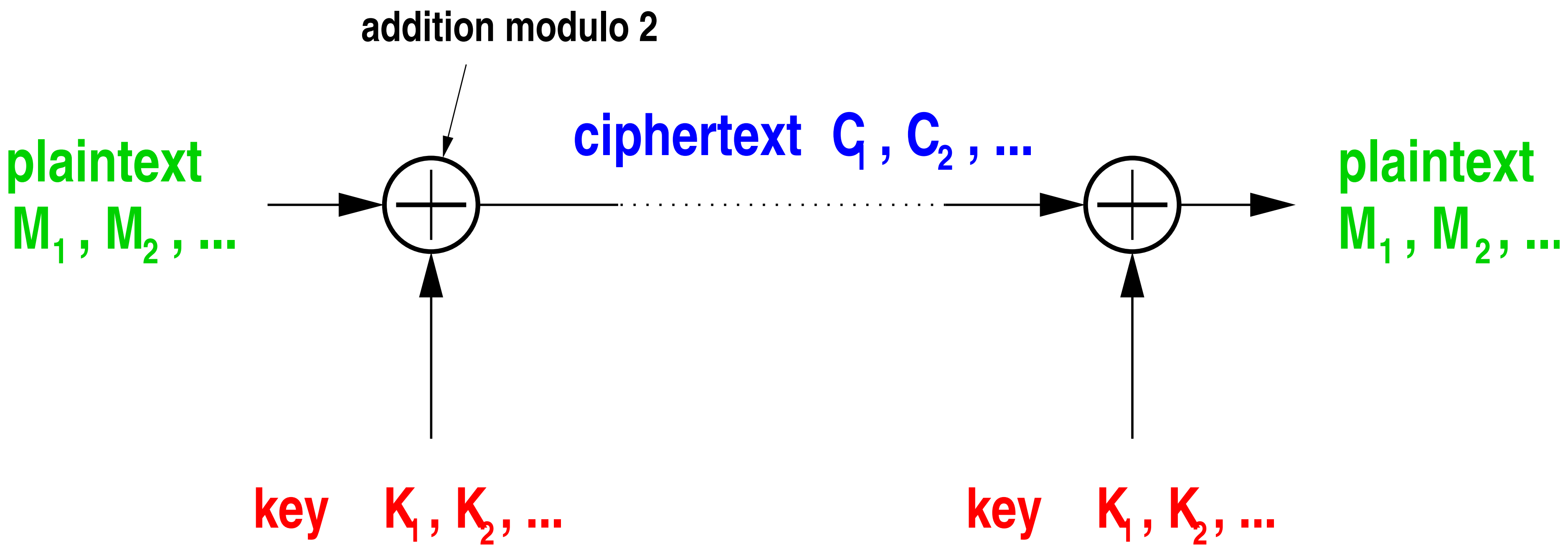
Examples: group, field, vector space, relation, graph, ...

Goals of abstraction:

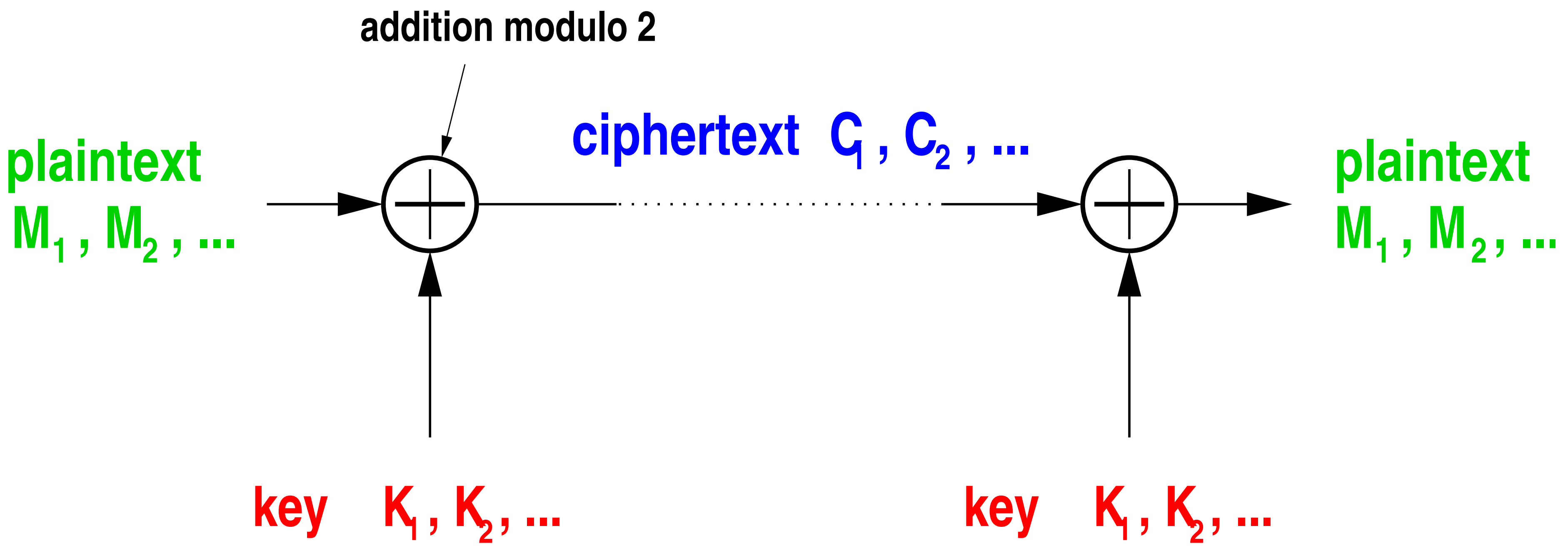
Goals of this talk:

- Introduce layers of abstraction in cryptography.
- Examples of abstract definitions and proofs.
- Announce a new security framework "abstract cryptography" (with Renato Renner).

Motivating example: One-time pad

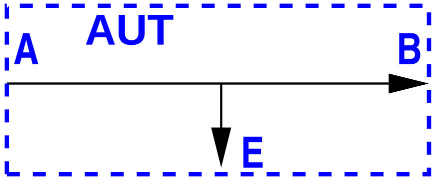


Motivating example: One-time pad

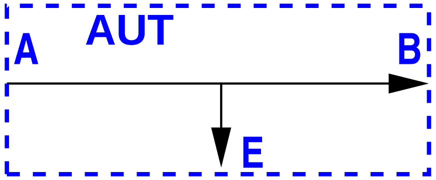


Perfect secrecy (Shannon): C and M statist. independent.

One-time pad in terms of systems

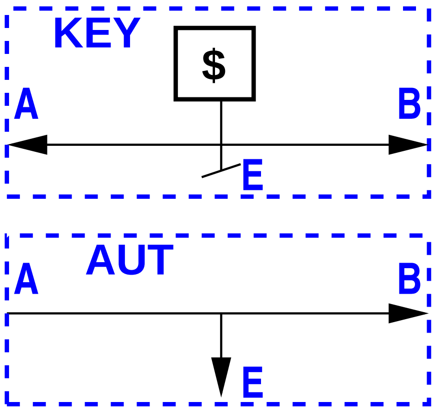


One-time pad in terms of systems



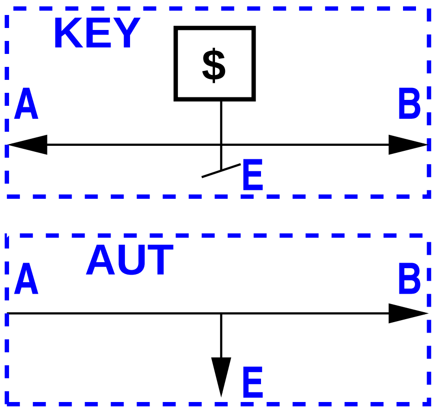
AUT

One-time pad in terms of systems



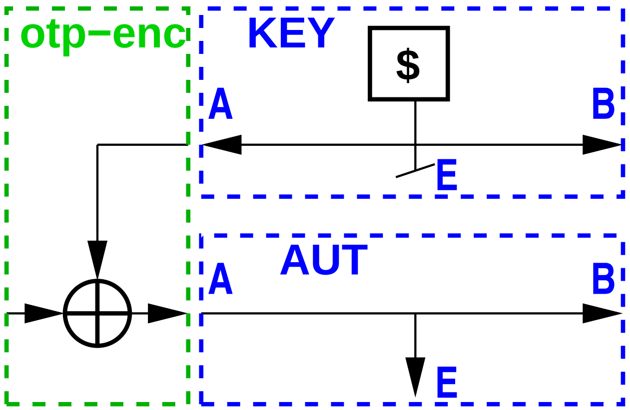
KEY||AUT

One-time pad in terms of systems



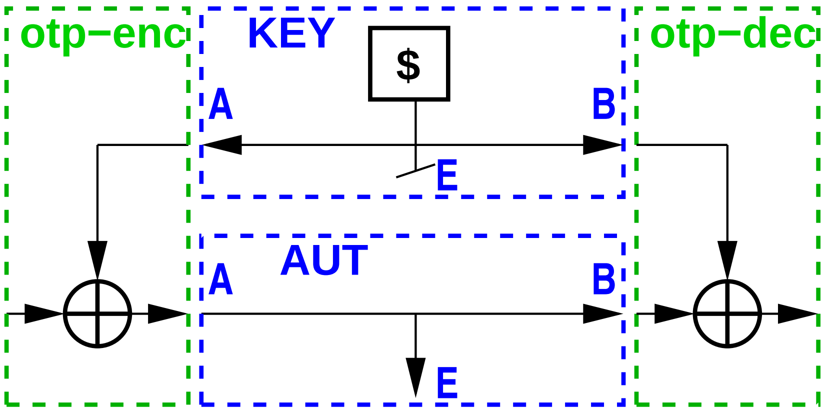
KEY||AUT

One-time pad in terms of systems



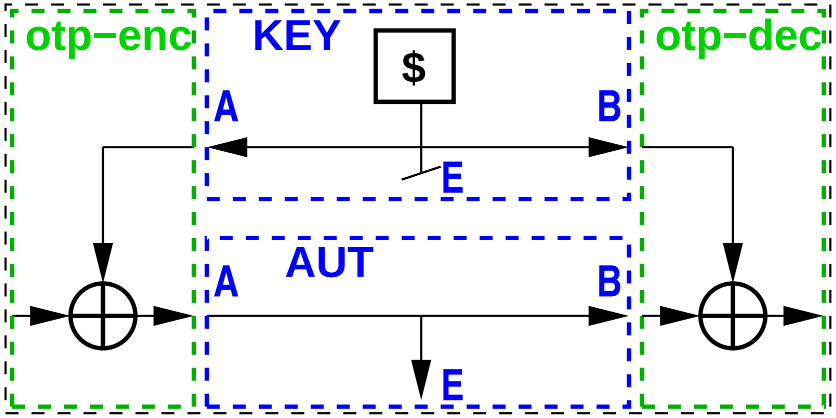
otp-enc^A (**KEY**||**AUT**)

One-time pad in terms of systems



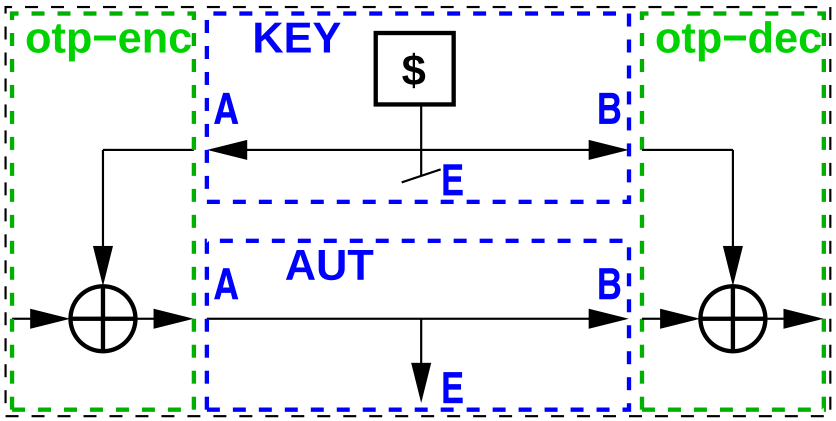
otp-dec^{B} **otp-enc**^{A} (**KEY**||**AUT**)

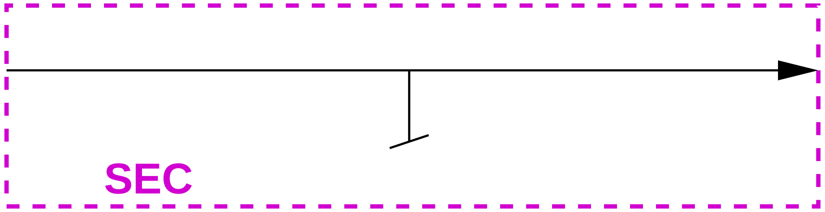
One-time pad in terms of systems



otp-dec^{B} otp-enc^{A} (**KEY**||**AUT**)

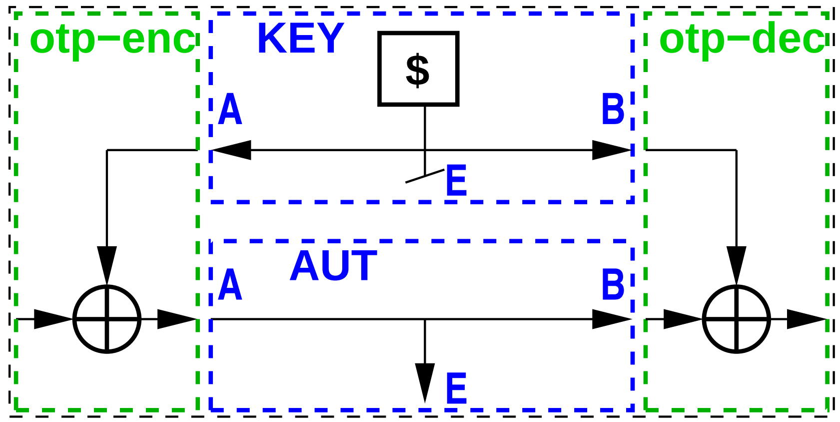
One-time pad in terms of systems

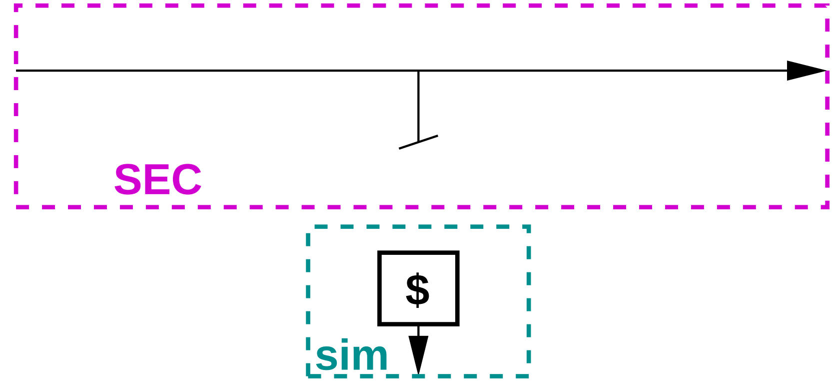




otp-dec^{B} otp-enc^{A} (KEY||AUT) SEC

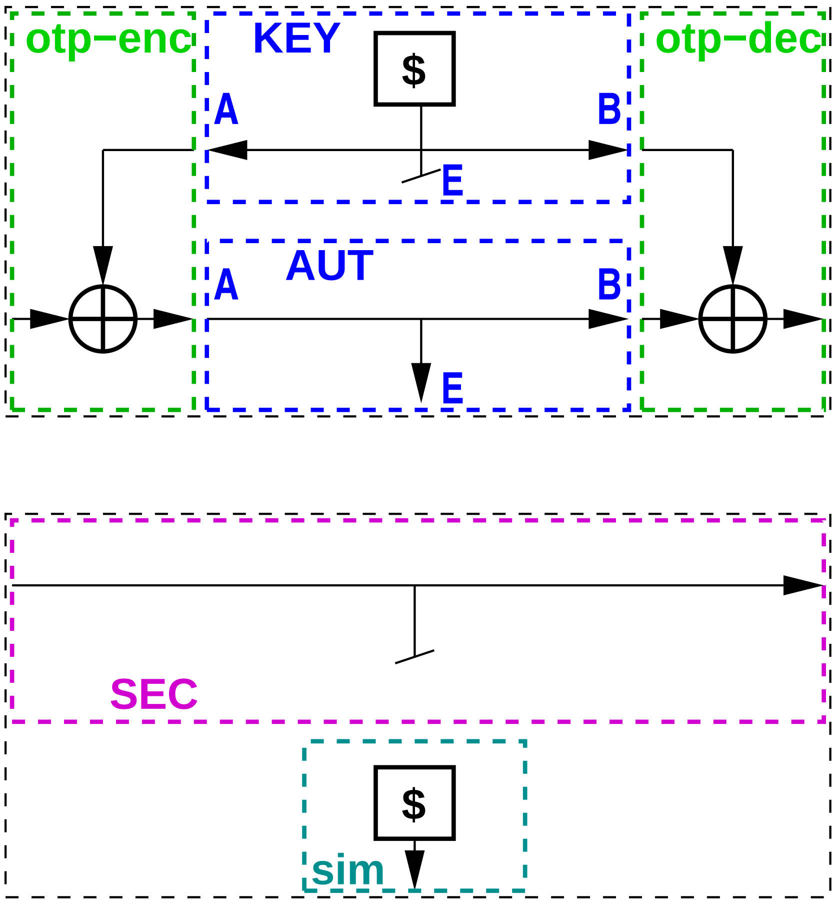
One-time pad in terms of systems





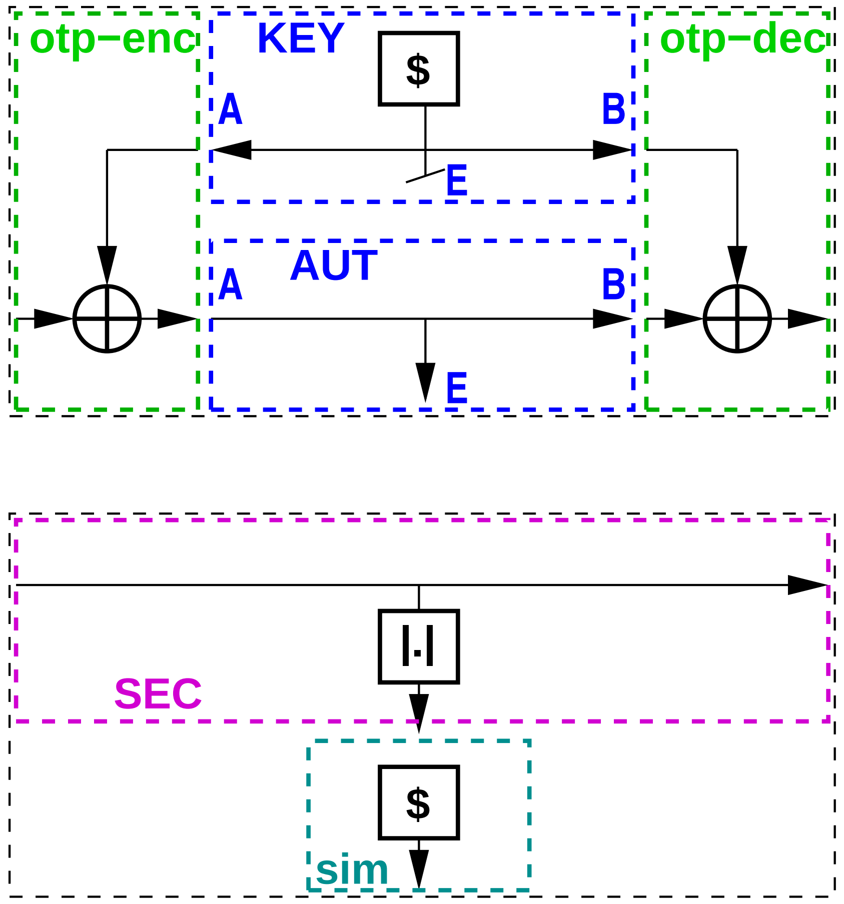
$\text{otp-dec}^B\ \text{otp-enc}^A\ (\text{KEY}\,||\,\text{AUT})$ $\qquad\qquad$ $\text{sim}^E\ \text{SEC}$

One-time pad in terms of systems



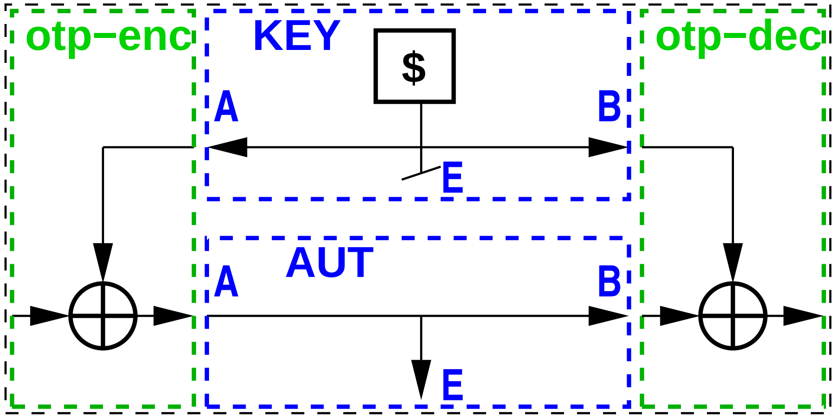
$$\mathbf{otp\text{-}dec}^{B}\ \mathbf{otp\text{-}enc}^{A}\ (\mathbf{KEY}\,||\,\mathbf{AUT}) \quad \equiv \quad \mathbf{sim}^{E}\ \mathbf{SEC}$$

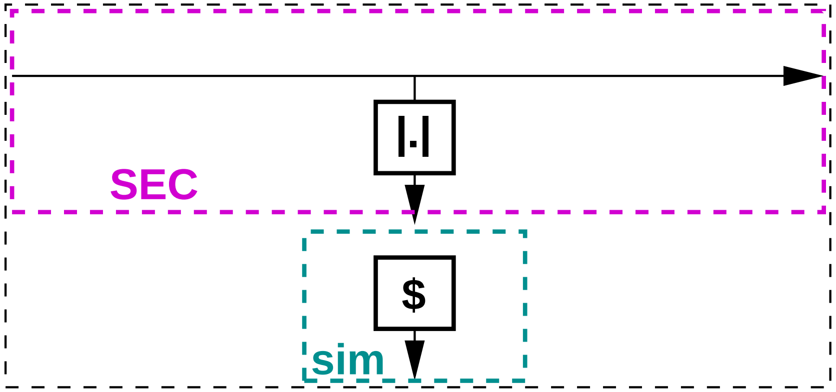
One-time pad in terms of systems



$$\text{otp-dec}^{B}\ \text{otp-enc}^{A}\ (\text{KEY} \| \text{AUT}) \equiv \text{sim}^{E}\ \text{SEC}$$

One-time pad in terms of systems

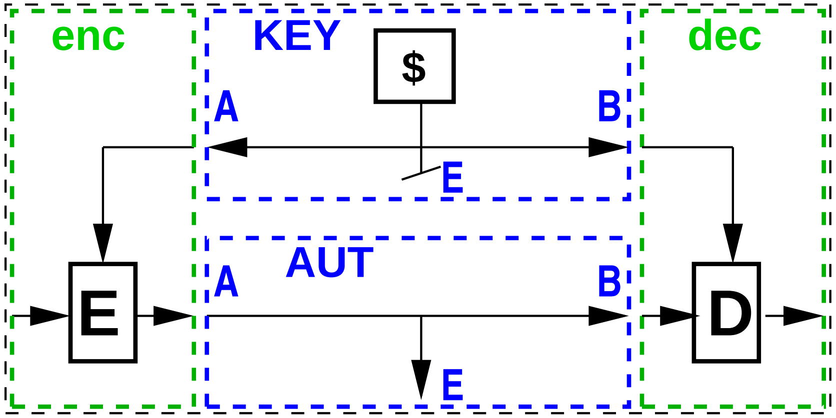


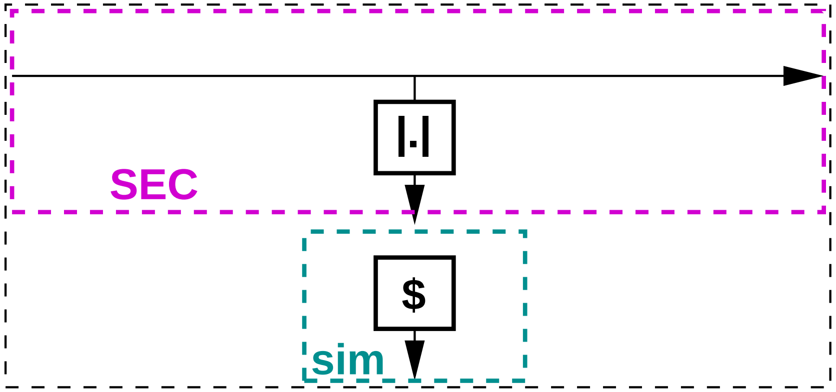


$$\textbf{otp-dec}^{B}\ \textbf{otp-enc}^{A}\ (\textbf{KEY}||\textbf{AUT}) \equiv \textbf{sim}^{E}\ \textbf{SEC}$$

written as a reduction: $(\textbf{KEY}||\textbf{AUT}) \xrightarrow{\textbf{otp}} \textbf{SEC}$

Symmetric encryption





$$\mathbf{dec}^{B}\,\mathbf{enc}^{A}\,(\mathbf{KEY}\,\|\,\mathbf{AUT}) \;\approx\; \mathbf{sim}^{E}\,\mathbf{SEC}$$

written as a reduction: $(\mathbf{KEY}\,\|\,\mathbf{AUT}) \xrightarrow{\mathbf{sym}} \mathbf{SEC}$

Constructive cryptography

Reduction concept:

$$\textbf{real system R} \xrightarrow{\textbf{protocol } \pi} \textbf{ideal system S}$$

Resource **S** is constructed from (reduced to) **R** by protocol π

Constructive cryptography

Reduction concept:

$$\text{real system } \mathbf{R} \xrightarrow{\text{protocol } \pi} \text{ideal system } \mathbf{S}$$

Resource **S** is constructed from (reduced to) **R** by protocol π

Example: Alice-Bob-Eve setting $\pi = (\pi_1, \pi_2)$

Constructive cryptography

Reduction concept:

$$\textbf{real system R} \xrightarrow{\textbf{protocol } \pi} \textbf{ideal system S}$$

Resource **S** is constructed from (reduced to) **R** by protocol π

Example: Alice-Bob-Eve setting $\pi = (\pi_1, \pi_2)$

$$\mathbf{R} \xrightarrow{\pi} \mathbf{S} \quad :\Leftrightarrow \quad \exists \sigma : \; \pi_1^{A} \pi_2^{B} \mathbf{R} \approx \sigma^{E} \mathbf{S}$$

Constructive cryptography

Reduction concept:

$$\textbf{real system R} \xrightarrow{\textbf{protocol } \pi} \textbf{ideal system S}$$

Resource **S** is constructed from (reduced to) **R** by protocol π

Example: Alice-Bob-Eve setting $\pi = (\pi_1, \pi_2)$

$$\mathbf{R} \xrightarrow{\pi} \mathbf{S} \quad :\Leftrightarrow \quad \exists \sigma : \ \pi_1^{A}\, \pi_2^{B}\, \mathbf{R} \approx \sigma^{E}\, \mathbf{S}$$

and

$$\pi_1^{A}\, \pi_2^{B}\, \perp^{E}\, \mathbf{R} \approx \perp^{E}\, \mathbf{S}$$

Constructive cryptography

Reduction concept:

$$\textbf{real system R} \xrightarrow{\textbf{protocol } \pi} \textbf{ideal system S}$$

Re … π

Composability of a reduction:

$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S} \;\wedge\; \mathbf{S} \xrightarrow{\beta} \mathbf{T} \;\Rightarrow\; \mathbf{R} \xrightarrow{\alpha\circ\beta} \mathbf{T}$$

Example: Alice-Bob-Eve setting $\pi = (\pi_1, \pi_2)$

$$\mathbf{R} \xrightarrow{\pi} \mathbf{S} \;:\Leftrightarrow\; \exists \sigma : \; \pi_1^{\mathsf{A}} \pi_2^{\mathsf{B}} \mathbf{R} \approx \sigma^{\mathsf{E}} \mathbf{S}$$

and

$$\pi_1^{\mathsf{A}} \pi_2^{\mathsf{B}} \perp^{\mathsf{E}} \mathbf{R} \approx \perp^{\mathsf{E}} \mathbf{S}$$

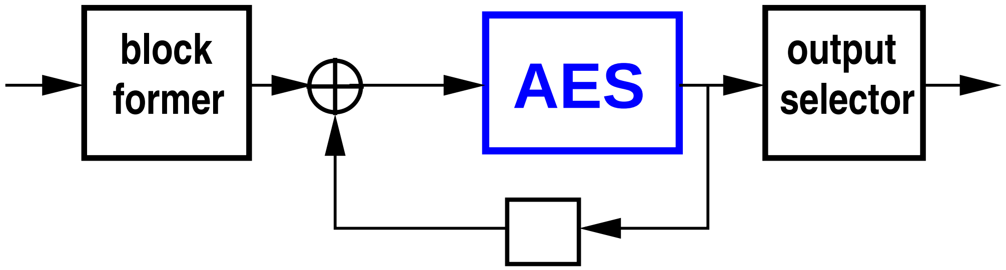
Levels of abstraction in cryptography

#	possible name	concepts treated at this level
1.	Reductions	def. of (universal) composability
2.	Abstract resources	isomorphism
3.	Abstract systems	distinguisher, hybrid argument, secure reduction, compos. proof
4.	Discrete systems	games, equivalence, indistinguishability proofs
5.	System implem.	complexity, efficiency notion
6.	Physical models	timing, power, side-channels

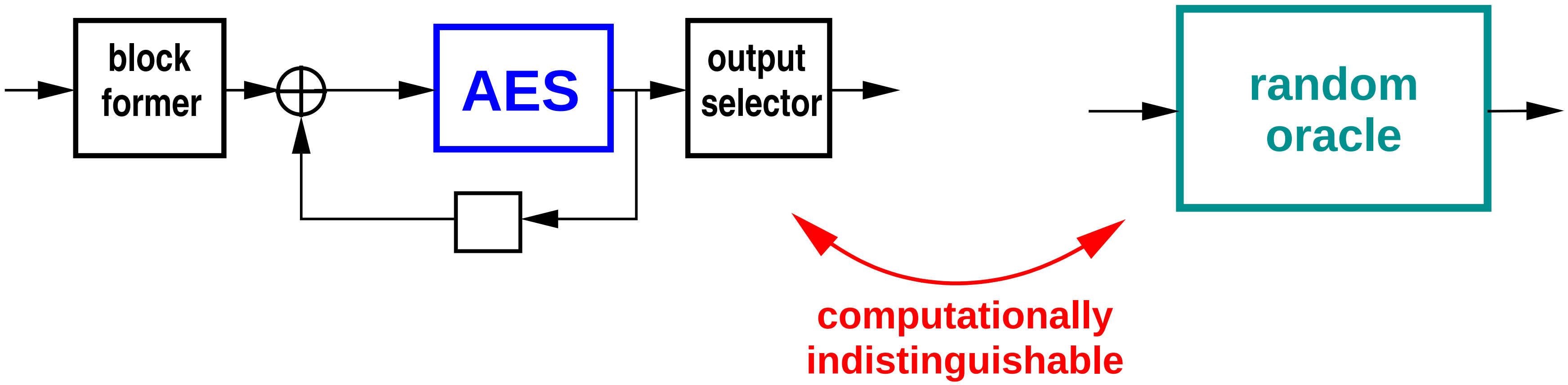
Levels of abstraction in cryptography

#	possible name	concepts treated at this level
1.	Reductions	def. of (universal) composability
2.	Abstract resources	isomorphism
3.	Abstract systems	distinguisher, hybrid argument, secure reduction, compos. proof
4.	Discrete systems	games, equivalence, indistinguishability proofs
5.	System implem.	complexity, efficiency notion
6.	Physical models	timing, power, side-channels

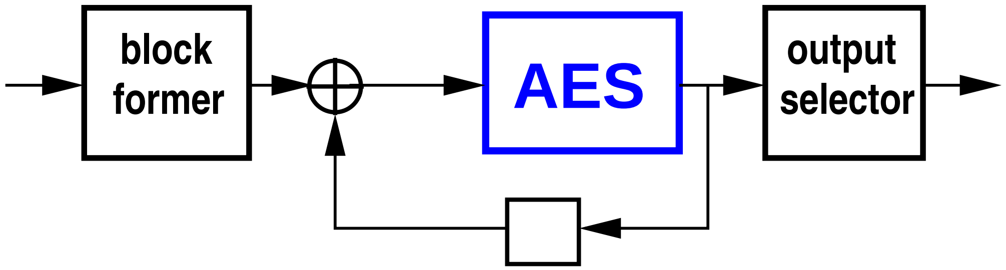
Example: CBC-MAC



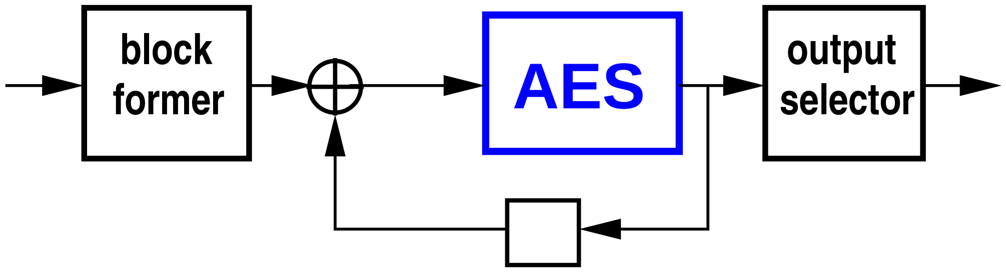
Example: CBC-MAC

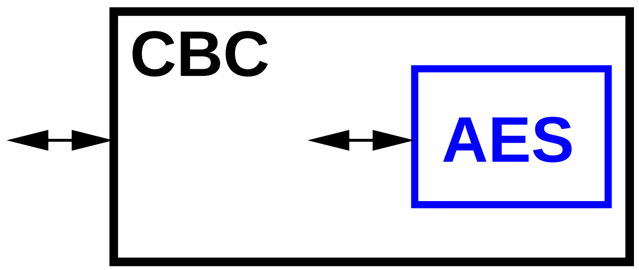


Example: CBC-MAC

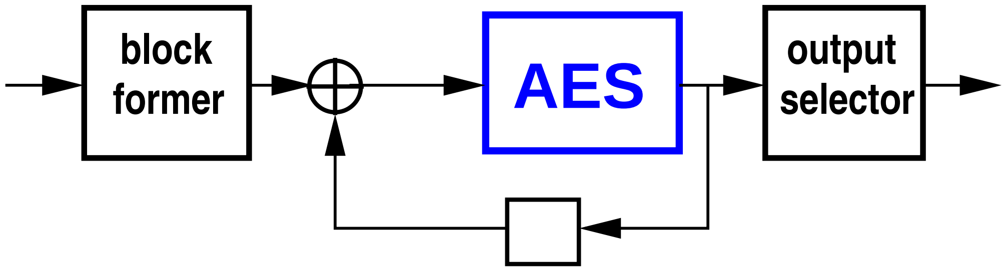


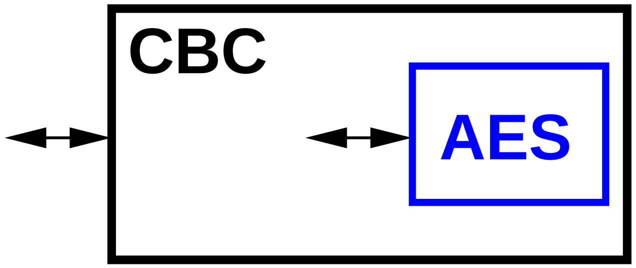
Example: CBC-MAC





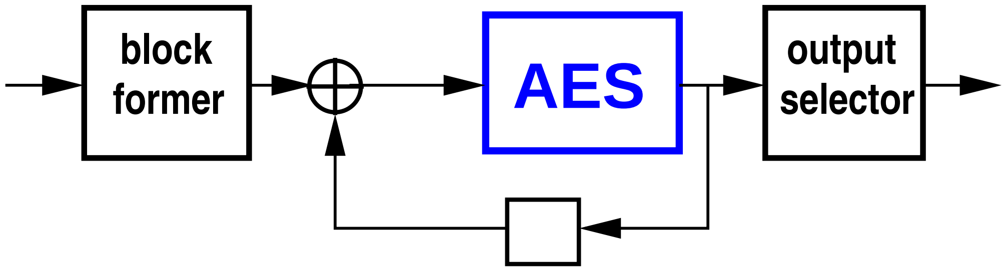
Example: CBC-MAC

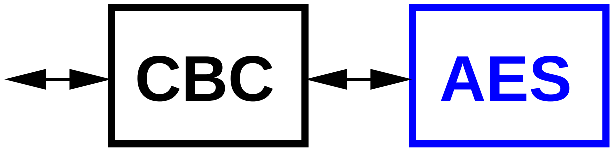




Notation: CBC(AES)

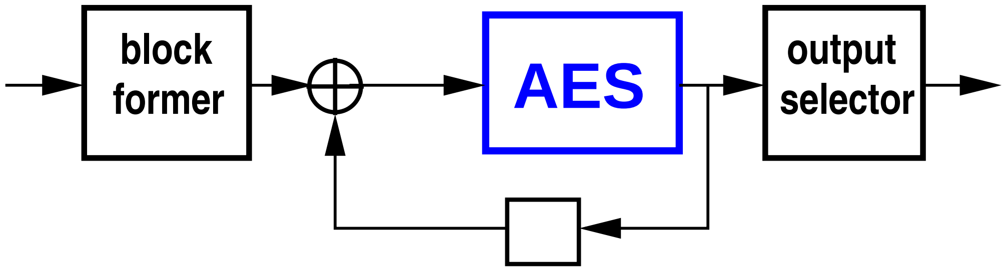
Example: CBC-MAC

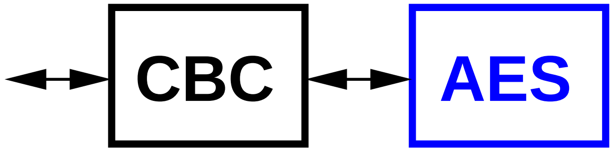




Notation: $\mathbf{CBC} \circ \mathbf{AES}$

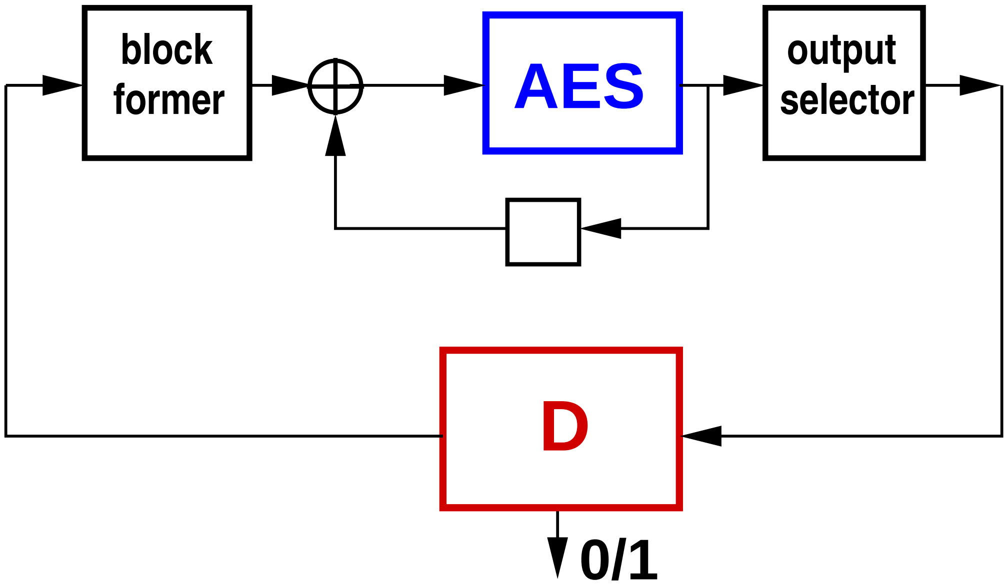
Example: CBC-MAC

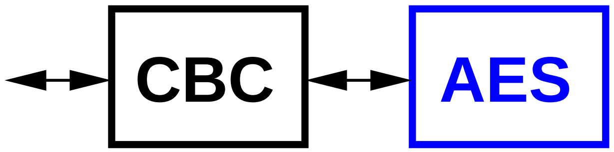




Notation: **CBC AES**

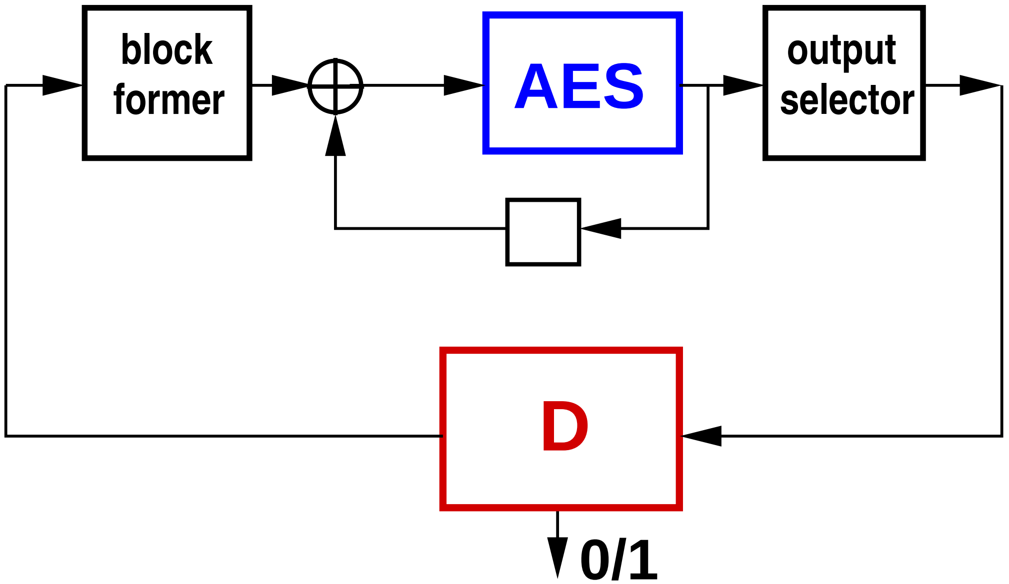
Example: CBC-MAC

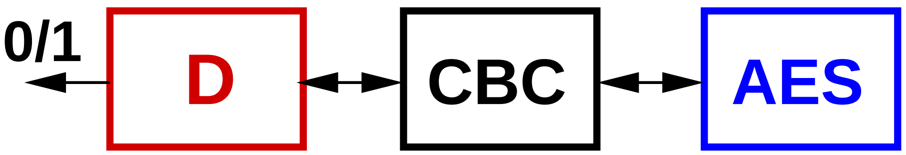




CBC AES

Example: CBC-MAC





D CBC AES

Security proof for CBC-MAC [3]

CBC AES $\approx$ RO

Security proof for CBC-MAC

D CBC AES $\approx$ D RO

Security proof for CBC-MAC

$$\mathbf{D}\ \mathbf{CBC}\ \mathbf{AES} \approx \mathbf{D}\ \mathbf{RO}$$

To show: $\Delta^{\mathbf{D}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \approx 0$

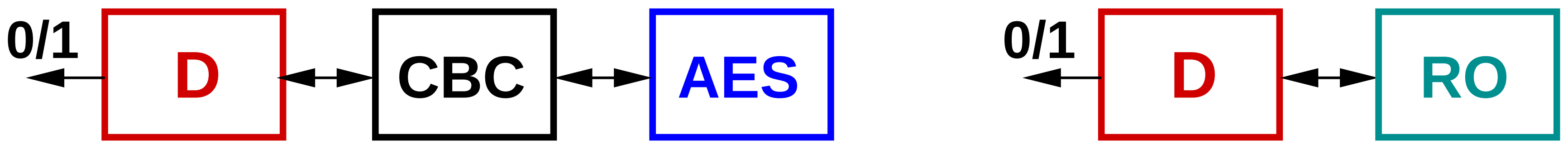
Security proof for CBC-MAC

$$\mathbf{D}\ \mathbf{CBC}\ \mathbf{AES} \approx \mathbf{D}\ \mathbf{RO}$$

To show: $\Delta^{\mathbf{D}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \approx 0$

Note: $\Delta^{\mathbf{D}}(\mathbf{S}, \mathbf{T}) = |\mathbf{DS}, \mathbf{DT}|$ (stat. distance of binary r.v.)

Security proof for CBC-MAC



$$D\ CBC\ AES \approx D\ RO$$

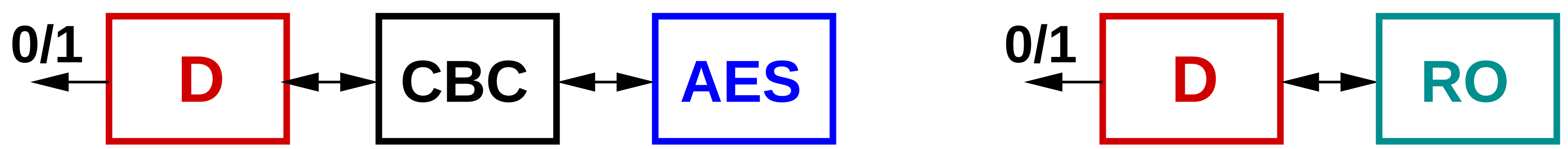
To show: $\Delta^{D}(CBC\ AES, RO) \approx 0$

Security proof for CBC-MAC

$$\mathbf{D}\ \mathbf{CBC}\ \mathbf{AES} \quad \approx \quad \mathbf{D}\ \mathbf{RO}$$

To show: $\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \approx 0$

Security proof for CBC-MAC



$$\mathbf{D}\ \mathbf{CBC}\ \mathbf{AES} \approx \mathbf{D}\ \mathbf{RO}$$

To show: $\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \approx 0$

$$\boxed{\Delta^{\mathcal{E}}(\mathbf{S}, \mathbf{T}) := \max_{\mathbf{D} \in \mathcal{E}} \Delta^{\mathbf{D}}(\mathbf{S}, \mathbf{T})}$$

Security proof for CBC-MAC

D CBC AES $\approx$ **D RO**

To show: $\Delta^{\mathcal{E}}(\text{CBC AES}, \text{RO}) \approx 0$

Security proof for CBC-MAC

D CBC AES $\approx$ **D RO**

To show: $\Delta^{\mathcal{E}}(\textbf{CBC AES}, \textbf{RO}) \approx 0$

Lemma: $\Delta^{\textbf{D}}$ and $\Delta^{\mathcal{E}}$ are pseudo-metrics:

- $\Delta^{\mathcal{E}}(\textbf{S}, \textbf{S}) = 0$
- $\Delta^{\mathcal{E}}(\textbf{R}, \textbf{T}) \leq \Delta^{\mathcal{E}}(\textbf{R}, \textbf{S}) + \Delta^{\mathcal{E}}(\textbf{S}, \textbf{T})$

Security proof for CBC-MAC

$$\mathbf{D}\ \mathbf{CBC}\ \mathbf{AES} \approx \mathbf{D}\ \mathbf{RO}$$

To show: $\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \approx 0$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \leq \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) + \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{RF}, \mathbf{RO})$$

Lemma: $\Delta^{\mathbf{D}}$ and $\Delta^{\mathcal{E}}$ are pseudo-metrics:

- $\Delta^{\mathcal{E}}(\mathbf{S}, \mathbf{S}) = 0$
- $\Delta^{\mathcal{E}}(\mathbf{R}, \mathbf{T}) \leq \Delta^{\mathcal{E}}(\mathbf{R}, \mathbf{S}) + \Delta^{\mathcal{E}}(\mathbf{S}, \mathbf{T})$

Security proof for CBC-MAC [3]

$$\mathbf{D}\;\mathbf{CBC}\;\mathbf{AES} \;\approx\; \mathbf{D}\;\mathbf{RO}$$

To show: $\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \approx 0$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \leq \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) + \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{RF}, \mathbf{RO})$$

Security proof for CBC-MAC

$$\mathbf{D}\ \mathbf{CBC}\ \mathbf{AES} \approx \mathbf{D}\ \mathbf{RO}$$

To show: $\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \approx 0$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \leq \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) + \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{RF}, \mathbf{RO})$$

Absorption lemma: $\Delta^{\mathbf{D}}(\mathbf{CS}, \mathbf{CT}) = \Delta^{\mathbf{DC}}(\mathbf{S}, \mathbf{T})$

Proof: $\mathbf{DCS} = \mathbf{D}(\mathbf{CS}) = (\mathbf{DC})\mathbf{S}$

Security proof for CBC-MAC

$$\mathbf{D}\ \mathbf{CBC}\ \mathbf{AES} \approx \mathbf{D}\ \mathbf{RO}$$

To show: $\quad \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \approx 0$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \leq \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) + \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{RF}, \mathbf{RO})$$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) = \Delta^{\mathcal{E}\mathbf{CBC}}(\mathbf{AES}, \mathbf{RF})$$

Absorption lemma: $\Delta^{\mathbf{D}}(\mathbf{C}\mathbf{S}, \mathbf{C}\mathbf{T}) = \Delta^{\mathbf{D}\mathbf{C}}(\mathbf{S}, \mathbf{T})$

Proof: $\mathbf{D}\mathbf{C}\mathbf{S} = \mathbf{D}(\mathbf{C}\mathbf{S}) = (\mathbf{D}\mathbf{C})\mathbf{S}$

Security proof for CBC-MAC

[3]

$$\mathbf{D}\ \mathbf{CBC}\ \mathbf{AES} \approx \mathbf{D}\ \mathbf{RO}$$

To show: $\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \approx 0$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \leq \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) + \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{RF}, \mathbf{RO})$$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) = \Delta^{\mathcal{E}\,\mathbf{CBC}}(\mathbf{AES}, \mathbf{RF})$$

Non-expansion lemma:

$$\mathcal{D}\mathbf{C} \subseteq \mathcal{D} \Rightarrow \Delta^{\mathcal{D}}(\mathbf{C}\mathbf{S}, \mathbf{C}\mathbf{T}) \leq \Delta^{\mathcal{D}}(\mathbf{S}, \mathbf{T})$$

Security proof for CBC-MAC

$$\mathbf{D}\ \mathbf{CBC}\ \mathbf{AES} \quad \approx \quad \mathbf{D}\ \mathbf{RO}$$

To show: $\quad \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \approx 0$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \leq \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF} \quad \mathbf{F}, \mathbf{RO})$$

$$\boxed{\mathcal{E}\,\mathbf{CBC} \subseteq \mathcal{E}}$$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) = \Delta^{\mathcal{E}\mathbf{CBC}}(\mathbf{AES}, \mathbf{RF})$$

Non-expansion lemma:

$$\mathcal{D}\mathbf{C} \subseteq \mathcal{D} \ \Rightarrow\ \Delta^{\mathcal{D}}(\mathbf{C}\mathbf{S}, \mathbf{C}\mathbf{T}) \leq \Delta^{\mathcal{D}}(\mathbf{S}, \mathbf{T})$$

Security proof for CBC-MAC

$$\mathbf{D}\ \mathbf{CBC}\ \mathbf{AES} \ \approx\ \mathbf{D}\ \mathbf{RO}$$

To show: $\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \approx 0$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \le \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF} \ \ldots\ \mathbf{F}, \mathbf{RO})$$

$$\boxed{\mathcal{E}\,\mathbf{CBC} \subseteq \mathcal{E}}$$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) = \Delta^{\mathcal{E}\mathbf{CBC}}(\mathbf{AES}, \mathbf{RF}) \le \Delta^{\mathcal{E}}(\mathbf{AES}, \mathbf{RF})$$

Non-expansion lemma:

$$\mathcal{D}\mathbf{C} \subseteq \mathcal{D} \ \Rightarrow\ \Delta^{\mathcal{D}}(\mathbf{C}\mathbf{S}, \mathbf{C}\mathbf{T}) \le \Delta^{\mathcal{D}}(\mathbf{S}, \mathbf{T})$$

Security proof for CBC-MAC

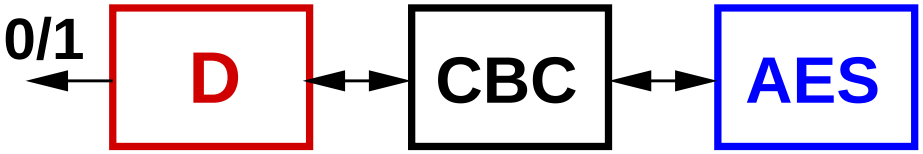
$$\mathbf{D}\ \mathbf{CBC}\ \mathbf{AES} \quad \approx \quad \mathbf{D}\ \mathbf{RO}$$

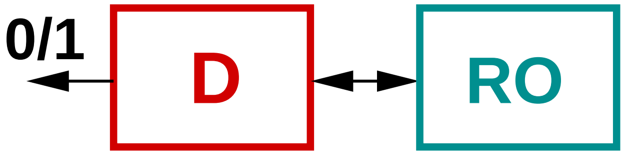
To show: $\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \approx 0$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \leq \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) + \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{RF}, \mathbf{RO})$$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) = \Delta^{\mathcal{E}\,\mathbf{CBC}}(\mathbf{AES}, \mathbf{RF}) \leq \Delta^{\mathcal{E}}(\mathbf{AES}, \mathbf{RF})$$

Security proof for CBC-MAC [3,4]





$$\mathbf{D}\ \mathbf{CBC}\ \mathbf{AES} \approx \mathbf{D}\ \mathbf{RO}$$

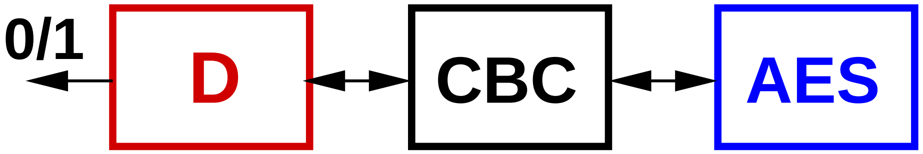
To show: $\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \approx 0$

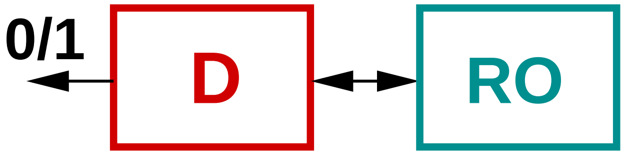
$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \leq \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) + \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{RF}, \mathbf{RO})$$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) = \Delta^{\mathcal{E}\,\mathbf{CBC}}(\mathbf{AES}, \mathbf{RF}) \leq \Delta^{\mathcal{E}}(\mathbf{AES}, \mathbf{RF})$$

$$\Delta(\mathbf{CBC}\,\mathbf{RF}, \mathbf{RO}) \leq \frac{1}{2}\ell^2 2^{-n}$$ [BKR94,...] [4]

Security proof for CBC-MAC [3,4]





Note: Many security proofs can be phrased at this level of abstraction and become quite simple or even trivial.

To

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{RO}) \leq \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) + \Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{RF}, \mathbf{RO})$$

$$\Delta^{\mathcal{E}}(\mathbf{CBC}\,\mathbf{AES}, \mathbf{CBC}\,\mathbf{RF}) = \Delta^{\mathcal{E}\mathbf{CBC}}(\mathbf{AES}, \mathbf{RF}) \leq \Delta^{\mathcal{E}}(\mathbf{AES}, \mathbf{RF})$$

$$\Delta(\mathbf{CBC}\,\mathbf{RF}, \mathbf{RO}) \leq \tfrac{1}{2}\ell^2 2^{-n}$$ [BKR94,...] [4]

Levels of abstraction in cryptography

#	possible name	concepts treated at this level
1.	Reductions	def. of (universal) composability
2.	Abstract resources	isomorphism
3.	Abstract systems	distinguisher, hybrid argument, secure reduction, compos. proof
4.	Discrete systems	games, equivalence, indistinguishability proofs
5.	System implem.	complexity, efficiency notion
6.	Physical models	timing, power, side-channels

Levels of abstraction in cryptography

#	possible name	concepts treated at this level
1.	Reductions	def. of (universal) composability
2.	Abstract resources	isomorphism
3.	Abstract systems	distinguisher, hybrid argument, secure reduction, compos. proof
4.	Discrete systems	games, equivalence, indistinguishability proofs
5.	System implem.	complexity, efficiency notion
6.	Physical models	timing, power, side-channels

Efficient, infeasible, negligible

We need notions for

- the complexity of system implementation
- what is efficient (for the good guys)
- what is infeasible (for the bad guys)
- what is negligible

Efficient, infeasible, negligible

We need notions for

- the complexity of system implementation
- what is efficient (for the good guys)
- what is infeasible (for the bad guys)
- what is negligible

$\mathcal{E}$ = set of efficiently impl. systems.

Efficient, infeasible, negligible [5,3]

We need notions for

- the complexity of system implementation
- what is efficient (for the good guys)
- what is infeasible (for the bad guys)
- what is negligible

$\mathcal{E}$ = set of efficiently impl. systems. $\boxed{\mathcal{E} \circ \mathcal{E} \subseteq \mathcal{E}, \quad \mathcal{E}||\mathcal{E} \subseteq \mathcal{E}}$

Efficient, infeasible, negligible [5,3]

We need notions for

- the complexity of system implementation
- what is efficient (for the good guys)
- what is infeasible (for the bad guys)
- what is negligible

$\mathcal{E}$ = set of efficiently impl. systems. $\boxed{\mathcal{E} \circ \mathcal{E} \subseteq \mathcal{E}, \quad \mathcal{E}||\mathcal{E} \subseteq \mathcal{E}}$

$\mathcal{F}$ = set of feasibly impl. systems ($\mathcal{E} \subseteq \mathcal{F}$)

Efficient, infeasible, negligible

We need notions for

- the complexity of system implementation
- what is efficient (for the good guys)
- what is infeasible (for the bad guys)
- what is negligible

$\mathcal{E}$ = set of efficiently impl. systems.

$$\boxed{\mathcal{E} \circ \mathcal{E} \subseteq \mathcal{E}, \quad \mathcal{E}||\mathcal{E} \subseteq \mathcal{E}}$$

$\mathcal{F}$ = set of feasibly impl. systems (

$$\boxed{\mathcal{F} \circ \mathcal{F} \subseteq \mathcal{F}, \quad \mathcal{F}||\mathcal{F} \subseteq \mathcal{F}}$$

Efficient, infeasible, negligible

We need notions for

- the complexity of system implementation
- what is efficient (for the good guys)
- what is infeasible (for the bad guys)
- what is negligible

$\mathcal{E}$ = set of efficiently impl. systems.

$$\boxed{\mathcal{E} \circ \mathcal{E} \subseteq \mathcal{E}, \quad \mathcal{E}||\mathcal{E} \subseteq \mathcal{E}}$$

$\mathcal{F}$ = set of feasibly impl. systems (

$$\boxed{\mathcal{F} \circ \mathcal{F} \subseteq \mathcal{F}, \quad \mathcal{F}||\mathcal{F} \subseteq \mathcal{F}}$$

No reason to set $\mathcal{E} = \mathcal{F}$!

Efficient, infeasible, negligible [5,3]

We need notions for

- the complexity of system implementation
- what is efficient (for the good guys)
- what is infeasible (for the bad guys)
- what is negligible

$\mathcal{E}$ = set of efficiently impl. systems.

$$\mathcal{E} \circ \mathcal{E} \subseteq \mathcal{E}, \quad \mathcal{E} || \mathcal{E} \subseteq \mathcal{E}$$

$\mathcal{F}$ = set of feasibly impl. systems (

$$\mathcal{F} \circ \mathcal{F} \subseteq \mathcal{F}, \quad \mathcal{F} || \mathcal{F} \subseteq \mathcal{F}$$

$\mathcal{N}$ = set of negligible functions

Efficient, infeasible, negligible

We need notions for

- the complexity of system implementation
- what is efficient (for the good guys)
- what is infeasible (for the bad guys)
- what is negligible

$\mathcal{E}$ = set of efficiently impl. systems.

$$\mathcal{E} \circ \mathcal{E} \subseteq \mathcal{E}, \quad \mathcal{E} || \mathcal{E} \subseteq \mathcal{E}$$

$\mathcal{F}$ = set of feasibly impl. systems (

$$\mathcal{F} \circ \mathcal{F} \subseteq \mathcal{F}, \quad \mathcal{F} || \mathcal{F} \subseteq \mathcal{F}$$

$\mathcal{N}$ = set of negligible functions

$$\mathcal{F} \cdot \mathcal{N} \subseteq \mathcal{N}$$

Efficient, infeasible, negligible [5,3]

We

Note: The usual poly-time notions (i.e., $n^{O(1)}$) are of course composable, but so are many other notions, e.g. $n^{O(\log\log n)}$ or $n^{O(\sqrt{\log\log\log n})}$.

$\mathcal{E}$ = set of efficiently impl. systems.

$$\mathcal{E} \circ \mathcal{E} \subseteq \mathcal{E}, \quad \mathcal{E}||\mathcal{E} \subseteq \mathcal{E}$$

$\mathcal{F}$ = set of feasibly impl. systems (

$$\mathcal{F} \circ \mathcal{F} \subseteq \mathcal{F}, \quad \mathcal{F}||\mathcal{F} \subseteq \mathcal{F}$$

$\mathcal{N}$ = set of negligible functions

$$\mathcal{F} \cdot \mathcal{N} \subseteq \mathcal{N}$$

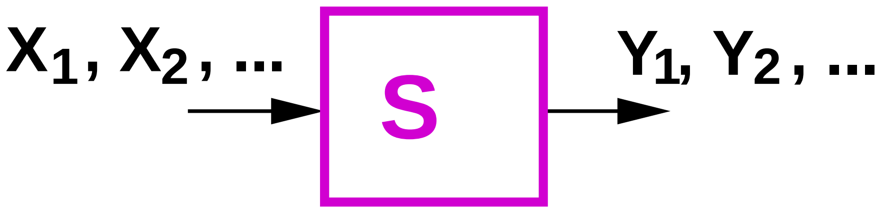
Levels of abstraction in cryptography

#	possible name	concepts treated at this level
1.	**Reductions**	def. of (universal) composability
2.	**Abstract resources**	isomorphism
3.	**Abstract systems**	distinguisher, hybrid argument, secure reduction, compos. proof
4.	**Discrete systems**	games, equivalence, indistinguishability proofs
5.	**System implem.**	complexity, efficiency notion
6.	**Physical models**	timing, power, side-channels

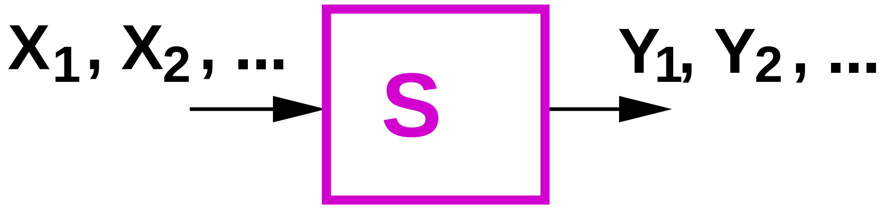
Levels of abstraction in cryptography

#	possible name	concepts treated at this level
1.	**Reductions**	def. of (universal) composability
2.	**Abstract resources**	isomorphism
3.	**Abstract systems**	distinguisher, hybrid argument, secure reduction, compos. proof
4.	**Discrete systems**	games, equivalence, indistinguishability proofs
5.	**System implem.**	complexity, efficiency notion
6.	**Physical models**	timing, power, side-channels

Discrete systems

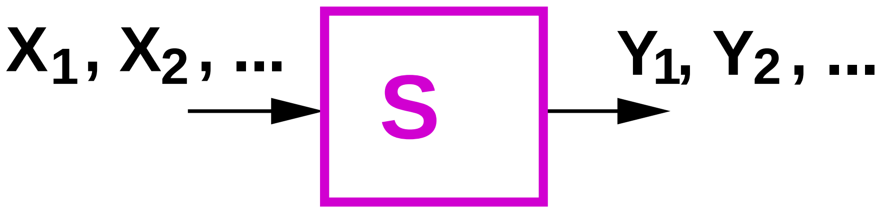


Discrete systems



Description of **S**: figure, pseudo-code, text, ...

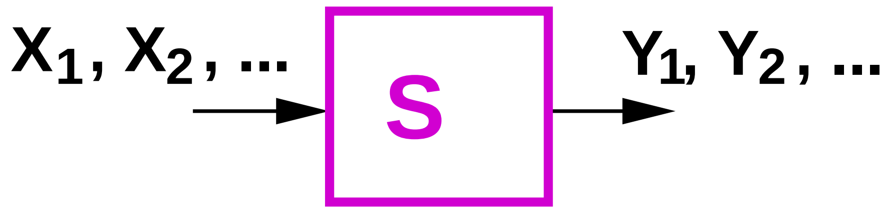
Discrete systems



Description of **S**: figure, pseudo-code, text, ...

What kind of mathematical object is the behavior of **S**?

Discrete systems



Description of **S**: figure, pseudo-code, text, ...

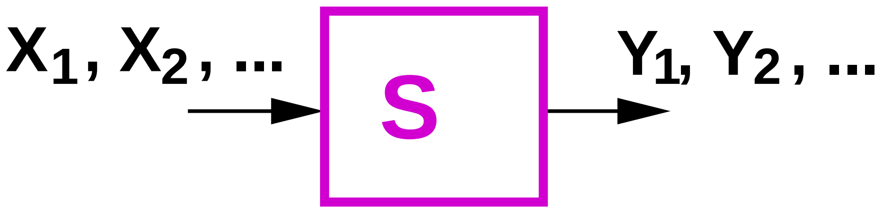
What kind of mathematical object is the behavior of **S**?

> Characterized by: $p^{\mathbf{S}}_{Y^i|X^i}$ for $i = 1, 2, \ldots$

(where $X^i = (X_1, \ldots, X_i)$)

This abstraction is called a random system [Mau02].

Discrete systems



Description of **S**: figure, pseudo-code, text, ...

What kind of mathematical object is the behavior of **S**?

Characterized by: $p^{\mathbf{S}}_{Y^i|X^i}$ for $i = 1, 2, \ldots$

(where $X^i = (X_1, \ldots, X_i)$)

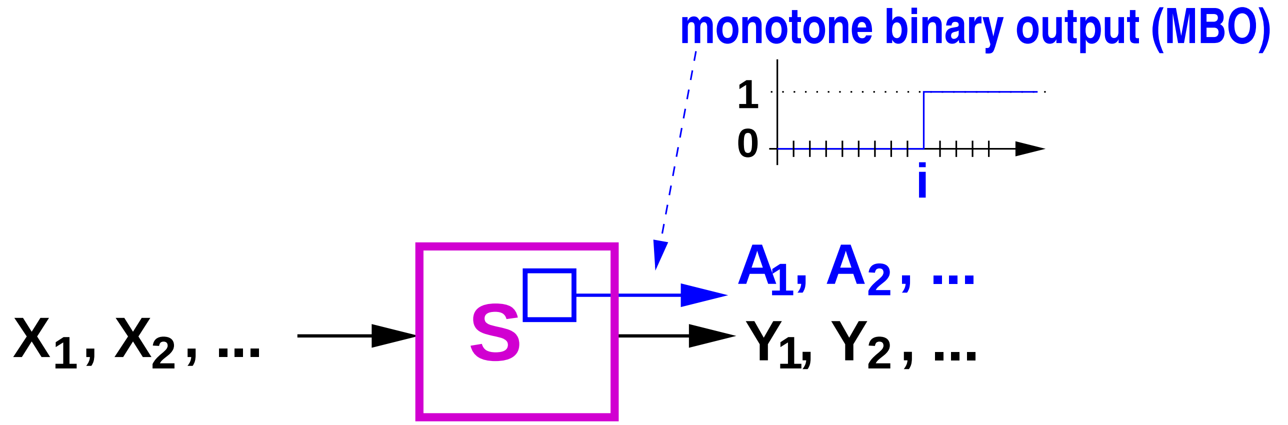
This abstraction is called a random system [Mau02].

Equivalence of systems: $\mathbf{S} \equiv \mathbf{T}$ if same behavior

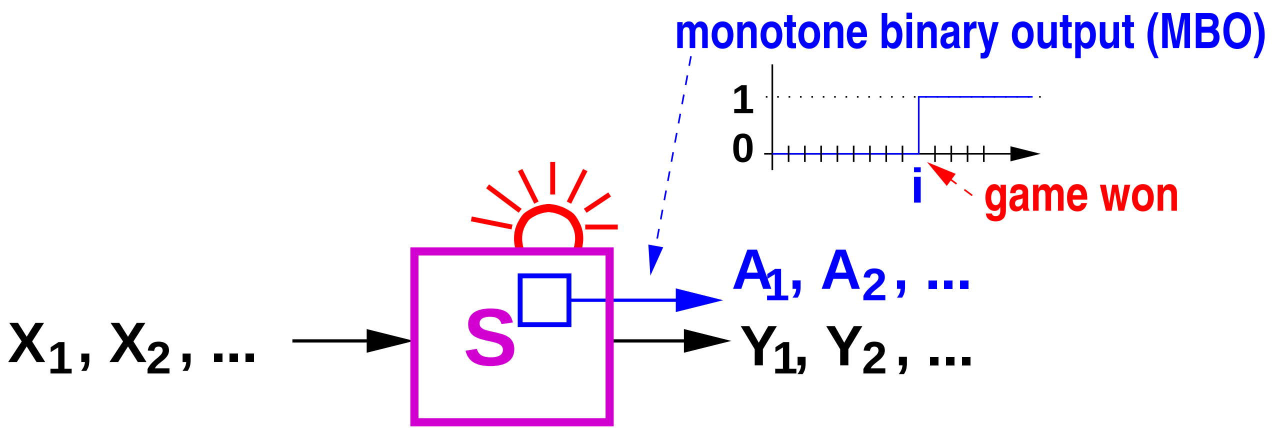
Games

$$X_1, X_2, \ldots \longrightarrow \boxed{S} \longrightarrow Y_1, Y_2, \ldots$$

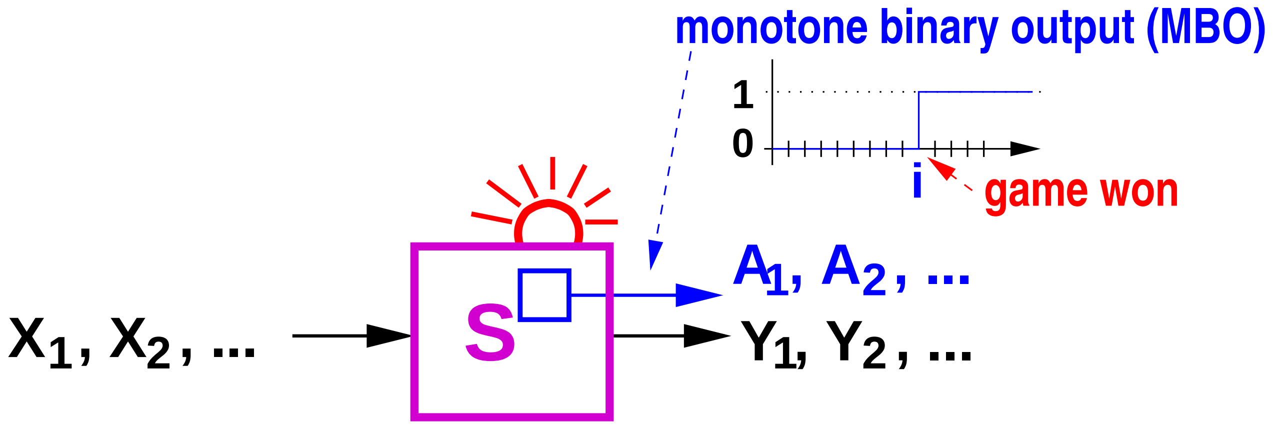
Games



Games

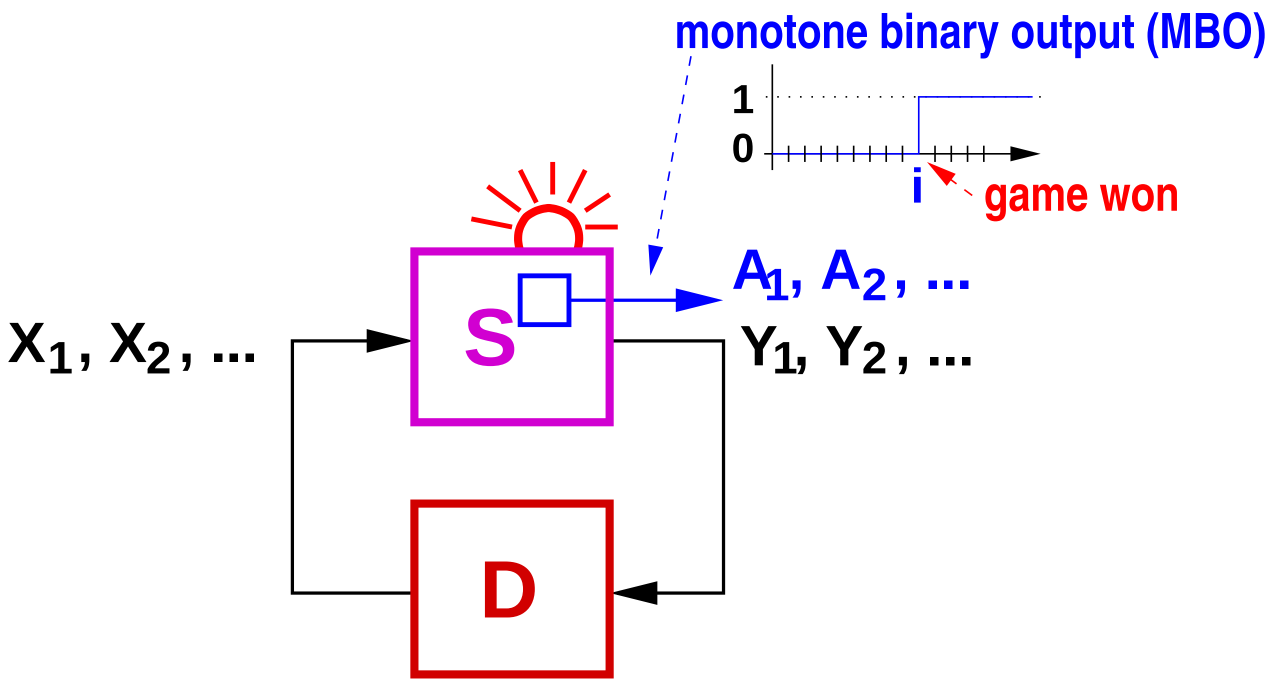

monotone binary output (MBO)
1
0
i
game won
S
$X_1, X_2, \ldots$
$A_1, A_2, \ldots$
$Y_1, Y_2, \ldots$

Games



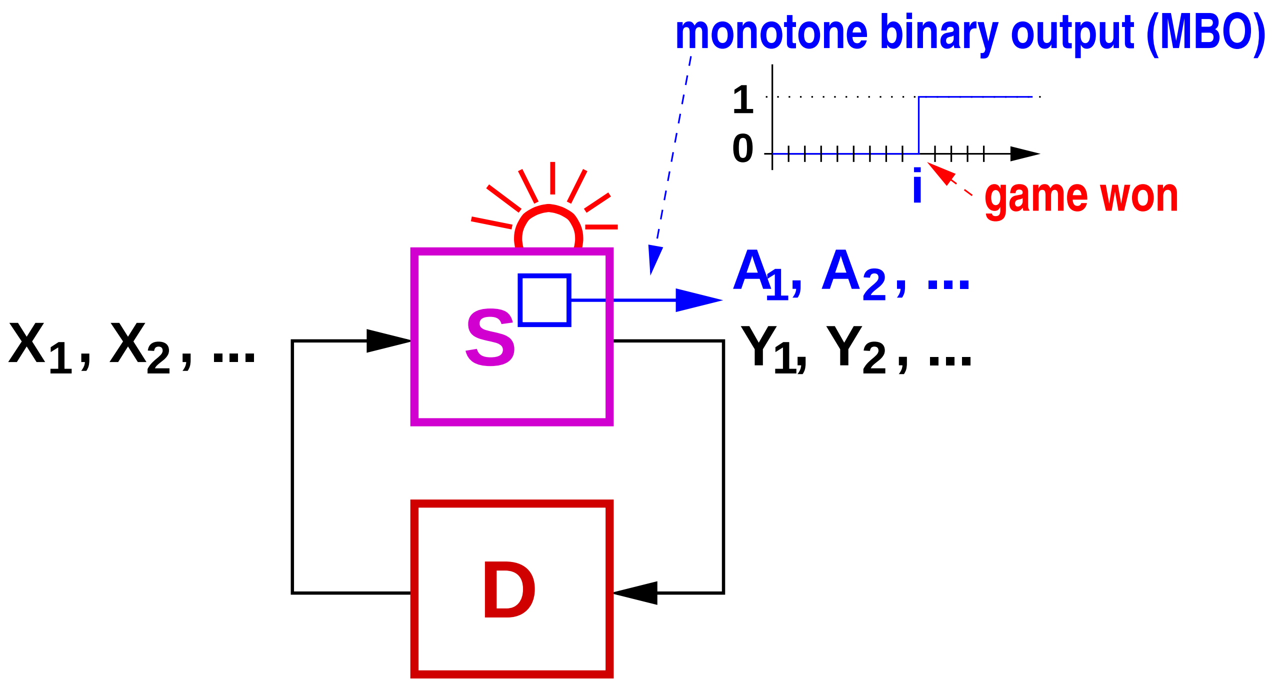
Characterized by: $p^{\mathbf{S}}_{Y^i A_i | X^i}$ for $i = 1, 2, \ldots$

Games



Characterized by: $p^{\mathbf{S}}_{Y^i A_i | X^i}$ for $i = 1, 2, \ldots$

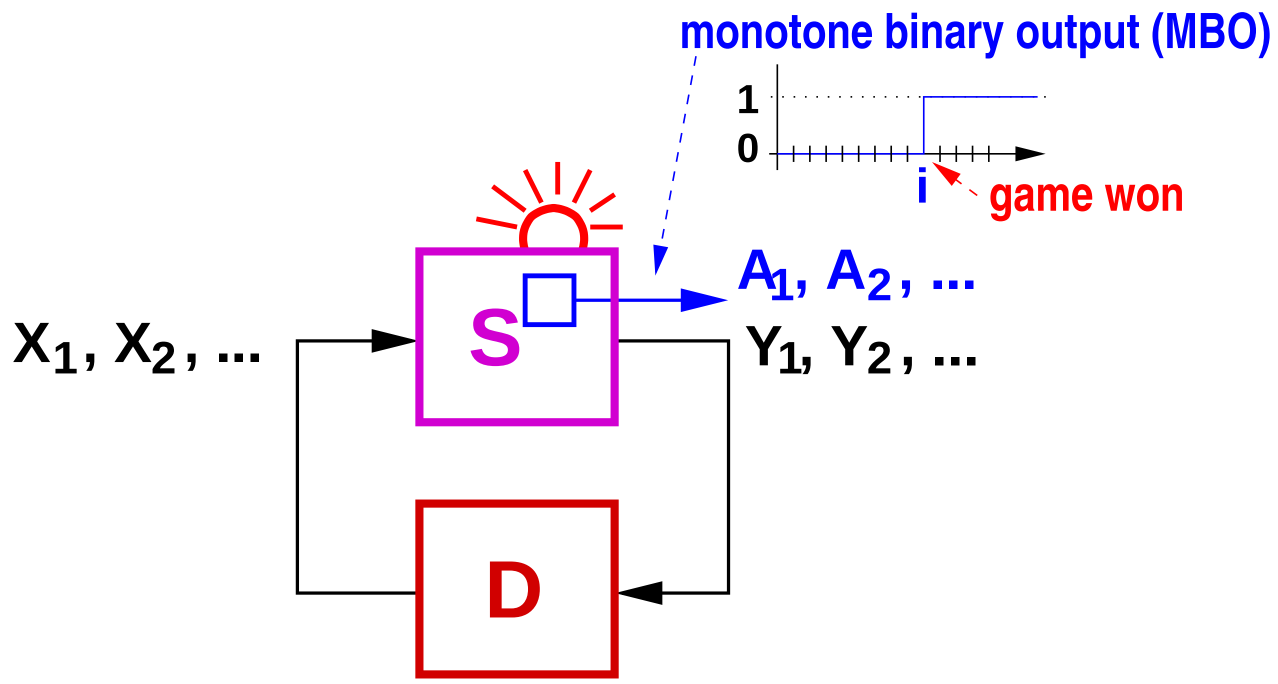
Games



Characterized by: $p^{\mathbf{S}}_{Y^i A_i | X^i}$ for $i = 1, 2, \ldots$

Conditional equivalence: $\mathbf{S}|\mathcal{A} \equiv \mathbf{T}$ $:\Leftrightarrow$ $p^{\mathbf{S}}_{Y^i | X^i A_i} = p^{\mathbf{T}}_{Y^i | X^i}$

Games



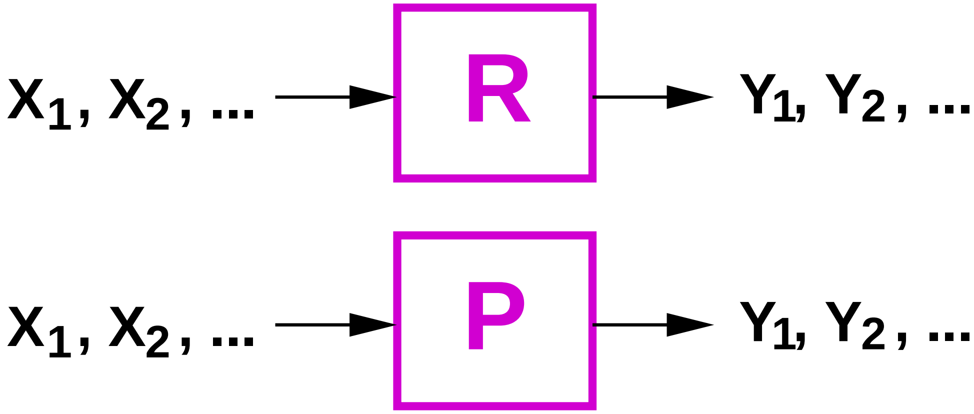
Characterized by: $\mathrm{p}^{\mathbf{S}}_{Y^i A_i | X^i}$ for $i = 1, 2, \ldots$

Conditional equivalence: $\mathbf{S}|\mathcal{A} \equiv \mathbf{T}$ $:\Leftrightarrow$ $\mathrm{p}^{\mathbf{S}}_{Y^i | X^i A_i} = \mathrm{p}^{\mathbf{T}}_{Y^i | X^i}$

Lemma [M02]: $\mathbf{S}|\mathcal{A} \equiv \mathbf{T} \Rightarrow \Delta(\mathbf{S}, \mathbf{T}) \leq$ optimal prob. of provoking the MBO non-adaptively in **S** (same # of queries).

Games

PRP-PRF switching lemma:

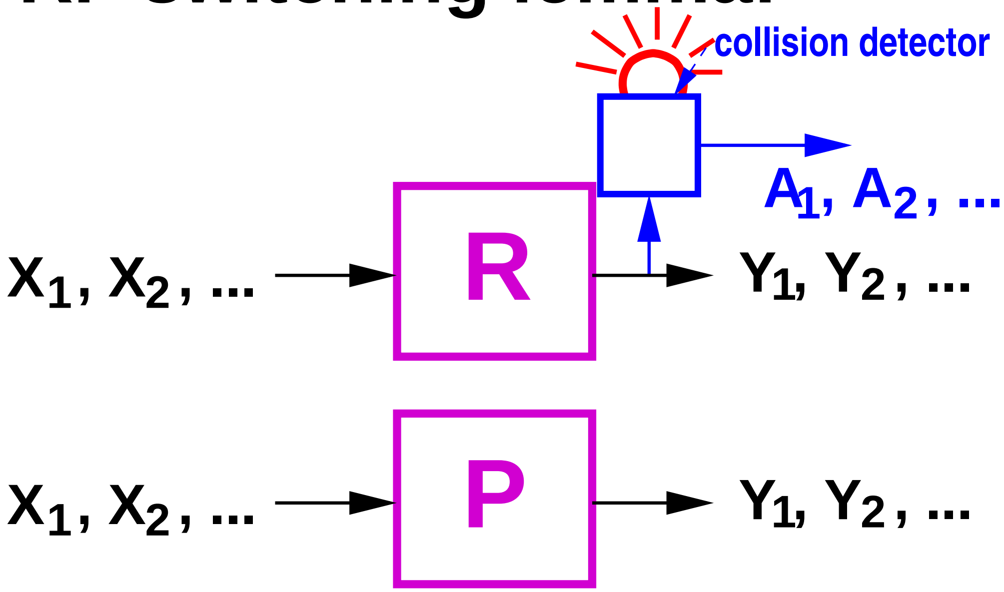


Characterized by: $\mathrm{p}^{\mathbf{S}}_{Y^i A_i | X^i}$ for $i = 1, 2, \ldots$

Conditional equivalence: $\mathbf{S}|\mathcal{A} \equiv \mathbf{T} \;:\Leftrightarrow\; \mathrm{p}^{\mathbf{S}}_{Y^i | X^i A_i} = \mathrm{p}^{\mathbf{T}}_{Y^i | X^i}$

Lemma [M02]: $\mathbf{S}|\mathcal{A} \equiv \mathbf{T} \;\Rightarrow\; \Delta(\mathbf{S}, \mathbf{T}) \leq$ optimal prob. of provoking the MBO non-adaptively in $\mathbf{S}$ (same $\#$ of queries).

PRP-PRF switching lemma:

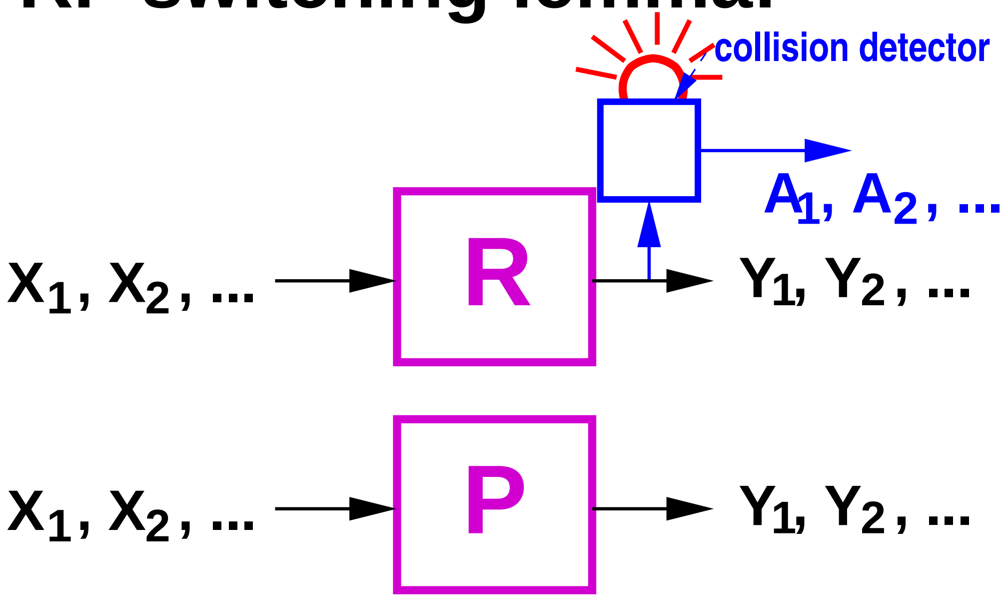


Characterized by: $\mathsf{p}^{\mathbf{S}}_{Y^i A_i | X^i}$ for $i = 1, 2, \ldots$

Conditional equivalence: $\mathbf{S}|\mathcal{A} \equiv \mathbf{T}$ $:\Leftrightarrow$ $\mathsf{p}^{\mathbf{S}}_{Y^i | X^i A_i} = \mathsf{p}^{\mathbf{T}}_{Y^i | X^i}$

Lemma [M02]: $\mathbf{S}|\mathcal{A} \equiv \mathbf{T} \Rightarrow \Delta(\mathbf{S}, \mathbf{T}) \leq$ optimal prob. of provoking the MBO non-adaptively in $\mathbf{S}$ (same # of queries).

PRP-PRF switching lemma:

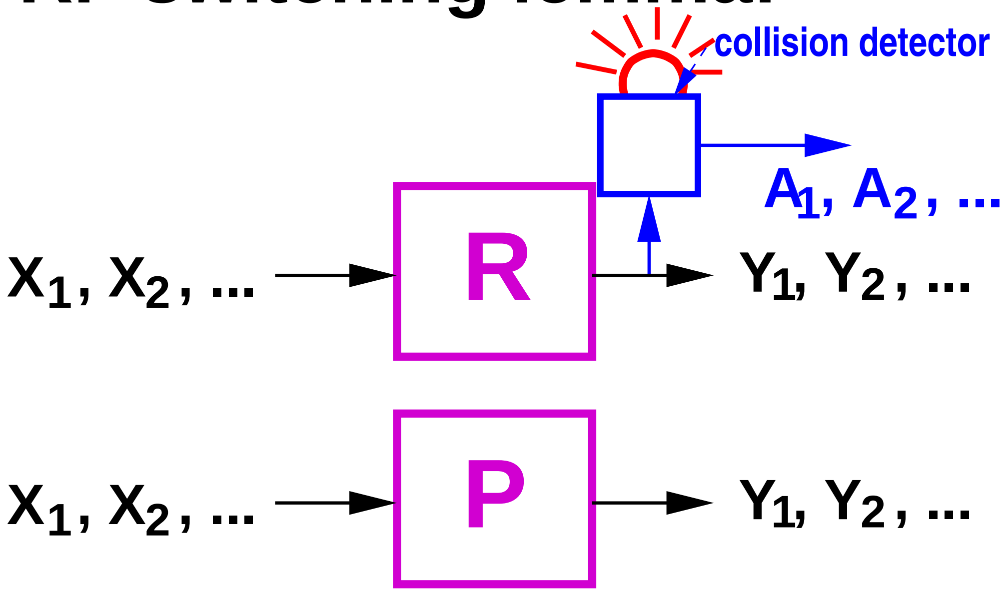


Characterized by: $\mathbf{R}|\mathcal{A} \equiv \mathbf{P} \;\Rightarrow\; \Delta_k(\mathbf{R}, \mathbf{P}) \leq \binom{k}{k} 2^{-n}$

Conditional equivalence: $\mathbf{S}|\mathcal{A} \equiv \mathbf{T} \;:\Leftrightarrow\; \mathrm{p}^{\mathbf{S}}_{Y^i|X^i A_i} = \mathrm{p}^{\mathbf{T}}_{Y^i|X^i}$

Lemma [M02]: $\mathbf{S}|\mathcal{A} \equiv \mathbf{T} \;\Rightarrow\; \Delta(\mathbf{S}, \mathbf{T}) \leq$ optimal prob. of provoking the MBO non-adaptively in $\mathbf{S}$ (same # of queries).

PRP-PRF switching lemma:



Characterized by:

$\mathbf{R}|\mathcal{A} \equiv \mathbf{P} \;\Rightarrow\; \Delta_k(\mathbf{R},\mathbf{P}) < \binom{k}{k}2^{-n}$

C... X^i

Le...

provoking the MBO non-adaptively in **S** (same # of queries).

Similarly simple proof of CBC-MAC security:

$$(\mathbf{CBCRF})|\mathcal{A} \equiv \mathbf{RO} \;\Rightarrow\; \Delta(\mathbf{CBCRF},\mathbf{RO}) \;\le\; \tfrac{1}{2}\ell^2 2^{-n}$$

Levels of abstraction in cryptography

#	possible name	concepts treated at this level
1.	Reductions	def. of (universal) composability
2.	Abstract resources	isomorphism
3.	Abstract systems	distinguisher, hybrid argument, secure reduction, compos. proof
4.	Discrete systems	games, equivalence, indistinguishability proofs
5.	System implem.	complexity, efficiency notion
6.	Physical models	timing, power, side-channels

Levels of abstraction in cryptography

#	possible name	concepts treated at this level
1.	Reductions	def. of (universal) composability
2.	Abstract resources	isomorphism
3.	Abstract systems	distinguisher, hybrid argument, secure reduction, compos. proof
4.	Discrete systems	games, equivalence, indistinguishability proofs
5.	System implem.	complexity, efficiency notion
6.	Physical models	timing, power, side-channels

Abstract Cryptography (with Renato Renner) [1-3]

Abstract Cryptography (with Renato Renner) [1-3]

Goals:

- capture the constructive security paradigm at high(est) abstraction level

Abstract Cryptography (with Renato Renner) [1-3]

Goals:

- capture the constructive security paradigm at high(est) abstraction level
- define strongest possible reduction between resources

Abstract Cryptography (with Renato Renner) [1-3]

Goals:

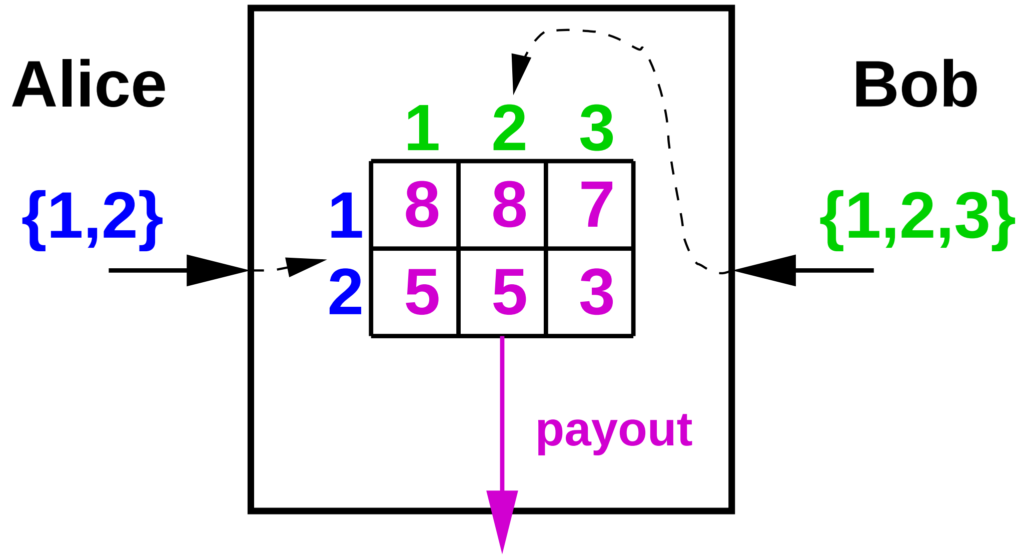
- capture the constructive security paradigm at high(est) abstraction level
- define strongest possible reduction between resources
- see other frameworks as special cases
  - universal composability (UC) by Canetti
  - reactive simulatability by Pfitzmann/Waidner/Backes
  - indifferentiability [MRH04]

Abstract Cryptography (with Renato Renner) [1-3]

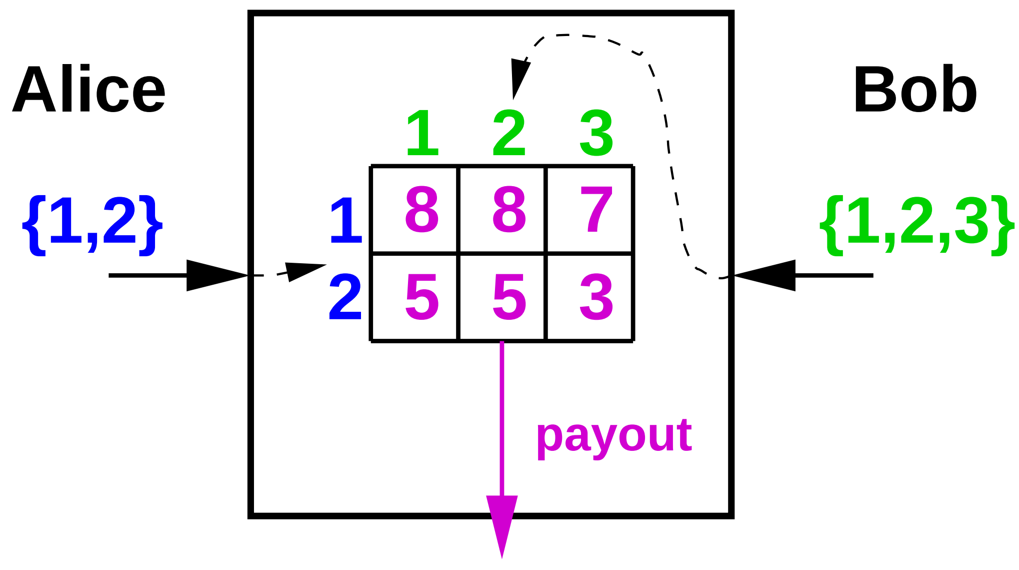
Goals:

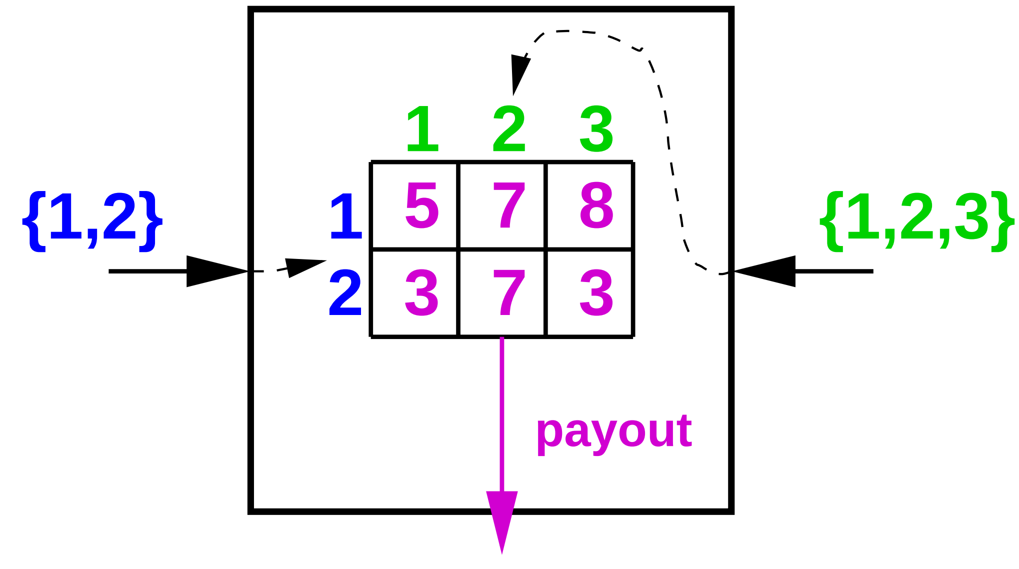
- capture the constructive security paradigm at high(est) abstraction level
- define strongest possible reduction between resources
- see other frameworks as special cases
  - universal composability (UC) by Canetti
  - reactive simulatability by Pfitzmann/Waidner/Backes
  - indifferentiability [MRH04]
- capture scenarios that could previously not be modeled.

Resources and isomorphisms

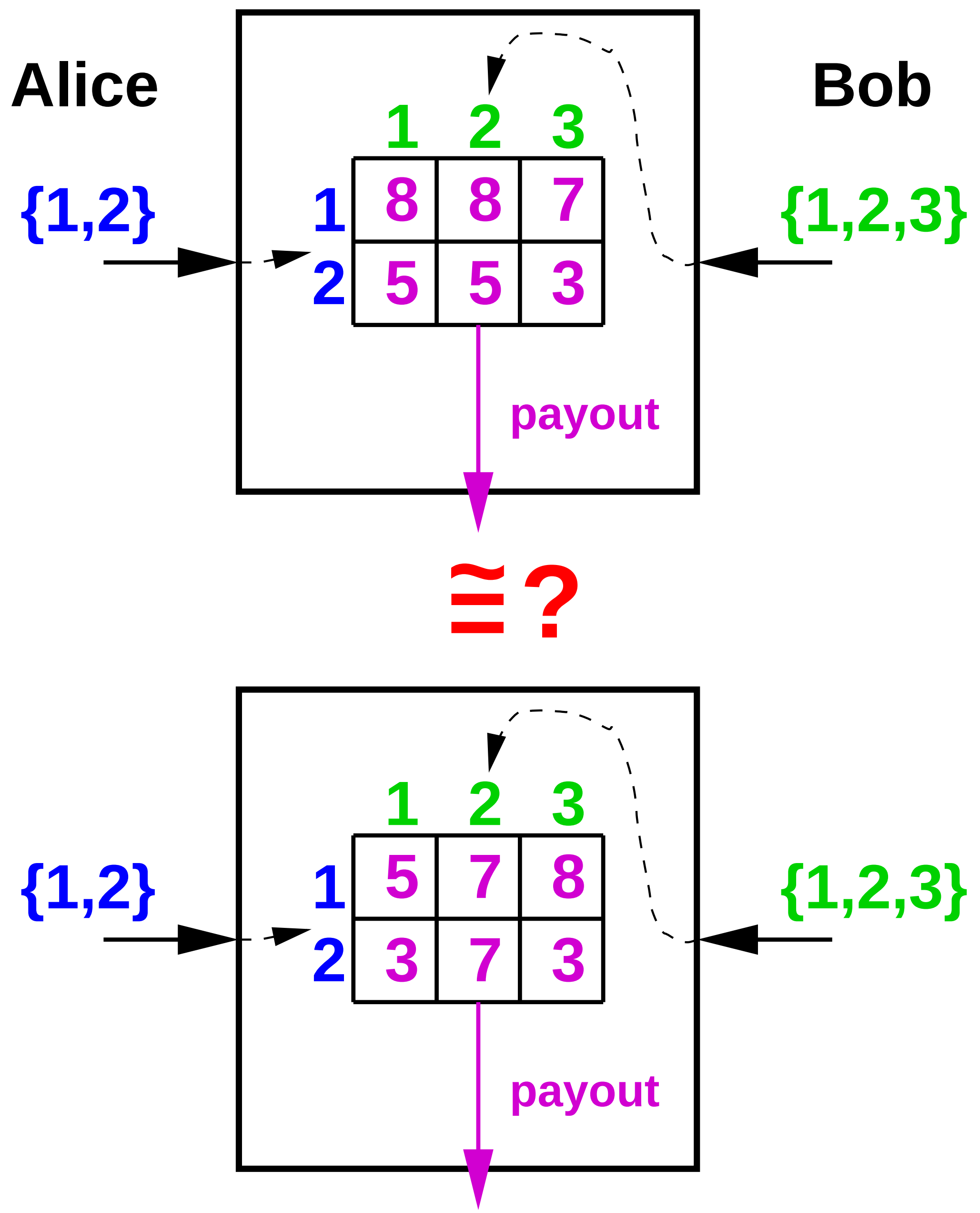


Resources and isomorphisms

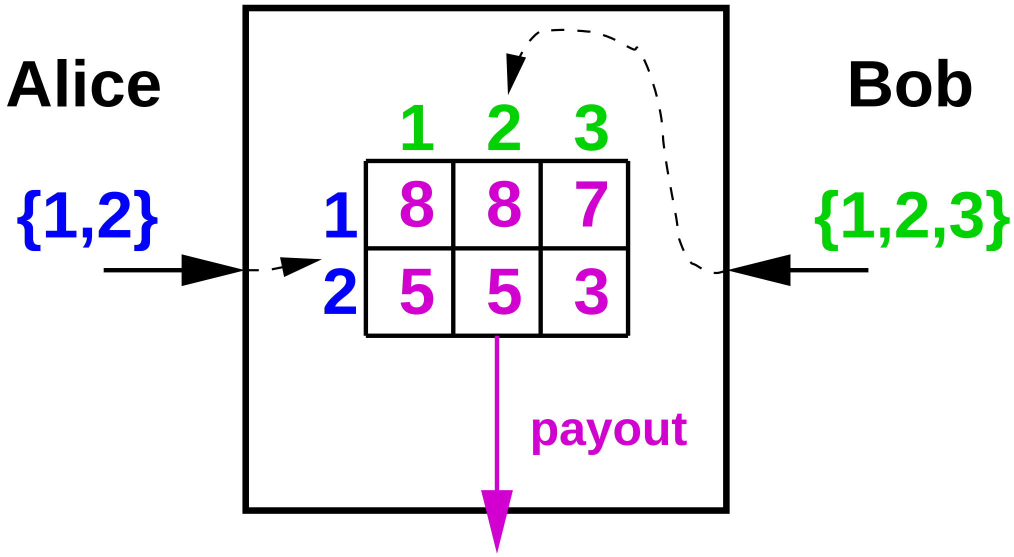




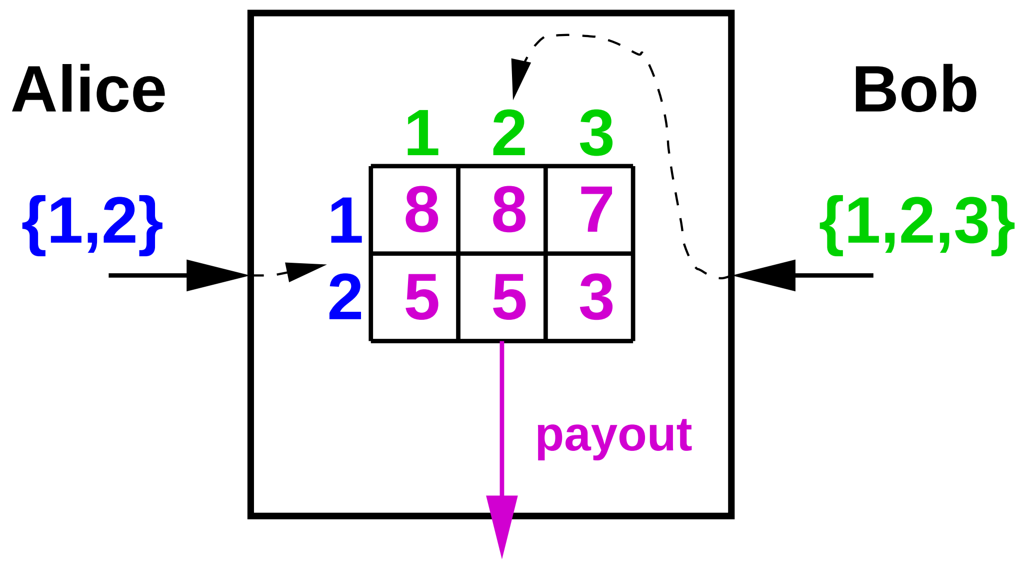
Resources and isomorphisms

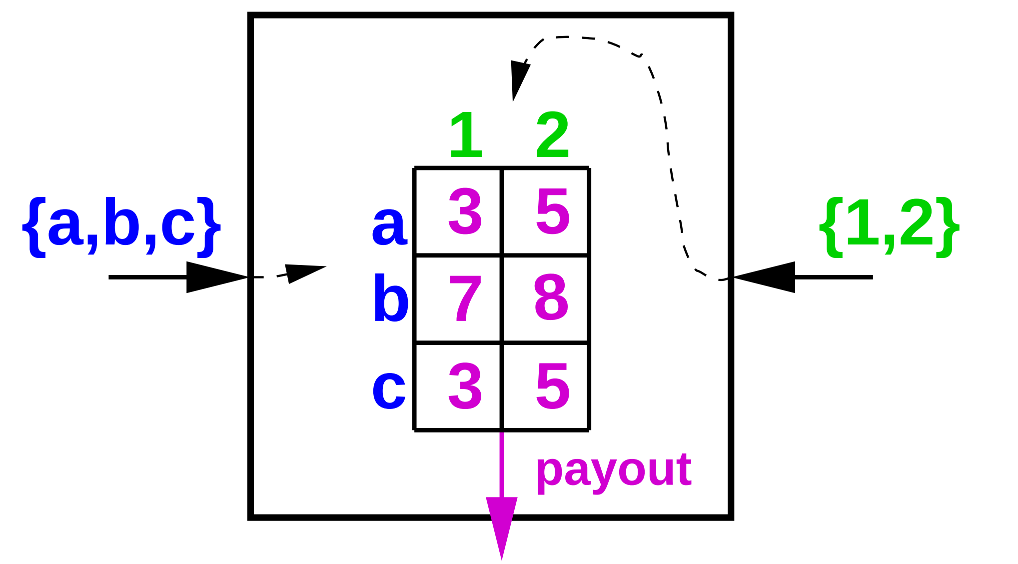


Resources and isomorphisms

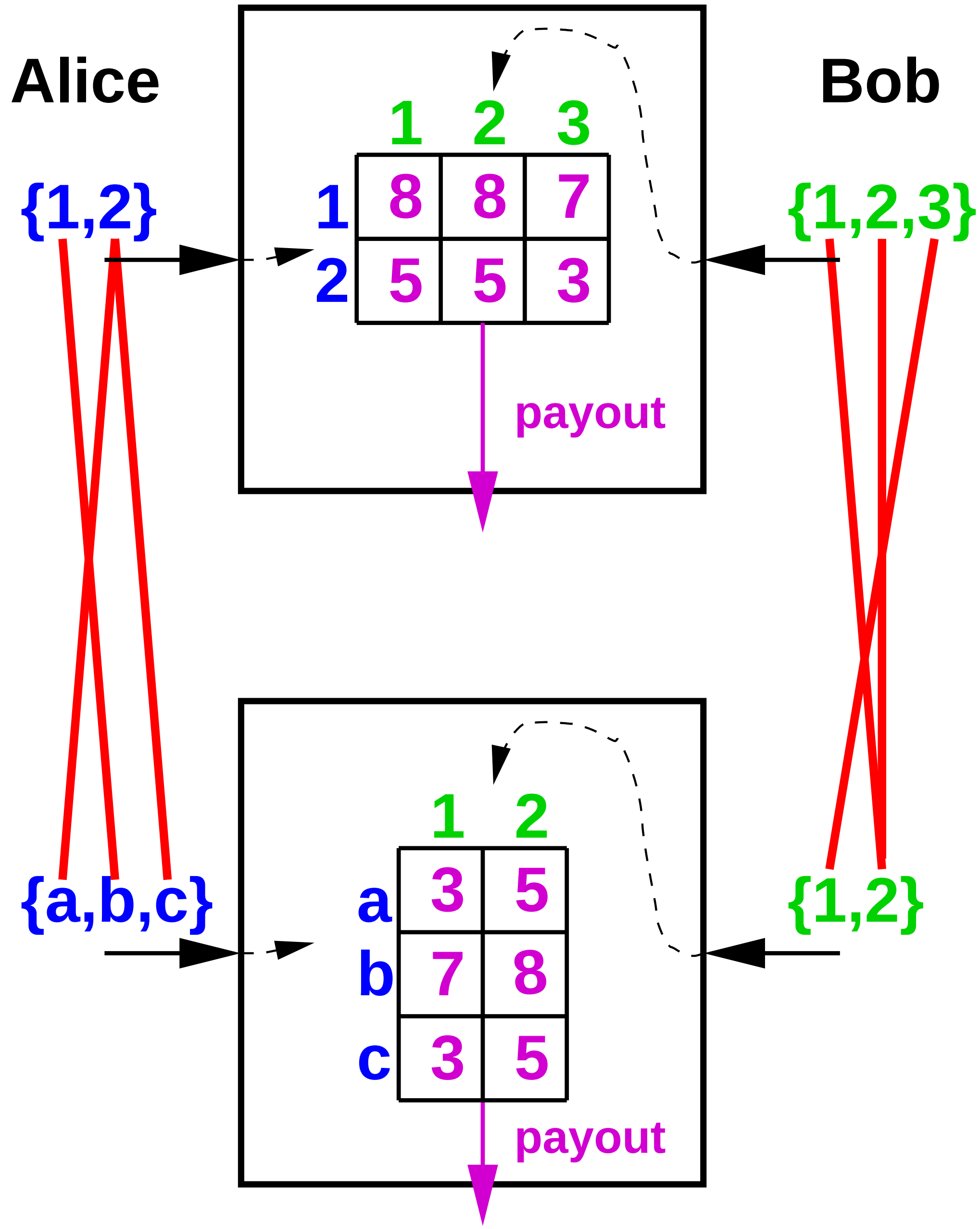


Resources and isomorphisms

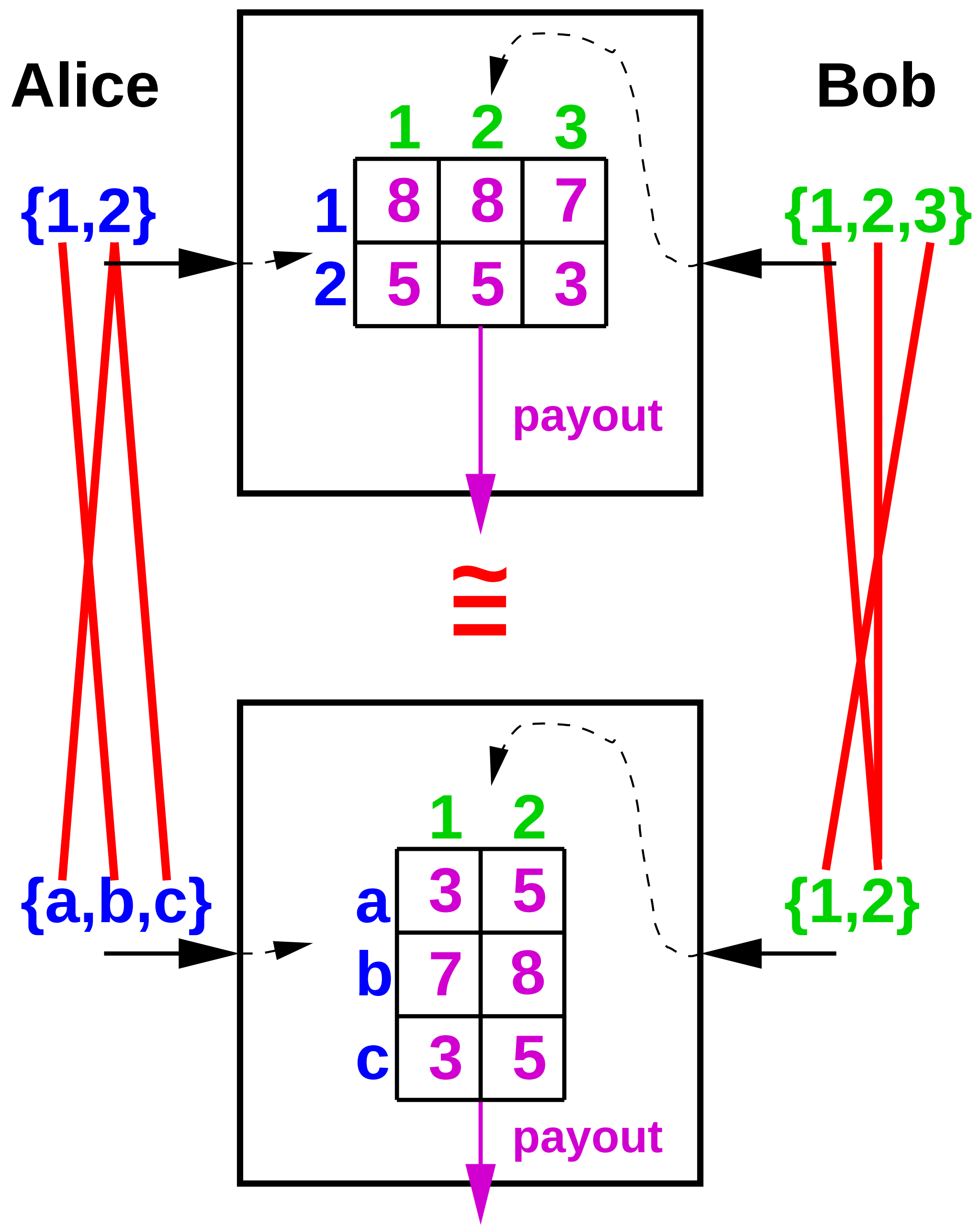




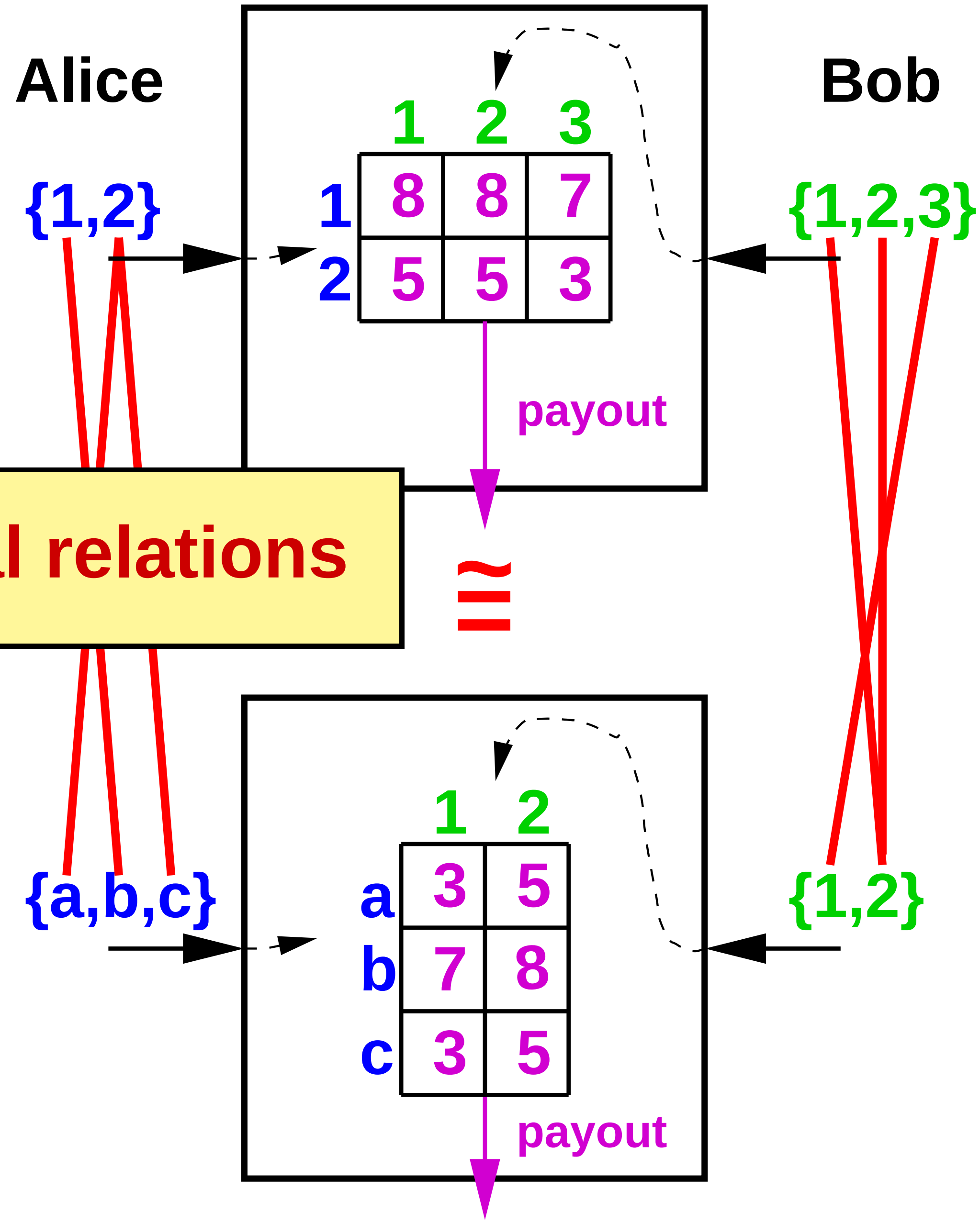
Resources and isomorphisms



Resources and isomorphisms

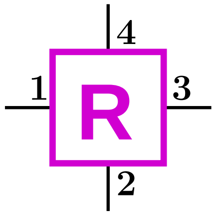


Resources and isomorphisms

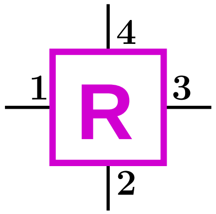


Complete local relations

Abstract multi-party setting [3]

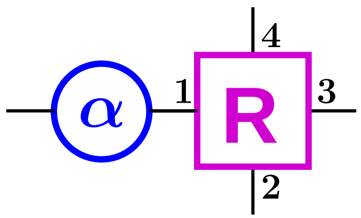


Abstract multi-party setting



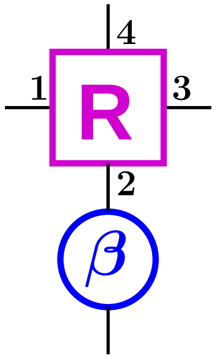
R

Abstract multi-party setting



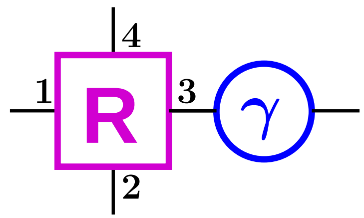
$$\alpha^1 \mathbf{R}$$

Abstract multi-party setting [3]



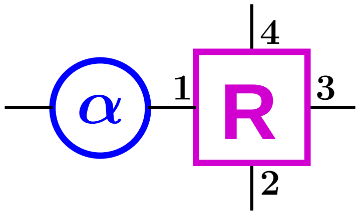
β^2R

Abstract multi-party setting [3]



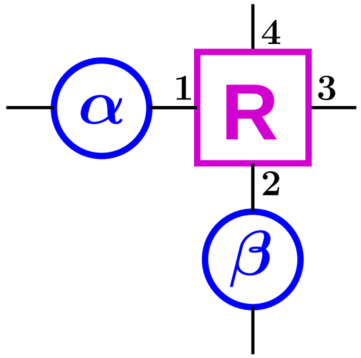
$$\gamma^{\mathbf{3}}\mathsf{R}$$

Abstract multi-party setting [3]



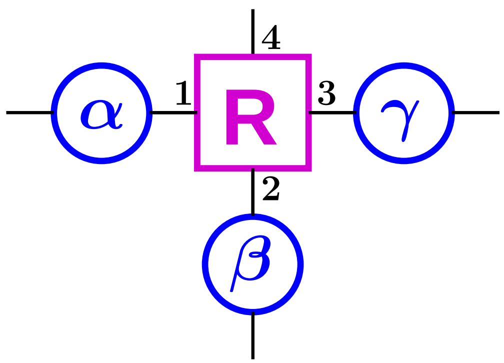
$$\alpha^1\mathbf{R}$$

Abstract multi-party setting [3]



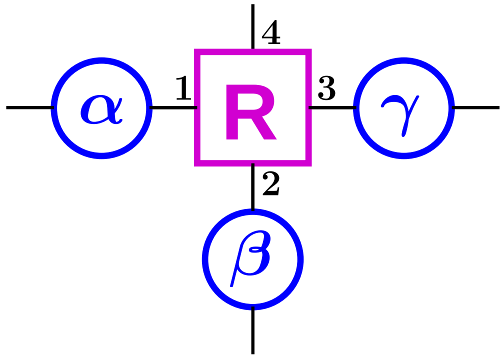
$$\beta^{\mathbf{2}}\alpha^{1}\mathbf{R}$$

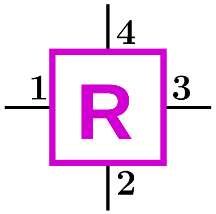
Abstract multi-party setting [3]



$$\gamma^{\mathbf{3}}\beta^{\mathbf{2}}\alpha^{1}\mathsf{R}$$

Abstract multi-party setting [3]

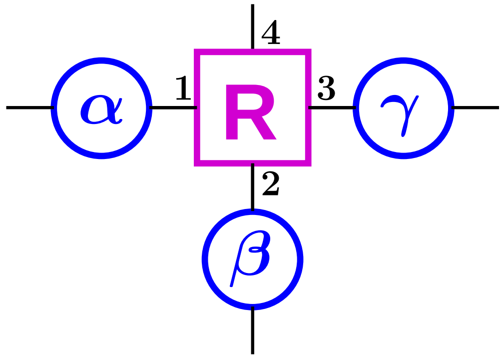




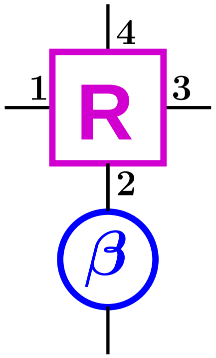
$\gamma^{3}\beta^{2}\alpha^{1}\mathsf{R}$

R

Abstract multi-party setting [3]

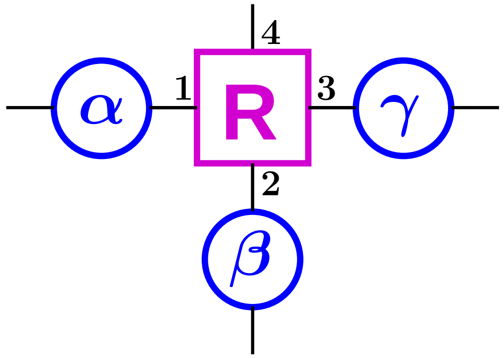


$$\gamma^{\mathbf{3}}\beta^{\mathbf{2}}\alpha^{\mathbf{1}}\mathbf{R}$$

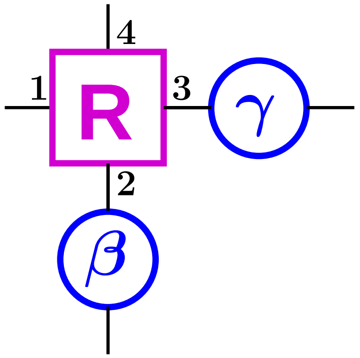


$$\beta^{\mathbf{2}}\mathbf{R}$$

Abstract multi-party setting [3]

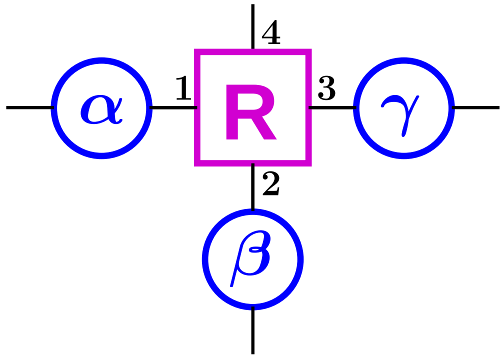


$$\gamma^{\mathbf{3}}\beta^{\mathbf{2}}\alpha^{\mathbf{1}}\mathbf{R}$$

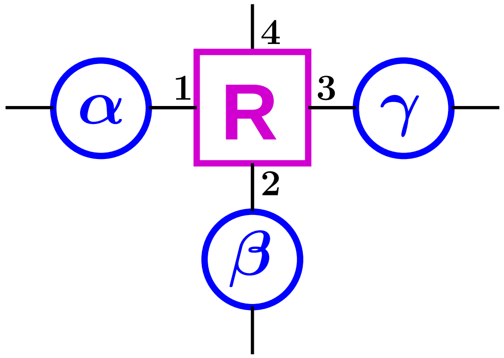


$$\gamma^{\mathbf{3}}\beta^{\mathbf{2}}\mathbf{R}$$

Abstract multi-party setting [3]

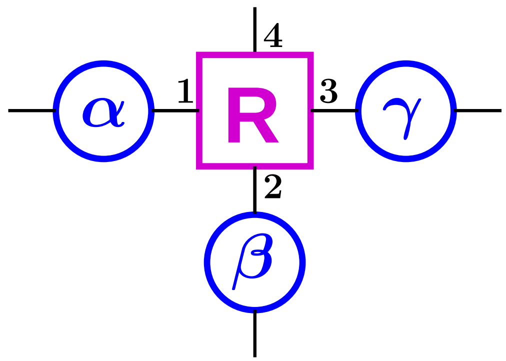


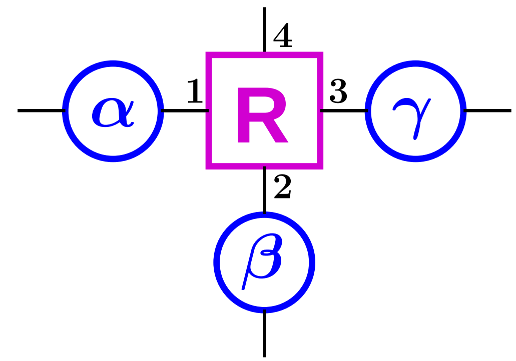
$$\gamma^3 \beta^2 \alpha^1 \mathbf{R}$$



$$\alpha^1 \gamma^3 \beta^2 \mathbf{R}$$

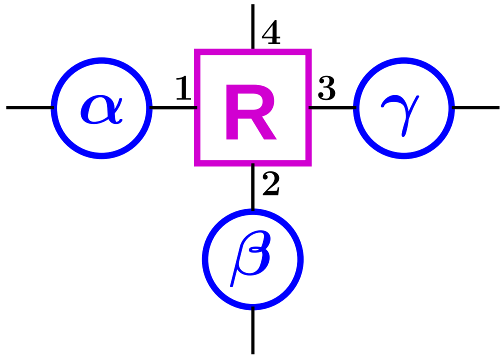
Abstract multi-party setting [3]

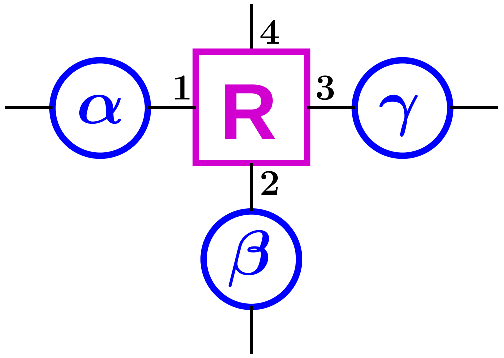




$$\gamma^{3}\beta^{2}\alpha^{1}\mathbf{R} \quad = \quad \alpha^{1}\gamma^{3}\beta^{2}\mathbf{R}$$

Abstract multi-party setting [3]

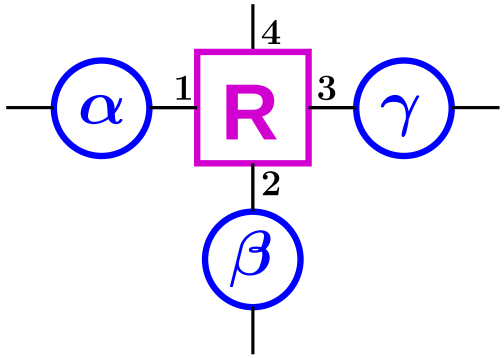


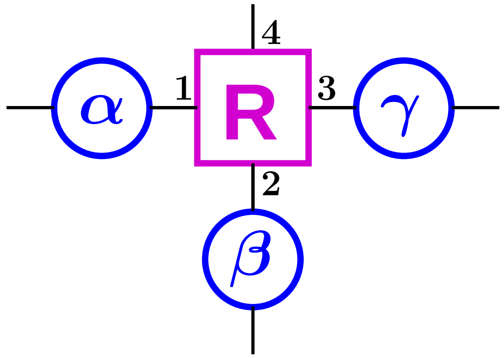


$$\boldsymbol{\gamma}^{\mathbf{3}}\boldsymbol{\beta}^{\mathbf{2}}\boldsymbol{\alpha}^{\mathbf{1}}\mathbf{R} \quad = \quad \boldsymbol{\alpha}^{\mathbf{1}}\boldsymbol{\gamma}^{\mathbf{3}}\boldsymbol{\beta}^{\mathbf{2}}\mathbf{R}$$

Resource set Φ for interface set $\mathcal{I} = \{1, 2, 3, 4\}$, oper. $||$

Abstract multi-party setting [3]



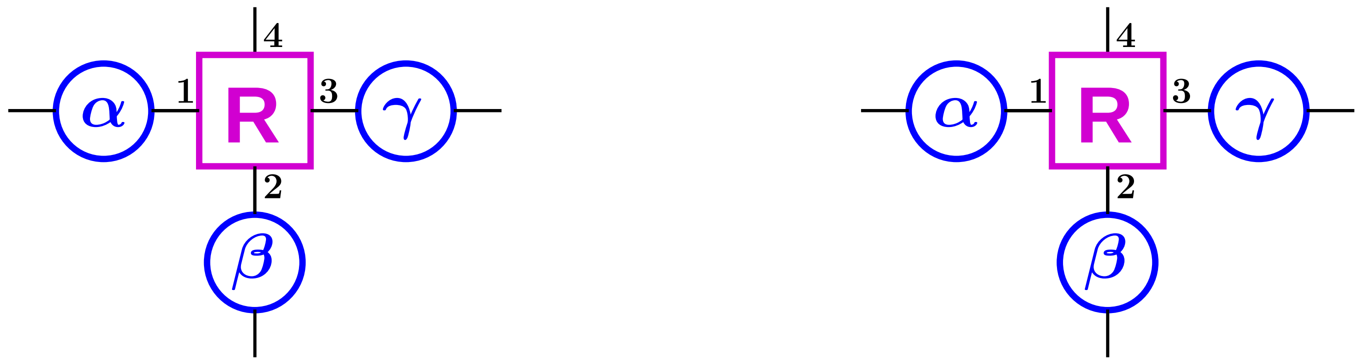


$$\gamma^{\mathbf{3}}\beta^{\mathbf{2}}\alpha^{\mathbf{1}}\mathbf{R} \quad = \quad \alpha^{\mathbf{1}}\gamma^{\mathbf{3}}\beta^{\mathbf{2}}\mathbf{R}$$

Resource set Φ for interface set $\mathcal{I} = \{1, 2, 3, 4\}$, oper. $||$

Converter set Σ, with operation $\circ$

Abstract multi-party setting [3]



$$\gamma^{\mathbf{3}}\beta^{\mathbf{2}}\alpha^{\mathbf{1}}\mathbf{R} \quad = \quad \alpha^{\mathbf{1}}\gamma^{\mathbf{3}}\beta^{\mathbf{2}}\mathbf{R}$$

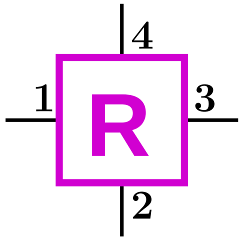
Resource set Φ for interface set $\mathcal{I} = \{1, 2, 3, 4\}$, oper. $||$

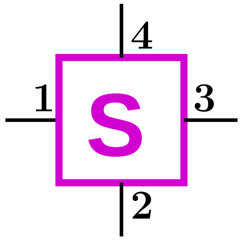
Converter set Σ, with operation $\circ$

Algebraic laws:

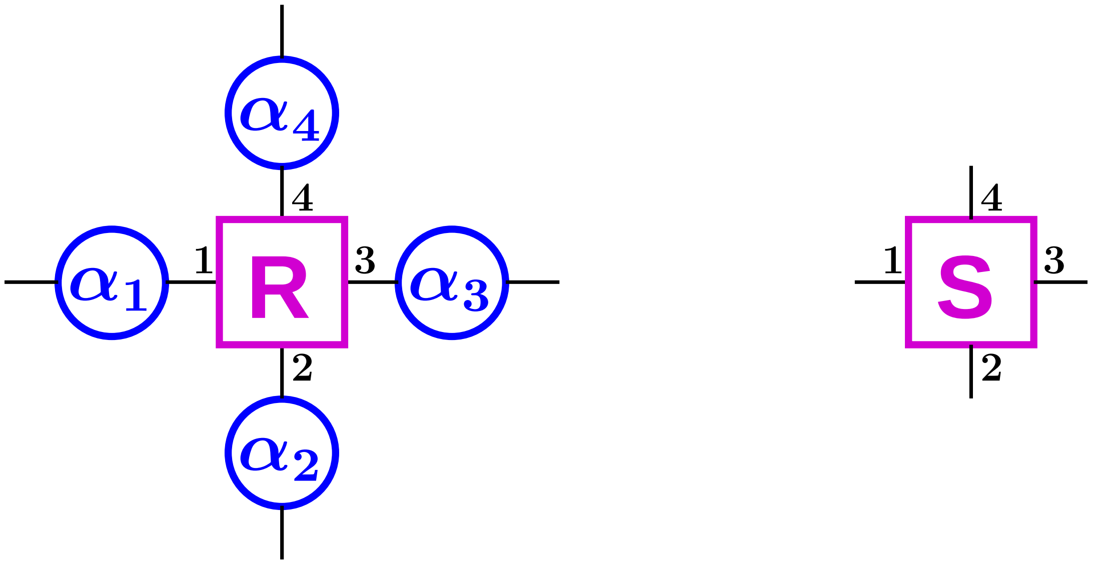
- $\alpha^i\mathbf{R} \in \Phi$ for all $\mathbf{R} \in \Phi$, $\alpha \in \Sigma$, $i \in \mathcal{I}$
- $\alpha^i\beta^j\mathbf{R} \equiv \beta^j\alpha^i\mathbf{R}$ for all $i \neq j$

Resource isomorphisms

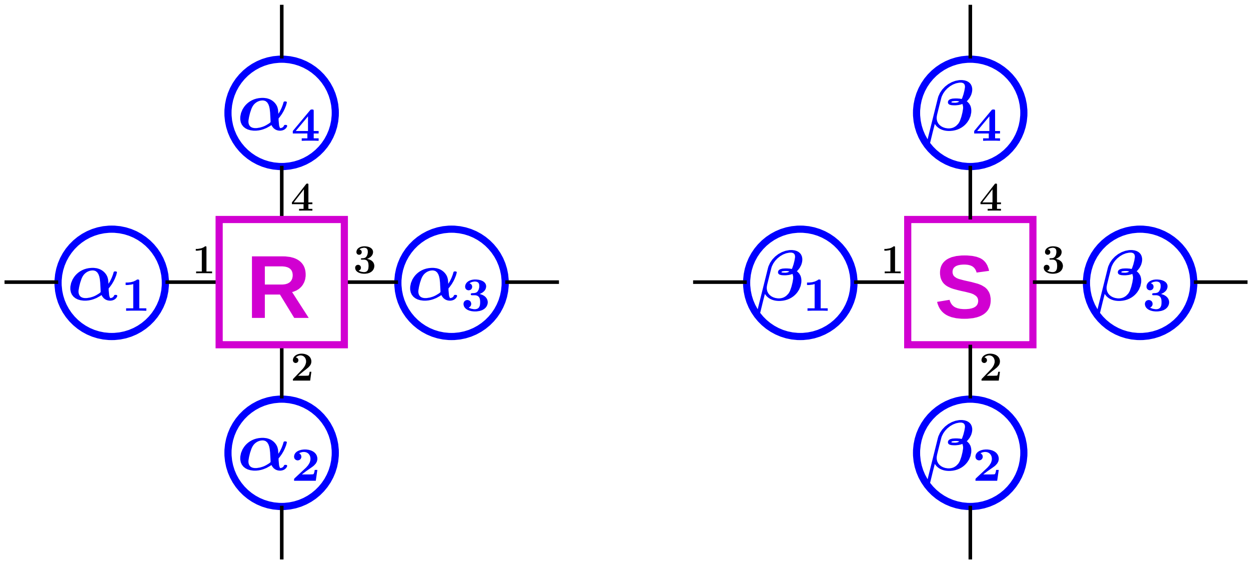




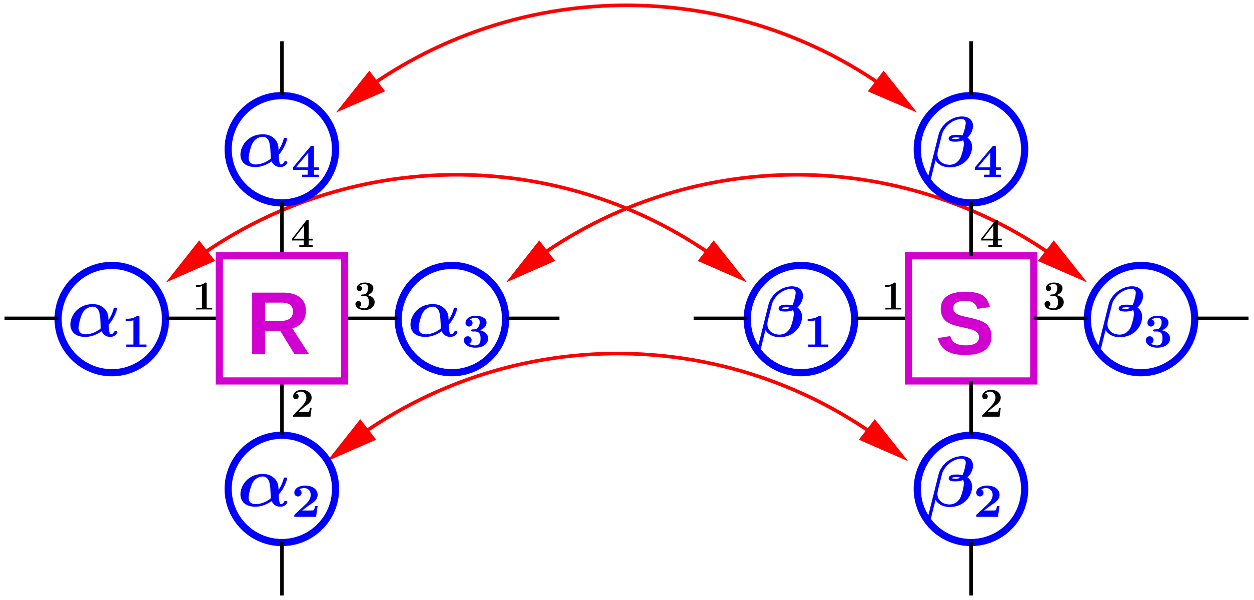
Resource isomorphisms



Resource isomorphisms



Resource isomorphisms

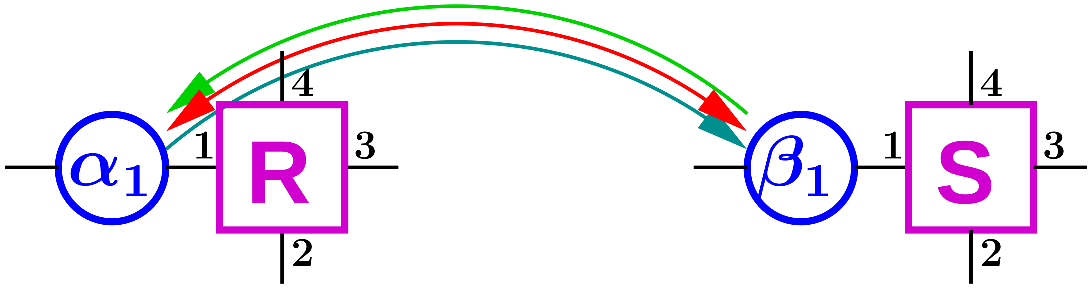


Resource isomorphisms

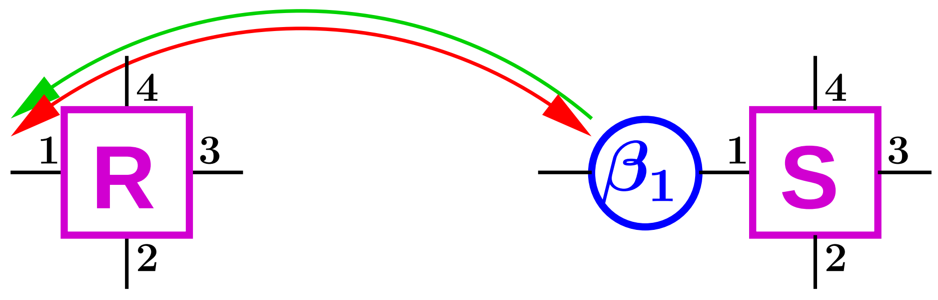
[3]

Resource isomorphisms

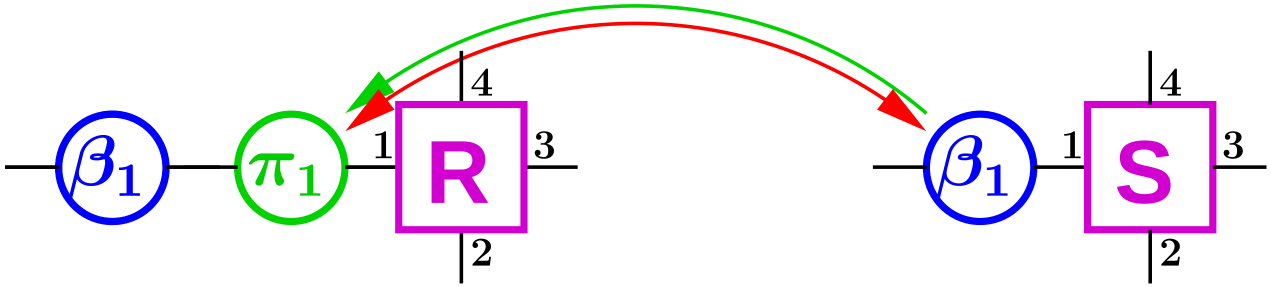
[3]



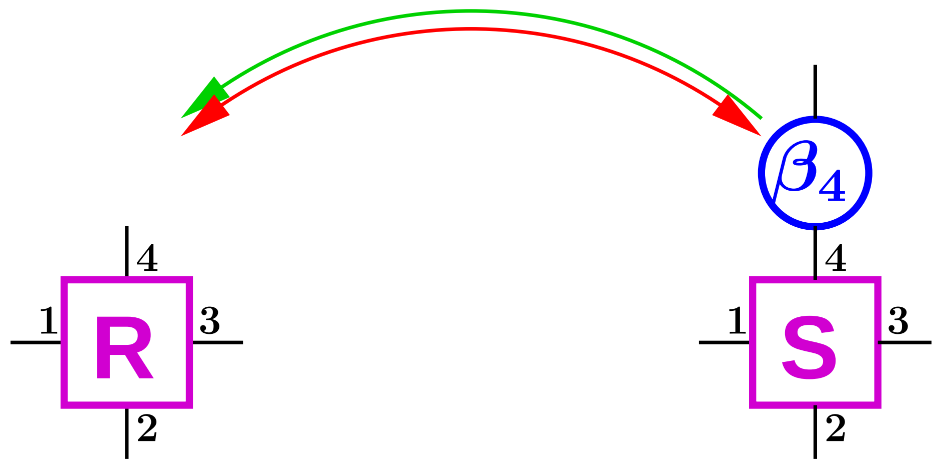
Resource isomorphisms



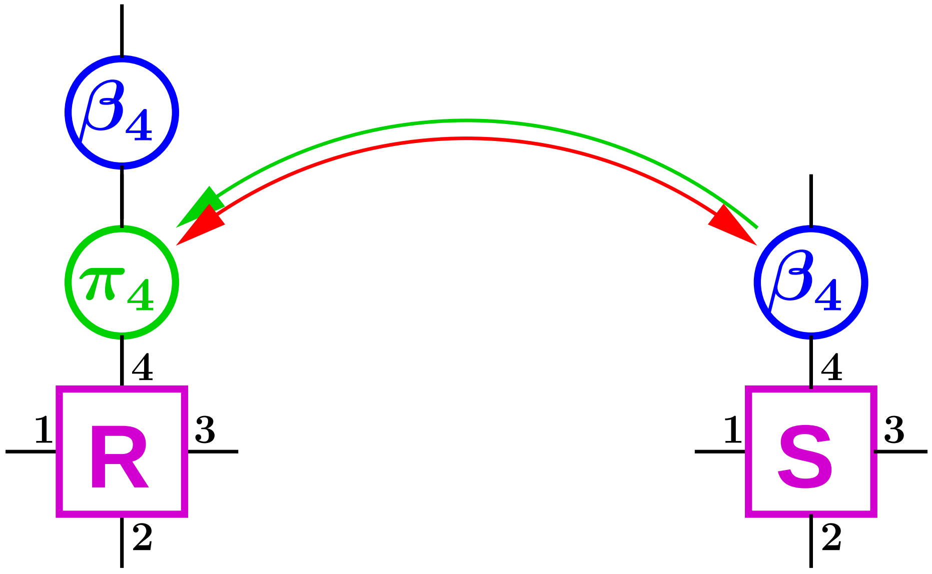
Resource isomorphisms



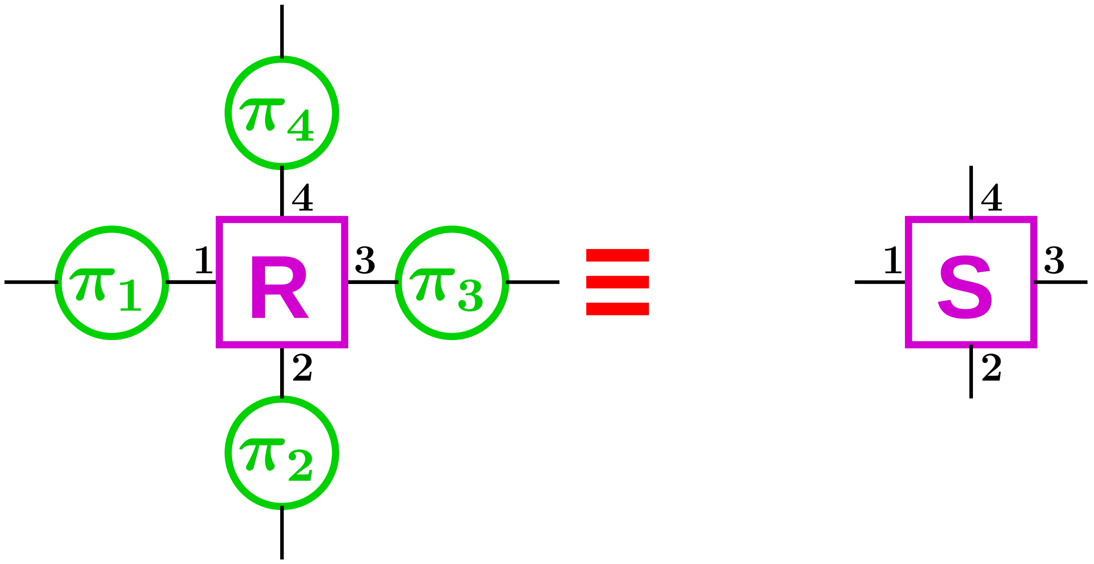
Resource isomorphisms



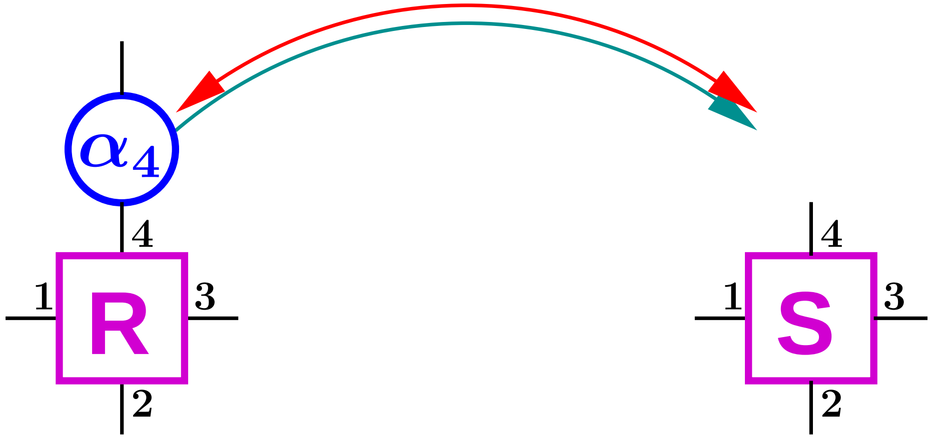
Resource isomorphisms



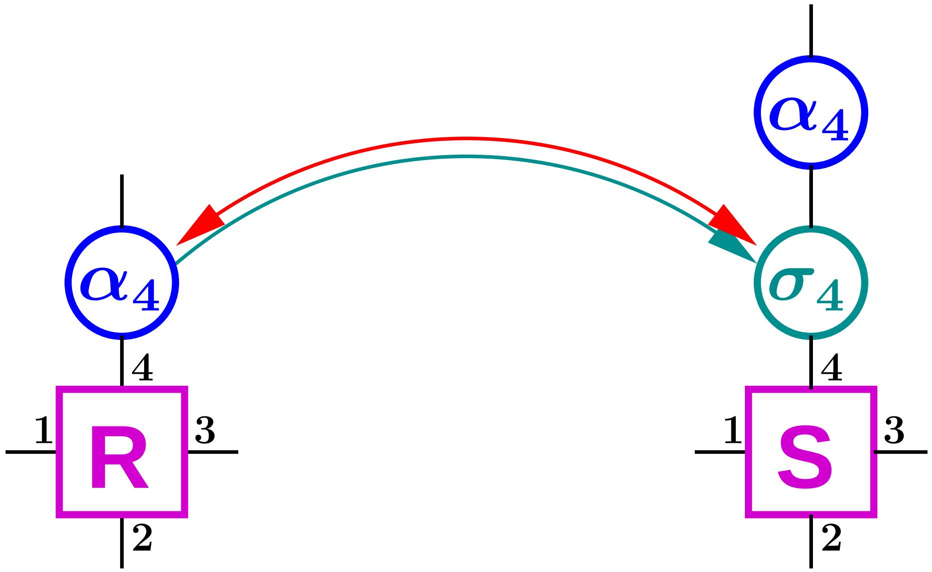
Resource isomorphisms



Resource isomorphisms

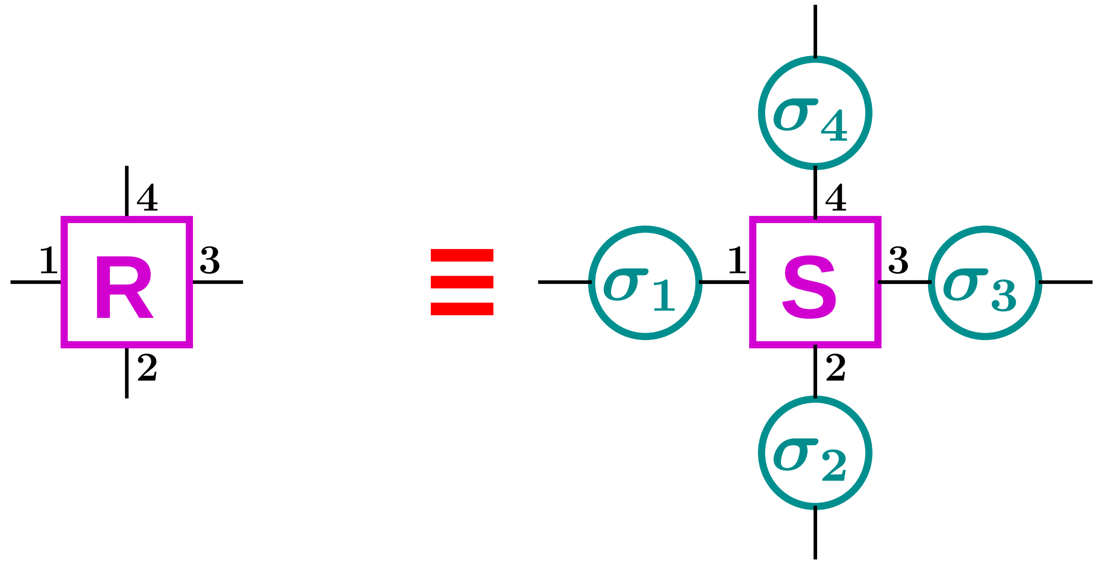


Resource isomorphisms

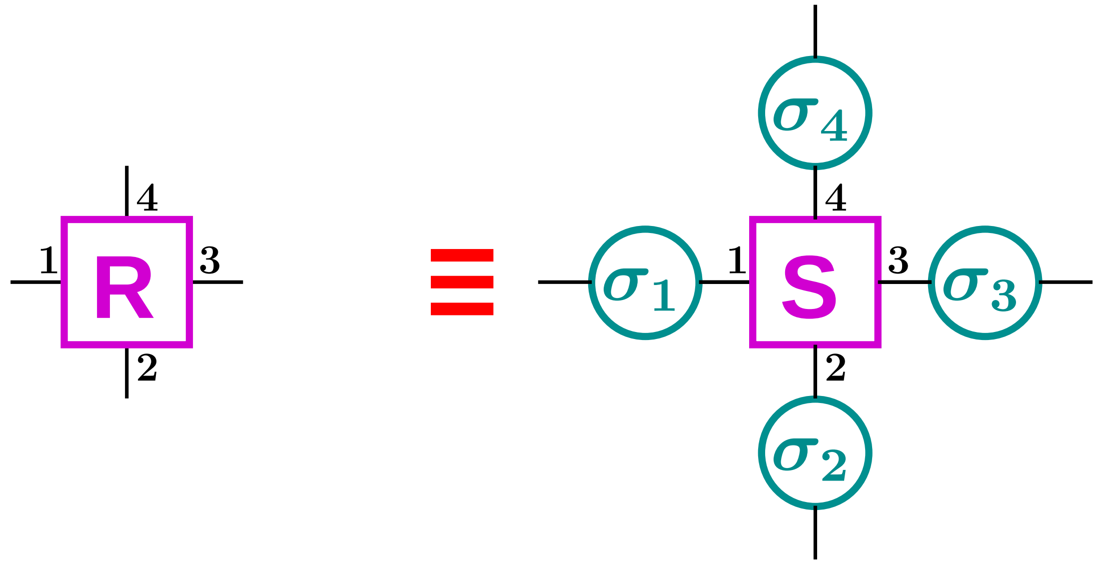


Resource isomorphisms

[3]

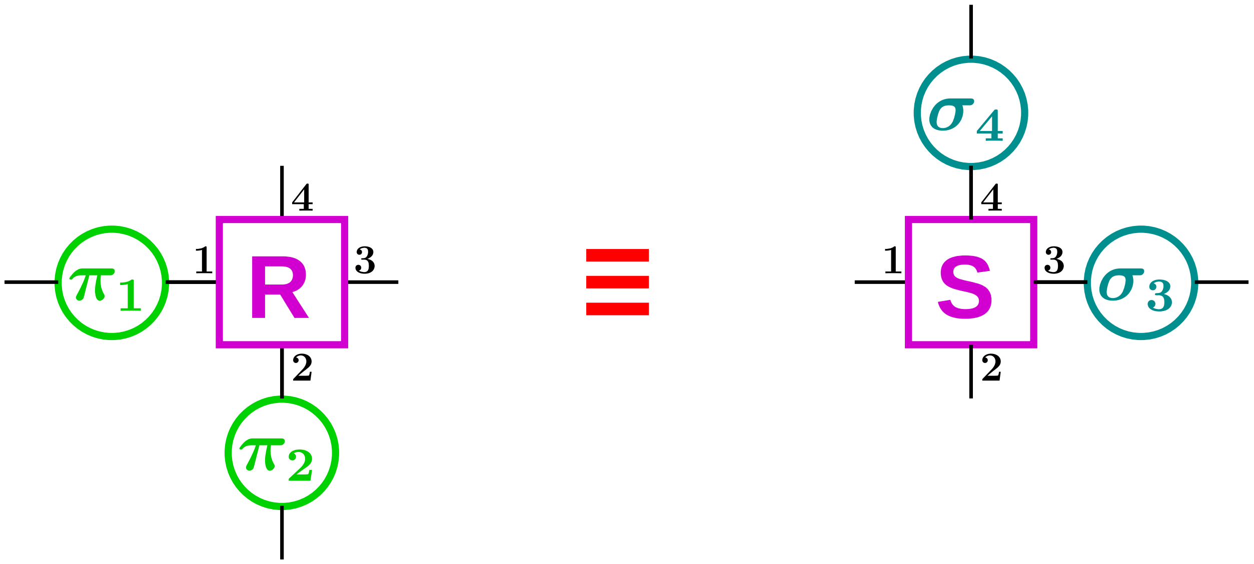


Resource isomorphisms [3]



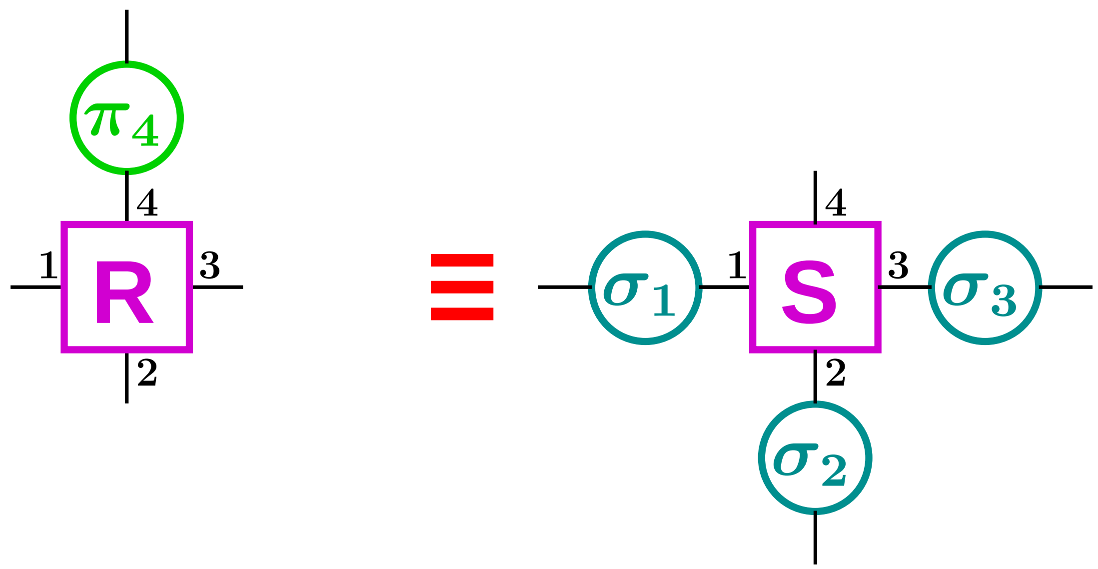
Definition: **R** *is isomorphic to* **S** via π, denoted **R** $\cong^{\pi}$ **S**, if

Resource isomorphisms



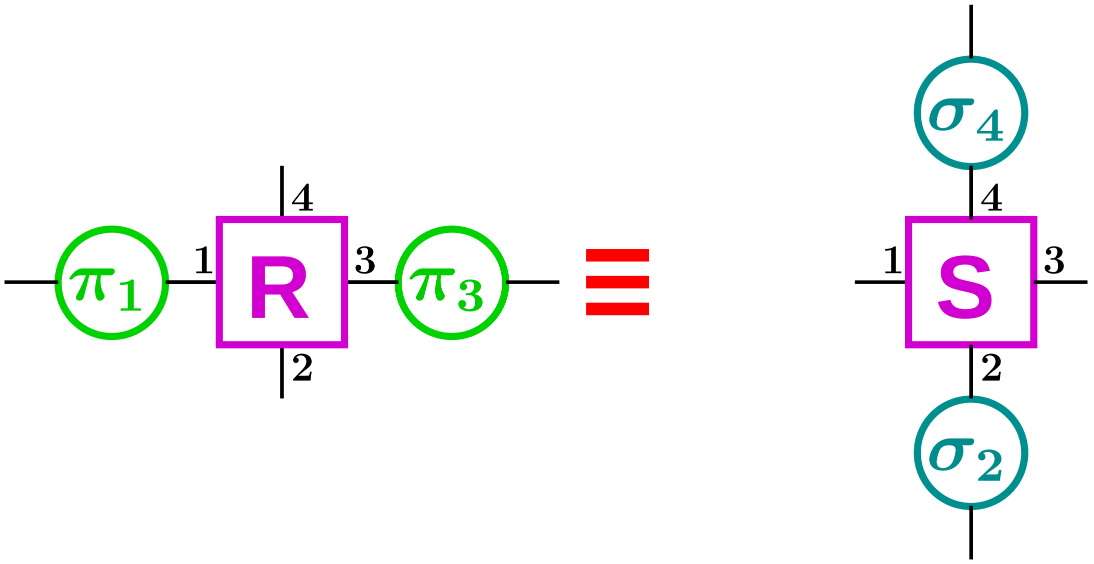
Definition: **R** *is isomorphic to* **S** via π, denoted **R** $\cong^{\pi}$ **S**, if

Resource isomorphisms [3]



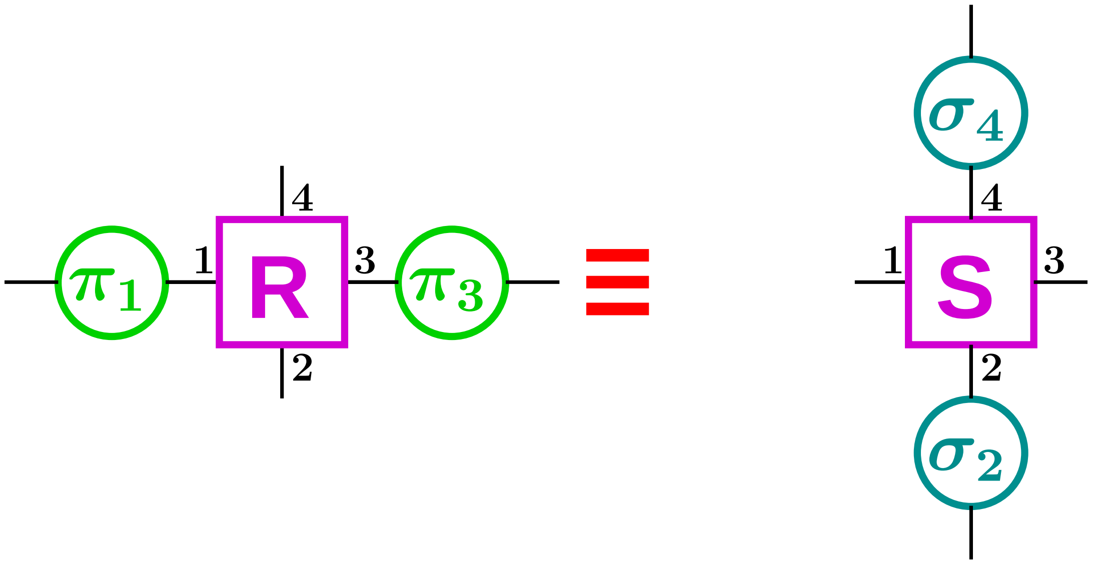
Definition: **R** *is isomorphic to* **S** via π, denoted **R** $\cong^{\pi}$ **S**, if

Resource isomorphisms [3]



Definition: **R** *is isomorphic to* **S** via π, denoted **R** $\cong^{\pi}$ **S**, if

Resource isomorphisms



Definition: R *is isomorphic to* S via π, denoted R $\cong^{\pi}$ S, if

$$\mathsf{R} \cong^{\pi} \mathsf{S} \quad :\Longleftrightarrow \quad \exists \sigma\ \forall \mathcal{P} \subseteq \mathcal{I} : \ \pi_{\mathcal{P}}\,\mathsf{R} \equiv \sigma_{\overline{\mathcal{P}}}\,\mathsf{S}$$

Example: 2-party resources

$$\mathbf{R} \cong^{\pi} \mathbf{S} :\Longleftrightarrow \begin{cases} \pi_1 \mathbf{R} \pi_2 \approx \mathbf{S} \\ \pi_1 \mathbf{R} \approx \mathbf{S} \sigma_2 \\ \mathbf{R} \pi_2 \approx \sigma_1 \mathbf{S} \\ \mathbf{R} \approx \sigma_1 \mathbf{S} \sigma_2 \end{cases}$$

Example: 2-party resources [2]

$$\mathbf{R} \cong^{\pi} \mathbf{S} :\Longleftrightarrow \left\{ \begin{array}{lcl} \pi_1 \mathbf{R} \pi_2 & \approx & \mathbf{S} \\ \pi_1 \mathbf{R} & \approx & \mathbf{S} \sigma_2 \\ \mathbf{R} \pi_2 & \approx & \sigma_1 \mathbf{S} \\ \mathbf{R} & \approx & \sigma_1 \mathbf{S} \sigma_2 \end{array} \right.$$

$$\boxed{\left.\begin{array}{l} \\ \\ \end{array}\right\} \Leftrightarrow \text{abstract UC}}$$

Example: 2-party resources [2]

$$\mathbf{R} \cong^{\pi} \mathbf{S} :\iff \begin{cases} \pi_1 \mathbf{R} \pi_2 \approx \mathbf{S} \\ \pi_1 \mathbf{R} \approx \mathbf{S} \sigma_2 \\ \mathbf{R} \pi_2 \approx \sigma_1 \mathbf{S} \\ \mathbf{R} \approx \sigma_1 \mathbf{S} \sigma_2 \end{cases}$$

Special case: $\mathbf{R}$ = channel (neutral element, e.g. $\pi_1 \mathbf{R} = \pi_1$)

Example: 2-party resources [2]

$$\mathbf{R} \cong^{\pi} \mathbf{S} :\Longleftrightarrow \begin{cases} \pi_1 \quad \pi_2 \approx \quad \mathbf{S} \\ \pi_1 \quad\quad\; \approx \quad \mathbf{S}\sigma_2 \\ \quad\;\; \pi_2 \approx \sigma_1\mathbf{S} \\ \quad\quad\quad\;\; \approx \sigma_1\mathbf{S}\sigma_2 \end{cases}$$

Special case: **R** = channel (neutral element, e.g. $\pi_1\mathbf{R} = \pi_1$)

Example: 2-party resources

$$\mathbf{R} \cong^{\pi} \mathbf{S} :\Longleftrightarrow \left\{ \begin{array}{llll} \pi_1 & \pi_2 \approx & & \mathbf{S} \\ \pi_1 & & \approx & \mathbf{S}\sigma_2 \\ & \pi_2 & \approx & \sigma_1 \mathbf{S} \\ & & \approx & \sigma_1 \mathbf{S} \sigma_2 \end{array} \right.$$

$$\boxed{\left.\right\} \Rightarrow \pi_1 \pi_2 \approx \mathbf{S}\sigma_2\sigma_1\mathbf{S} \approx \mathbf{S}}$$

Special case: **R** = channel (neutral element, e.g. $\pi_1 \mathbf{R} = \pi_1$)

Example: 2-party resources [2]

$$\mathbf{R} \cong^{\pi} \mathbf{S} :\Longleftrightarrow \left\{ \begin{array}{lllr} \pi_1 & \pi_2 & \approx & \mathbf{S} \\ \pi_1 & & \approx & \mathbf{S}\sigma_2 \\ & \pi_2 & \approx & \sigma_1\mathbf{S} \\ & & \approx & \sigma_1\mathbf{S}\sigma_2 \end{array} \right.$$

$$\boxed{\Bigg\} \Rightarrow \pi_1\pi_2 \approx \mathbf{S}\sigma_2\sigma_1\mathbf{S} \approx \mathbf{S}}$$

Special case: **R** = channel (neutral element, e.g. $\pi_1\mathbf{R} = \pi_1$)

Theorem: A resource **S** such that $\mathbf{S}\alpha\mathbf{S} \not\approx \mathbf{S}$ for all α cannot be realized from a communication channel.

Example: 2-party resources [2]

$$\mathbf{R} \cong^{\pi} \mathbf{S} :\Longleftrightarrow \left\{ \begin{array}{rrcr} \pi_1 & \pi_2 & \approx & \mathbf{S} \\ \pi_1 & & \approx & \mathbf{S}\sigma_2 \\ & \pi_2 & \approx & \sigma_1\mathbf{S} \\ & & \approx & \sigma_1\mathbf{S}\sigma_2 \end{array} \right. \left. \vphantom{\begin{array}{c} a \\ b \end{array}} \right\} \Rightarrow \pi_1\pi_2 \approx \mathbf{S}\sigma_2\sigma_1\mathbf{S} \approx \mathbf{S}$$

Special case: **R** = channel (neutral element, e.g. $\pi_1\mathbf{R} = \pi_1$)

Theorem: A resource **S** such that $\mathbf{S}\alpha\mathbf{S} \not\approx \mathbf{S}$ for all α cannot be realized from a communication channel.

Corollary [CF01]: Commitment cannot be realized (from a communication channel).

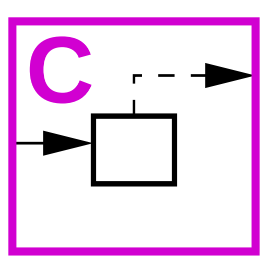
Example: 2-party resources [2]

$$\mathbf{R} \cong^{\pi} \mathbf{S} :\Longleftrightarrow \left\{ \begin{array}{llcl} \pi_1 & \pi_2 & \approx & \mathbf{S} \\ \pi_1 & & \approx & \mathbf{S}\sigma_2 \\ & \pi_2 & \approx & \sigma_1\mathbf{S} \\ & & \approx & \sigma_1\mathbf{S}\sigma_2 \end{array} \right. \quad \boxed{\Big\} \Rightarrow \pi_1\pi_2 \approx \mathbf{S}\sigma_2\sigma_1\mathbf{S} \approx \mathbf{S}}$$

Special case: **R** = channel (neutral element, e.g. $\pi_1\mathbf{R} = \pi_1$)

Theorem: A resource **S** such that $\mathbf{S}\alpha\mathbf{S} \not\approx \mathbf{S}$ for all α cannot be realized from a communication channel.

Corollary [CF01]: Commitment cannot be realized (from a communication channel).



Example: 2-party resources

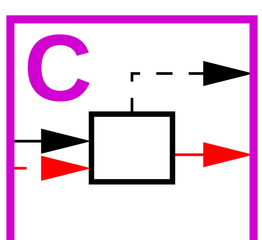
$$\mathbf{R} \cong^{\pi} \mathbf{S} :\Longleftrightarrow \left\{ \begin{array}{lll} \pi_1 & \pi_2 \approx & \mathbf{S} \\ \pi_1 & \approx & \mathbf{S}\sigma_2 \\ & \pi_2 \approx & \sigma_1\mathbf{S} \\ & \approx & \sigma_1\mathbf{S}\sigma_2 \end{array} \right.$$

$$\boxed{\left.\vphantom{\begin{array}{l}a\\b\end{array}}\right\} \Rightarrow \pi_1\pi_2 \approx \mathbf{S}\sigma_2\sigma_1\mathbf{S} \approx \mathbf{S}}$$

Special case: **R** = channel (neutral element, e.g. $\pi_1\mathbf{R} = \pi_1$)

Theorem: A resource **S** such that $\mathbf{S}\alpha\mathbf{S} \not\approx \mathbf{S}$ for all α cannot be realized from a communication channel.

Corollary [CF01]: Commitment cannot be realized (from a communication channel).



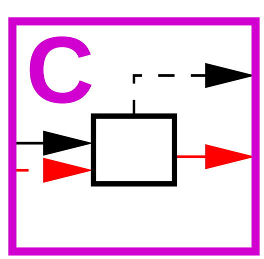
Example: 2-party resources [2]

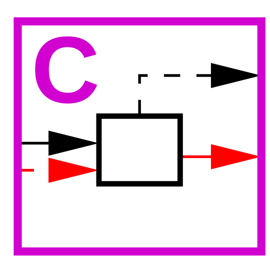
$$\mathbf{R} \cong^{\pi} \mathbf{S} :\Longleftrightarrow \left\{ \begin{array}{llll} \pi_1 & \pi_2 & \approx & \mathbf{S} \\ \pi_1 & & \approx & \mathbf{S}\sigma_2 \\ & \pi_2 & \approx & \sigma_1\mathbf{S} \\ & & \approx & \sigma_1\mathbf{S}\sigma_2 \end{array} \right. \boxed{\left. \vphantom{\begin{array}{l} a \\ b \end{array}} \right\} \Rightarrow \pi_1\pi_2 \approx \mathbf{S}\sigma_2\sigma_1\mathbf{S} \approx \mathbf{S}}$$

Special case: **R** = channel (neutral element, e.g. $\pi_1\mathbf{R} = \pi_1$)

Theorem: A resource **S** such that $\mathbf{S}\alpha\mathbf{S} \not\approx \mathbf{S}$ for all α cannot be realized from a communication channel.

Corollary [CF01]: Commitment cannot be realized (from a communication channel).





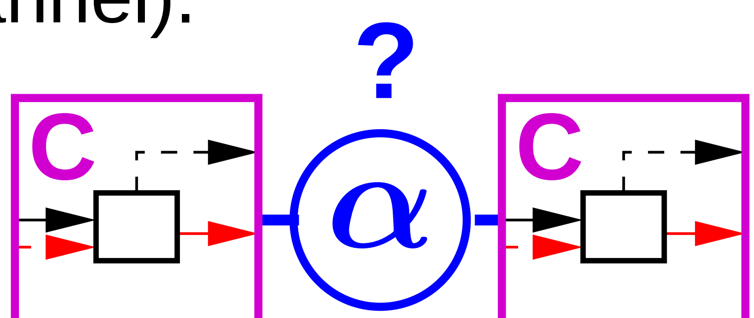
Example: 2-party resources [2]

$$\mathbf{R} \cong^{\pi} \mathbf{S} :\Longleftrightarrow \left\{ \begin{array}{llll} \pi_1 & \pi_2 & \approx & \mathbf{S} \\ \pi_1 & & \approx & \mathbf{S}\sigma_2 \\ & \pi_2 & \approx & \sigma_1\mathbf{S} \\ & & \approx & \sigma_1\mathbf{S}\sigma_2 \end{array} \right. \boxed{\Big\} \Rightarrow \pi_1\pi_2 \approx \mathbf{S}\sigma_2\sigma_1\mathbf{S} \approx \mathbf{S}}$$

Special case: **R** = channel (neutral element, e.g. $\pi_1\mathbf{R} = \pi_1$)

Theorem: A resource **S** such that $\mathbf{S}\alpha\mathbf{S} \not\approx \mathbf{S}$ for all α cannot be realized from a communication channel.

Corollary [CF01]: Commitment cannot be realized (from a communication channel).



Example: 2-party resources [2]

$$\mathbf{R} \cong^{\pi} \mathbf{S} :\Longleftrightarrow \left\{\begin{array}{llll} \pi_1 & \pi_2 & \approx & \mathbf{S} \\ \pi_1 & & \approx & \mathbf{S}\sigma_2 \\ & \pi_2 & \approx & \sigma_1\mathbf{S} \\ & & \approx & \sigma_1\mathbf{S}\sigma_2 \end{array}\right.$$

$$\boxed{\left.\begin{array}{l} \\ \\ \end{array}\right\} \Rightarrow \pi_1\pi_2 \approx \mathbf{S}\sigma_2\sigma_1\mathbf{S} \approx \mathbf{S}}$$

Special case: **R** = channel (neutral element, e.g. $\pi_1\mathbf{R} = \pi_1$)

Theorem: A resource **S** such that $\mathbf{S}\alpha\mathbf{S} \not\approx \mathbf{S}$ for all α cannot be realized from a communication channel.

Corollary [CF01]: Commitment cannot be realized (from a communication channel).

Corollary: A delayed communication channel cannot be realized (from a communication channel).

Example: 2-party resources

$$\mathbf{R} \cong^{\pi} \mathbf{S} :\Longleftrightarrow \left\{ \begin{array}{llcl} \pi_1 & \pi_2 & \approx & \mathbf{S} \\ \pi_1 & & \approx & \mathbf{S}\sigma_2 \\ & \pi_2 & \approx & \sigma_1\mathbf{S} \\ & & \approx & \sigma_1\mathbf{S}\sigma_2 \end{array} \right.$$

$$\left.\right\} \Rightarrow \pi_1\pi_2 \approx \mathbf{S}\sigma_2\sigma_1\mathbf{S} \approx \mathbf{S}$$

Special case: **R** = channel (neutral element, e.g. $\pi_1\mathbf{R} = \pi_1$)

Th ... t

be

Note: Isomorphism is the precisest possible relation between resources, but as such is completely rigid.

Corollary [CF01]: Commitment cannot be realized (from a communication channel).

Corollary: A delayed communication channel cannot be realized (from a communication channel).

Abstraction by Sets of Resources

Abstraction of a concept corresponds to a set!

Abstraction by Sets of Resources

Abstraction of a concept corresponds to a set!

Consider sets $\mathcal{R}$ and $\mathcal{S}$ of resources.

Abstraction by Sets of Resources

Abstraction of a concept corresponds to a set!

Consider sets $\mathcal{R}$ and $\mathcal{S}$ of resources.

Of special interest: Resources specified by (for each party)

- a guaranteed action space
- a possible action space

Abstraction by Sets of Resources

Abstraction of a concept corresponds to a set!

Consider sets $\mathcal{R}$ and $\mathcal{S}$ of resources.

Of special interest: Resources specified by (for each party)

- a guaranteed action space
- a possible action space

Definition: $\mathcal{S}$ *is an abstraction of* $\mathcal{R}$ via π:

$$\mathcal{R} \sqsubseteq^{\pi} \mathcal{S} \quad :\Longleftrightarrow \quad \forall \mathbf{R} \in \mathcal{R} \ \exists \mathbf{S} \in \mathcal{S} : \ \mathbf{R} \cong^{\pi} \mathbf{S}$$

Abstraction by Sets of Resources

Abstraction of a concept corresponds to a set!

Consider sets $\mathcal{R}$ and $\mathcal{S}$ of resources.

Of special interest: Resources specified by (for each party)

- a guaranteed action space
- a possible action space

Definition: $\mathcal{S}$ *is an abstraction of* $\mathcal{R}$ via π:

$$\mathcal{R} \sqsubseteq^{\pi} \mathcal{S} \quad :\Longleftrightarrow \quad \forall \mathbf{R} \in \mathcal{R} \;\; \exists \mathbf{S} \in \mathcal{S} : \;\; \mathbf{R} \cong^{\pi} \mathbf{S}$$

Theorem: $\mathcal{R} \sqsubseteq^{\pi} \mathcal{S}$ is a universally composable reduction.

Reductions

The reduction

$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S}$$

is called sequentially composable if

1. $\mathbf{R} \xrightarrow{\alpha} \mathbf{S} \wedge \mathbf{S} \xrightarrow{\beta} \mathbf{T} \Rightarrow \mathbf{R} \xrightarrow{\alpha \circ \beta} \mathbf{T}$

Reductions

The reduction

$$\mathbf{R} \xrightarrow{\alpha} \mathbf{S}$$

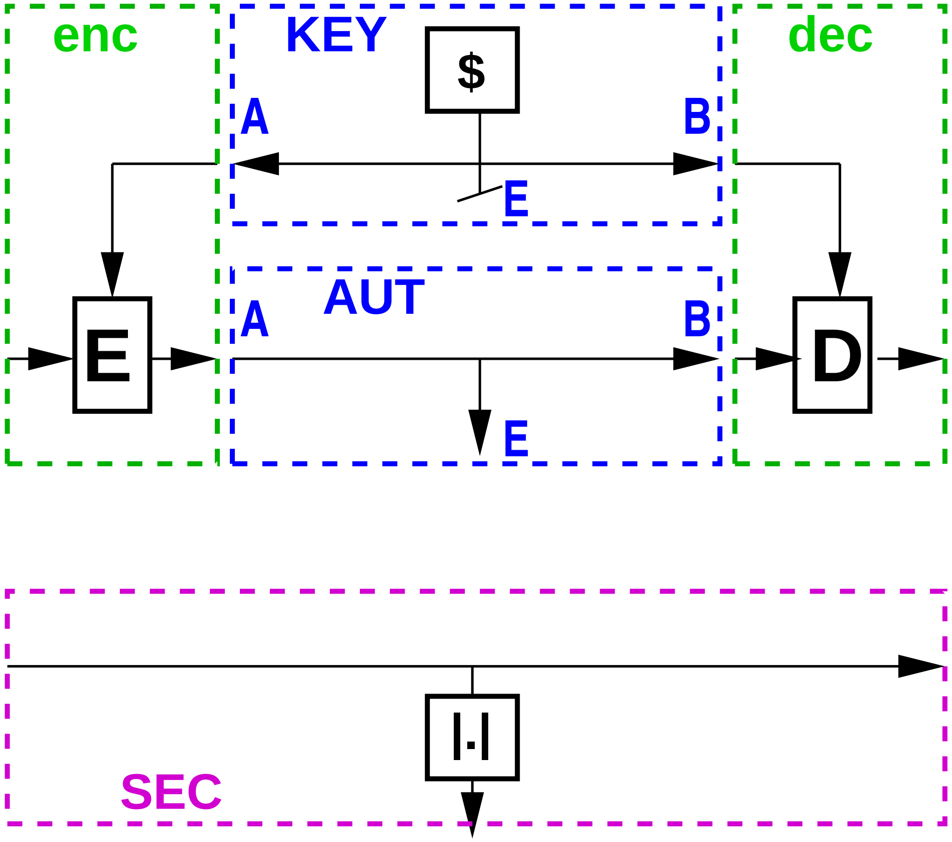
is called sequentially composable if

1. $\mathbf{R} \xrightarrow{\alpha} \mathbf{S} \;\wedge\; \mathbf{S} \xrightarrow{\beta} \mathbf{T} \;\Rightarrow\; \mathbf{R} \xrightarrow{\alpha \circ \beta} \mathbf{T}$

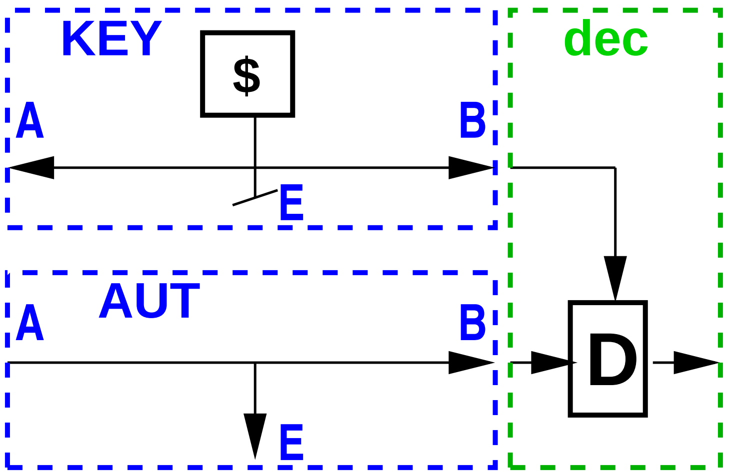
It is called universally composable if in addition:

2. $\mathbf{R} \xrightarrow{\mathrm{id}} \mathbf{R}$
3. $\mathbf{R} \xrightarrow{\alpha} \mathbf{S} \;\Rightarrow\; \mathbf{R} \| \mathbf{T} \xrightarrow{\alpha | \mathrm{id}} \mathbf{S} \| \mathbf{T}$

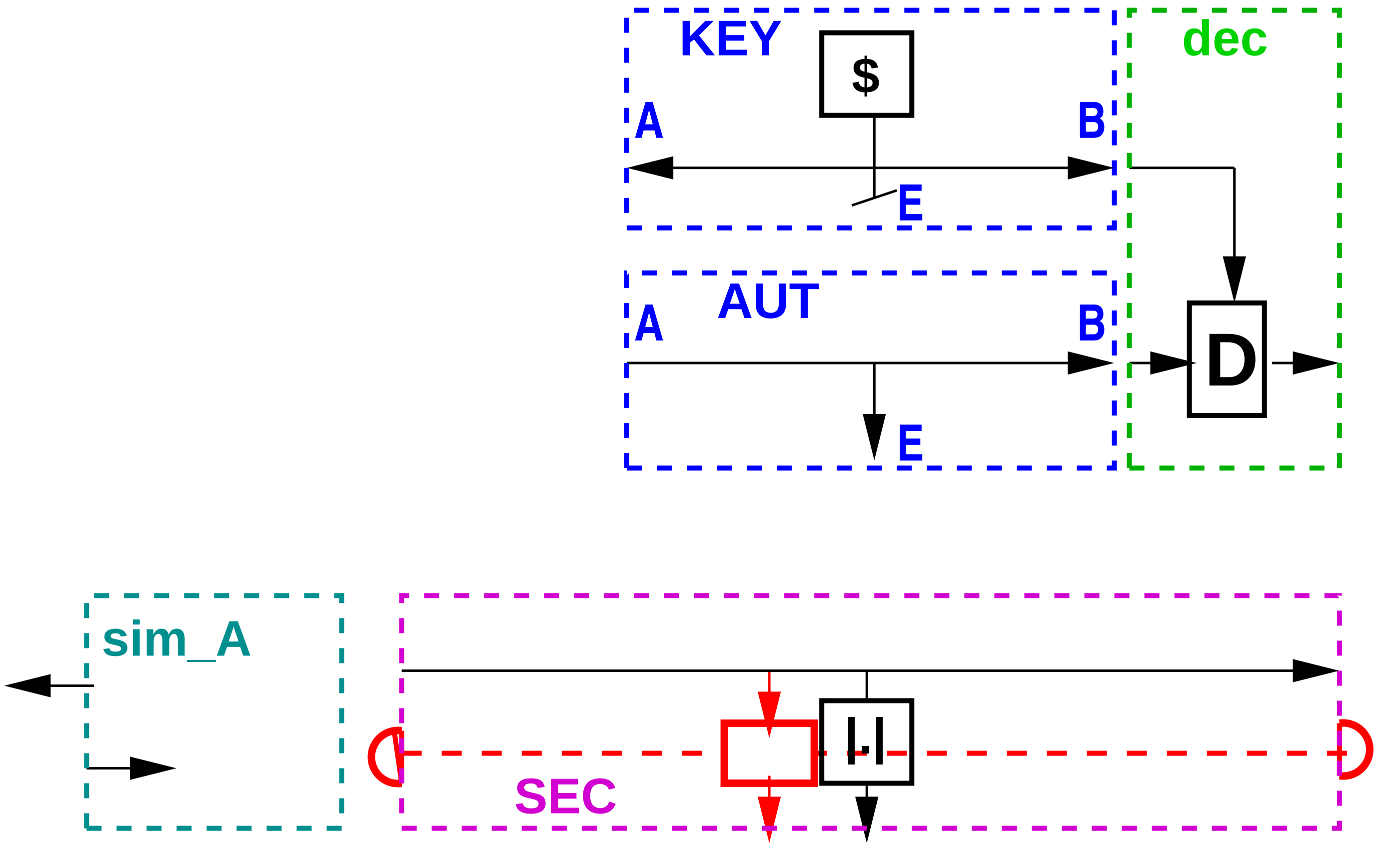
Example: Encryption



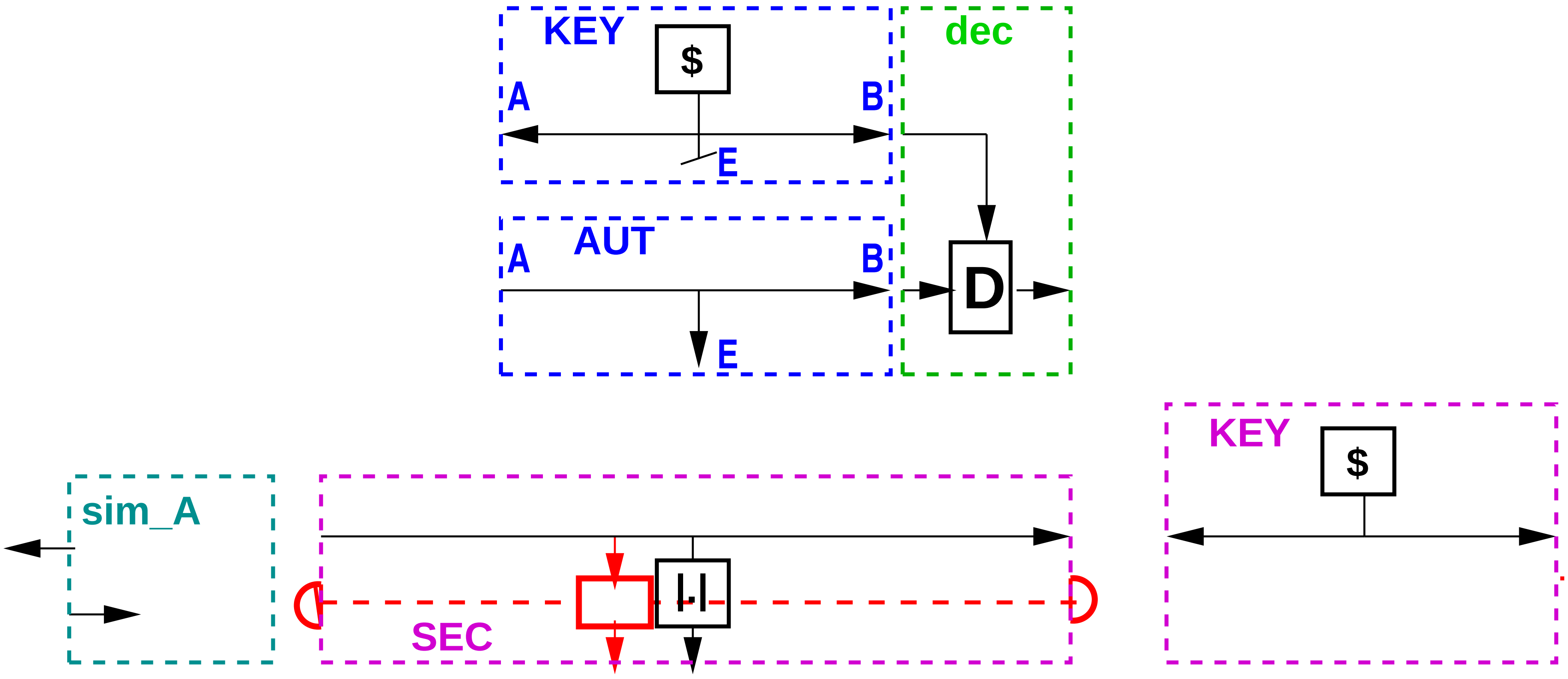
Example: Encryption



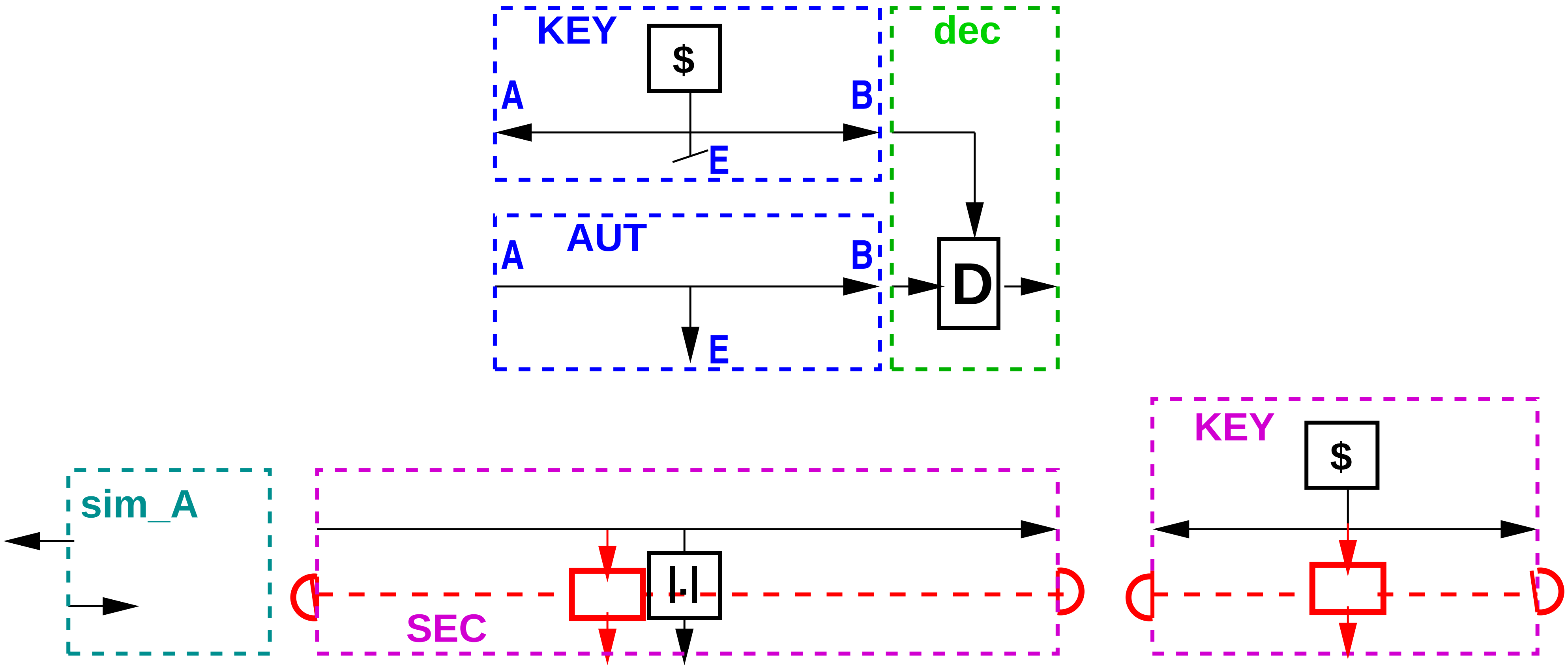
Example: Encryption



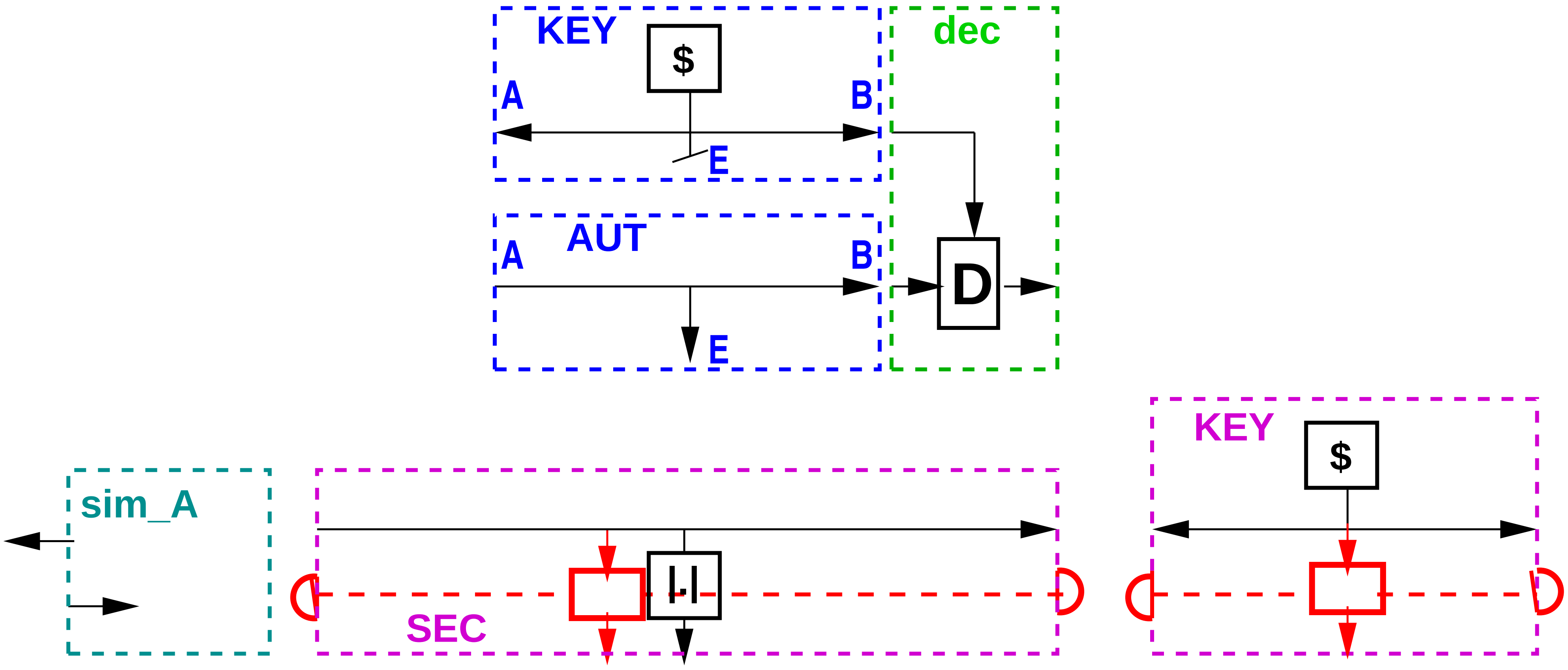
Example: Encryption



Example: Encryption



Example: Encryption



Theorem: An unleakable (uncoercible) secure communication channel cannot be realized from an authenticated channel and a secret key.

Features of Abstract Cryptography

Features of Abstract Cryptography

- strongest notion of reduction (isomorphism)

Features of Abstract Cryptography

- strongest notion of reduction (isomorphism)
- existing frameworks can be captured as special cases
  - universal composability (UC) by Canetti
  - reactive simulatability by Pfitzmann/Waidner/Backes
  - indifferentiability [MRH04]

Features of Abstract Cryptography

- strongest notion of reduction (isomorphism)
- existing frameworks can be captured as special cases
  - universal composability (UC) by Canetti
  - reactive simulatability by Pfitzmann/Waidner/Backes
  - indifferentiability [MRH04]
- communication model, complexity/efficiency notions, ...
  treated at lower abstraction levels (not hard-wired)

Features of Abstract Cryptography

- strongest notion of reduction (isomorphism)
- existing frameworks can be captured as special cases
  - universal composability (UC) by Canetti
  - reactive simulatability by Pfitzmann/Waidner/Backes
  - indifferentiability [MRH04]
- communication model, complexity/efficiency notions, ... treated at lower abstraction levels (not hard-wired)
- reductions among resources, all resources captured

Features of Abstract Cryptography

- strongest notion of reduction (isomorphism)
- existing frameworks can be captured as special cases
  - universal composability (UC) by Canetti
  - reactive simulatability by Pfitzmann/Waidner/Backes
  - indifferentiability [MRH04]
- communication model, complexity/efficiency notions, ... treated at lower abstraction levels (not hard-wired)
- reductions among resources, all resources captured
- sets of resources: guaranteed/possible action spaces

Features of Abstract Cryptography

- strongest notion of reduction (isomorphism)
- existing frameworks can be captured as special cases
  - universal composability (UC) by Canetti
  - reactive simulatability by Pfitzmann/Waidner/Backes
  - indifferentiability [MRH04]
- communication model, complexity/efficiency notions, ... treated at lower abstraction levels (not hard-wired)
- reductions among resources, all resources captured
- sets of resources: guaranteed/possible action spaces
- no central adversary $\longrightarrow$ local simulators (see [AsV08])

Features of Abstract Cryptography

- strongest notion of reduction (isomorphism)
- existing frameworks can be captured as special cases
  - universal composability (UC) by Canetti
  - reactive simulatability by Pfitzmann/Waidner/Backes
  - indifferentiability [MRH04]
- communication model, complexity/efficiency notions, ... treated at lower abstraction levels (not hard-wired)
- reductions among resources, all resources captured
- sets of resources: guaranteed/possible action spaces
- no central adversary $\longrightarrow$ local simulators (see [AsV08])
- general notion of interfaces: consistency domains

Features of Abstract Cryptography

- strongest notion of reduction (isomorphism)
- existing frameworks can be captured as special cases
  - universal composability (UC) by Canetti
  - reactive simulatability by Pfitzmann/Waidner/Backes
  - indifferentiability [MRH04]
- communication model, complexity/efficiency notions, ...

Let's try to identify the right level of abstraction of what we do in cryptography.

- sets of resources: guaranteed/possible action spaces
- no central adversary $\longrightarrow$ local simulators (see [AsV08])
- general notion of interfaces: consistency domains