Indistinguishability Theory

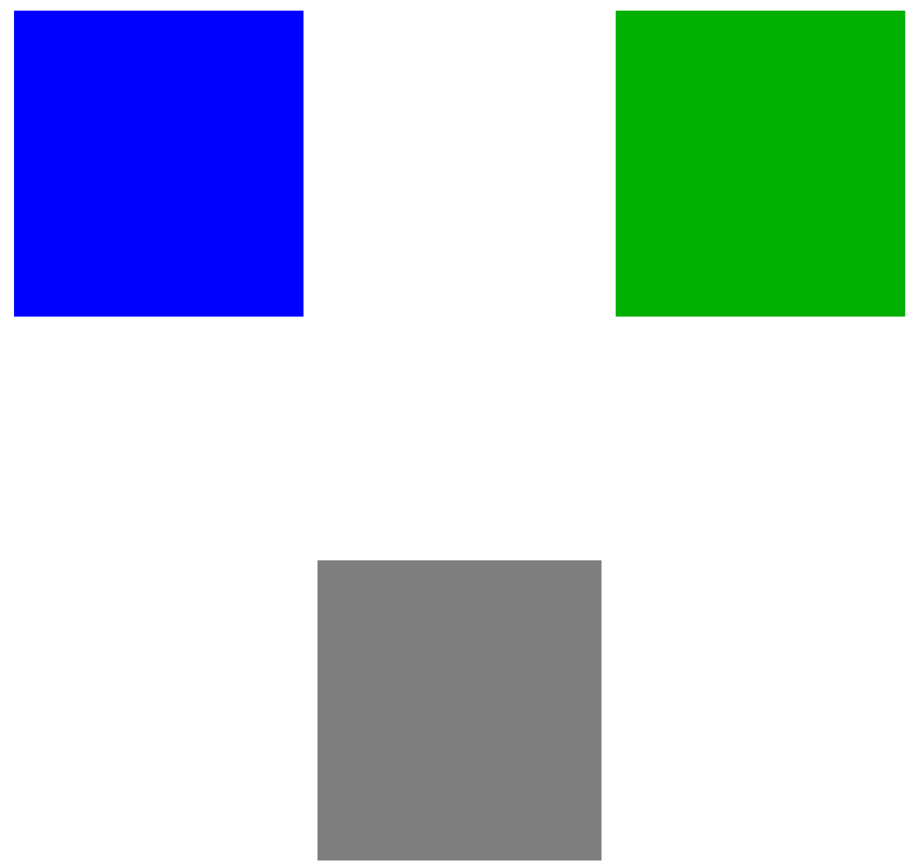
Ueli Maurer

ETH Zurich

FOSAD 2009, Bertinoro, Sept. 2009.

Distinguishing two objects:

Distinguishing two objects:



left or right?

Distinguishing two types of numbers

Set A:

2048-bit integers with exactly **2** prime factors, each with at least 512 bits.

Set B:

2048-bit integers with exactly **3** prime factors, each with at least 512 bits.

Distinguishing two types of numbers

Set A:

2048-bit integers with exactly 2 prime factors, each with at least 512 bits.

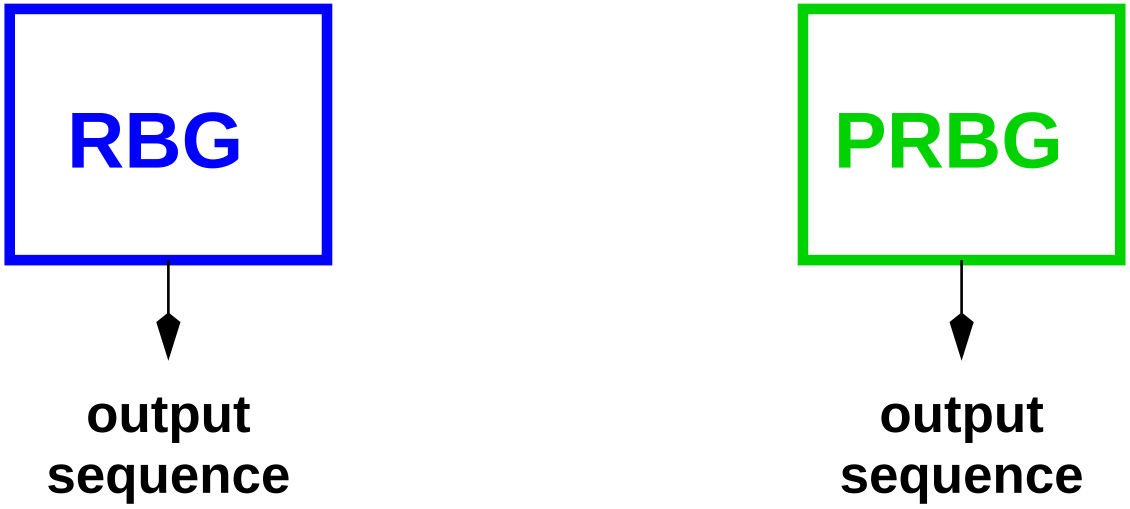
Set B:

2048-bit integers with exactly 3 prime factors, each with at least 512 bits.

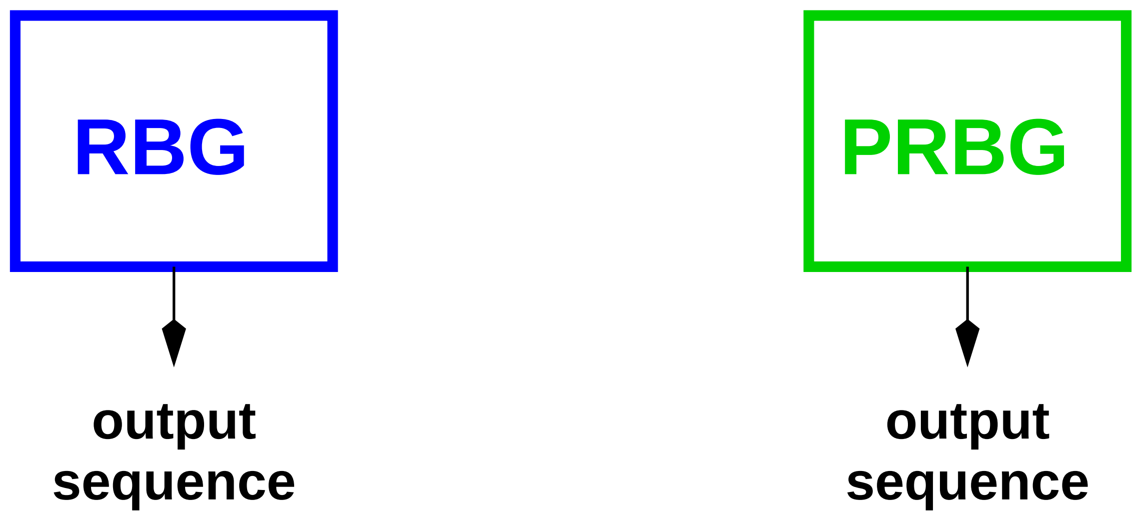
3740957629745118733980567439817539577832546738459678253645098713652955848823336449857660918528256405016387598795387626354856782430914257652536485263740991252317647489855766009633273939475861234987505334958620549877465243510897583932183674432789687645343127364987564354675092736565475849823142537584950243685261

left or right?

Random vs. pseudo-random bit generator



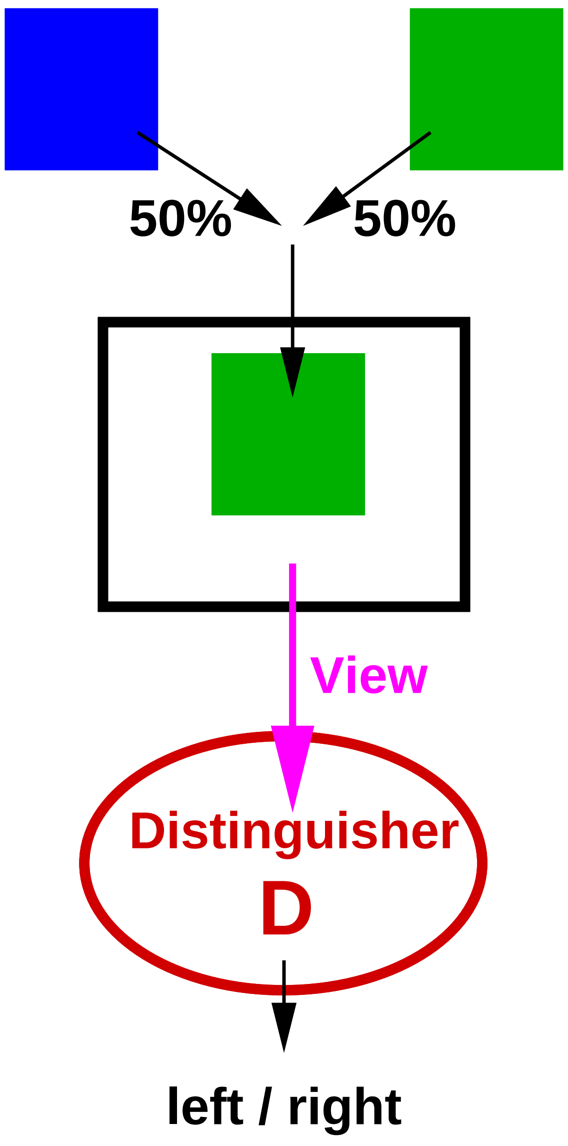
Random vs. pseudo-random bit generator



101100011101111001001110100010000011101100101110010111010001101
0000110110101111010100011010110101001001010111101010000001101101
111000111011000101111010010101101001010110000101011010101101001
110011001001100010110100011100101010001011010100001111000101010

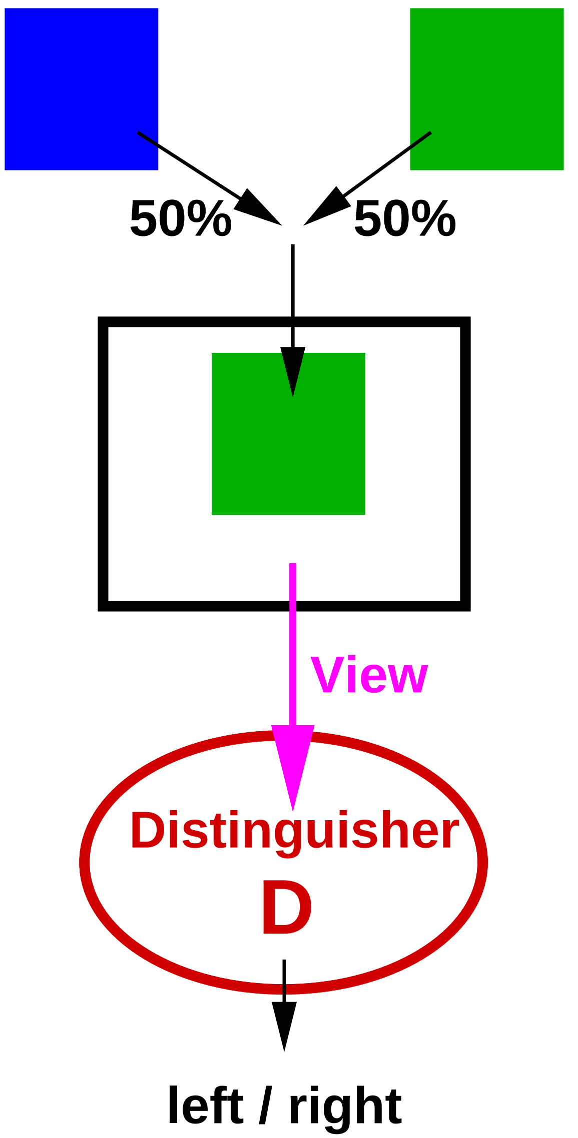
left or right?

Distinguisher's advantage



D's task: Guess left/right

Distinguisher's advantage

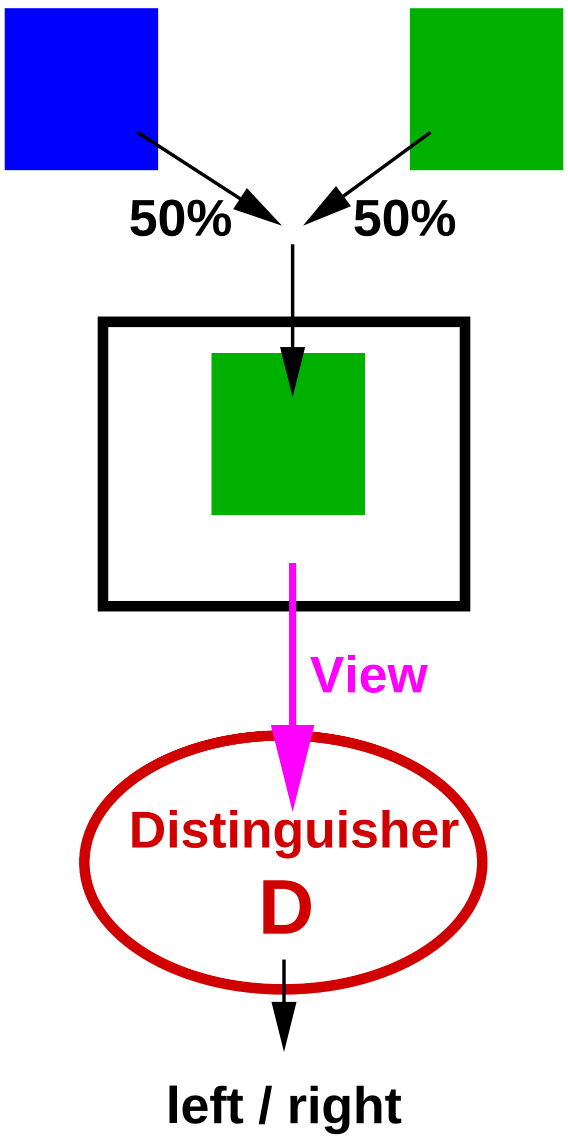


D's task: Guess left/right

Prob(correct guess) = 0.5 + α**/2**

$\alpha = \Delta^{D}(\blacksquare, \blacksquare)$ **(D's advantage)**

Distinguisher's advantage



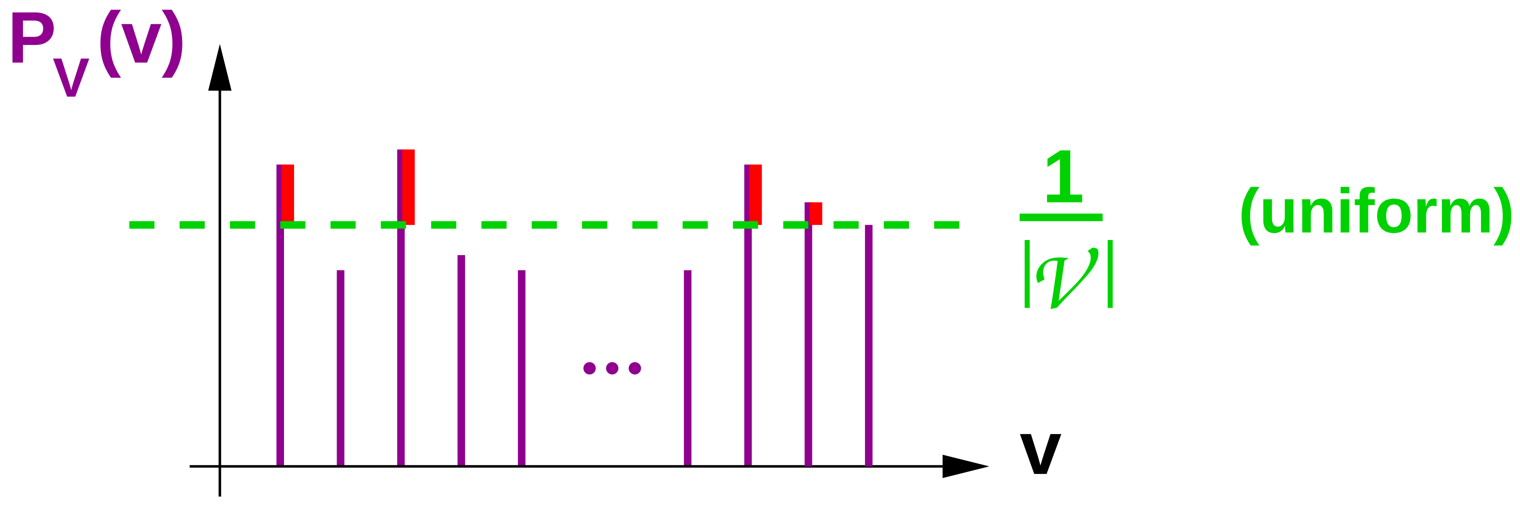
D's task: Guess left/right

Prob(correct guess) = 0.5 + α/2

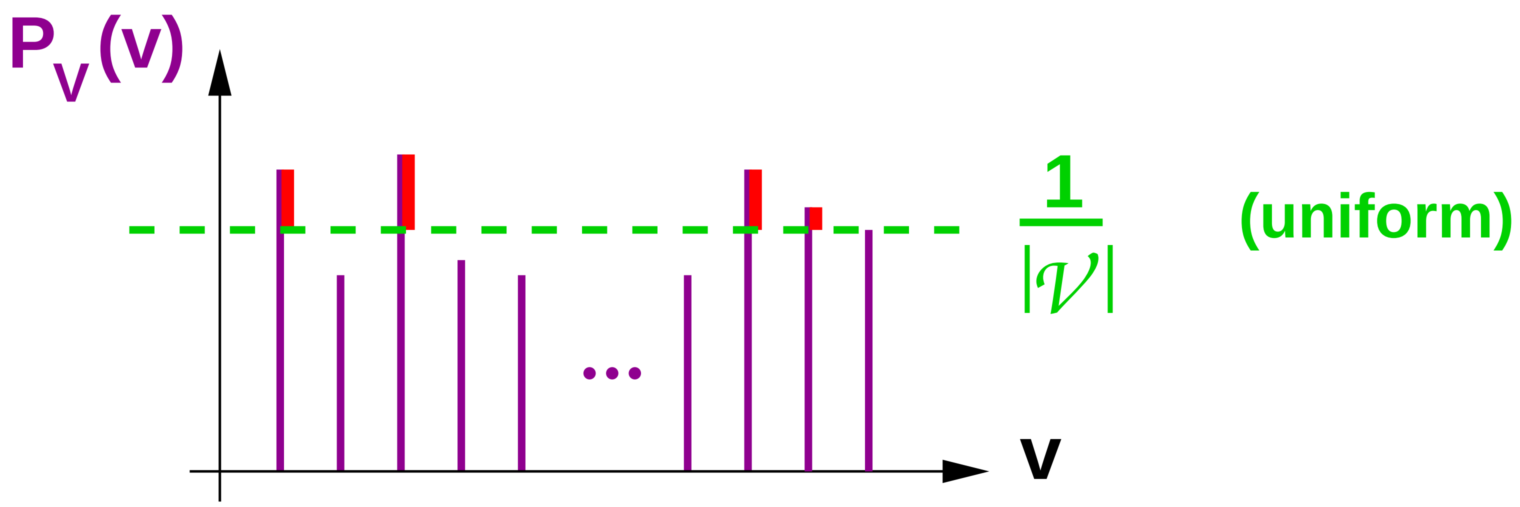
$\alpha = \Delta^{D}(■, ■)$ **(D's advantage)**

best D: $\Delta(■, ■)$

Distinguishing a RV V from a uniform RV U



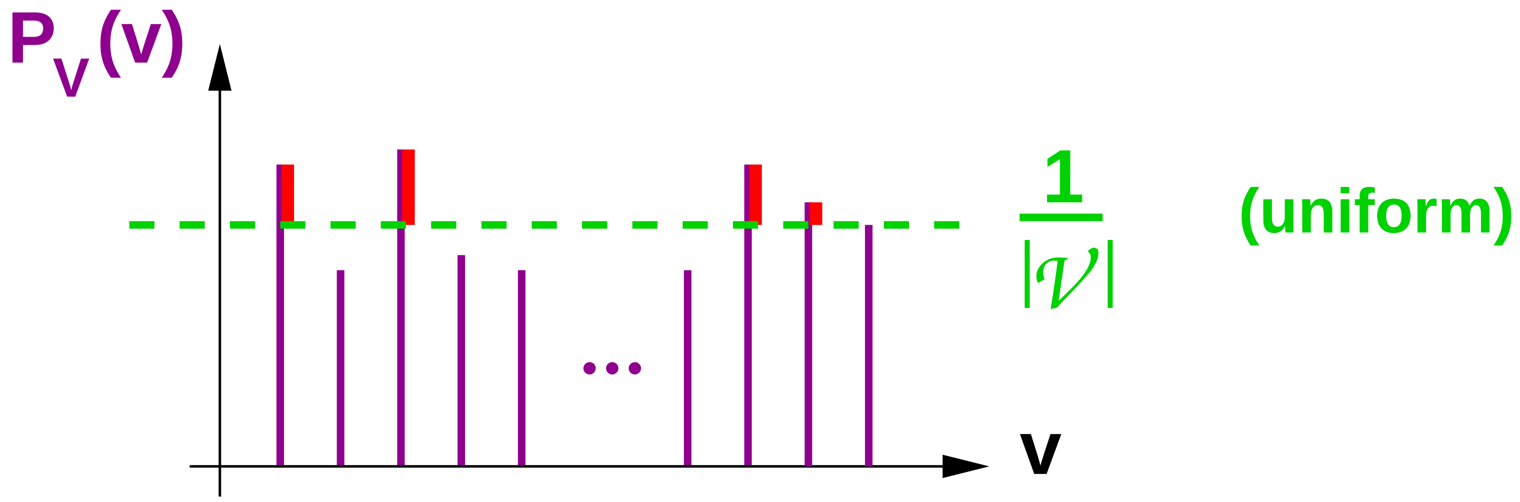
Distinguishing a RV V from a uniform RV U



Statistical distance:

$$\mathbf{d}(\mathbf{V},\mathbf{U}) := \frac{1}{2}\sum_{v\in\mathcal{V}}\left|\mathbf{P_V}(v) - \frac{1}{|\mathcal{V}|}\right|$$ **(sum of red quantities)**

Distinguishing a RV V from a uniform RV U

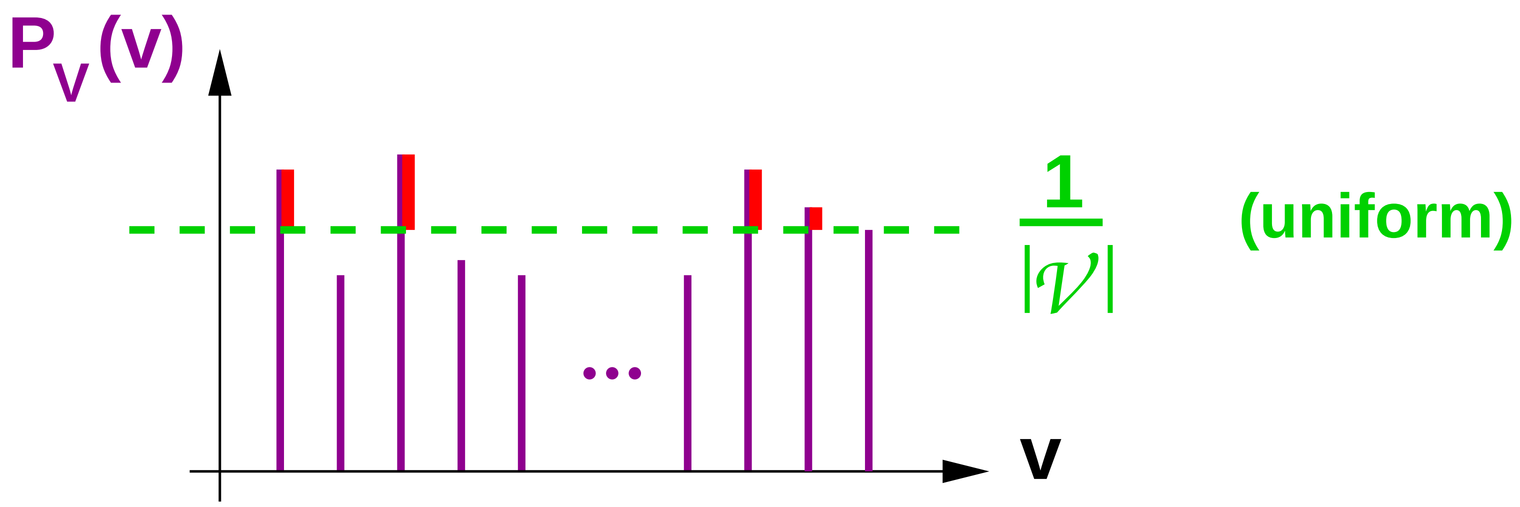


Statistical distance:

$$\mathbf{d}(\mathbf{V},\mathbf{U}) := \frac{1}{2}\sum_{v\in\mathcal{V}}\left|\mathbf{P_V}(v) - \frac{1}{|\mathcal{V}|}\right|$$ **(sum of red quantities)**

$$= \Delta(\mathbf{V},\mathbf{U})$$

Distinguishing a RV V from a uniform RV U



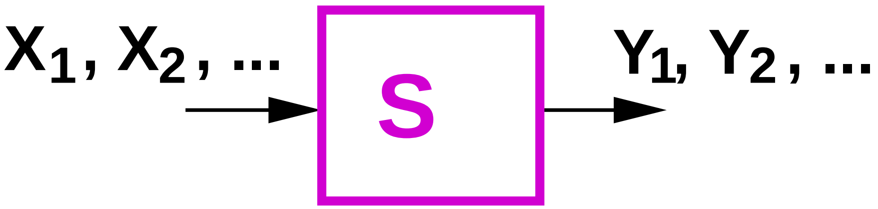
Statistical distance:

$$\mathbf{d}(\mathbf{V},\mathbf{U}) \;:=\; \frac{1}{2}\sum_{v\in\mathcal{V}}\left|P_{\mathbf{V}}(v) - \frac{1}{|\mathcal{V}|}\right|$$ **(sum of red quantities)**

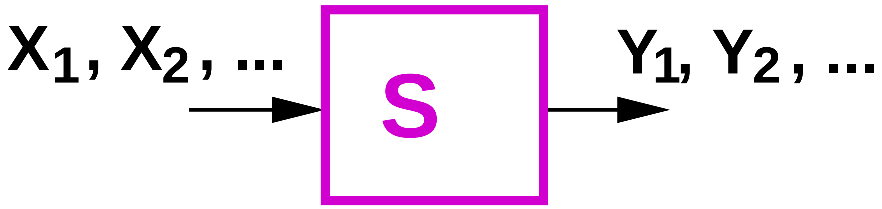
$$= \;\Delta(\mathbf{V},\mathbf{U})$$

Possible interpretation: $P(\mathbf{V}=\mathbf{U}) \;=\; 1 - \mathbf{d}(\mathbf{V},\mathbf{U})$

Discrete systems

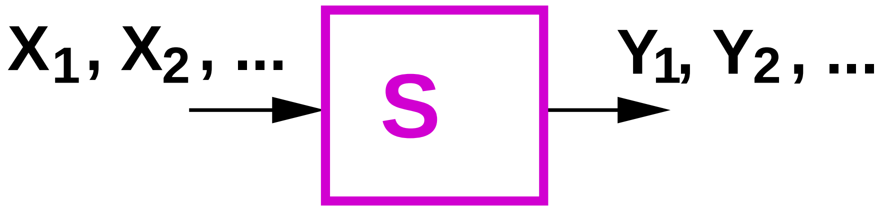


Discrete systems



Description of S: pseudo-code, figures, text, ...

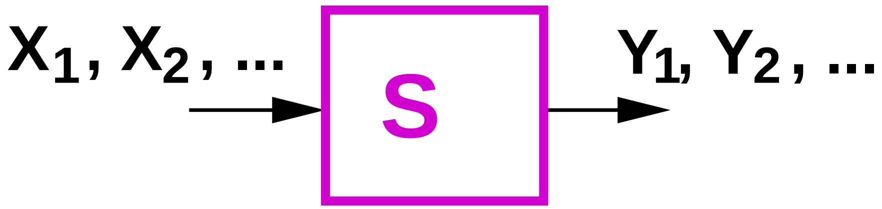
Discrete systems



Description of S: pseudo-code, figures, text, ...

What kind of mathematical object is the behavior?

Discrete systems

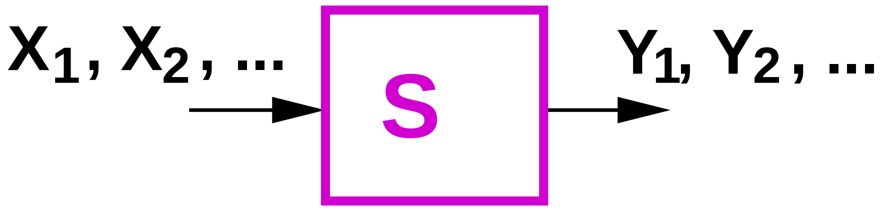


Description of S: pseudo-code, figures, text, ...

What kind of mathematical object is the behavior?

- **Only input-output behavior is relevant!**

Discrete systems

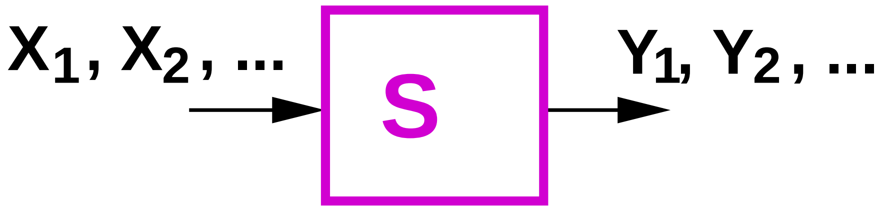


Description of S: pseudo-code, figures, text, ...

What kind of mathematical object is the behavior?

- Only input-output behavior is relevant!
- Characterized by: $p^{S}_{Y_i|X_1 \cdots X_i Y_1 \cdots Y_{i-1}}$ for $i = 1, 2, \ldots$

Discrete systems



Description of S: pseudo-code, figures, text, ...

What kind of mathematical object is the behavior?

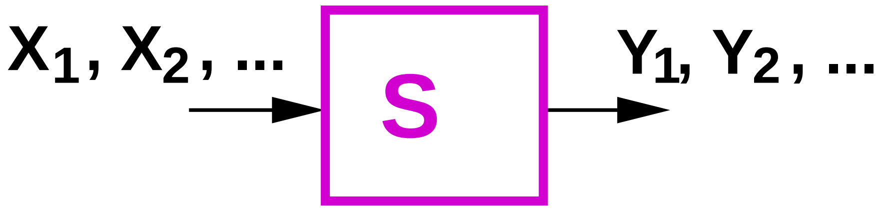
- **Only input-output behavior is relevant!**
- **Characterized by:** $\mathrm{p}^{\mathbf{S}}_{Y_i|X_1\cdots X_i Y_1\cdots Y_{i-1}}$ **for** $i = 1, 2, \ldots$

  $\rightarrow$ **abstraction called random system [Mau02]**

  $\rightarrow$ **This description is minimal!**

  $\rightarrow$ **Redundant (better) description:** $\mathrm{p}^{\mathbf{S}}_{Y_1\cdots Y_i|X_1\cdots X_i}$

Discrete systems



Description of S: pseudo-code, figures, text, ...

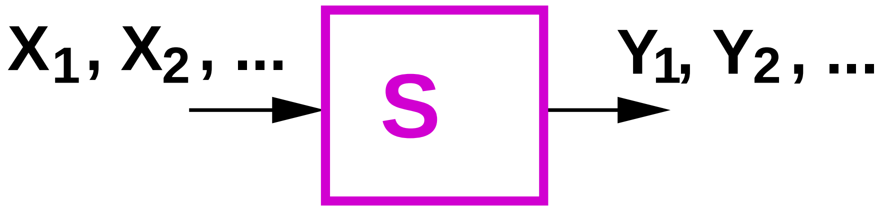
What kind of mathematical object is the behavior?

- **Only input-output behavior is relevant!**
- **Characterized by:** $\mathrm{p}^{\mathbf{S}}_{Y_i|X_1\cdots X_i Y_1\cdots Y_{i-1}}$ **for** $i = 1, 2, \ldots$

  $\rightarrow$ **abstraction called random system [Mau02]**
  $\rightarrow$ **This description is minimal!**
  $\rightarrow$ **Redundant (better) description:** $\mathrm{p}^{\mathbf{S}}_{Y_1\cdots Y_i|X_1\cdots X_i}$

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

Discrete systems



Description of S: pseudo-code, figures, text, ...

What kind of mathematical object is the behavior?

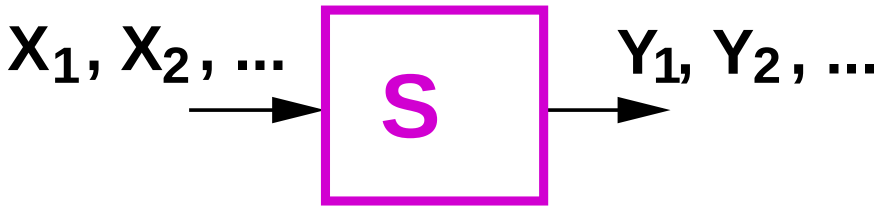
- **Only input-output behavior is relevant!**
- **Characterized by:** $\mathrm{p}^{\mathbf{S}}_{Y_i|X_1\cdots X_i Y_1 \cdots Y_{i-1}}$ **for** $i = 1, 2, \ldots$

  $\rightarrow$ **abstraction called random system [Mau02]**
  $\rightarrow$ **This description is minimal!**
  $\rightarrow$ **Redundant (better) description:** $\mathrm{p}^{\mathbf{S}}_{Y_1\cdots Y_i|X_1\cdots X_i}$

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

Realization of S from a RV (range $\mathcal{R}$**):** $f_i^{\mathbf{S}} : \mathcal{X}^i \times \mathcal{R} \rightarrow \mathcal{Y}$

Discrete systems



Description of S: pseudo-code, figures, text, ...

What kind of mathematical object is the behavior?

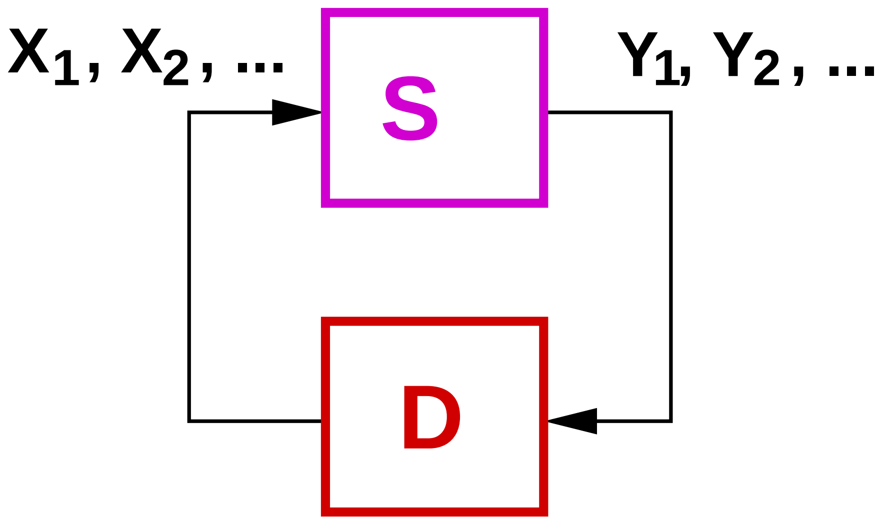
- **Only input-output behavior is relevant!**
- **Characterized by:** $\mathsf{p}^{\mathsf{S}}_{Y_i|X_1\cdots X_i Y_1 \cdots Y_{i-1}}$ **for** $i = 1, 2, \ldots$
  - $\rightarrow$ **abstraction called random system [Mau02]**
  - $\rightarrow$ **This description is minimal!**
  - $\rightarrow$ **Redundant (better) description:** $\mathsf{p}^{\mathsf{S}}_{Y_1\cdots Y_i|X_1\cdots X_i}$

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

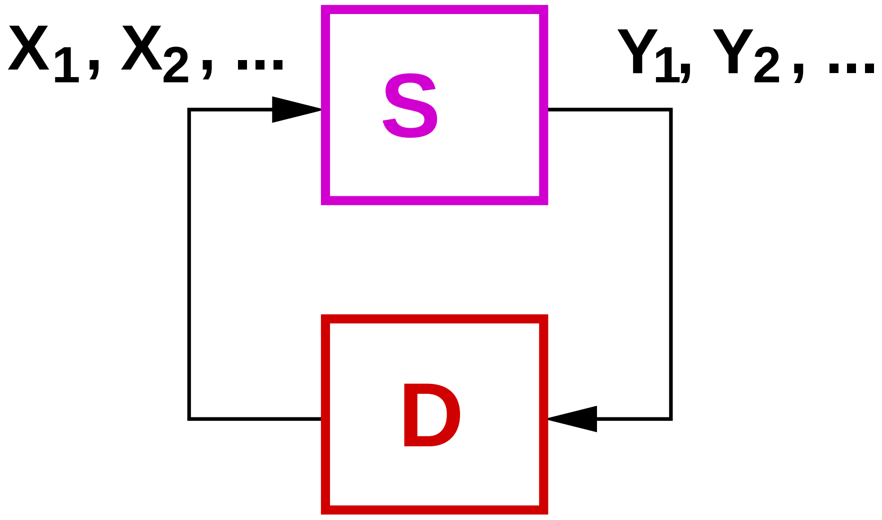
Realization of S from a RV (range $\mathcal{R}$): $f_i^{\mathsf{S}} : \mathcal{X}^i \times \mathcal{R} \rightarrow \mathcal{Y}$

$\rightarrow$ **notion of independence**

Distinguishers



Distinguishers

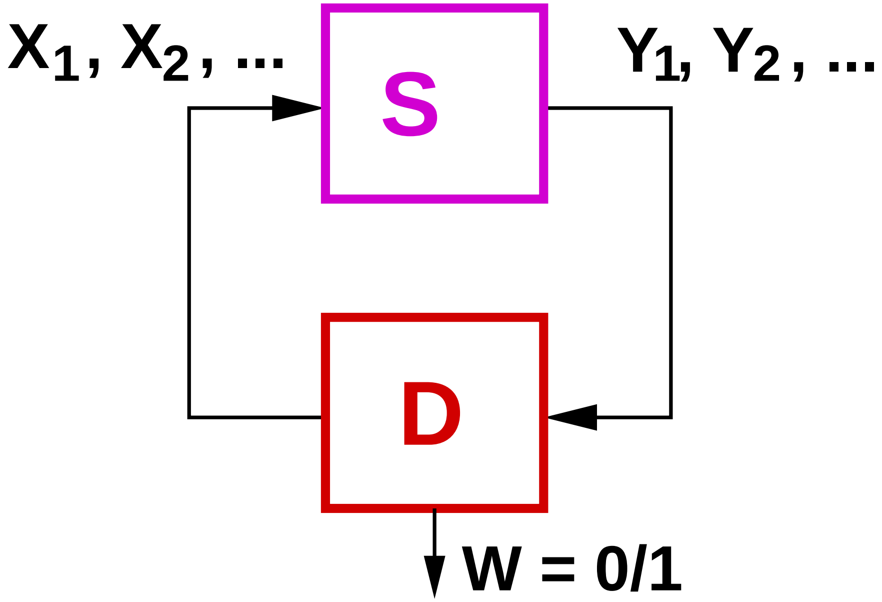


$$P^{DS}_{X^k Y^k} = \prod_{i=1}^{k} p^{S}_{Y_i|X^i Y^{i-1}} \cdot p^{D}_{X_i|X^{i-1} Y^{i-1}}$$

$$= p^{S}_{Y^k|X^k} \cdot p^{D}_{X^k|Y^{k-1}}$$

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

Distinguishers



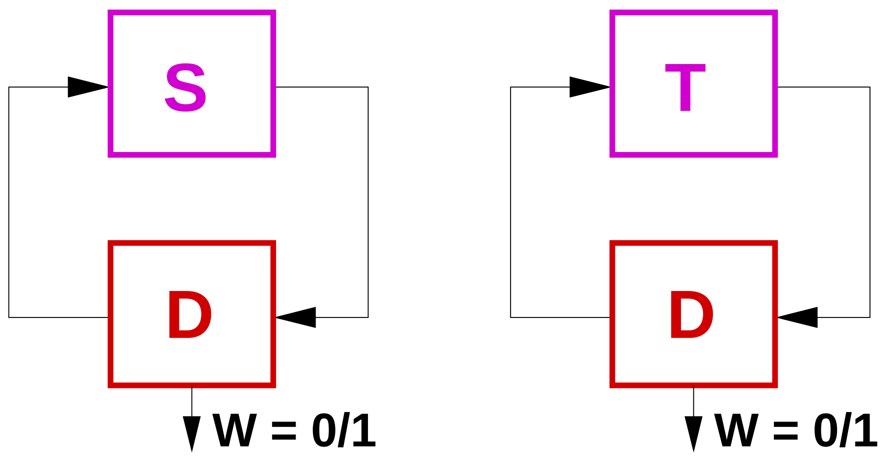
$$\mathbf{P}^{\mathbf{DS}}_{X^k Y^k} = \prod_{i=1}^{k} \mathbf{p}^{\mathbf{S}}_{Y_i | X^i Y^{i-1}} \cdot \mathbf{p}^{\mathbf{D}}_{X_i | X^{i-1} Y^{i-1}}$$

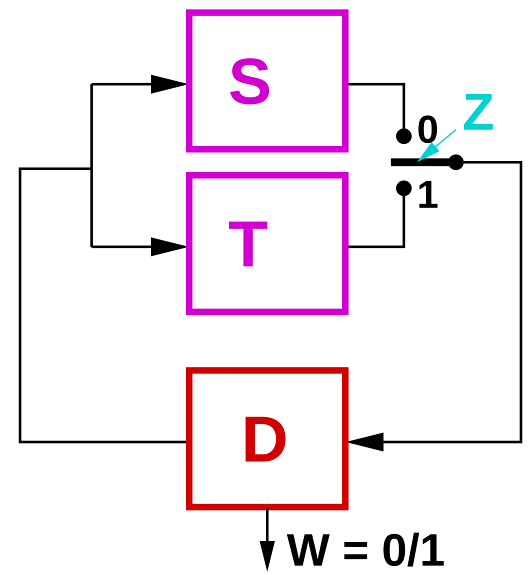
$$= \mathbf{p}^{\mathbf{S}}_{Y^k | X^k} \cdot \mathbf{p}^{\mathbf{D}}_{X^k | Y^{k-1}}$$

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

Distinguishing advantage

2 equivalent views:



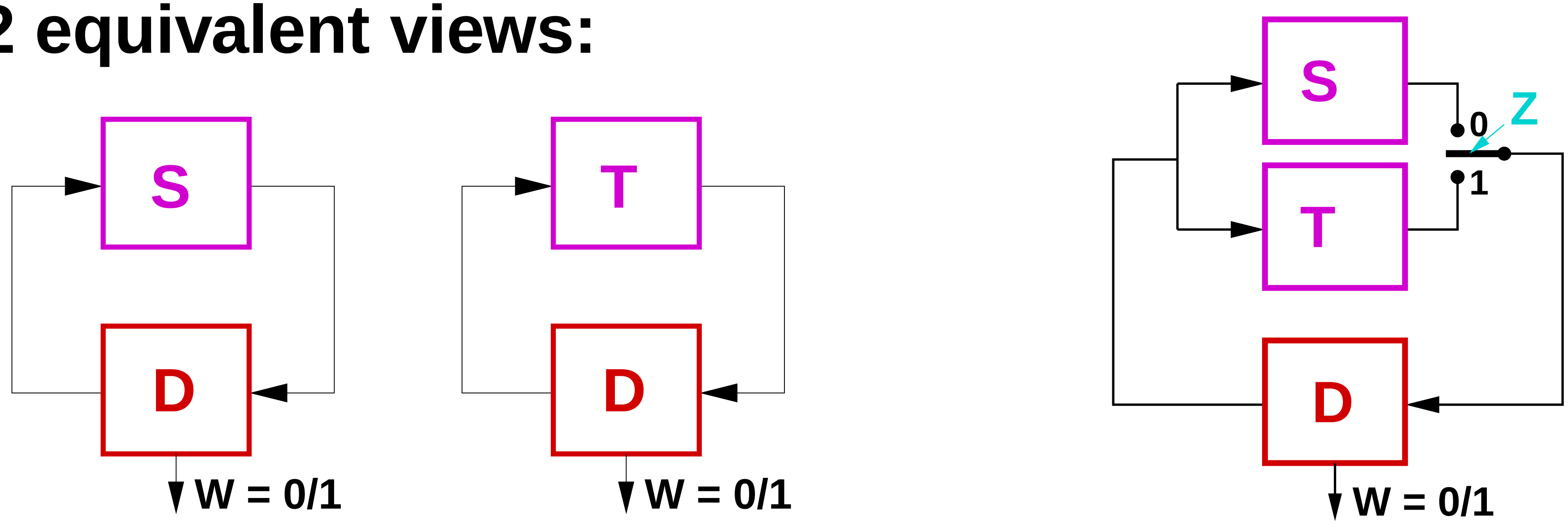


$$\Delta_k^{\mathbf{D}}(\mathbf{S},\mathbf{T}) \;:=\; \left|\mathbf{P}^{\mathbf{DS}}(\mathbf{W}=1) - \mathbf{P}^{\mathbf{DT}}(\mathbf{W}=1)\right|$$

$$= \; 2\left|\mathbf{P}^{\mathbf{DSTZ}}(\mathbf{W}=\mathbf{Z}) - \frac{1}{2}\right|$$

Distinguishing advantage

2 equivalent views:



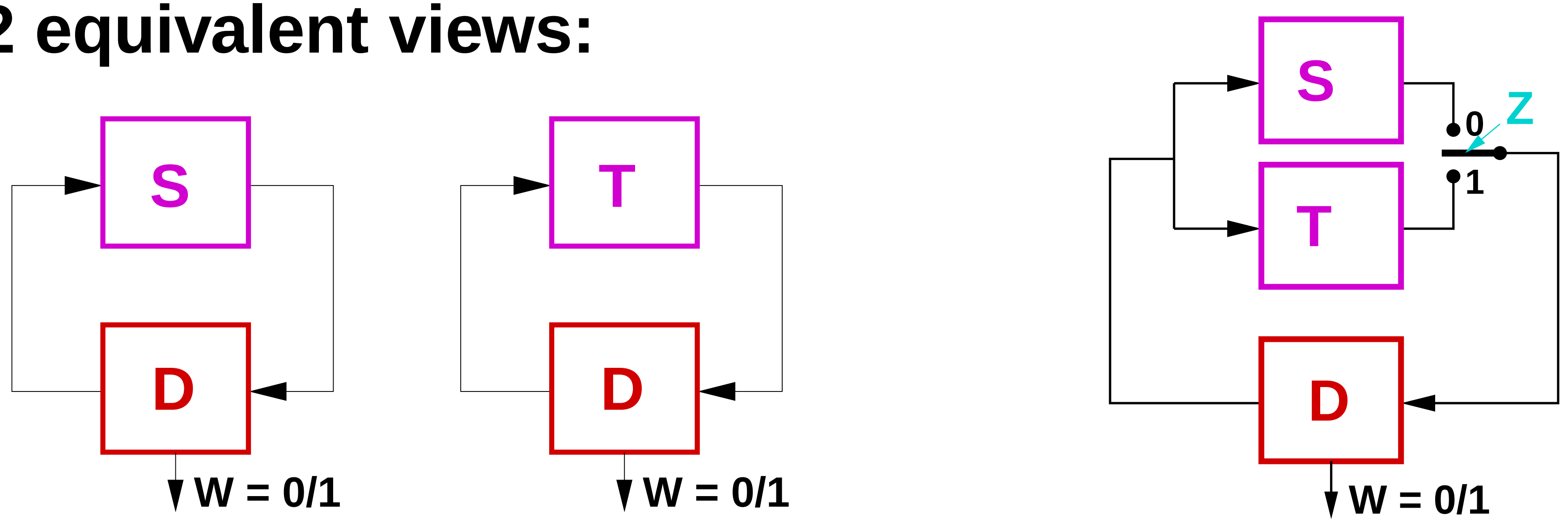
$$\Delta_k^{\mathbf{D}}(\mathbf{S},\mathbf{T}) \;:=\; \left|\mathbf{P}^{\mathbf{DS}}(\mathbf{W}=1) - \mathbf{P}^{\mathbf{DT}}(\mathbf{W}=1)\right|$$

$$= 2\left|\mathbf{P}^{\mathbf{DSTZ}}(\mathbf{W}=\mathbf{Z}) - \frac{1}{2}\right|$$

best (adaptive) D: $\Delta_k(\mathbf{S},\mathbf{T})$

Distinguishing advantage

2 equivalent views:



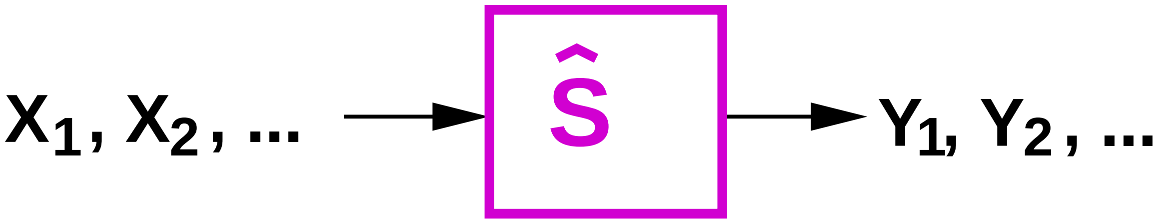
$$\Delta_k^{\mathsf{D}}(\mathsf{S},\mathsf{T}) \;:=\; \left|\mathsf{P}^{\mathsf{DS}}(\mathsf{W}=1) - \mathsf{P}^{\mathsf{DT}}(\mathsf{W}=1)\right|$$

$$=\; 2\left|\mathsf{P}^{\mathsf{DSTZ}}(\mathsf{W}=\mathsf{Z}) - \frac{1}{2}\right|$$

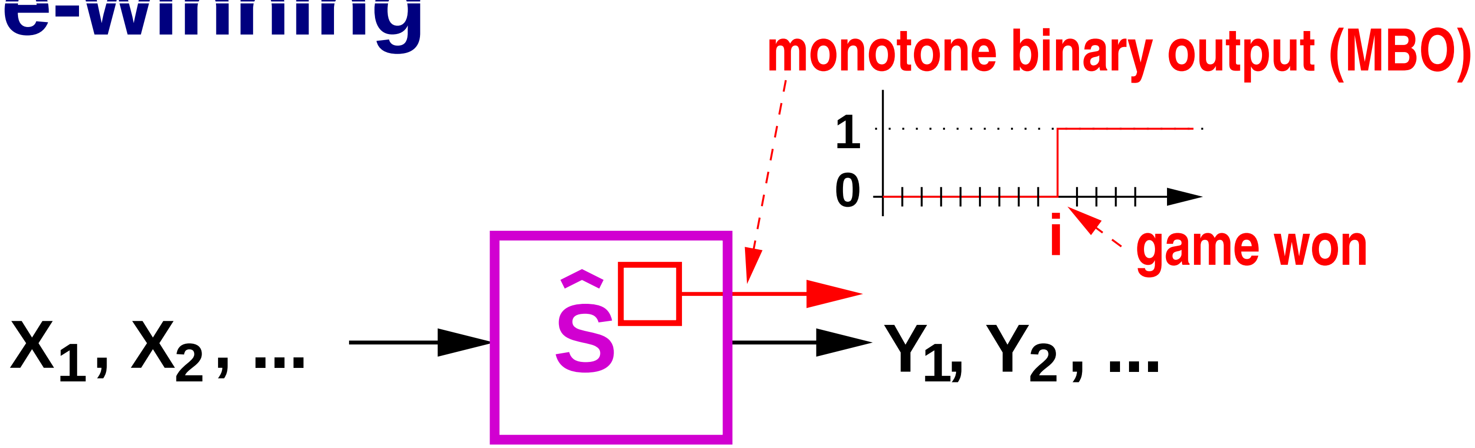
best (adaptive) D: $\Delta_k(\mathsf{S},\mathsf{T})$

best non-adapt. D: $\Delta_k^{\mathsf{NA}}(\mathsf{S},\mathsf{T})$

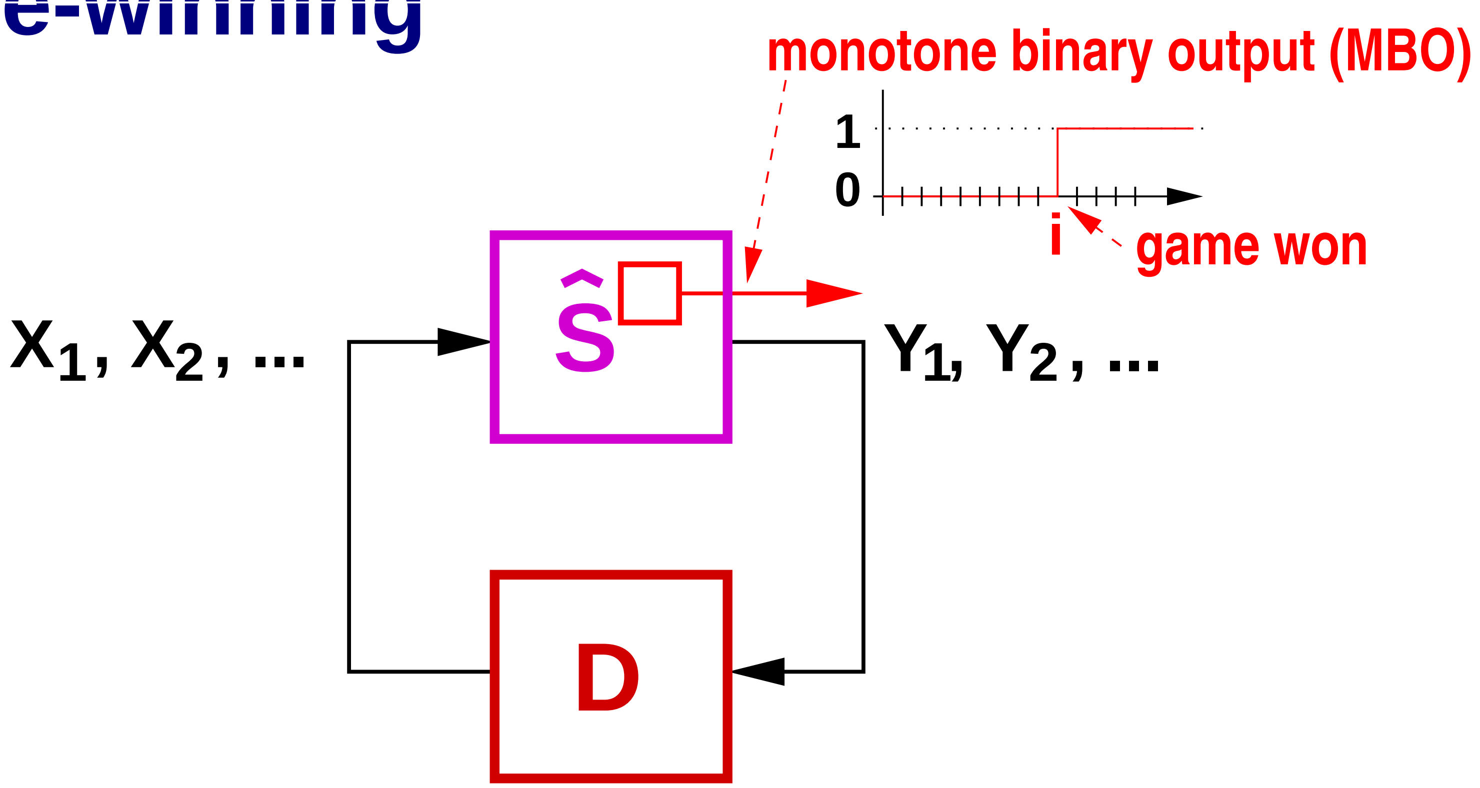
Game-winning



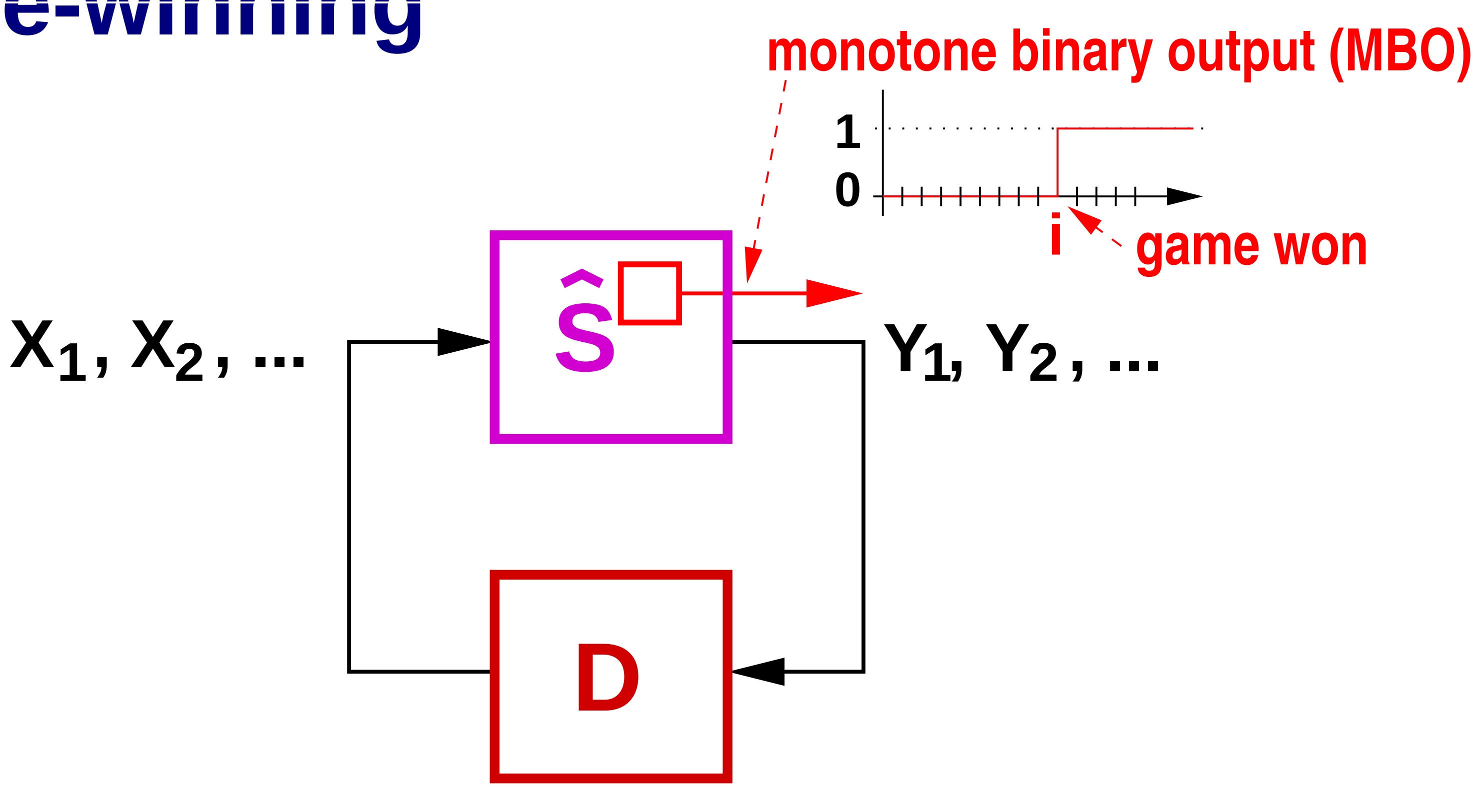
Game-winning



Game-winning

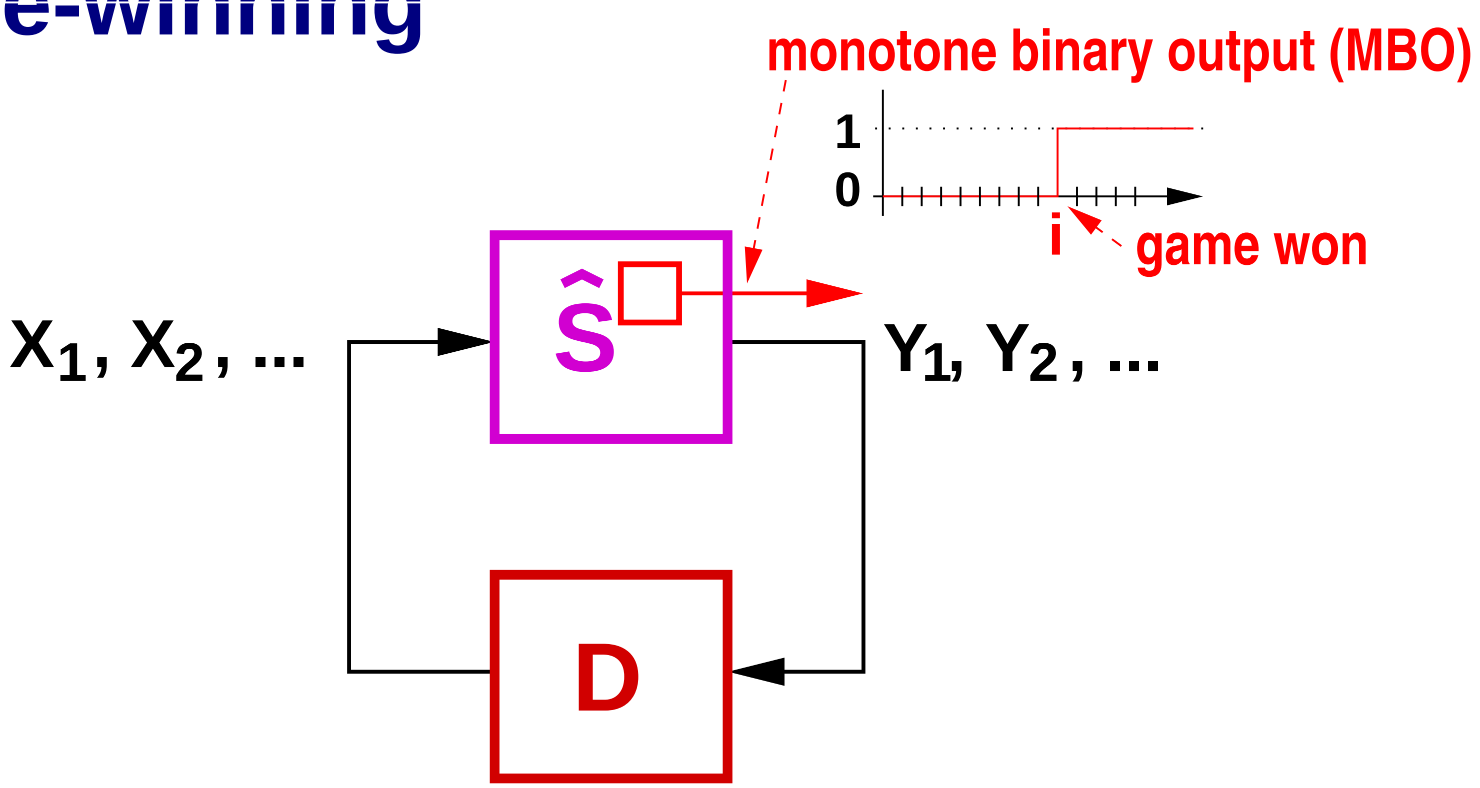


Game-winning



D's prob. of winning with k queries: $\nu_k^{\mathbf{D}}(\hat{\mathbf{S}})$

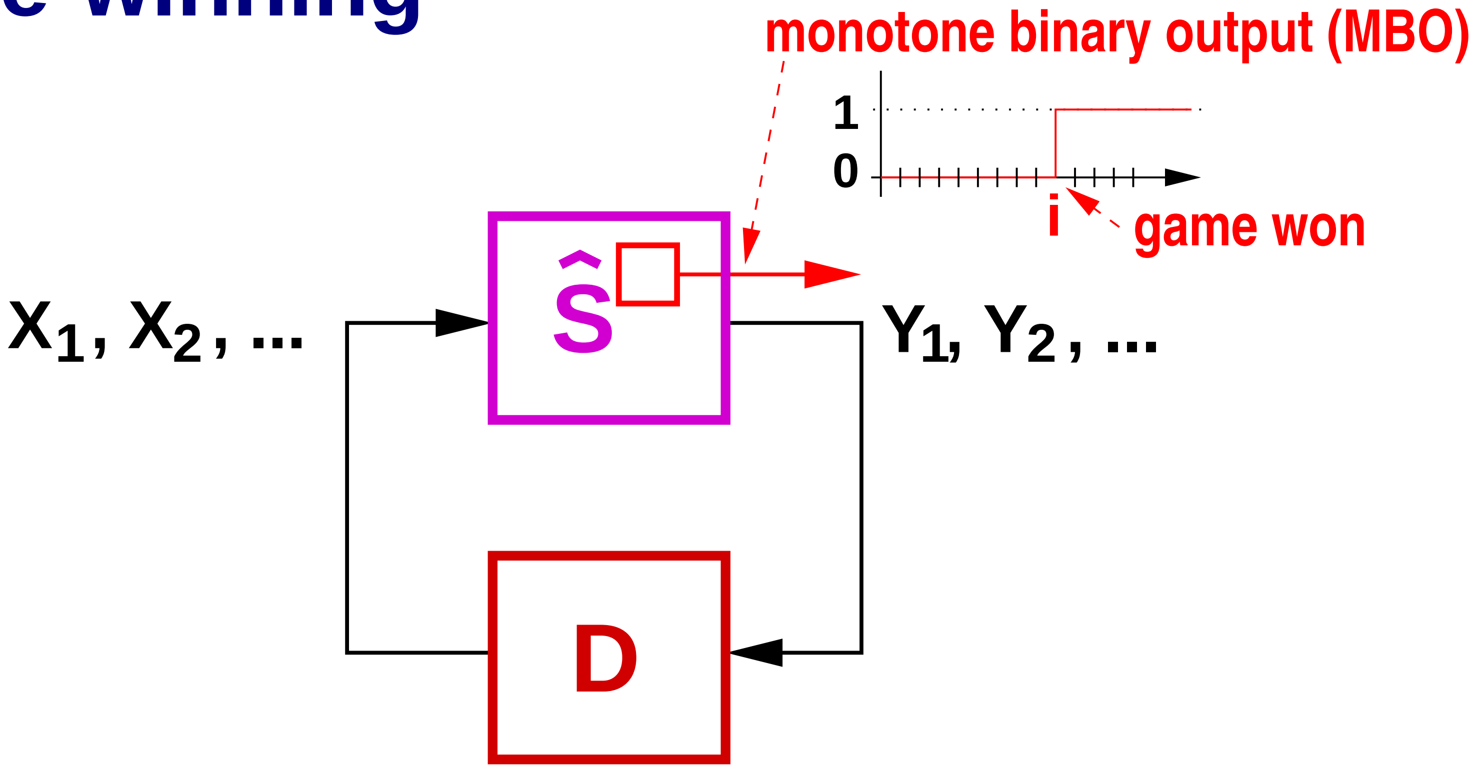
Game-winning



D's prob. of winning with k queries: $\nu_k^{D}(\hat{S})$

Optimal (adaptive) D: $\nu_k(\hat{S}) := \max_{D} \nu_k^{D}(\hat{S})$

Game-winning

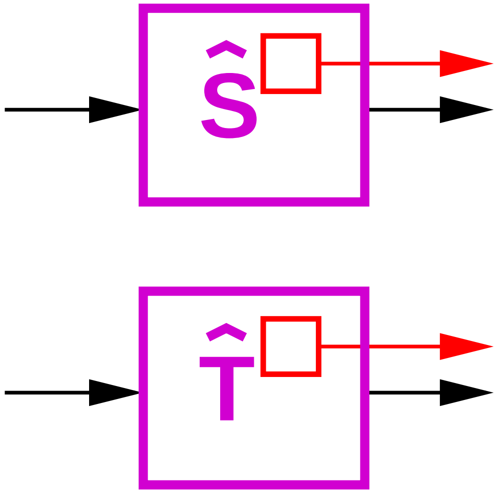


D's prob. of winning with k queries: $\nu_k^{\mathbf{D}}(\hat{\mathbf{S}})$

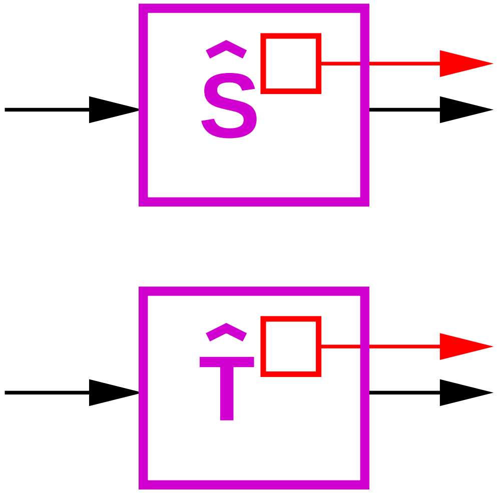
Optimal (adaptive) D: $\nu_k(\hat{\mathbf{S}}) := \max_{\mathbf{D}} \nu_k^{\mathbf{D}}(\hat{\mathbf{S}})$

Optimal non-adapt. D: $\nu_k^{\mathrm{NA}}(\hat{\mathbf{S}}) := \max_{\mathbf{D} \in \mathbf{NA}} \nu_k^{\mathbf{D}}(\hat{\mathbf{S}})$

Playing 2 games in parallel

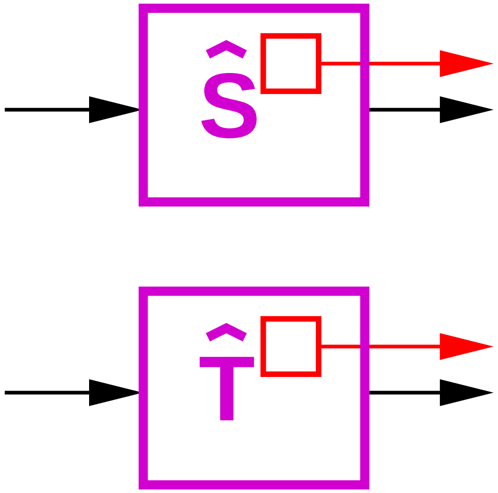


Playing 2 games in parallel



Can a combined strategy be better than optimal individual strategies?

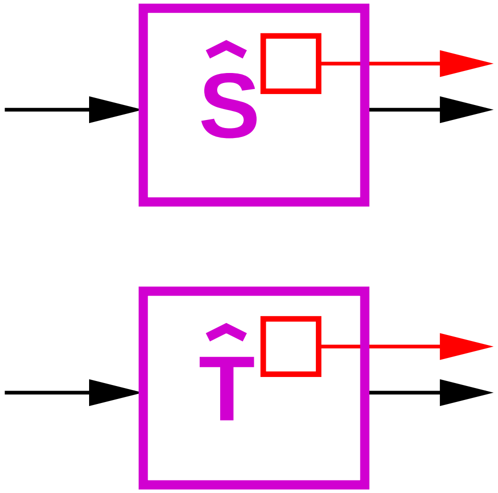
Playing 2 games in parallel



Can a combined strategy be better than optimal individual strategies?

YES!   Chess grand-masters' problem!

Playing 2 games in parallel

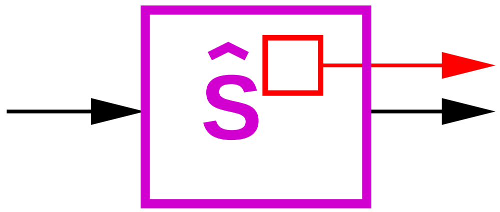


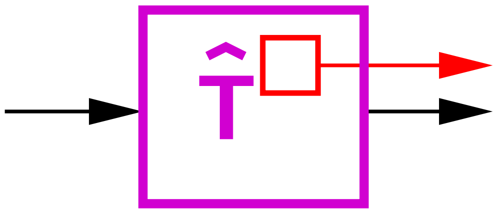
Can a combined strategy be better than optimal individual strategies?

YES! Chess grand-masters' problem!

Lemma [MPR07]: For winning both games, playing individual optimal strategies is optimal.

Game-winning $\Longleftrightarrow$ Distinguishing





Game-winning $\Longleftrightarrow$ Distinguishing

Def.: Ŝ and T̂ are restricted equivalent, denoted Ŝ $\stackrel{r}{\equiv}$ T̂, if the I/O behavior is identical as long as MBO =0.

Game-winning $\Longleftrightarrow$ Distinguishing

Def.: $\hat{S}$ and $\hat{T}$ are **restricted equivalent**, denoted $\hat{S} \stackrel{r}{\equiv} \hat{T}$, if the I/O behavior is identical as long as MBO $=0$.

Lemma ($\Rightarrow$) [Mau02]: If $\hat{S} \stackrel{r}{\equiv} \hat{T}$, then, for every D,

$$\Delta_k^{\mathbf{D}}(\mathbf{S},\mathbf{T}) \leq \nu_k^{\mathbf{D}}(\hat{\mathbf{S}}) \qquad \left(= \nu_k^{\mathbf{D}}(\hat{\mathbf{T}}) \right).$$

Game-winning $\Longleftrightarrow$ Distinguishing

Def.: Ŝ and T̂ are restricted equivalent, denoted $\hat{S} \overset{r}{\equiv} \hat{T}$, if the I/O behavior is identical as long as MBO $=$0.

Lemma ($\Rightarrow$) [Mau02]: If $\hat{S} \overset{r}{\equiv} \hat{T}$, then, for every D,

$$\Delta_k^{\mathbf{D}}(\mathbf{S},\mathbf{T}) \leq \nu_k^{\mathbf{D}}(\hat{\mathbf{S}}) \qquad (= \nu_k^{\mathbf{D}}(\hat{\mathbf{T}})).$$

In particular, $\Delta_k(\mathbf{S},\mathbf{T}) \leq \nu_k(\hat{\mathbf{S}})$

Game-winning $\Longleftrightarrow$ Distinguishing

Def.: Ŝ and T̂ are restricted equivalent, denoted Ŝ $\stackrel{r}{\equiv}$ T̂, if the I/O behavior is identical as long as MBO =0.

Lemma (⇒) [Mau02]: If Ŝ $\stackrel{r}{\equiv}$ T̂, then, for every D,

$$\Delta_k^{\mathbf{D}}(\mathbf{S},\mathbf{T}) \le \nu_k^{\mathbf{D}}(\hat{\mathbf{S}}) \qquad (= \nu_k^{\mathbf{D}}(\hat{\mathbf{T}})).$$

In particular, $\Delta_k(\mathbf{S},\mathbf{T}) \le \nu_k(\hat{\mathbf{S}})$

Note: This lemma talks about a system as a mathematical object and is independent of the description language used for systems!

Game-winning $\Longleftrightarrow$ Distinguishing

Def.: Ŝ and T̂ are restricted equivalent, denoted Ŝ $\overset{r}{\equiv}$ T̂, if the I/O behavior is identical as long as MBO =0.

Lemma ($\Rightarrow$) [Mau02]: If Ŝ $\overset{r}{\equiv}$ T̂, then, for every D,

$$\Delta_k^{\mathbf{D}}(\mathbf{S},\mathbf{T}) \leq \nu_k^{\mathbf{D}}(\hat{\mathbf{S}}) \qquad (= \nu_k^{\mathbf{D}}(\hat{\mathbf{T}})).$$

In particular, $\Delta_k(\mathbf{S},\mathbf{T}) \leq \nu_k(\hat{\mathbf{S}})$

Game-winning $\Longleftrightarrow$ Distinguishing

Def.: $\hat{S}$ and $\hat{T}$ are restricted equivalent, denoted $\hat{S} \stackrel{r}{\equiv} \hat{T}$, if the I/O behavior is identical as long as MBO $=$0.

Lemma ($\Rightarrow$) [Mau02]: If $\hat{S} \stackrel{r}{\equiv} \hat{T}$, then, for every D,

$$\Delta_k^{D}(S,T) \leq \nu_k^{D}(\hat{S}) \qquad (= \nu_k^{D}(\hat{T})).$$

In particular, $\Delta_k(S,T) \leq \nu_k(\hat{S})$

Lemma ($\Leftarrow$) [MPR07]: Any S and T can be enhanced by MBOs to systems $\hat{S}$ and $\hat{T}$ such that $\hat{S} \stackrel{r}{\equiv} \hat{T}$ and, for every D,

$$\nu_k^{D}(\hat{S}) = \Delta_k^{D}(S,T)$$

Security amplification paradigm

Security amplification paradigm

Idea: Combine several mildly secure systems to obtain a highly secure system.

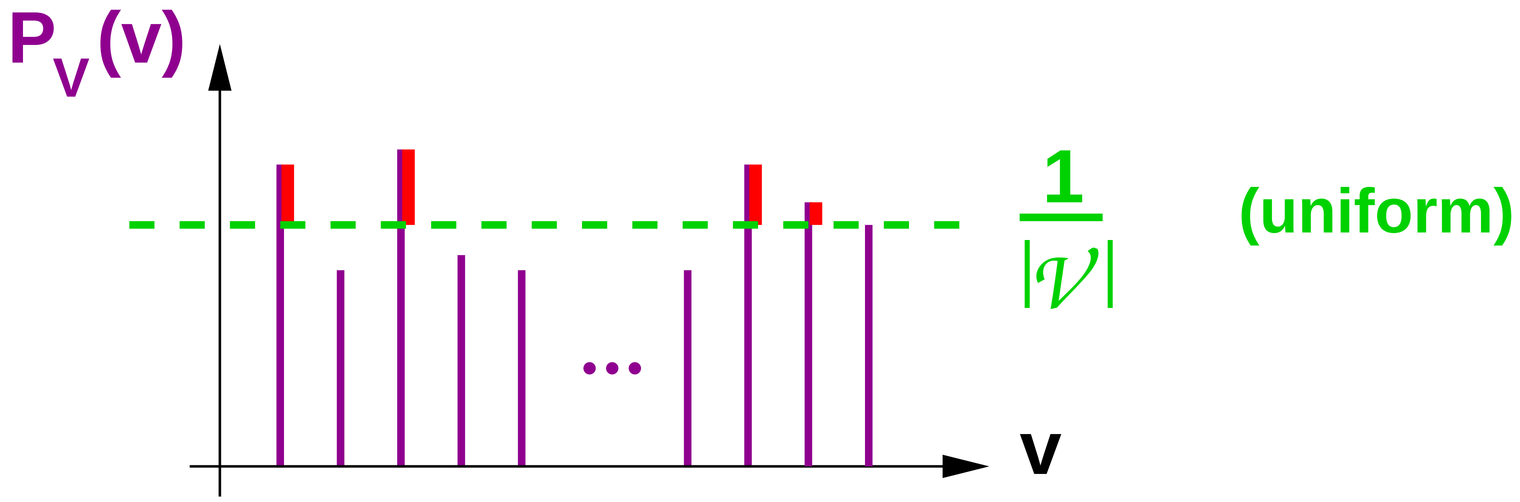
Example: XOR of mildly uniform independent keys yields a highly uniform key!

Security amplification paradigm

Idea: Combine several mildly secure systems to obtain a highly secure system.

Example: Cascade of mildly secure ciphers yields a highly secure cipher!

Distinguishing a RV V from a uniform RV U



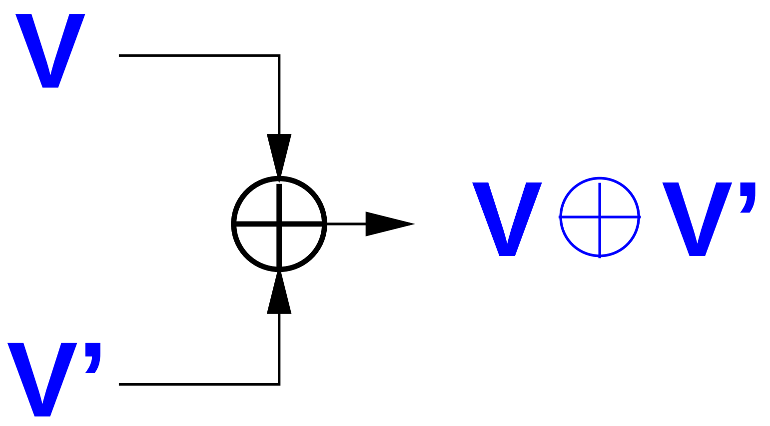
Statistical distance:

$$\mathbf{d}(\mathbf{V},\mathbf{U}) \;:=\; \frac{1}{2}\sum_{v\in\mathcal{V}}\left|P_{\mathbf{V}}(v) - \frac{1}{|\mathcal{V}|}\right| \quad \text{(sum of red quantities)}$$

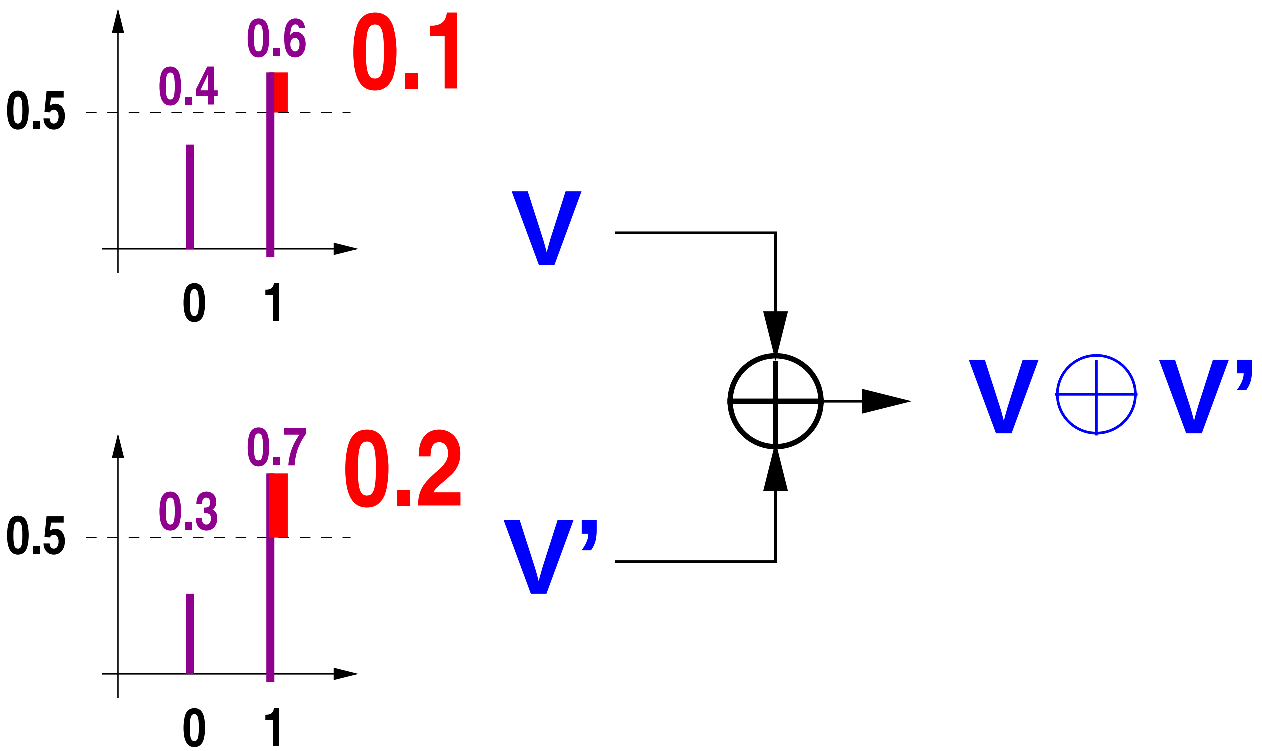
$$= \;\Delta(\mathbf{V},\mathbf{U})$$

Possible interpretation: $\mathbf{P}(\mathbf{V}=\mathbf{U}) \;=\; 1 - \mathbf{d}(\mathbf{V},\mathbf{U})$

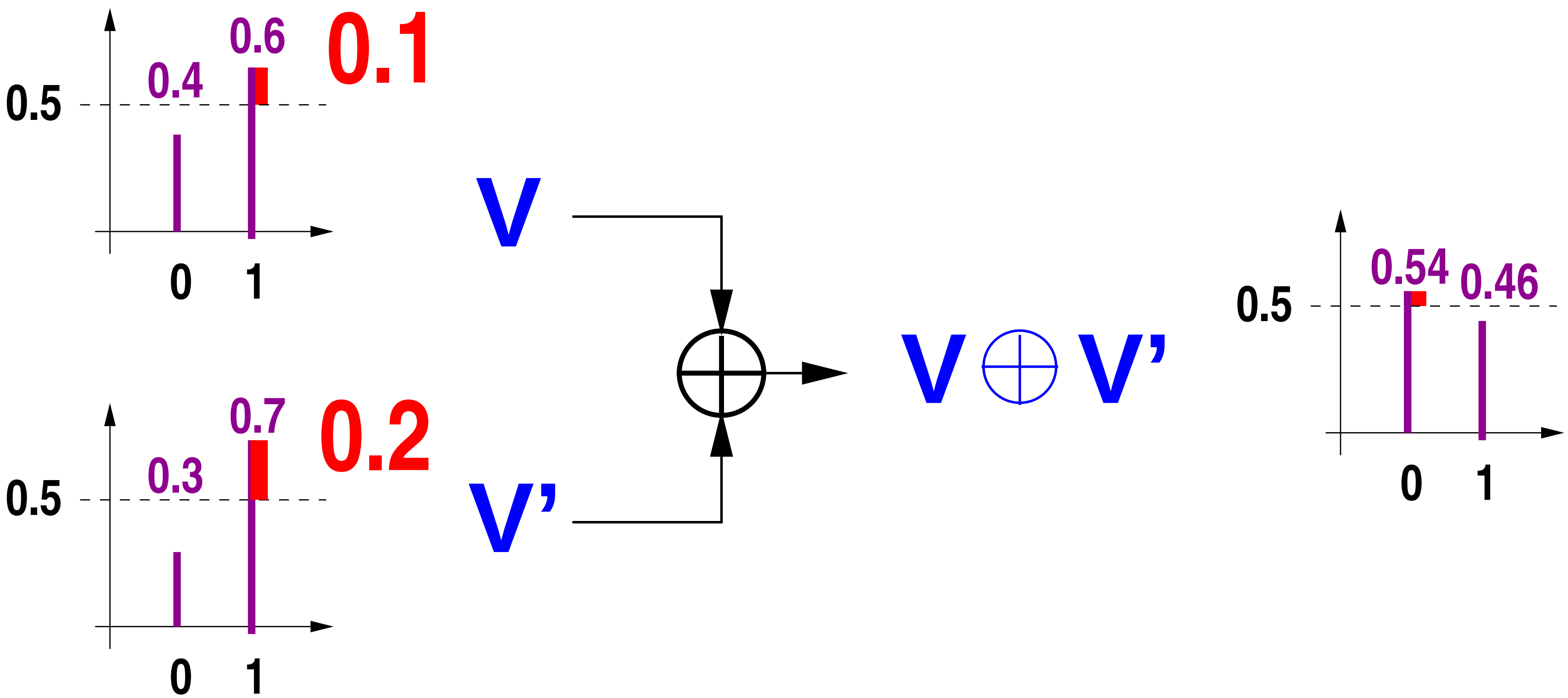
Product theorem for random variables



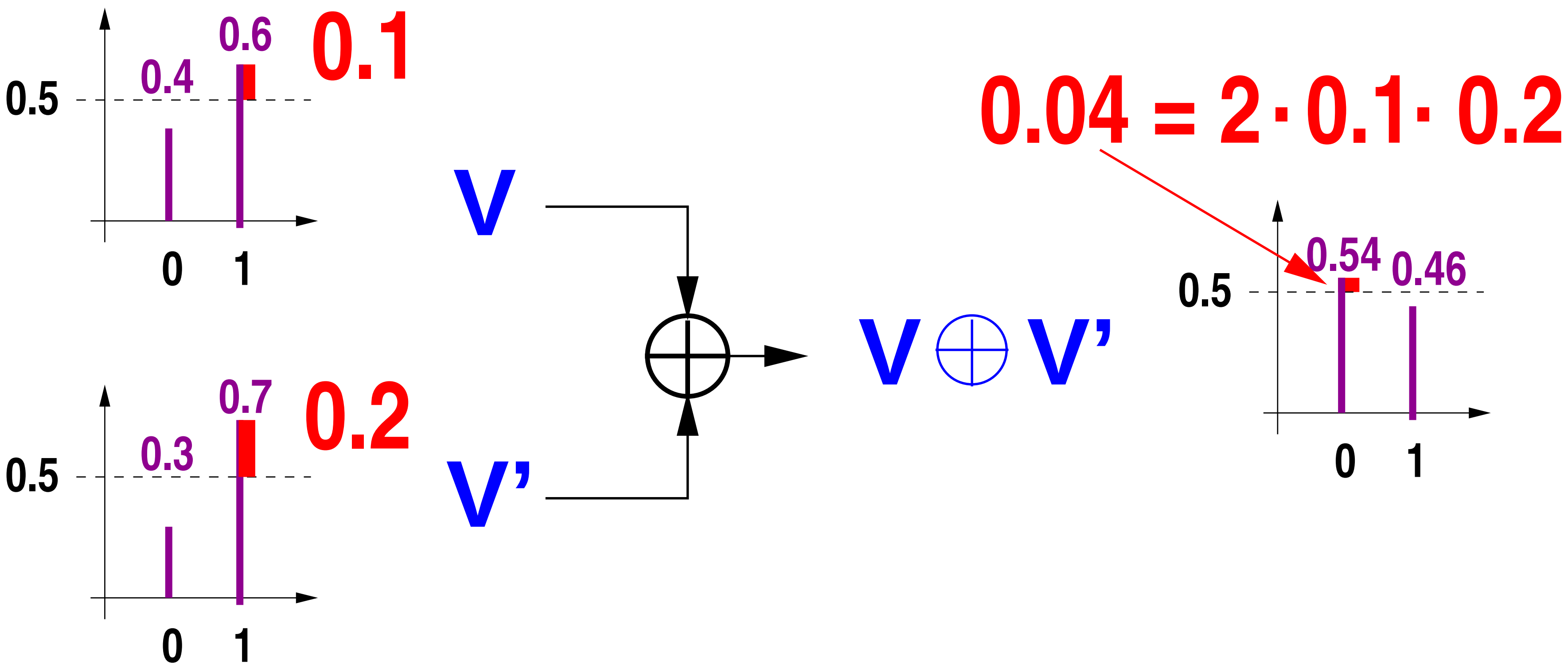
Product theorem for random variables



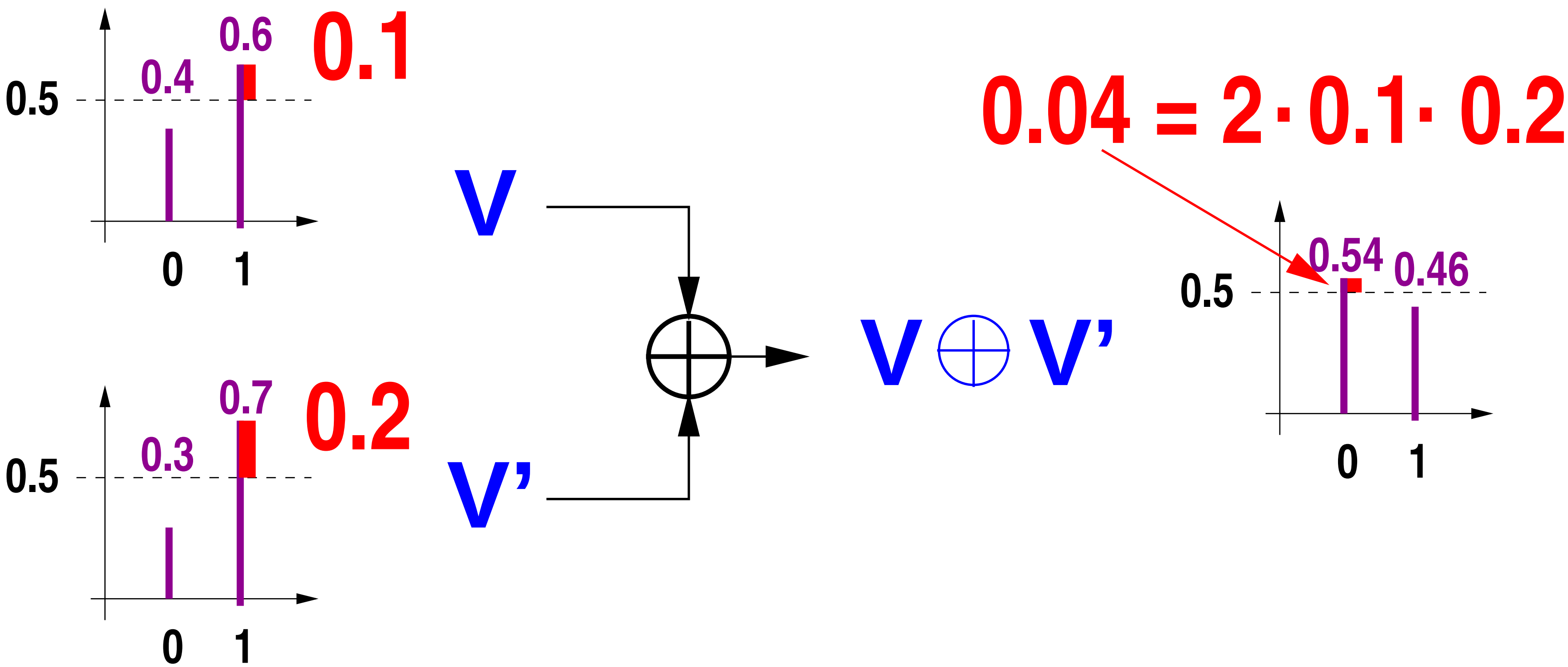
Product theorem for random variables



Product theorem for random variables

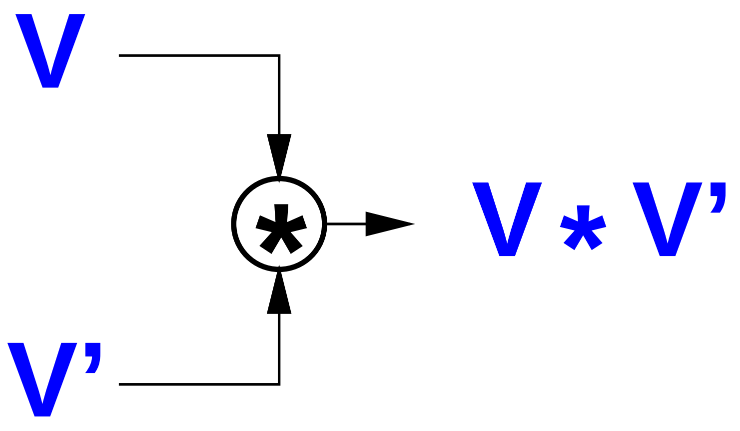


Product theorem for random variables



Theorem: $d(V \oplus V', U) \leq 2 \cdot d(V, U) \cdot d(V', U)$

Product theorem for random variables

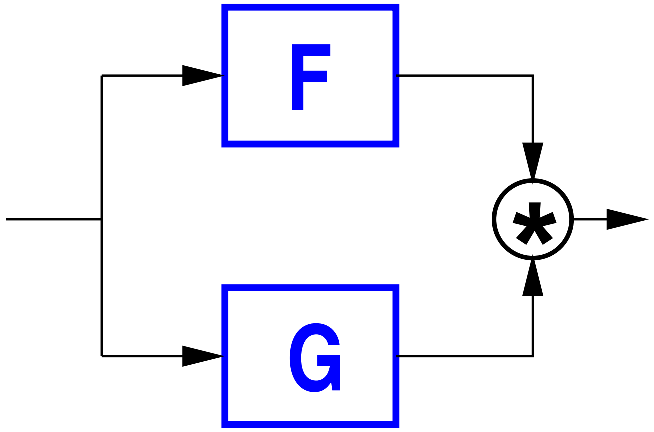


Theorem: $d(V \star V', U) \leq 2 \cdot d(V, U) \cdot d(V', U)$

for any quasi-group operation $\star$

Product theorems for systems ?

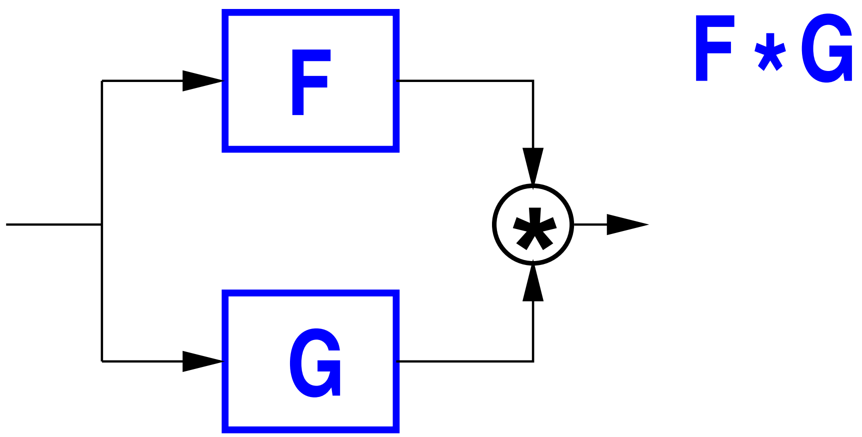
Let F and G be (possibly stateful) functions.



F*G

Product theorems for systems ? [MPR07]

Let F and G be (possibly stateful) functions.



Theorem: $\Delta_k(\mathbf{F} \star \mathbf{G}, \mathbf{R}) \;\leq\; \mathbf{2} \cdot \Delta_k(\mathbf{F}, \mathbf{R}) \cdot \Delta_k(\mathbf{G}, \mathbf{R})$

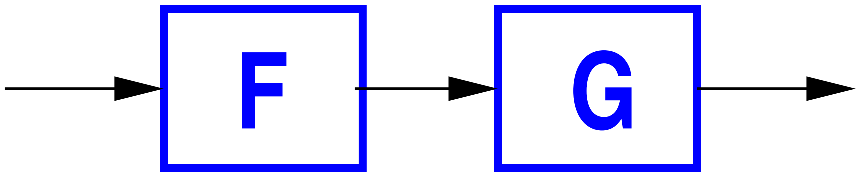
for any quasi-group operation $\star$.

($\mathbf{R}$ = uniform random function)

Product theorems for systems [MPR07]

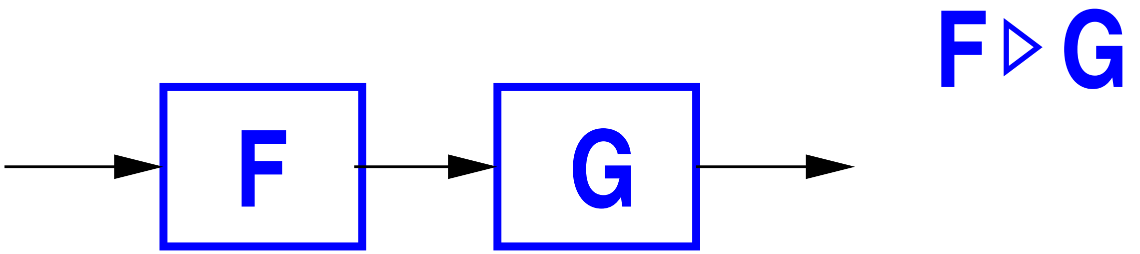
Let F and G be (possibly stateful) permutations.

$F \triangleright G$



Product theorems for systems [MPR07]

Let F and G be (possibly stateful) permutations.

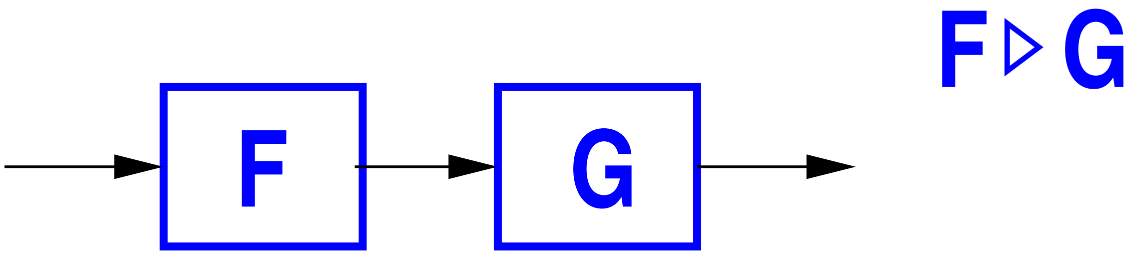


Theorem: $\Delta_k(\mathbf{F} \triangleright \mathbf{G}, \mathbf{P}) \leq \mathbf{2} \cdot \Delta_k(\mathbf{F}, \mathbf{P}) \cdot \Delta_k(\mathbf{G}, \mathbf{P})$

if G is stateless.

Product theorems for systems [MPR07]

Let F and G be (possibly stateful) permutations.



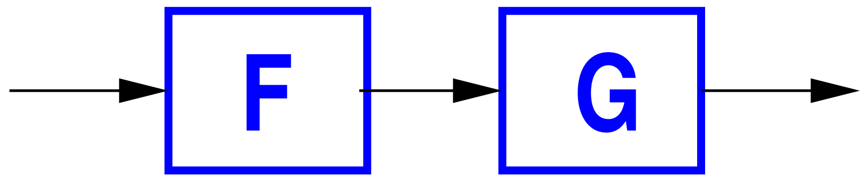
Theorem: $\Delta_k(\mathbf{F} \triangleright \mathbf{G}, \mathbf{P}) \leq \mathbf{2} \cdot \Delta_k(\mathbf{F}, \mathbf{P}) \cdot \Delta_k(\mathbf{G}, \mathbf{P})$

if G is stateless.

Special case: Vaudenay's decorrelation theorem

Product theorems for systems [MPR07]

Let F and G be (possibly stateful) permutations.



$\mathsf{F} \triangleright \mathsf{G}$

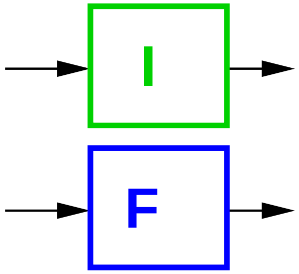
Theorem: $\Delta_k(\mathsf{F} \triangleright \mathsf{G}, \mathsf{P}) \leq \mathbf{2} \cdot \Delta_k(\mathsf{F}, \mathsf{P}) \cdot \Delta_k(\mathsf{G}, \mathsf{P})$

if G is stateless.

Special case: Vaudenay's decorrelation theorem

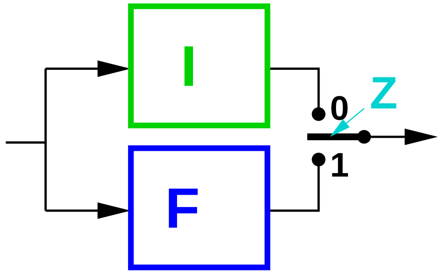
What is the general principle?

Neutralizing constructions [MPR07]



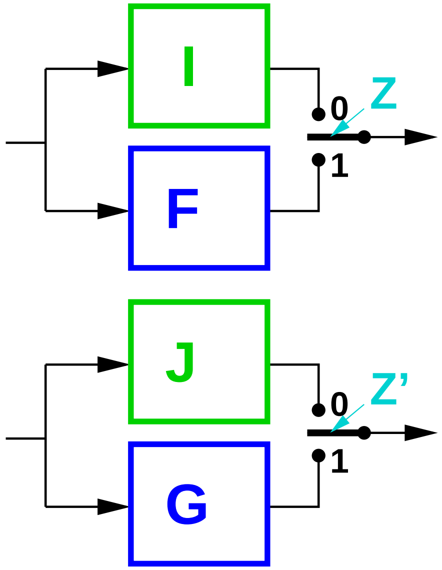
$$\Delta_k(\mathbf{F}, \mathbf{I})$$

Neutralizing constructions [MPR07]



$$\Delta_k(\mathbf{F}, \mathbf{I})$$

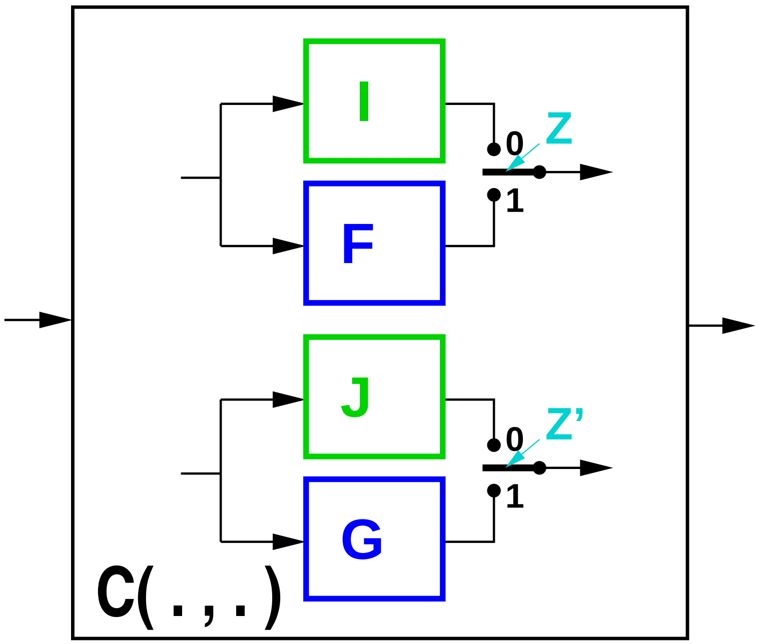
Neutralizing constructions [MPR07]



$$\Delta_k(\mathbf{F}, \mathbf{I})$$

$$\Delta_k(\mathbf{G}, \mathbf{J})$$

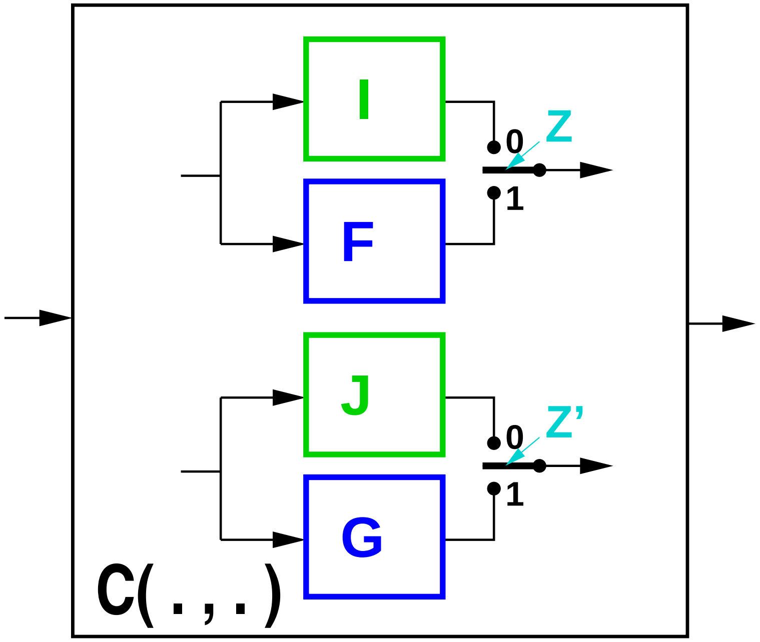
Neutralizing constructions [MPR07]



$$\Delta_k(F, I)$$

$$\Delta_k(G, J)$$

Neutralizing constructions [MPR07]

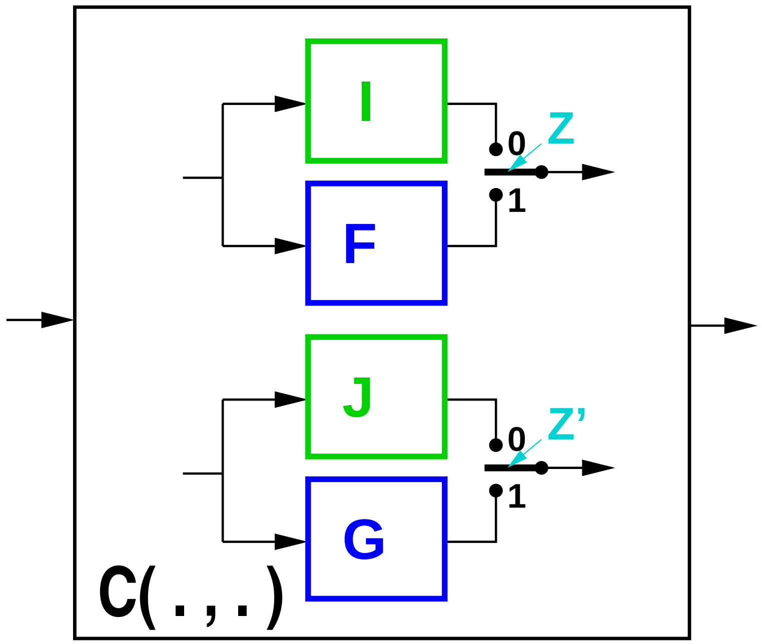


$\Delta_k($**F**, **I**$)$

$\Delta_k($**G**, **J**$)$

Def.: **C**$(.,.)$ **is neutralizing if C**$($**I**, **G**$) \equiv$ **C**$($**F**, **J**$) \equiv$ **C**$($**I**, **J**$) \equiv$ **Q**

Neutralizing constructions [MPR07]



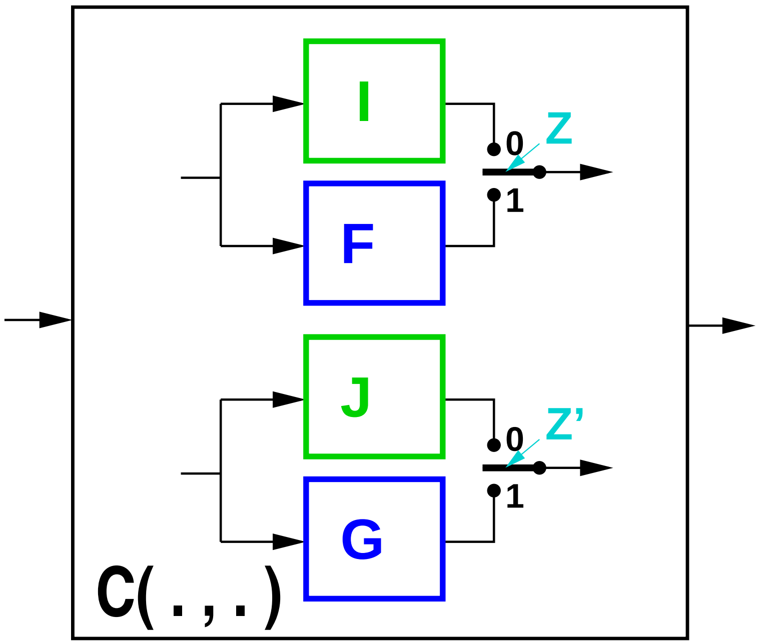
$\Delta_k($**F**, **I**$)$

$\Delta_k($**G**, **J**$)$

Def.: C$(.,.)$ is neutralizing if C$($I, G$) \equiv$ C$($F, J$) \equiv$ C$($I, J$) \equiv$ Q

Examples: C$($F, G$) =$ F $\star$ G, I $=$ J $=$ Q $=$ R

Neutralizing constructions [MPR07]



$\Delta_k(\mathbf{F}, \mathbf{I})$

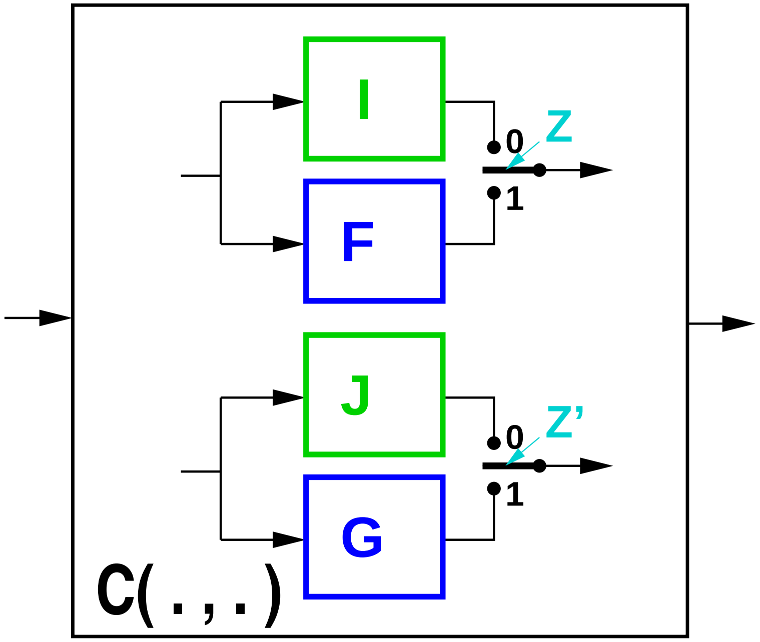
$\Delta_k(\mathbf{G}, \mathbf{J})$

Def.: $\mathbf{C}(., .)$ is neutralizing if $\mathbf{C}(\mathbf{I}, \mathbf{G}) \equiv \mathbf{C}(\mathbf{F}, \mathbf{J}) \equiv \mathbf{C}(\mathbf{I}, \mathbf{J}) \equiv \mathbf{Q}$

Examples: $\mathbf{C}(\mathbf{F}, \mathbf{G}) = \mathbf{F} \star \mathbf{G}$, $\quad \mathbf{I} = \mathbf{J} = \mathbf{Q} = \mathbf{R}$

$\mathbf{C}(\mathbf{F}, \mathbf{G}) = \mathbf{F} \triangleright \mathbf{G}$, $\quad \mathbf{I} = \mathbf{J} = \mathbf{Q} = \mathbf{P}$

Neutralizing constructions [MPR07]



$\Delta_k(\mathbf{F}, \mathbf{I})$

$\Delta_k(\mathbf{G}, \mathbf{J})$

Def.: $\mathbf{C}(.,.)$ is neutralizing if $\mathbf{C}(\mathbf{I}, \mathbf{G}) \equiv \mathbf{C}(\mathbf{F}, \mathbf{J}) \equiv \mathbf{C}(\mathbf{I}, \mathbf{J}) \equiv \mathbf{Q}$

Examples: $\mathbf{C}(\mathbf{F}, \mathbf{G}) = \mathbf{F} \star \mathbf{G}$, $\mathbf{I} = \mathbf{J} = \mathbf{Q} = \mathbf{R}$

$\mathbf{C}(\mathbf{F}, \mathbf{G}) = \mathbf{F} \triangleright \mathbf{G}$, $\mathbf{I} = \mathbf{J} = \mathbf{Q} = \mathbf{P}$

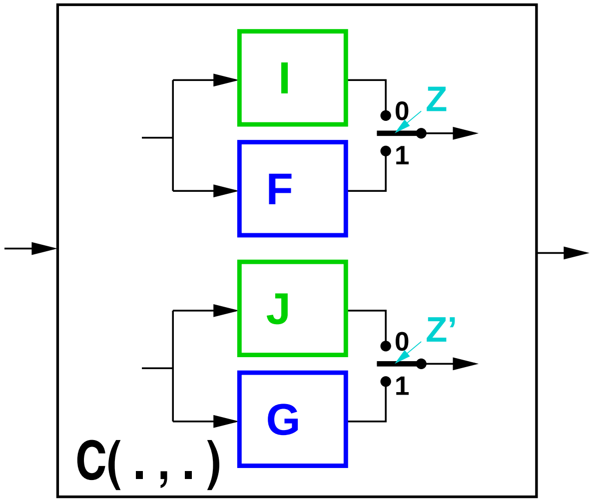
Theorem: $\Delta_k(\mathbf{C}(\mathbf{F}, \mathbf{G}), \mathbf{Q}) \leq 2 \cdot \Delta_k(\mathbf{F}, \mathbf{I}) \cdot \Delta_k(\mathbf{G}, \mathbf{J})$

Proof of the product theorem (1)

Theorem: $\Delta_k(\mathbf{C}(\mathbf{F}, \mathbf{G}), \mathbf{Q}) \leq \mathbf{2} \cdot \Delta_k(\mathbf{F}, \mathbf{I}) \cdot \Delta_k(\mathbf{G}, \mathbf{J})$

Proof of the product theorem (1)

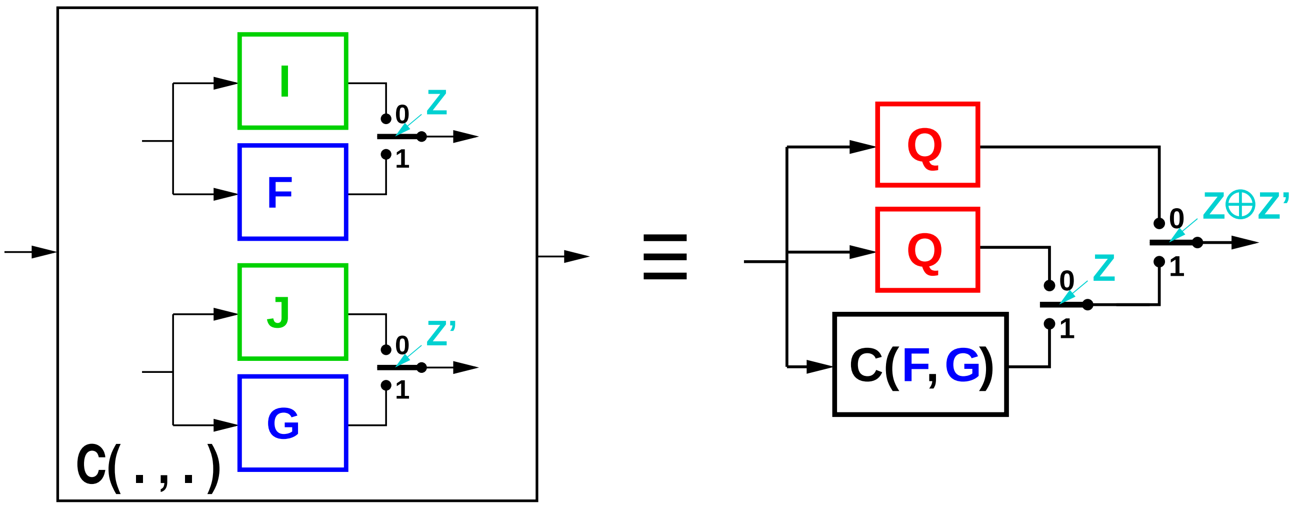
Theorem: $\Delta_k(\mathbf{C}(\mathbf{F},\mathbf{G}),\mathbf{Q}) \leq \mathbf{2}\cdot\Delta_k(\mathbf{F},\mathbf{I})\cdot\Delta_k(\mathbf{G},\mathbf{J})$



$\mathbf{C}(\mathbf{I}/\mathbf{F},\mathbf{J}/\mathbf{G})$

Proof of the product theorem (1)

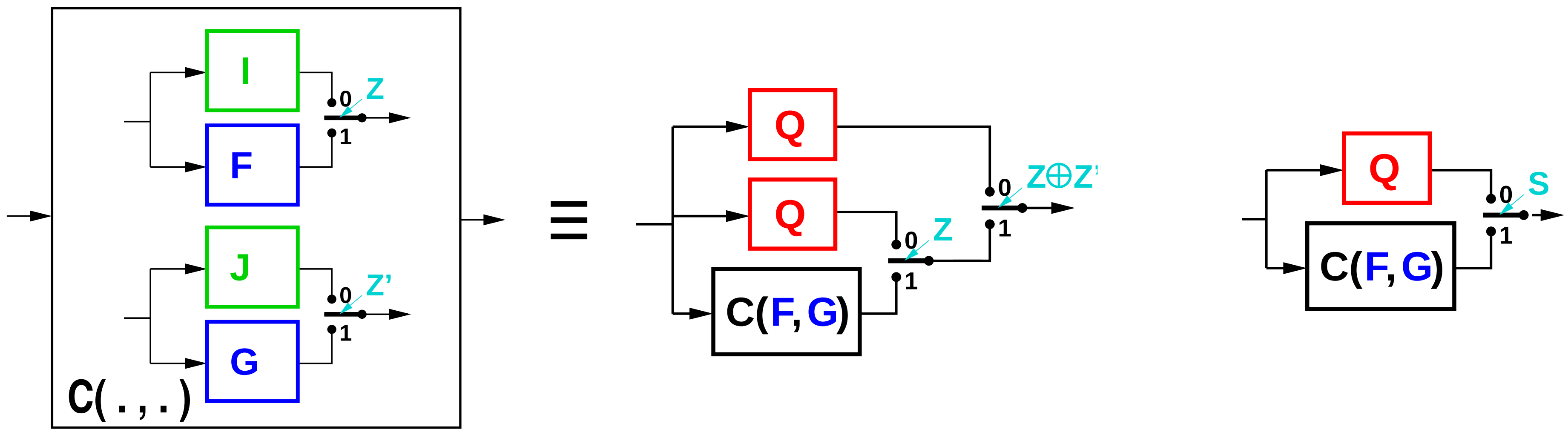
Theorem: $\Delta_k(\mathbf{C}(\mathbf{F},\mathbf{G}),\mathbf{Q}) \leq \mathbf{2}\cdot\Delta_k(\mathbf{F},\mathbf{I})\cdot\Delta_k(\mathbf{G},\mathbf{J})$



$\mathbf{C}(\mathbf{I}/\mathbf{F},\mathbf{J}/\mathbf{G})$

Proof of the product theorem (1)

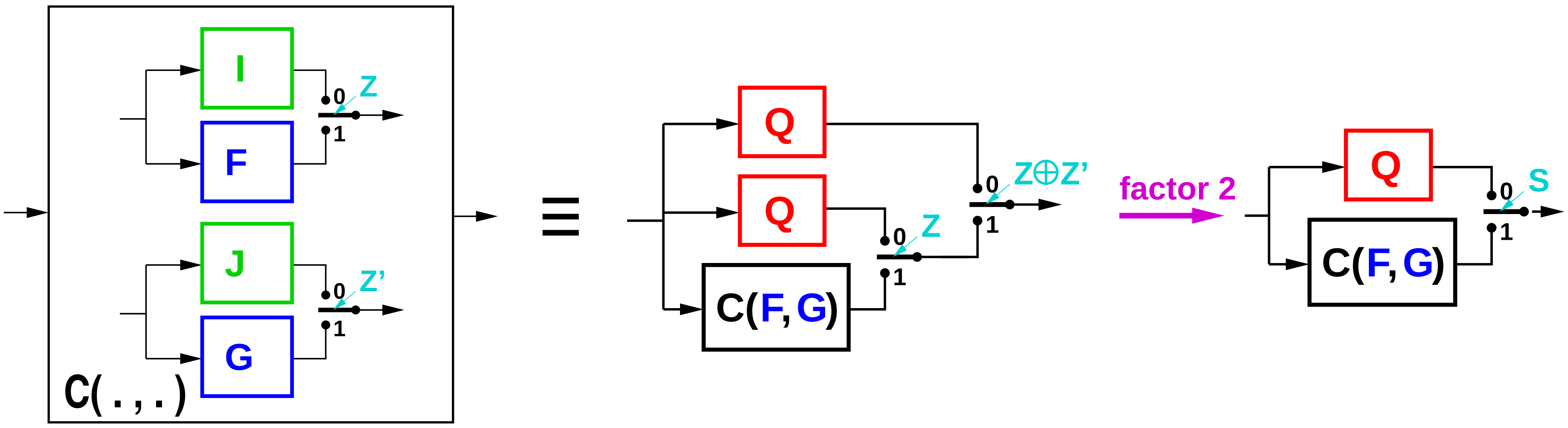
Theorem: $\Delta_k(\mathbf{C}(\mathbf{F},\mathbf{G}),\mathbf{Q}) \leq \mathbf{2}\cdot\Delta_k(\mathbf{F},\mathbf{I})\cdot\Delta_k(\mathbf{G},\mathbf{J})$



$\mathbf{C}(\mathbf{I}/\mathbf{F},\mathbf{J}/\mathbf{G})$

Proof of the product theorem (1)

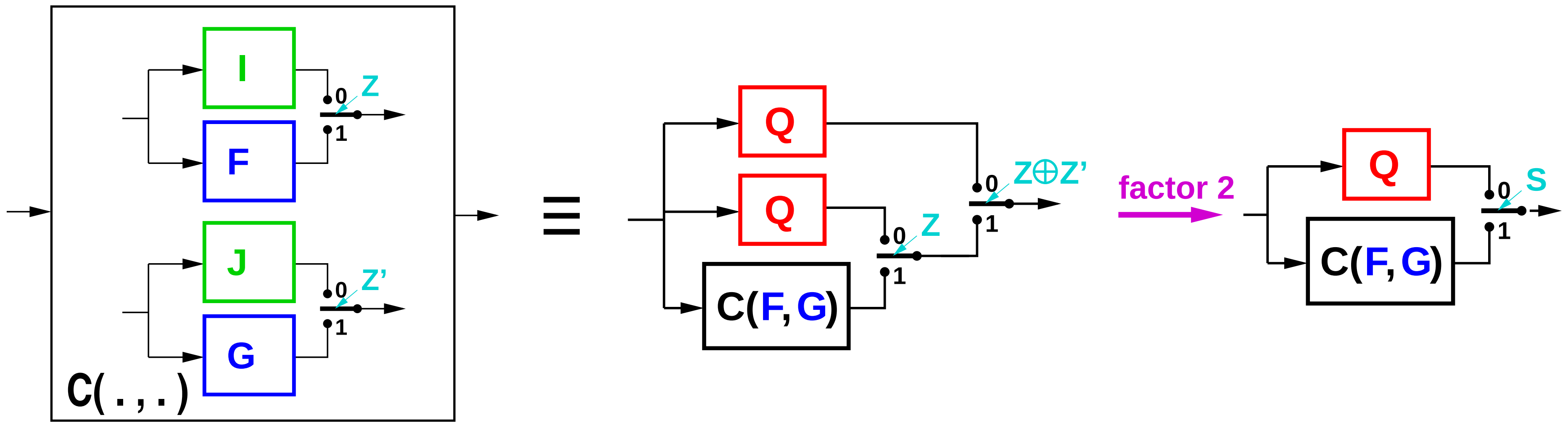
Theorem: $\Delta_k(\mathbf{C}(\mathbf{F},\mathbf{G}),\mathbf{Q}) \leq \mathbf{2}\cdot\Delta_k(\mathbf{F},\mathbf{I})\cdot\Delta_k(\mathbf{G},\mathbf{J})$



$\mathbf{C}(\mathbf{I}/\mathbf{F},\mathbf{J}/\mathbf{G})$

Proof of the product theorem (1)

Theorem: $\Delta_k(\mathbf{C}(\mathbf{F},\mathbf{G}),\mathbf{Q}) \;\leq\; \mathbf{2}\cdot\Delta_k(\mathbf{F},\mathbf{I})\cdot\Delta_k(\mathbf{G},\mathbf{J})$



$\mathbf{C}(\mathbf{I}/\mathbf{F},\mathbf{J}/\mathbf{G})$

$\Delta_k(\mathbf{C}(\mathbf{F},\mathbf{G}),\mathbf{Q}) = \mathbf{2}\cdot$ **adv. in guessing** $\mathbf{Z}\oplus\mathbf{Z}'$ **in** $\mathbf{C}(\mathbf{I}/\mathbf{F},\mathbf{J}/\mathbf{G})$

Game-winning $\Longleftrightarrow$ Indistinguishability

Def.: $\hat{\mathsf{S}}$ and $\hat{\mathsf{T}}$ are restricted equivalent, denoted $\hat{\mathsf{S}} \stackrel{r}{\equiv} \hat{\mathsf{T}}$, if the I/O behavior is identical as long as MBO $=$0.

Lemma ($\Rightarrow$) [Mau02]: If $\hat{\mathsf{S}} \stackrel{r}{\equiv} \hat{\mathsf{T}}$, then, for every D,

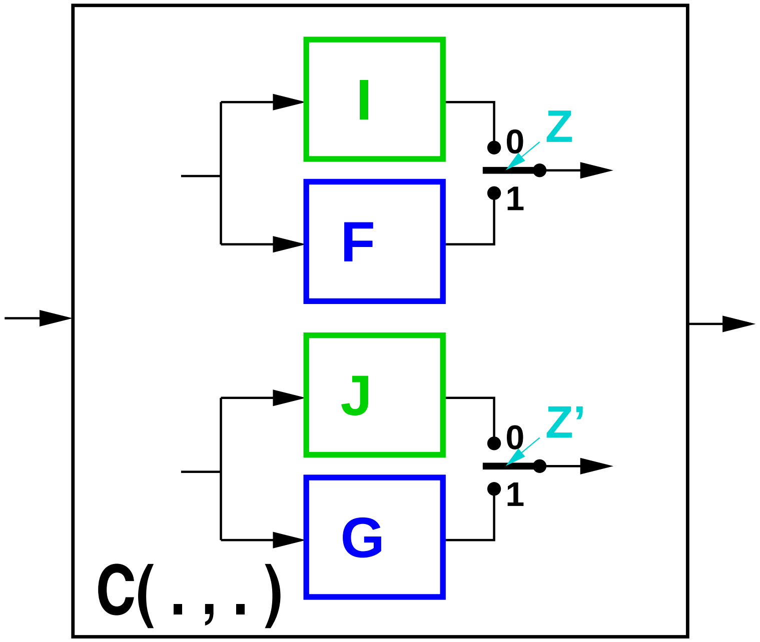
$$\Delta_k^{\mathsf{D}}(\mathsf{S},\mathsf{T}) \leq \nu_k^{\mathsf{D}}(\hat{\mathsf{S}}) \qquad (= \nu_k^{\mathsf{D}}(\hat{\mathsf{T}})\ ).$$

In particular, $\Delta_k(\mathsf{S},\mathsf{T}) \leq \nu_k(\hat{\mathsf{S}})$

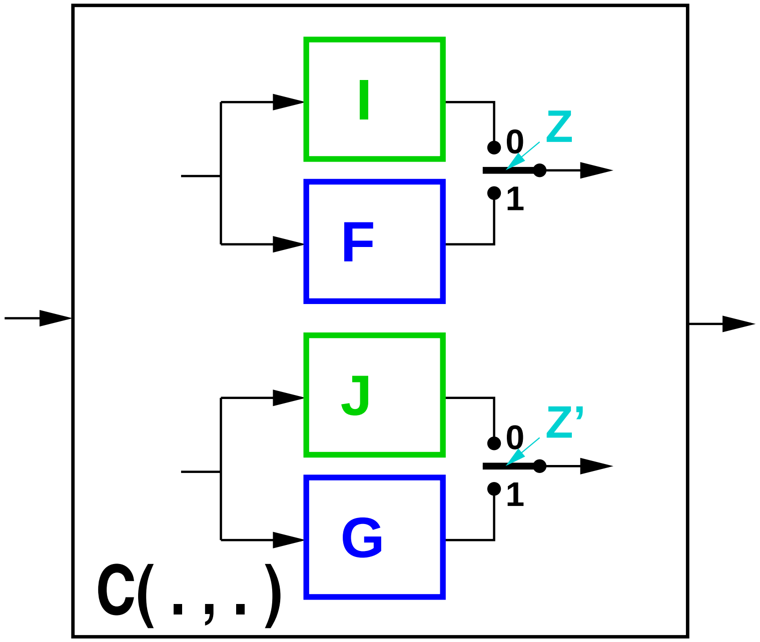
Lemma ($\Leftarrow$) [MPR07]: Any S and T can be enhanced by MBOs to systems $\hat{\mathsf{S}}$ and $\hat{\mathsf{T}}$ such that $\hat{\mathsf{S}} \stackrel{r}{\equiv} \hat{\mathsf{T}}$ and, for every D,

$$\nu_k^{\mathsf{D}}(\hat{\mathsf{S}}) = \Delta_k^{\mathsf{D}}(\mathsf{S},\mathsf{T})$$

Proof of the product theorem (2)

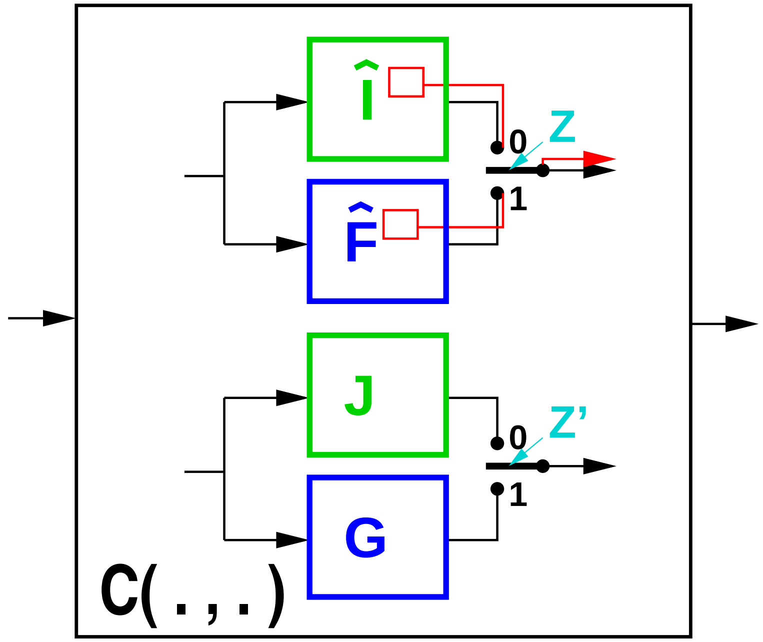


Proof of the product theorem (2)



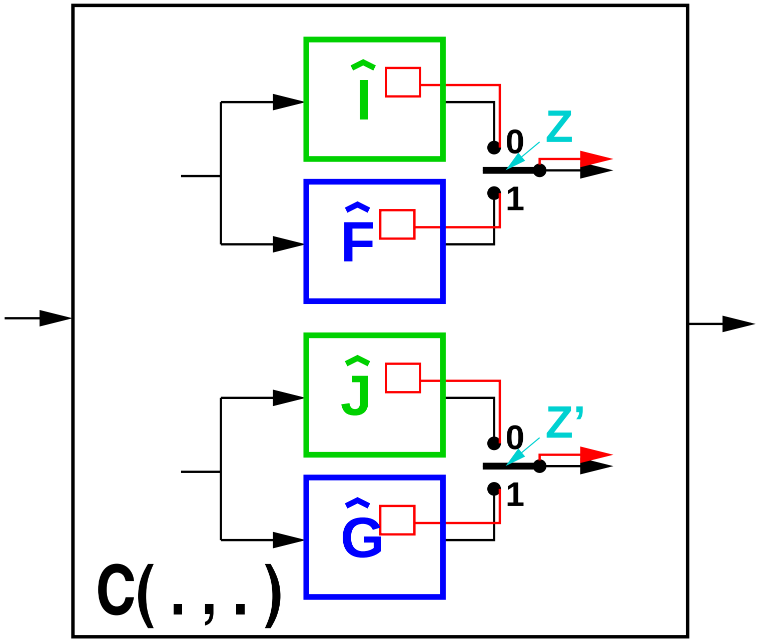
- **Task: Guess $Z \oplus Z'$**

Proof of the product theorem (2)



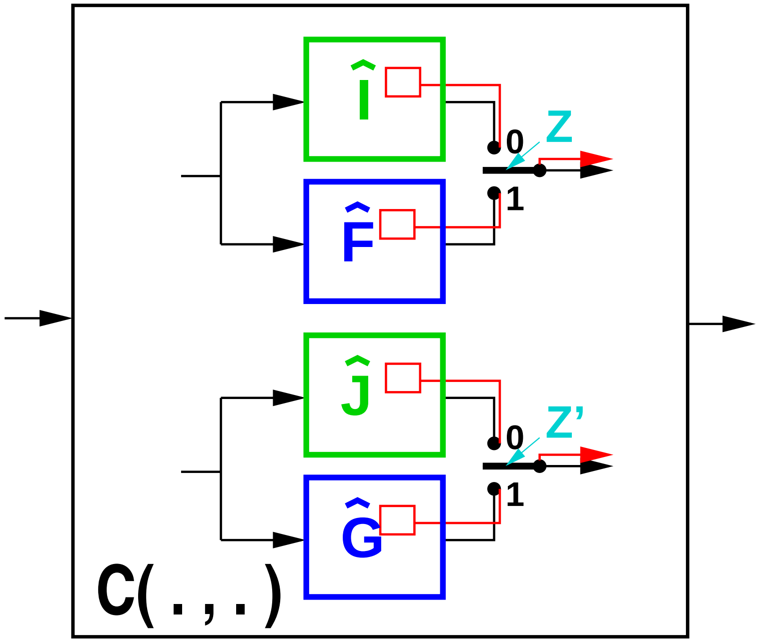
- **Task: Guess $Z \oplus Z'$**
- **Define MBOs and give the guesser access to them.**

Proof of the product theorem (2)



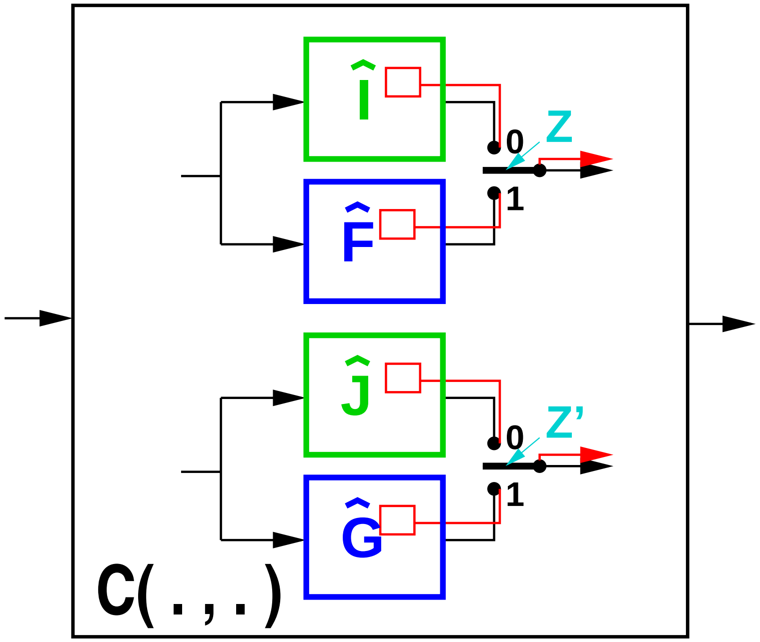
- Task: Guess $Z \oplus Z'$
- Define MBOs and give the guesser access to them.

Proof of the product theorem (2)



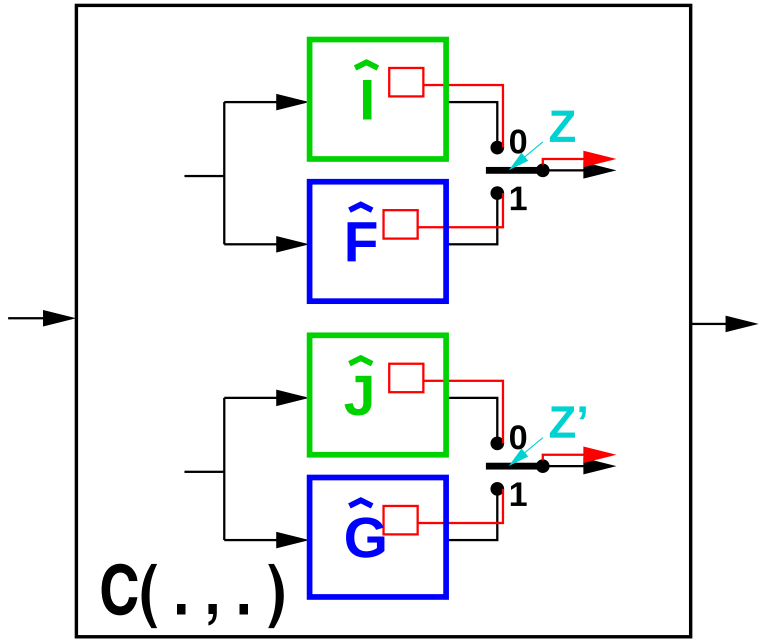
- **Task: Guess Z $\oplus$ Z$'$**
- **Define MBOs and give the guesser access to them.**
- **Game 1 not won $\Rightarrow$ advantage 0 in guessing Z**

Proof of the product theorem (2)



- **Task: Guess $Z \oplus Z'$**
- **Define MBOs and give the guesser access to them.**
- **Game 2 not won $\Rightarrow$ advantage 0 in guessing Z'**

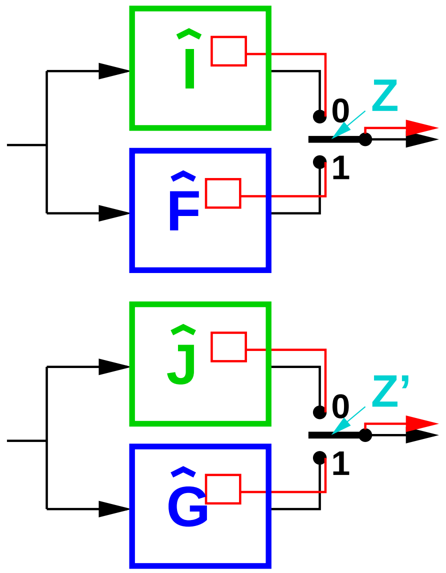
Proof of the product theorem (2)



- **Task: Guess $Z \oplus Z'$**
- **Define MBOs and give the guesser access to them.**
- **Game 2 not won $\Rightarrow$ advantage 0 in guessing Z'**
- **Game 1 or game 2 not won $\Rightarrow$ adv. 0 in guessing $Z \oplus Z'$.**

  $\Rightarrow$ advantage $\leq$ probability that both games won

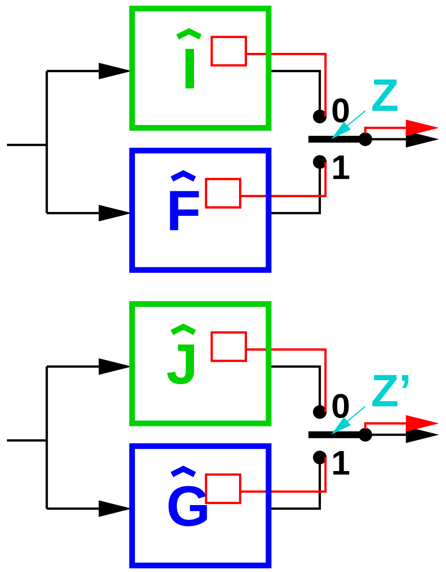
Proof of the product theorem (2)



- Task: Guess $Z \oplus Z'$
- Define MBOs and give the guesser access to them.
- Game 2 not won $\Rightarrow$ advantage 0 in guessing Z'
- Game 1 or game 2 not won $\Rightarrow$ adv. 0 in guessing $Z \oplus Z'$.

  $\Rightarrow$ advantage $\leq$ probability that both games won
- We give the guesser direct access to the 2 games.

Proof of the product theorem (2)



- Task: Guess $\mathsf{Z} \oplus \mathsf{Z}'$
- Define MBOs and give the guesser access to them.
- Game 2 not won $\Rightarrow$ advantage 0 in guessing Z'
- Game 1 or game 2 not won $\Rightarrow$ adv. 0 in guessing $\mathsf{Z} \oplus \mathsf{Z}'$.

  $\Rightarrow$ advantage $\leq$ probability that both games won
- We give the guesser direct access to the 2 games.
- Prob. of winning $=$ product of winning games 1 and 2.

  $= \Delta_k(\mathsf{F}, \mathsf{I}) \cdot \Delta_k(\mathsf{G}, \mathsf{J})$ q.e.d.

Computational indisting. amplification

Theorem [M-Tessaro09]: The previous statements hold also for computational indistinguishability.

Computational indisting. amplification

Theorem [M-Tessaro09]: **The previous statements hold also for computational indistinguishability.**

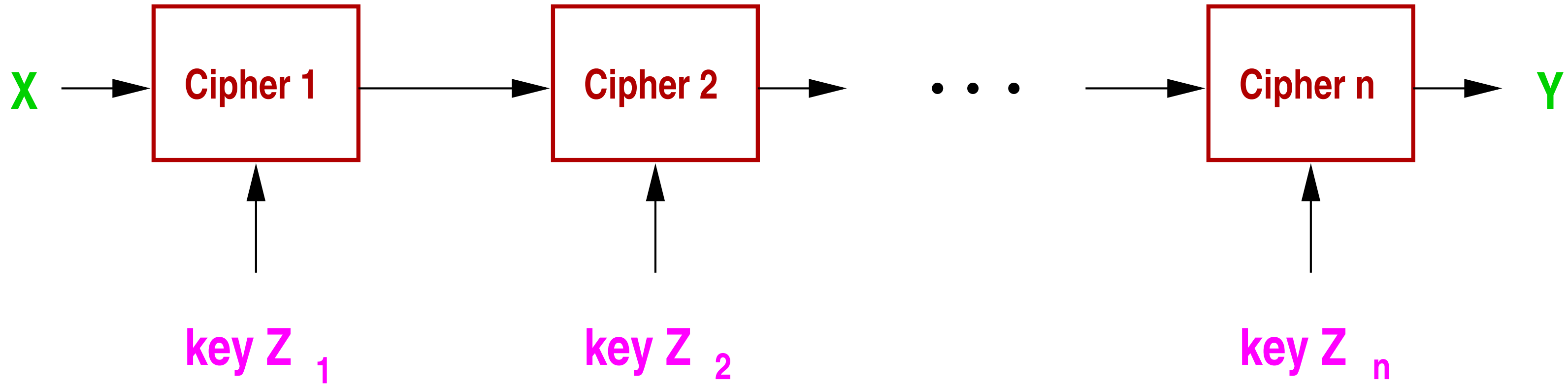
$\mathcal{E}$ **= class of efficient distinguishers (e.g. poly-time)**

Computational indisting. amplification

Theorem [M-Tessaro09]: The previous statements hold also for computational indistinguishability.

$\mathcal{E}$ **= class of efficient distinguishers (e.g. poly-time)**

Example:



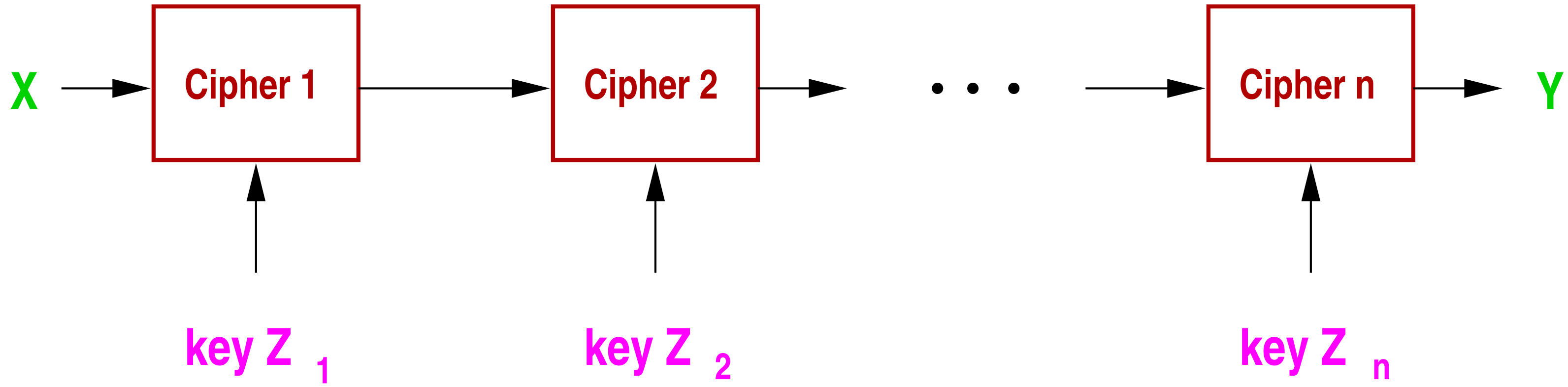
$$\Delta^{\mathcal{E}}(\mathbf{C}_i, \mathbf{P}) \leq \epsilon \;\Rightarrow\; \Delta^{\mathcal{E}}(\mathbf{C}_1 \cdots \mathbf{C}_n, \mathbf{P}) \approx 2^{n-1}\epsilon^n + \gamma$$

Computational indisting. amplification

Theorem [M-Tessaro09]: The previous statements hold also for computational indistinguishability.

$\mathcal{E}$ = class of efficient distinguishers (e.g. poly-time)

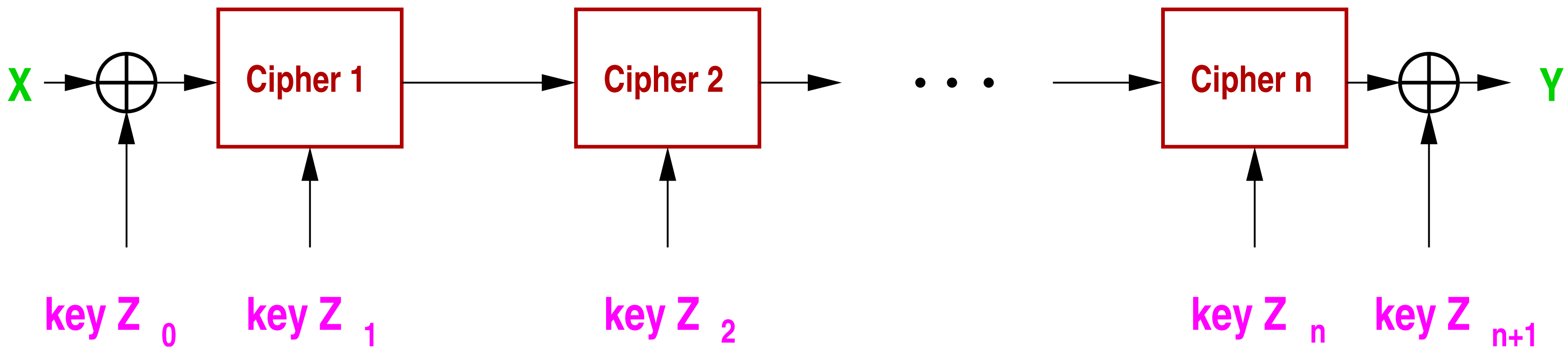
Example:



$$\Delta^{\mathcal{E}}(\mathbf{C}_i, \mathbf{P}) \leq \epsilon \;\Rightarrow\; \Delta^{\mathcal{E}}(\mathbf{C}_1 \cdots \mathbf{C}_n, \mathbf{P}) \approx 2^{n-1}\epsilon^n + \gamma$$

Problem: Amplification only if $\epsilon < 0.5$.

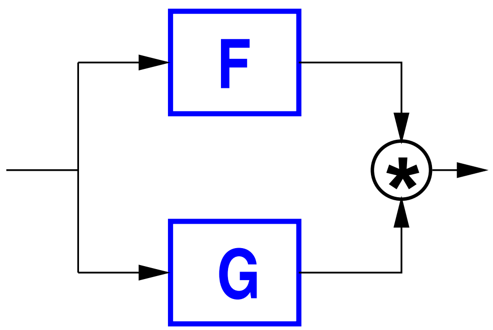
Strong security amplification



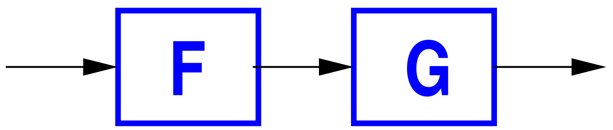
Theorem [MT09]:

$$\Delta^{\mathcal{E}}(\mathbf{C}_i, \mathbf{P}) \leq \epsilon \;\Rightarrow\; \Delta^{\mathcal{E}}(\oplus \mathbf{C}_1 \cdots \mathbf{C}_n \oplus, \mathbf{P}) \approx \epsilon^n + \gamma$$

Indistinguishability amplification: Type 2



F ⋆ G



F ▷ G

Theorem: $\Delta_k(\mathbf{F} \star \mathbf{G}, \mathbf{R}) \;\leq\; \Delta_k^{\mathrm{NA}}(\mathbf{F}, \mathbf{R}) + \Delta_k^{\mathrm{NA}}(\mathbf{G}, \mathbf{R}).$

Theorem: $\Delta_k(\mathbf{F} \triangleright \mathbf{G}, \mathbf{P}) \;\leq\; \Delta_k^{\mathrm{NA}}(\mathbf{F}, \mathbf{P}) + \Delta_k^{\mathrm{NA}}(\mathbf{G}, \mathbf{P}).$