Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Information Security
& Cryptography

Computational Indistinguishability Amplification: Tight Product Theorems for System Composition

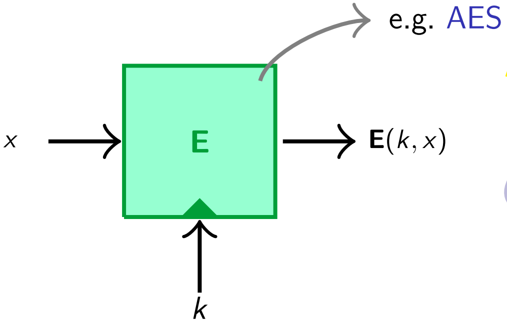
Ueli Maurer **Stefano Tessaro**

ETH Zurich

CRYPTO 2009
August 18th, 2009

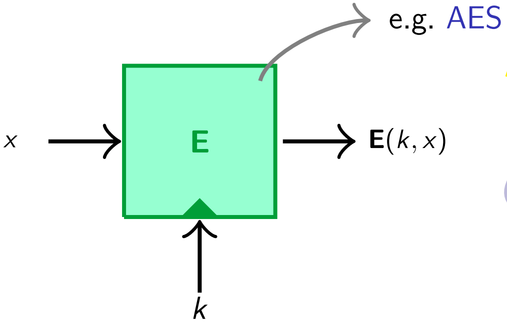
Motivation: Block Ciphers

Block cipher



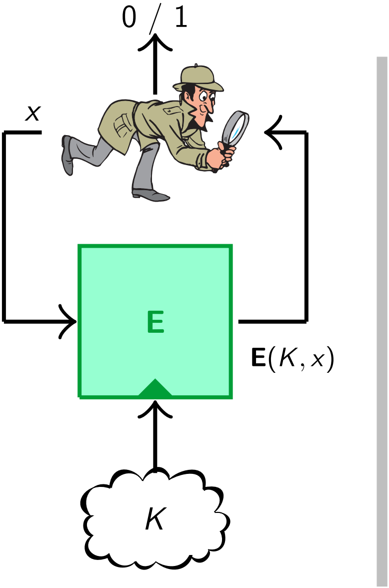
Motivation: Block Ciphers

Block cipher

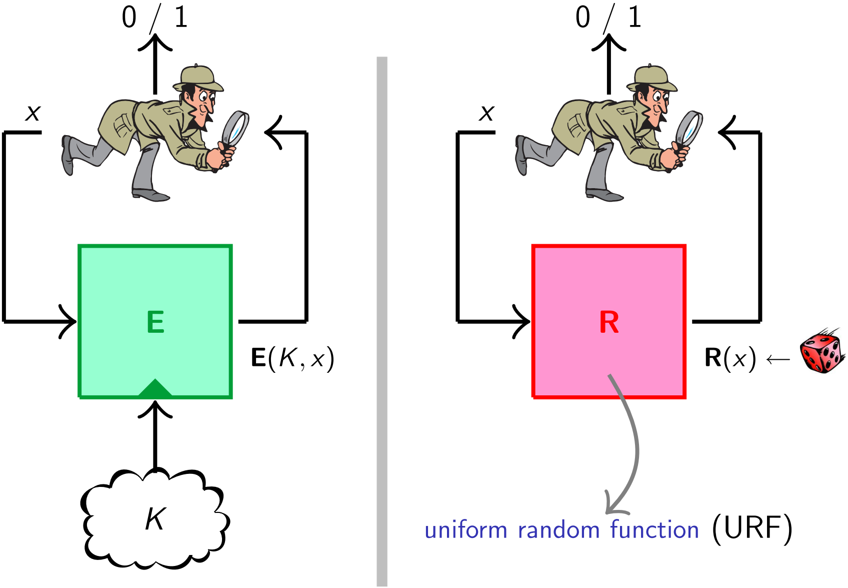


Security definition: **Computational Indistinguishability**

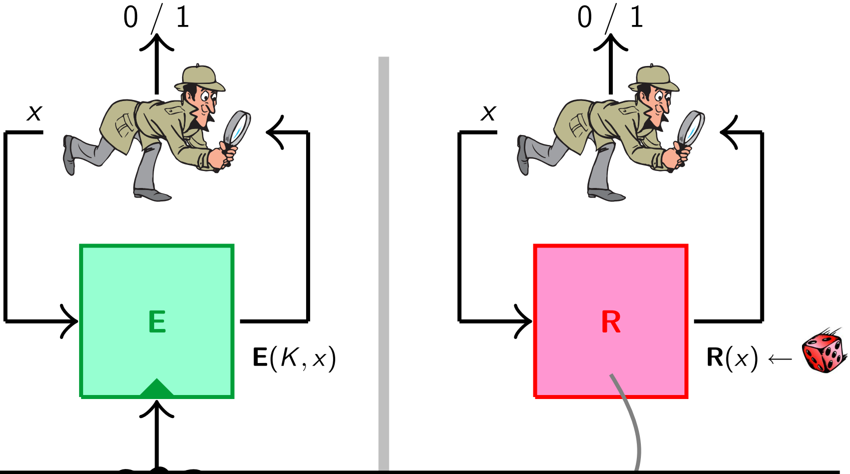
Motivation: Block Ciphers – Pseudorandom Functions



Motivation: Block Ciphers – Pseudorandom Functions



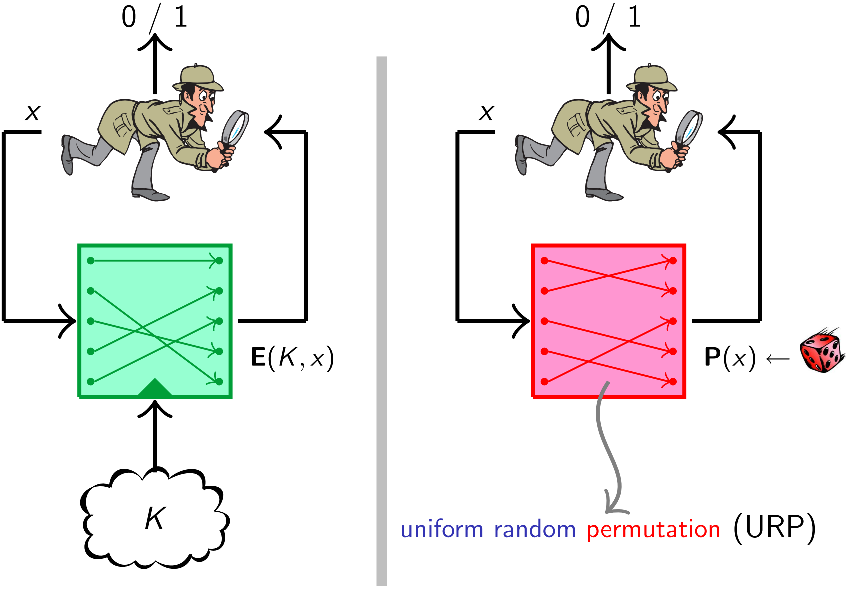
Motivation: Block Ciphers – Pseudorandom Functions



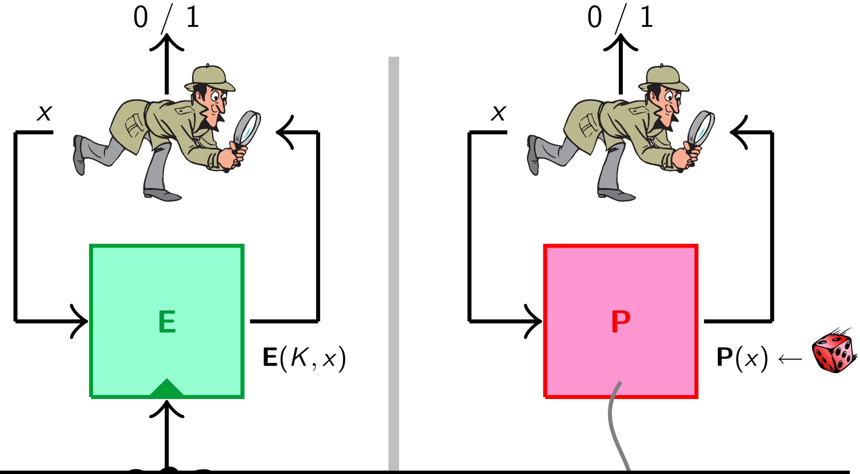
E **PRF**: $\forall$ efficient **D**:

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{R}) = \left|\Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{R}) = 1]\right| = \text{negl}$$

Motivation: Block Ciphers – Pseudorandom Permutations



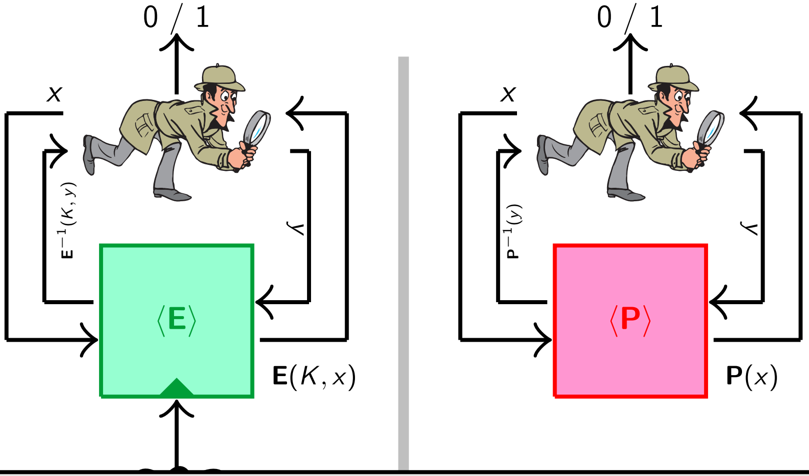
Motivation: Block Ciphers – Pseudorandom Permutations



E **PRP**: $\forall$ efficient **D**:

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{P}) = \left| \Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{P}) = 1] \right| = \text{negl}$$

Motivation: Block Ciphers – ↔-Pseudorandom Permutations



E ↔**PRP**: ∀ efficient **D**:

$$\Delta^{\mathbf{D}}(\langle \mathbf{E}_K \rangle, \langle \mathbf{P} \rangle) = \left| \Pr[\mathbf{D}(\langle \mathbf{E}_K \rangle) = 1] - \Pr[\mathbf{D}(\langle \mathbf{P} \rangle) = 1] \right| = \mathsf{negl}$$

Weakening Security Assumptions

E **PRF**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{R}) = \left|\Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{R}) = 1]\right| = \text{negl}$$

E **PRP**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{P}) = \left|\Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{P}) = 1]\right| = \text{negl}$$

E $\leftrightarrow$**PRP**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\langle \mathbf{E}_K \rangle, \langle \mathbf{P} \rangle) = \left|\Pr[\mathbf{D}(\langle \mathbf{E}_K \rangle) = 1] - \Pr[\mathbf{D}(\langle \mathbf{P} \rangle) = 1]\right| = \text{negl}$$

Weakening Security Assumptions

E **PRP**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{P}) = \Big|\Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{P}) = 1]\Big| = \mathrm{negl}$$

Weakening Security Assumptions

E **PRP**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{P}) = \Big| \Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{P}) = 1] \Big| = \text{negl}$$

Weakening Security Assumptions

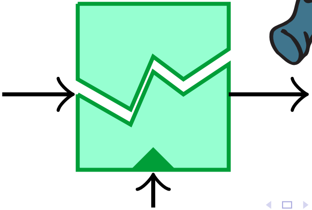
E **PRP**: $\forall$ efficient **D** :

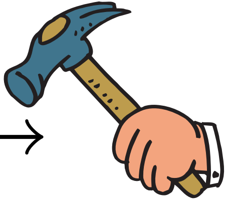
$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{P}) = \left| \Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{P}) = 1] \right| = \text{negl}$$

Weakening Security Assumptions

E **PRP**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{P}) = \left| \Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{P}) = 1] \right| = \text{negl}$$



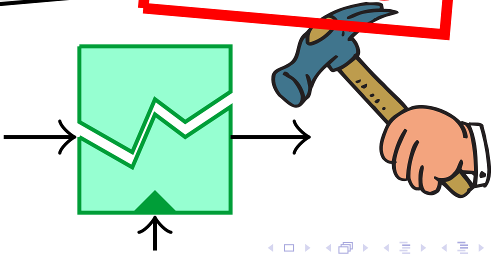


Weakening Security Assumptions

E **PRP**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{P}) = \left|\Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{P}) = 1]\right| = \text{negl}$$

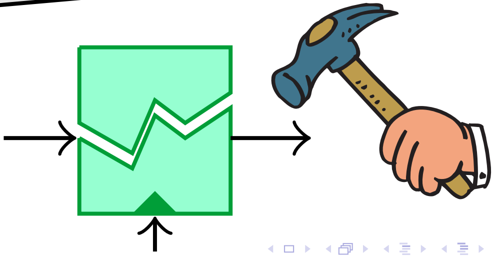
STRONG



Weakening Security Assumptions

E **PRP**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{P}) = \left| \Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{P}) = 1] \right| \leq \varepsilon$$

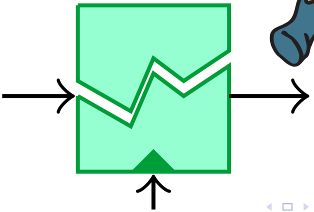


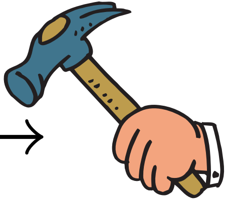
Weakening Security Assumptions

$\varepsilon = \text{negl},$

E PRP: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{P}) = \left|\Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{P}) = 1]\right| \leq \varepsilon$$



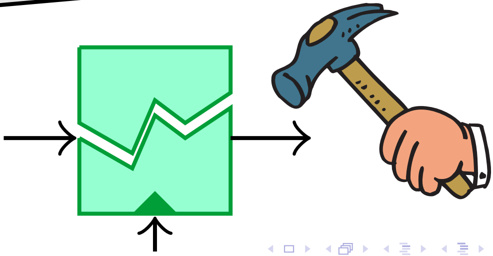


Weakening Security Assumptions

$\varepsilon = \text{negl}, \;\; 0.75$

E **PRP**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{P}) = \left| \Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{P}) = 1] \right| \leq \varepsilon$$

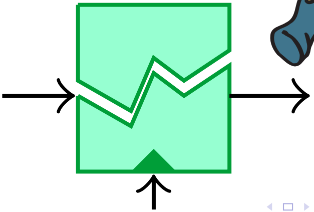


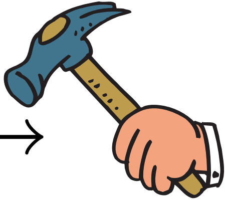
Weakening Security Assumptions

$$\varepsilon = \text{negl},\ 0.75,\ 1 - \frac{1}{\text{poly}},\ \ldots$$

E **PRP**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{P}) = \left|\Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{P}) = 1]\right| \leq \varepsilon$$



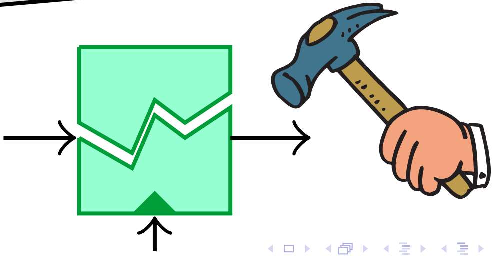


Weakening Security Assumptions

$$\varepsilon = \text{negl},\ \ 0.75,\ \ 1 - \frac{1}{\text{poly}},\ \ \ldots$$

E ε-**PRP**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{P}) = \left|\Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{P}) = 1]\right| \le \varepsilon$$



Weakening Security Assumptions

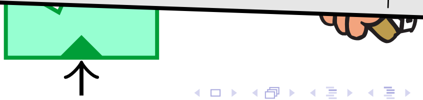
$$\varepsilon = \text{negl},\ 0.75,\ 1 - \frac{1}{\text{poly}},\ \ldots$$

E ε-**PRP**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{P}) = \left|\Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{P}) = 1]\right| \leq \varepsilon$$

E ε-$\longleftrightarrow$**PRP**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\langle\mathbf{E}_K\rangle, \langle\mathbf{P}\rangle) = \left|\Pr[\mathbf{D}(\langle\mathbf{E}_K\rangle) = 1] - \Pr[\mathbf{D}(\langle\mathbf{P}\rangle) = 1]\right| \leq \varepsilon$$



Weakening Security Assumptions

$\varepsilon = \text{negl},\ 0.75,\ 1 - \frac{1}{\text{poly}},\ \ldots$

E ε-**PRF**: $\forall$ efficient **D** 

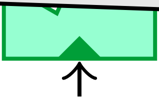
$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{R}) = \left|\Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{R}) = 1]\right| \leq \varepsilon$$

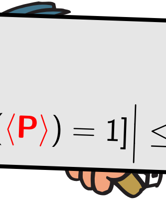
E ε-**PRP**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\mathbf{E}_K, \mathbf{P}) = \left|\Pr[\mathbf{D}(\mathbf{E}_K) = 1] - \Pr[\mathbf{D}(\mathbf{P}) = 1]\right| \leq \varepsilon$$

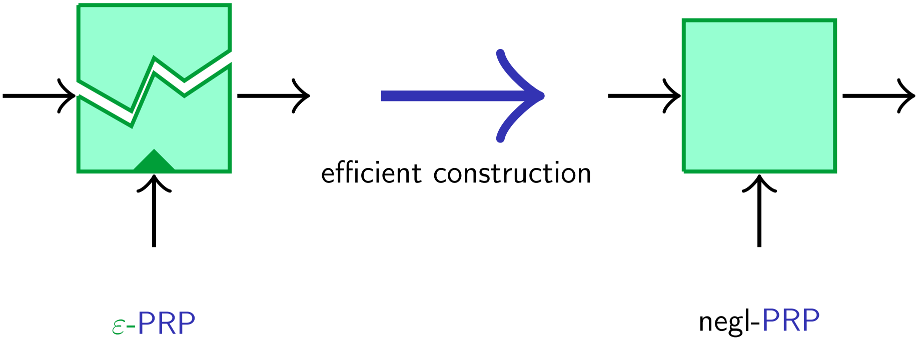
E ε-$\longleftrightarrow$**PRP**: $\forall$ efficient **D** :

$$\Delta^{\mathbf{D}}(\langle\mathbf{E}_K\rangle, \langle\mathbf{P}\rangle) = \left|\Pr[\mathbf{D}(\langle\mathbf{E}_K\rangle) = 1] - \Pr[\mathbf{D}(\langle\mathbf{P}\rangle) = 1]\right| \leq \varepsilon$$

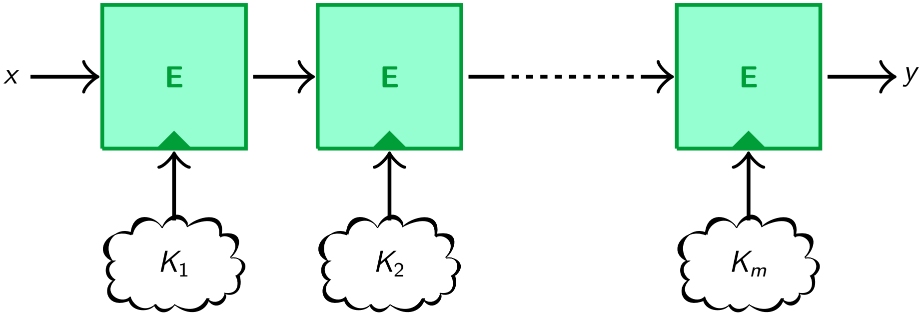




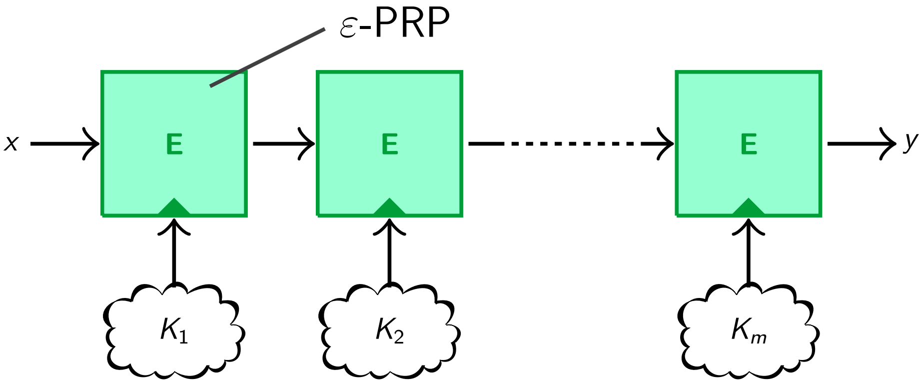
Security Amplification



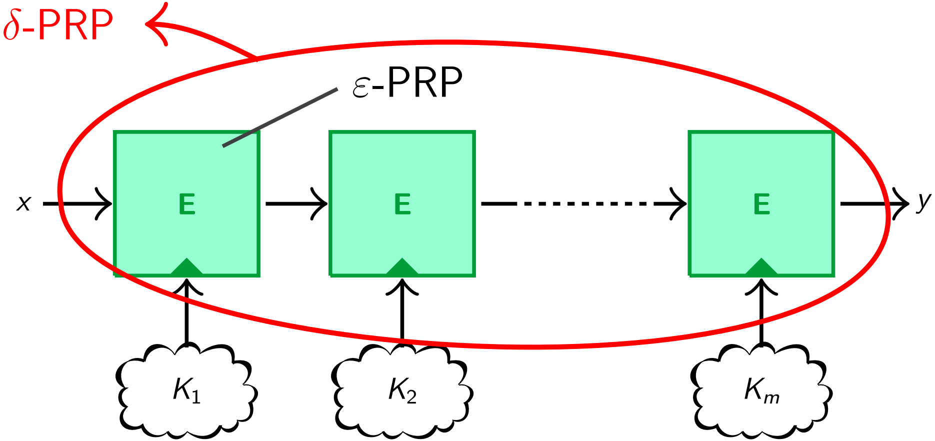
Cascaded Encryption



Cascaded Encryption

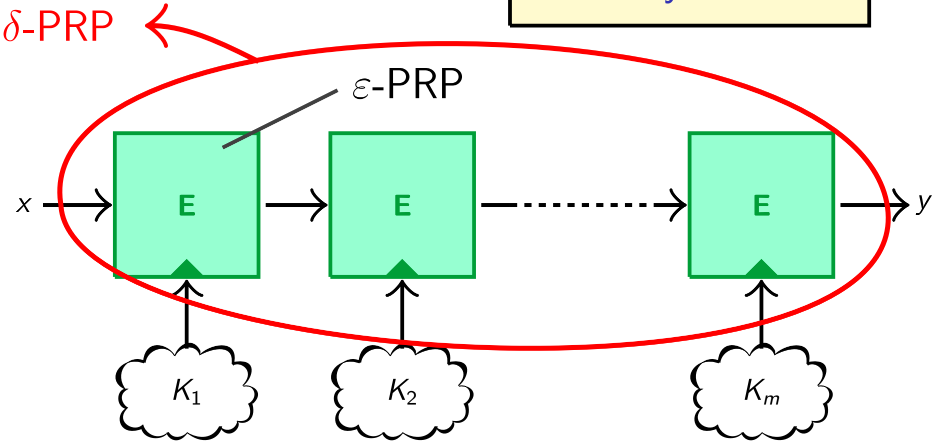


Cascaded Encryption



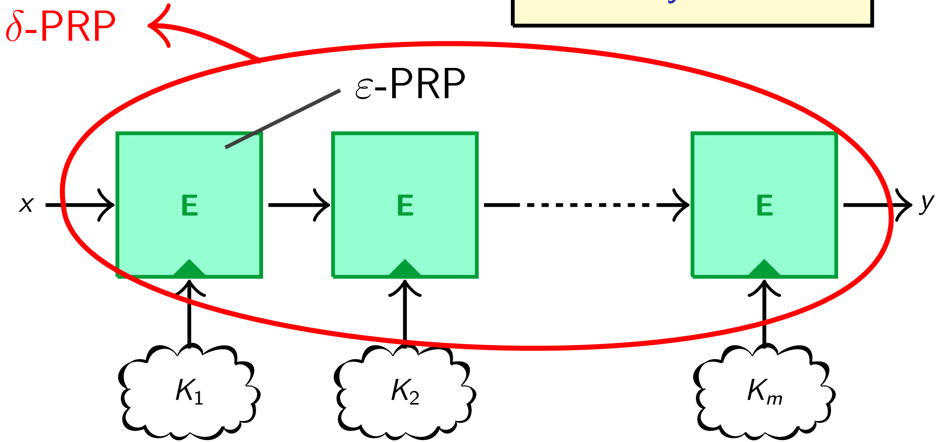
Cascaded Encryption

Ideally: $\delta \approx \varepsilon^m$



Cascaded Encryption

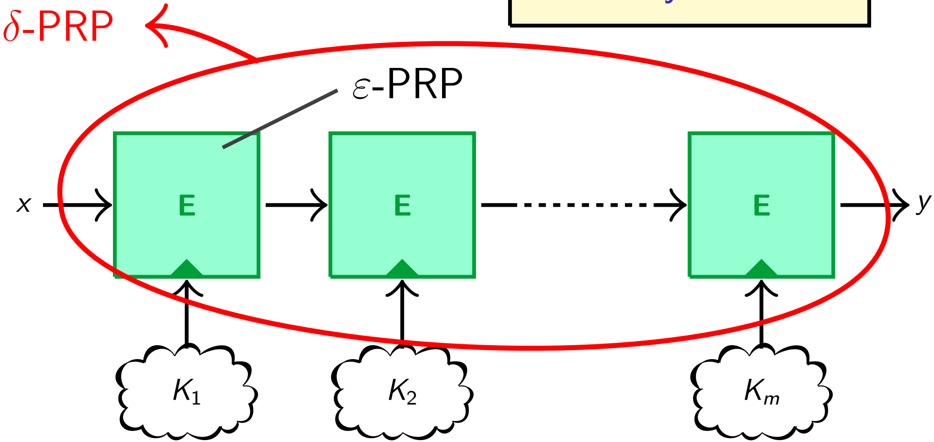
Ideally: $\delta \approx \varepsilon^m$



ideal/IT settings [BR06,MG09,V98,MPR07]

Cascaded Encryption

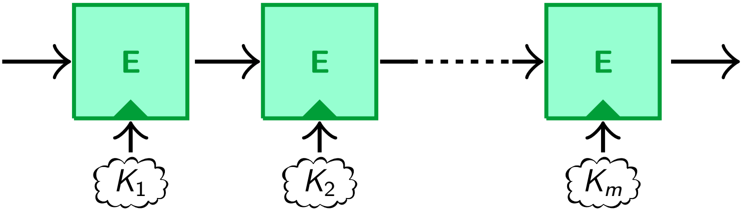
Ideally: $\delta \approx \varepsilon^m$



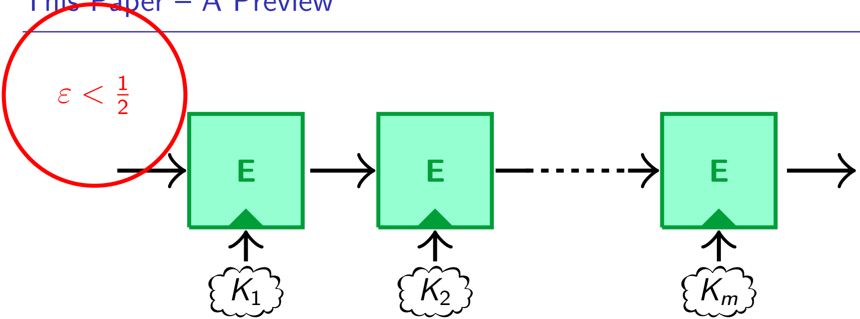
ideal/IT settings [BR06,MG09,V98,MPR07]

[LR86,M99]: small $m \implies$ **no** security amplification

This Paper – A Preview



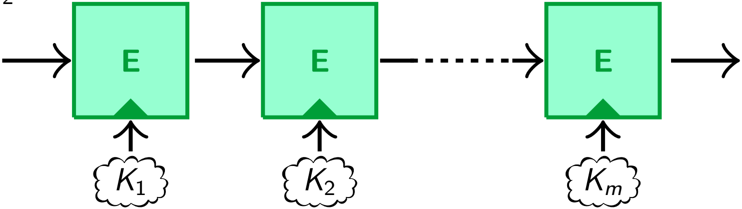
This Paper – A Preview



This Paper – A Preview

$$\delta = 2^{m-1} \cdot \varepsilon^m + \text{negl}$$

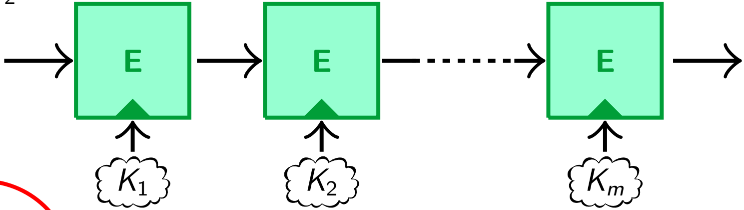
$\varepsilon < \frac{1}{2}$



This Paper – A Preview

$$\delta = 2^{m-1} \cdot \varepsilon^m + \text{negl}$$

$\varepsilon < \frac{1}{2}$

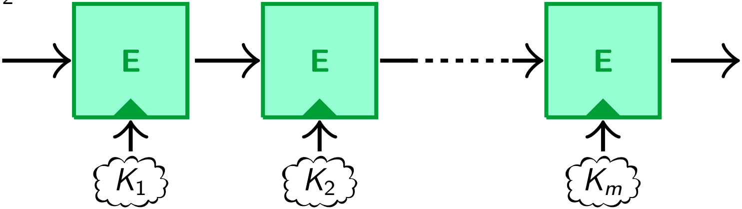


$\frac{1}{2} \leq \varepsilon < 1$

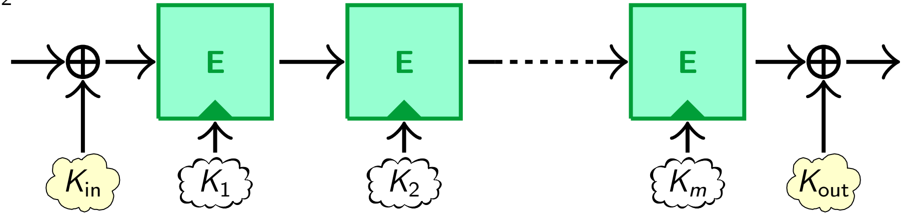
This Paper – A Preview

$$\delta = 2^{m-1} \cdot \varepsilon^m + \text{negl}$$

$\varepsilon < \frac{1}{2}$



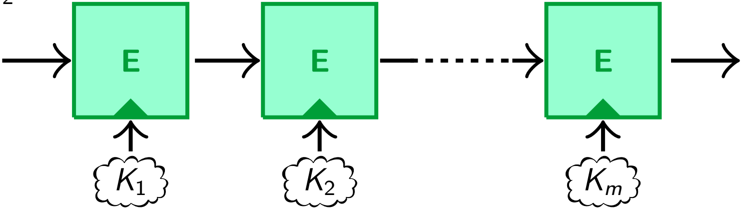
$\frac{1}{2} \leq \varepsilon < 1$



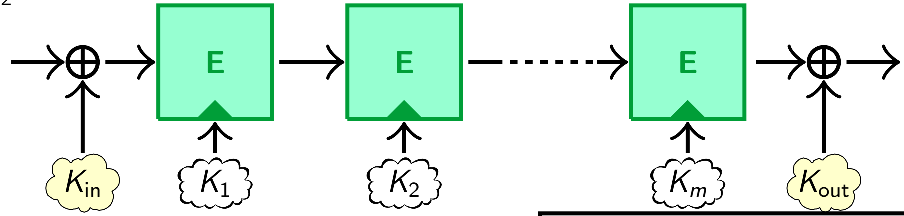
This Paper – A Preview

$$\delta = 2^{m-1} \cdot \varepsilon^m + \text{negl}$$

$\varepsilon < \frac{1}{2}$

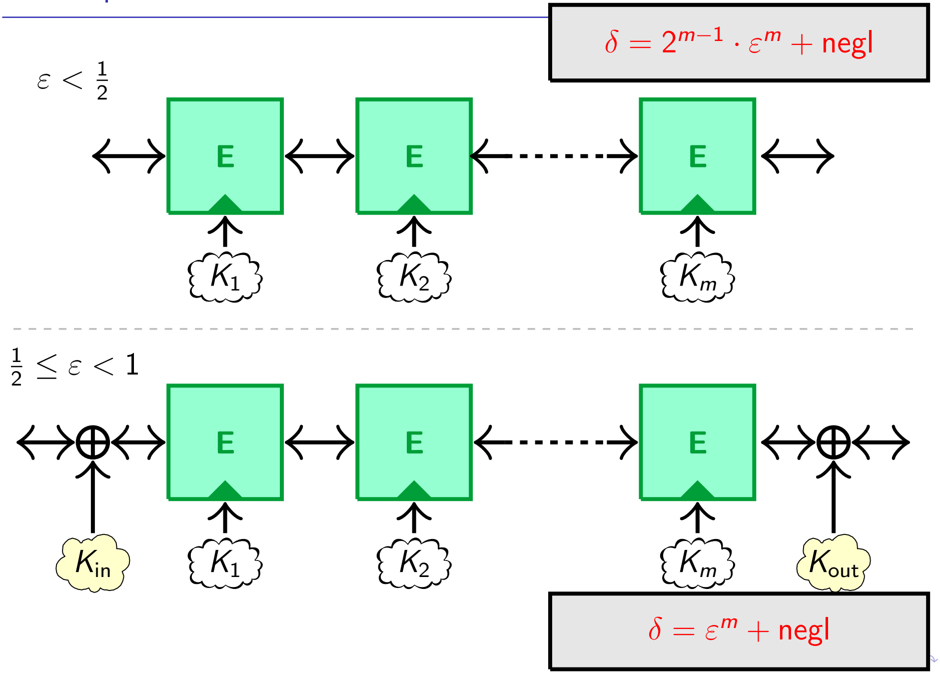


$\frac{1}{2} \leq \varepsilon < 1$

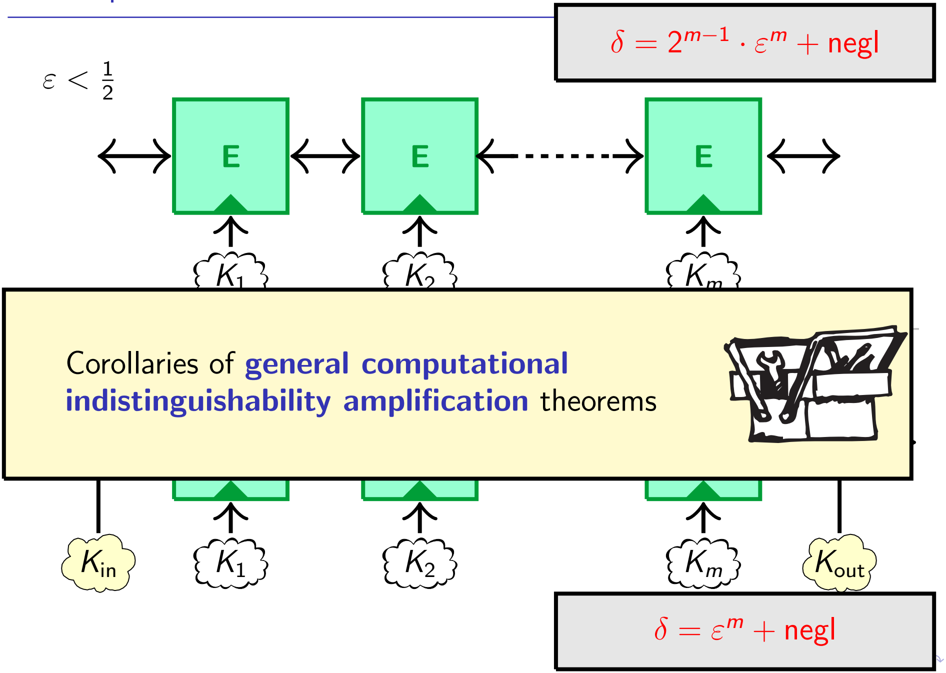


$$\delta = \varepsilon^m + \text{negl}$$

This Paper – A Preview



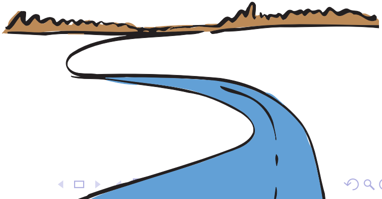
This Paper – A Preview



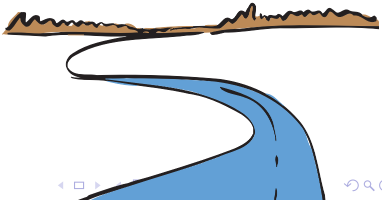
Corollaries of **general computational indistinguishability amplification** theorems

Outline

1. Generalizing Yao's XOR Lemma
2. Neutralizing Constructions
3. Strong Indistinguishability Amplification
4. Concluding Remarks

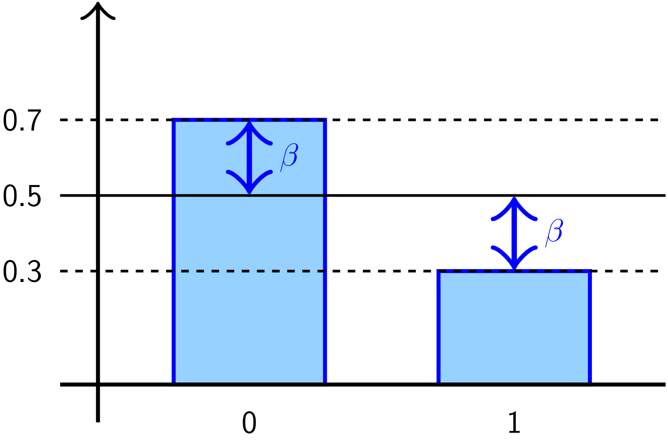


Outline



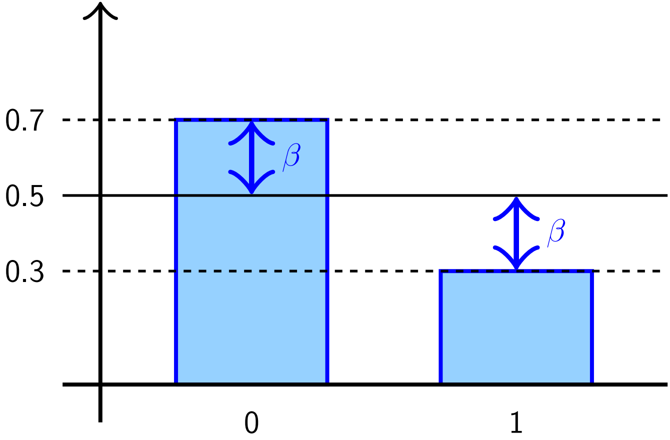
Biased Bits

x	**0**	**1**
$\Pr[B = x]$	0.7	0.3



Biased Bits

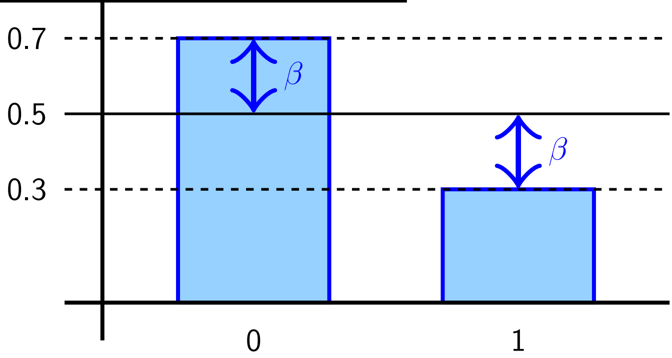
x	**0**	**1**
$\Pr[B = x]$	0.7	0.3



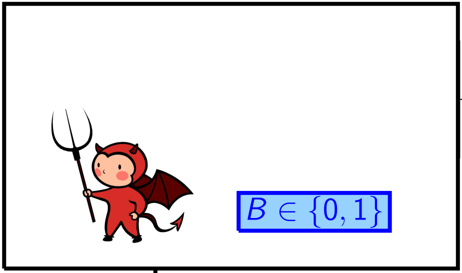
Biased Bits

$B \in \{0, 1\}$

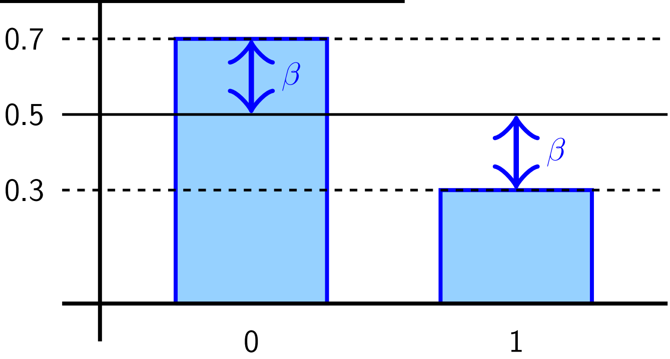
0	**1**
0.7	0.3



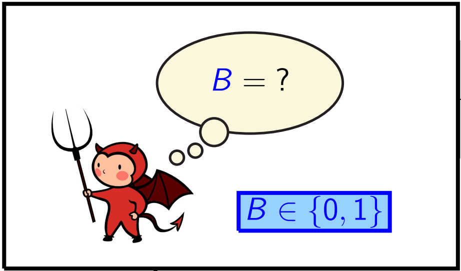
Biased Bits



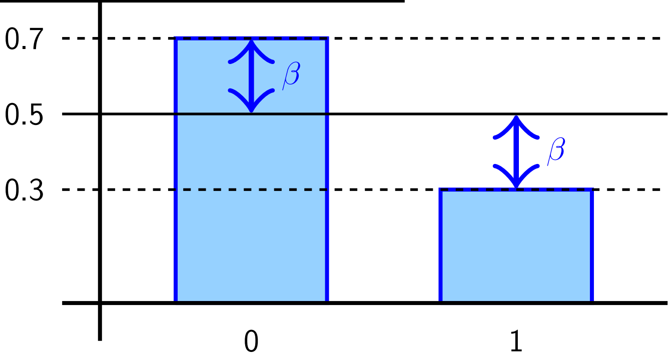
0	**1**
0.7	0.3



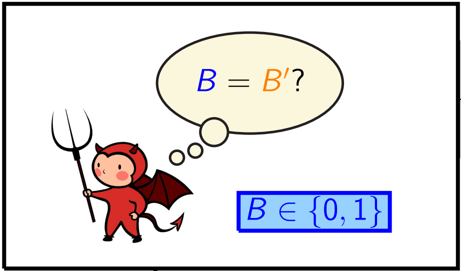
Biased Bits



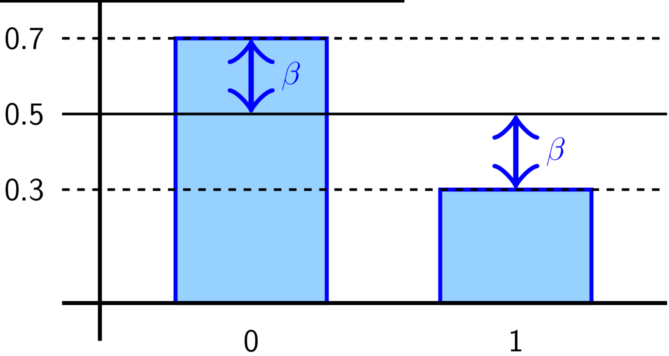
0	1
0.7	0.3



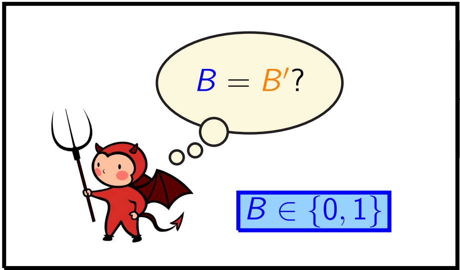
Biased Bits



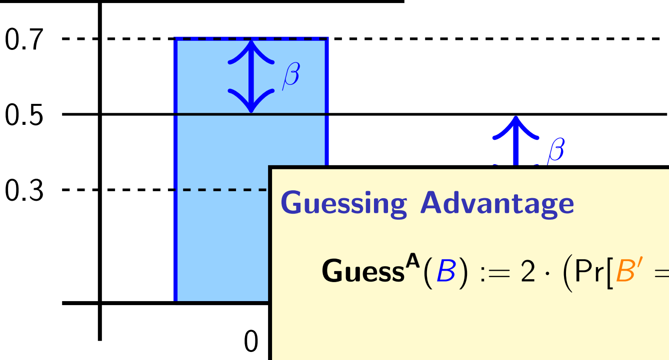
0	1
0.7	0.3



Biased Bits

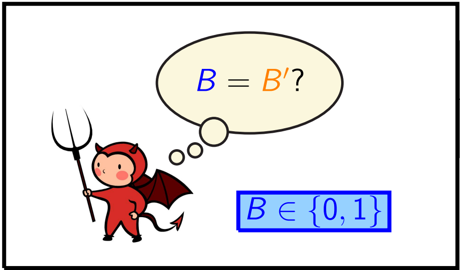


0	**1**
0.7	0.3

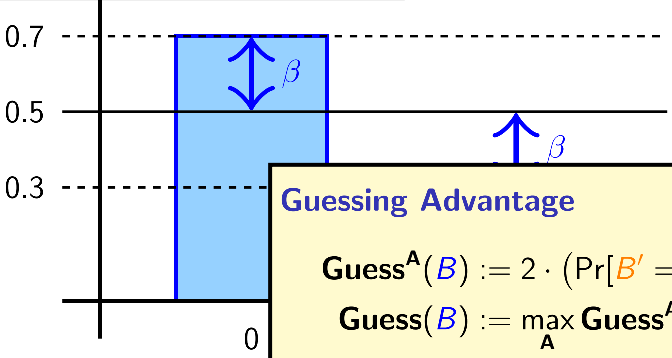


Guessing Advantage

$$\mathbf{Guess}^{\mathbf{A}}(B) := 2 \cdot \left(\Pr[B' = B] - \frac{1}{2}\right)$$



0	1
0.7	0.3

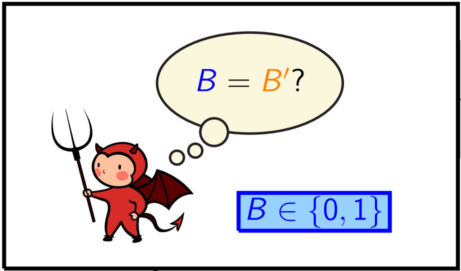


Guessing Advantage

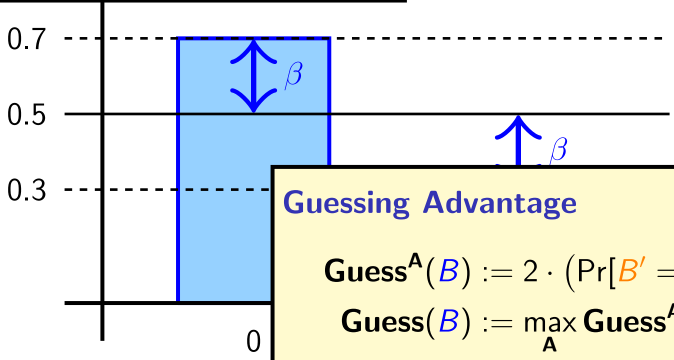
$$\mathbf{Guess}^{\mathbf{A}}(B) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

$$\mathbf{Guess}(B) := \max_{\mathbf{A}} \mathbf{Guess}^{\mathbf{A}}(B)$$

Biased Bits



0	1
0.7	0.3

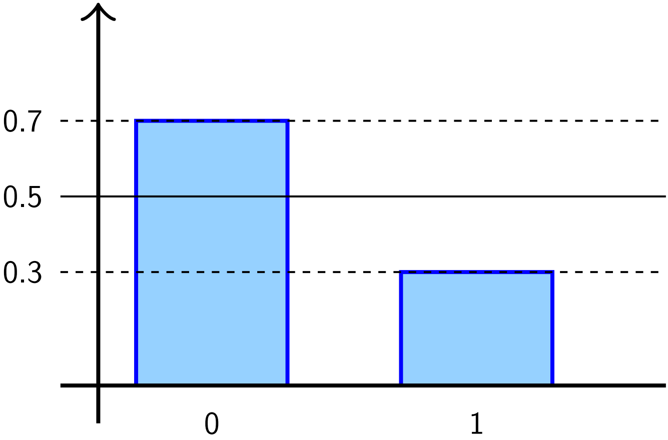


Guessing Advantage

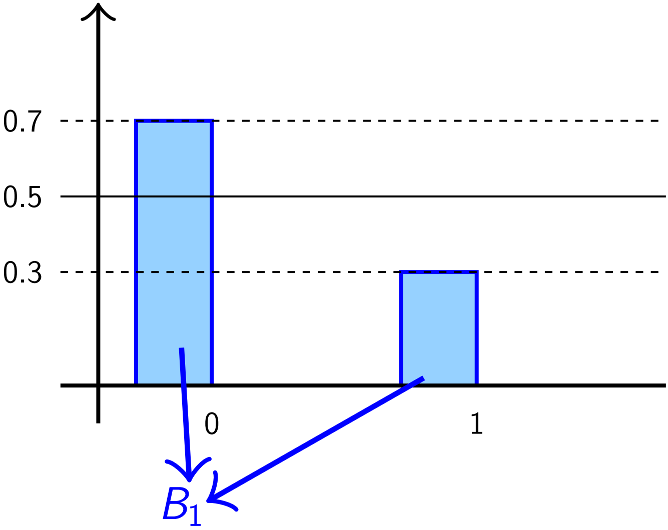
$$\mathbf{Guess}^{\mathbf{A}}(B) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

$$\mathbf{Guess}(B) := \max_{\mathbf{A}} \mathbf{Guess}^{\mathbf{A}}(B) = 2\beta$$

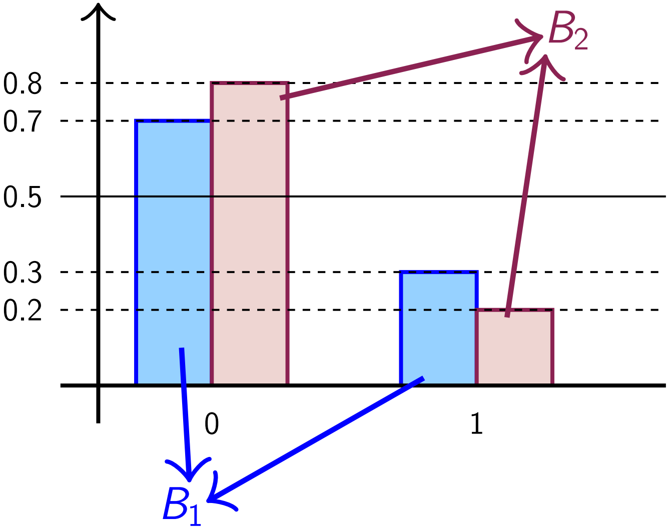
Biased Bits – XOR



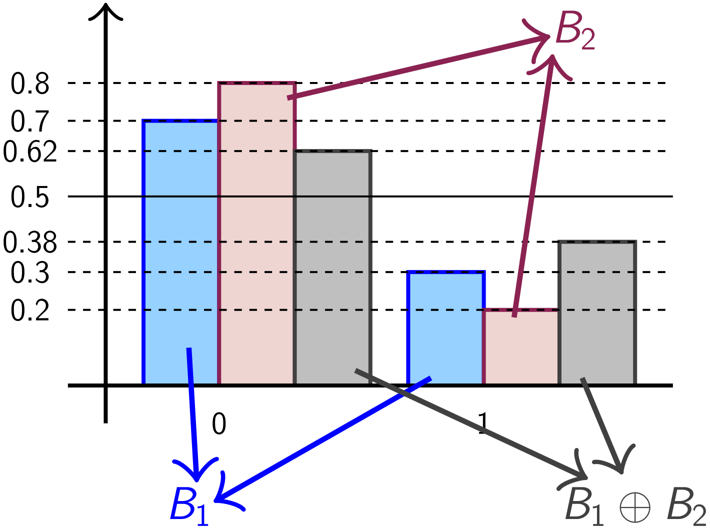
Biased Bits – XOR



Biased Bits – XOR

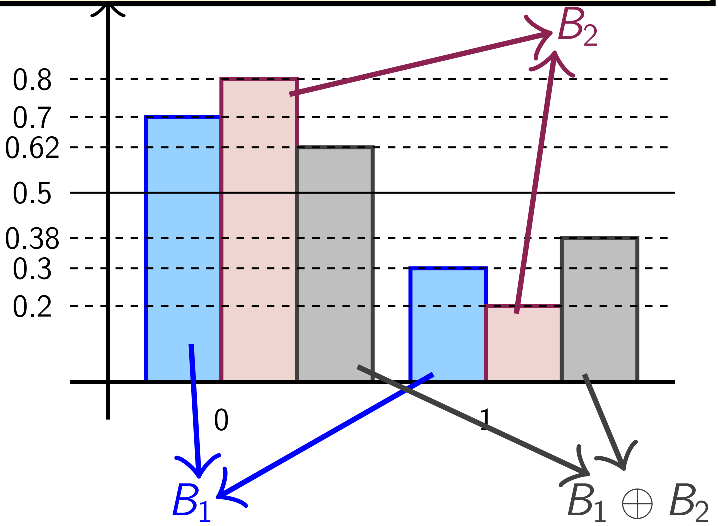


Biased Bits – XOR



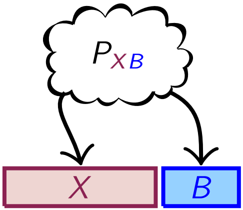
Biased Bits – XOR

Theorem. $\textbf{Guess}(B_1 \oplus B_2) = \textbf{Guess}(B_1) \cdot \textbf{Guess}(B_2)$

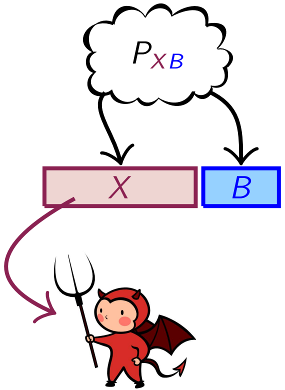


Yao's XOR Lemma

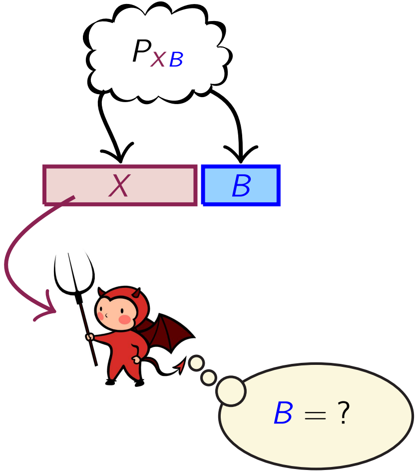
Yao's XOR Lemma



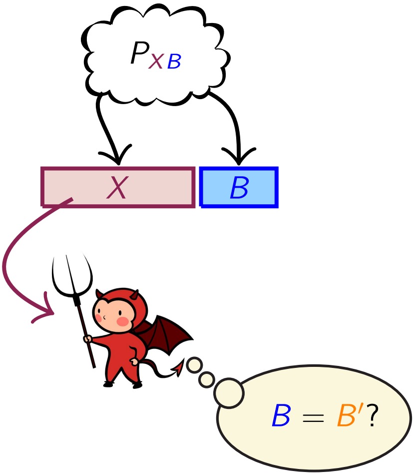
Yao's XOR Lemma



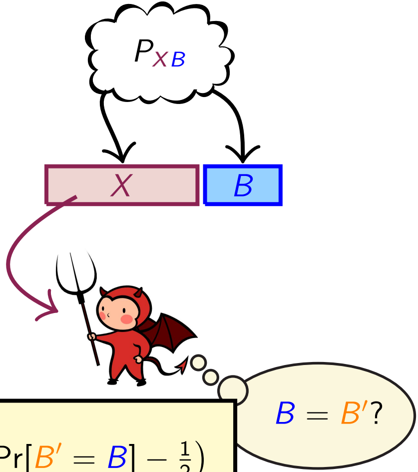
Yao's XOR Lemma



Yao's XOR Lemma

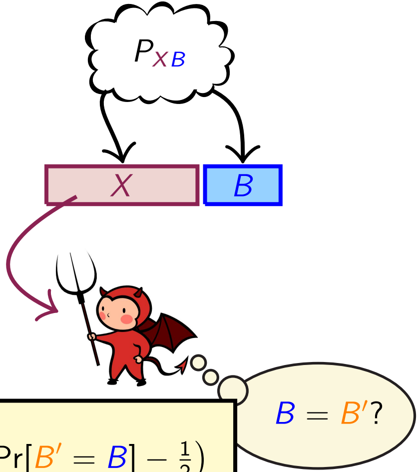


Yao's XOR Lemma



$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

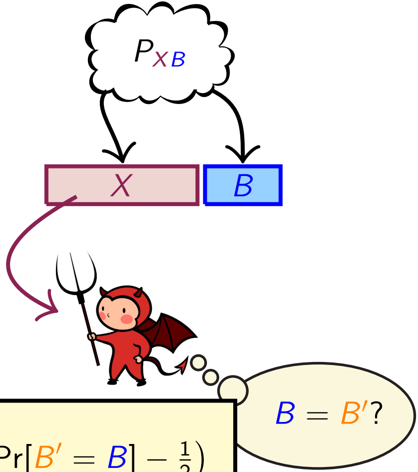
Yao's XOR Lemma



$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \leq t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$

Yao's XOR Lemma



$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \leq t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$

Yao's XOR Lemma

Example. $f : \{0,1\}^n \to \{0,1\}^n$, $P : \{0,1\}^n \to \{0,1\}$

$$U \xleftarrow{\$} \{0,1\}^n,\ X := f(U),\ B := P(U)$$

$B = B'$?

$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \le t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$

Yao's XOR Lemma

Example. $f : \{0,1\}^n \to \{0,1\}^n$, $P : \{0,1\}^n \to \{0,1\}$

$$U \xleftarrow{\$} \{0,1\}^n,\ X := f(U),\ B := P(U)$$

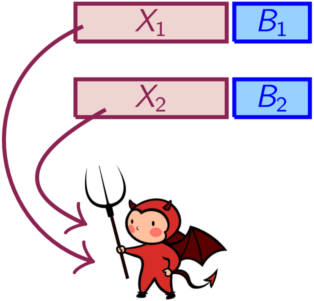
$\mathbf{Guess}_{\mathrm{poly}}(B \mid X) = \mathrm{negl} \iff P$ is hardcore predicate for f

$B = B'$?

$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

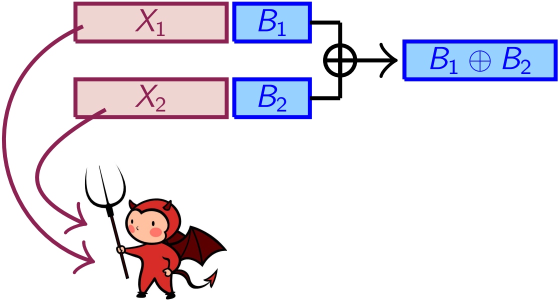
$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \le t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$

Yao's XOR Lemma



$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$
$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \leq t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$

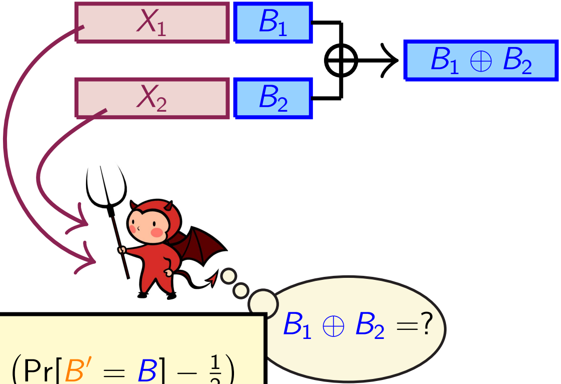
Yao's XOR Lemma



$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \leq t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$

Yao's XOR Lemma

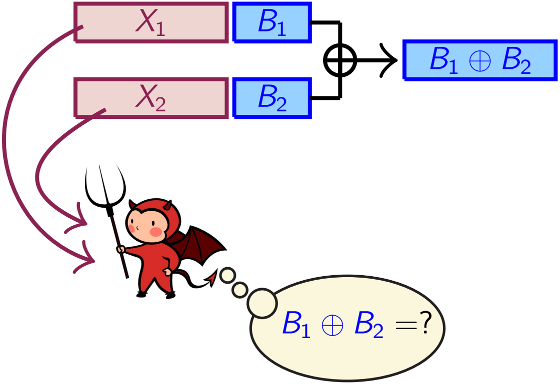


$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \leq t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$

Yao's XOR Lemma

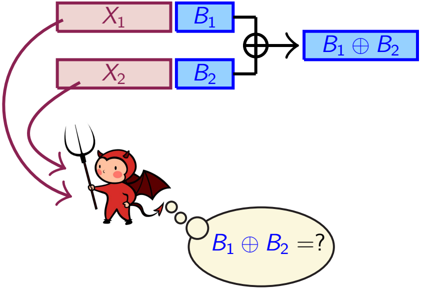
$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$
$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \leq t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$



Yao's XOR Lemma

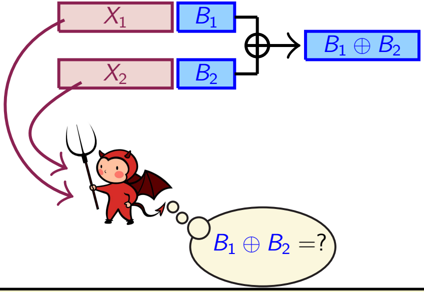
$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \leq t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$



Yao's XOR Lemma

$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$
$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \le t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$

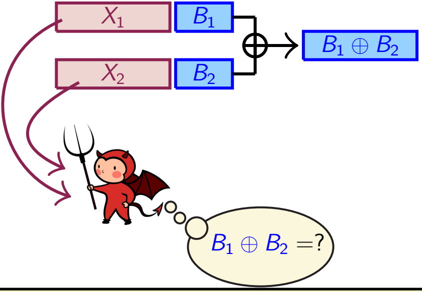


Theorem [Y82]. $\forall\, (X_1, B_1), \ldots, (X_m, B_m)$,

$$\mathbf{Guess}_t(B_1 \oplus \cdots \oplus B_m \mid X_1, \ldots, X_m)$$

Yao's XOR Lemma

$$\mathbf{Guess}^{\mathsf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$
$$\mathbf{Guess}_t(B \mid X) := \max_{\mathsf{A}: t_{\mathsf{A}} \le t} \mathbf{Guess}^{\mathsf{A}}(B \mid X)$$

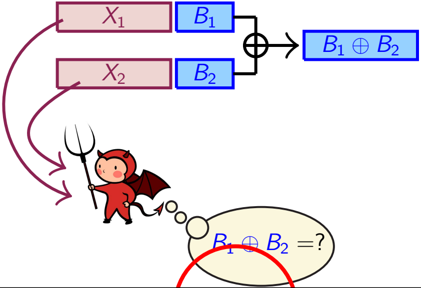


Theorem [Y82]. $\forall\ (X_1, B_1), \ldots, (X_m, B_m)$,

$$\mathbf{Guess}_t(B_1 \oplus \cdots \oplus B_m \mid X_1, \ldots, X_m) = \prod_{i=1}^{m} \mathbf{Guess}_t(B_i \mid X_i)$$

Yao's XOR Lemma

$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$
$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \le t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$

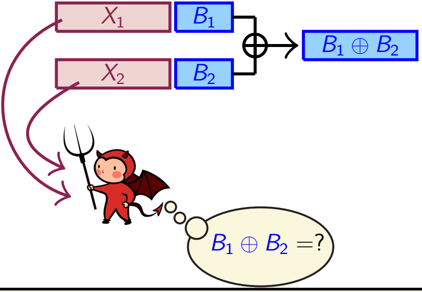


Theorem [Y82]. $\forall\, (X_1, B_1), \ldots, (X_m, B_m)$, $\forall \gamma > 0$

$$\mathbf{Guess}_t(B_1 \oplus \cdots \oplus B_m \mid X_1, \ldots, X_m) = \prod_{i=1}^{m} \mathbf{Guess}_t(B_i \mid X_i)$$

Yao's XOR Lemma

$$\textbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$
$$\textbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \leq t} \textbf{Guess}^{\mathbf{A}}(B \mid X)$$

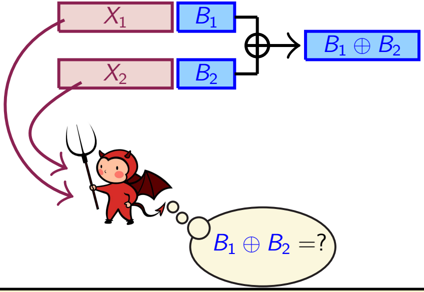


Theorem [Y82]. $\forall\ (X_1, B_1), \ldots, (X_m, B_m)$, $\forall \gamma > 0$

$$\textbf{Guess}_t(B_1 \oplus \cdots \oplus B_m \mid X_1, \ldots, X_m) \leq \prod_{i=1}^{m} \textbf{Guess}_t(B_i \mid X_i) + \gamma$$

Yao's XOR Lemma

$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$
$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \le t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$



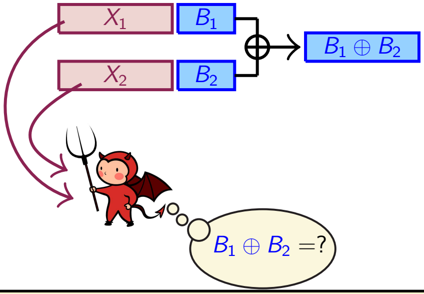
Theorem [Y82]. $\forall\, (X_1, B_1), \ldots, (X_m, B_m)$, $\forall \gamma > 0$

$$\mathbf{Guess}_t(B_1 \oplus \cdots \oplus B_m \mid X_1, \ldots, X_m) \le \prod_{i=1}^{m} \mathbf{Guess}_{t'}(B_i \mid X_i) + \gamma$$

where $t' := \mathcal{O}\left(\frac{t}{\gamma^2}\right)$

Yao's XOR Lemma

$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$
$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \leq t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$



Theorem [Y82]. $\forall\ (X_1, B_1), \ldots, (X_m, B_m)$, $\forall \gamma > 0$

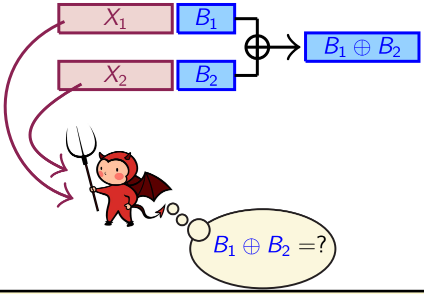
$$\mathbf{Guess}_t(B_1 \oplus \cdots \oplus B_m \mid X_1, \ldots, X_m) \leq \prod_{i=1}^{m} \mathbf{Guess}_{t'}(B_i \mid X_i) + \gamma$$

where $t' := \mathcal{O}\left(\frac{t}{\gamma^2}\right)$

TRADE OFF

Yao's XOR Lemma

$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$
$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \le t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$



Theorem [Y82]. $\forall\ (X_1, B_1), \ldots, (X_m, B_m)$, $\forall \gamma > 0$

$$\mathbf{Guess}_t(B_1 \oplus \cdots \oplus B_m \mid X_1, \ldots, X_m) \le \prod_{i=1}^{m} \mathbf{Guess}_{t'}(B_i \mid X_i) + \gamma$$

where $t' := \mathcal{O}\left(\frac{t}{\gamma^2}\right)$

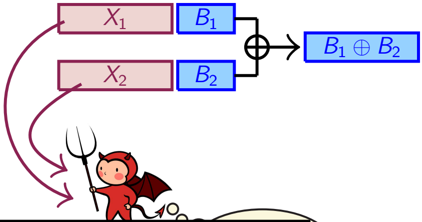
TRADE OFF

Several proofs [L87,I95,GNW95,...]

Yao's XOR Lemma

$$\mathbf{Guess}^{\mathbf{A}}(B \mid X) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

$$\mathbf{Guess}_t(B \mid X) := \max_{\mathbf{A}: t_{\mathbf{A}} \leq t} \mathbf{Guess}^{\mathbf{A}}(B \mid X)$$



Asymptotically: $\mathbf{Guess}_{\text{poly}}(B_i \mid X_i) \leq \varepsilon \implies$

$$\mathbf{Guess}_{\text{poly}}(B_1 \oplus \cdots \oplus B_m \mid X_1, \ldots, X_m) \leq \varepsilon^m + \text{negl}$$

$$\mathbf{Guess}_t(B_1 \oplus \cdots \oplus B_m \mid X_1, \ldots, X_m) \leq \prod_{i=1}^{m} \mathbf{Guess}_{t'}(B_i \mid X_i) + \gamma$$

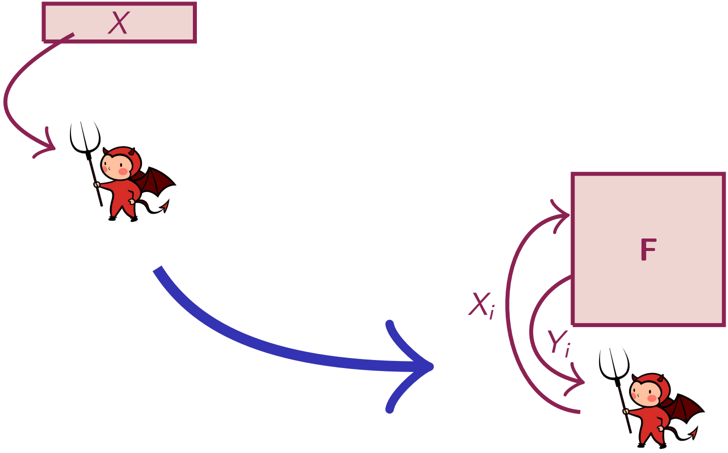
where $t' := \mathcal{O}\left(\frac{t}{\gamma^2}\right)$

TRADE OFF

Several proofs [L87,I95,GNW95,...]

This Paper: Generalization

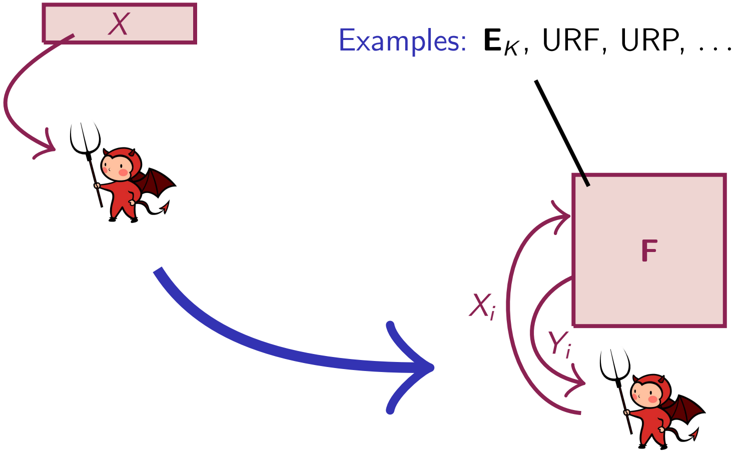
random variables



interactive systems

This Paper: Generalization

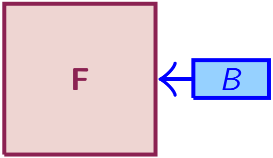
random variables



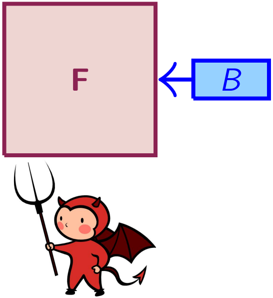
interactive systems

System-Bit Pairs

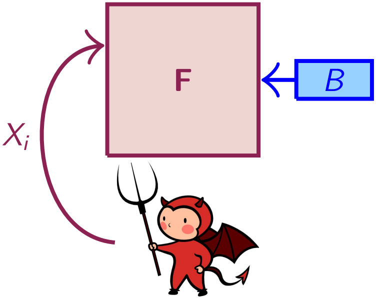
System-Bit Pairs



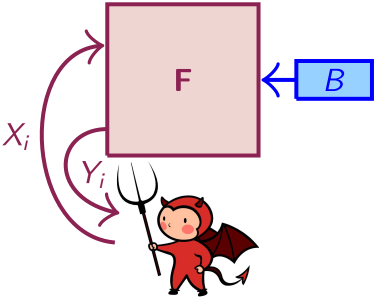
System-Bit Pairs



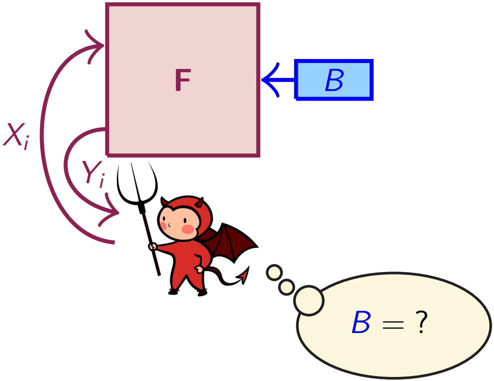
System-Bit Pairs



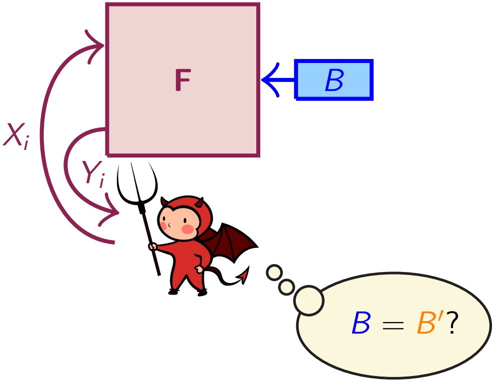
System-Bit Pairs



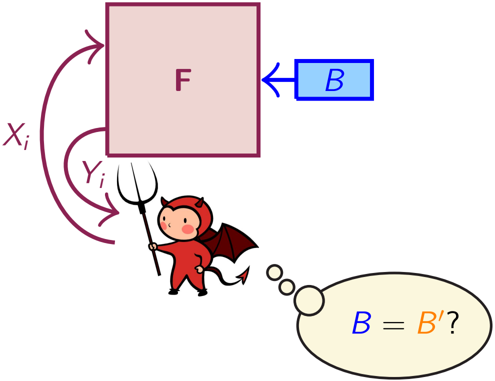
System-Bit Pairs



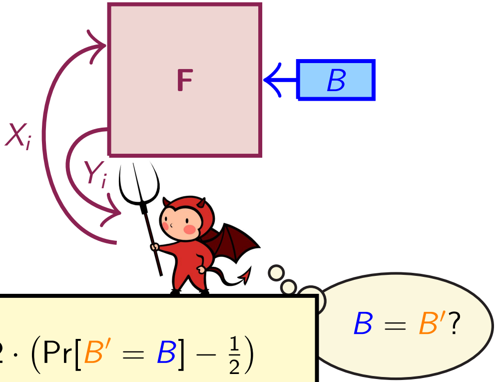
System-Bit Pairs



System-Bit Pairs

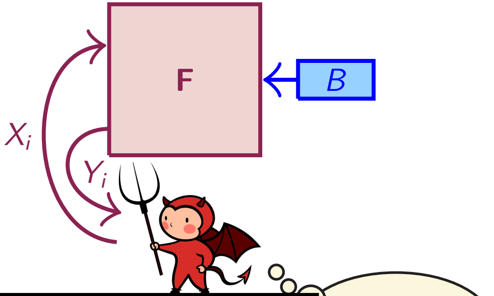


System-Bit Pairs



$$\mathbf{Guess}^{\mathbf{A}}(B \mid \mathbf{F}) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

System-Bit Pairs



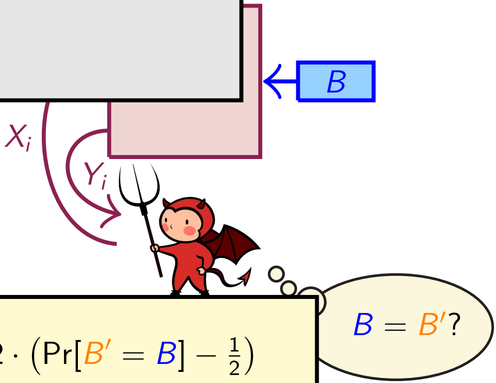
$$\mathbf{Guess}^{\mathbf{A}}(B \mid \mathbf{F}) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

$$\mathbf{Guess}_{t,q}(B \mid \mathbf{F}) := \max_{\mathbf{A}: t_{\mathbf{A}} \leq t, q_{\mathbf{A}} \leq q} \mathbf{Guess}^{\mathbf{A}}(B \mid \mathbf{F})$$

System-Bit Pairs

Example. B unbiased random bit

- $B = 0 \Longrightarrow \mathbf{F} := \mathbf{E}_K$
- $B = 1 \Longrightarrow \mathbf{F} := \mathbf{R}$ URF



$$\mathbf{Guess}^{\mathbf{A}}(B \mid \mathbf{F}) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

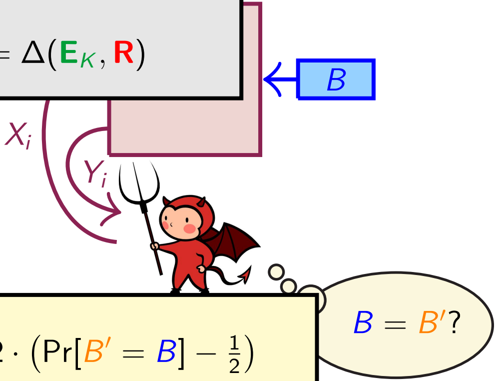
$$\mathbf{Guess}_{t,q}(B \mid \mathbf{F}) := \max_{\mathbf{A}: t_{\mathbf{A}} \le t, q_{\mathbf{A}} \le q} \mathbf{Guess}^{\mathbf{A}}(B \mid \mathbf{F})$$

System-Bit Pairs

Example. B unbiased random bit

- $B = 0 \implies \mathbf{F} := \mathbf{E}_K$
- $B = 1 \implies \mathbf{F} := \mathbf{R}$ URF

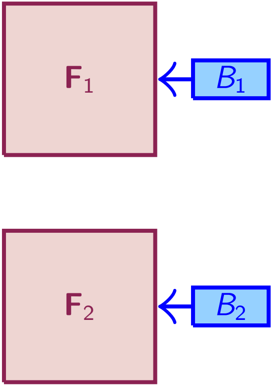
$$\mathbf{Guess}(B \mid \mathbf{F}) = \Delta(\mathbf{E}_K, \mathbf{R})$$



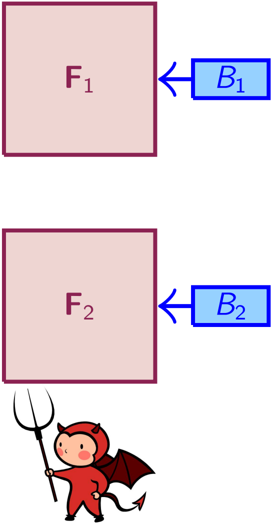
$$\mathbf{Guess}^{\mathbf{A}}(B \mid \mathbf{F}) := 2 \cdot \left(\Pr[B' = B] - \tfrac{1}{2}\right)$$

$$\mathbf{Guess}_{t,q}(B \mid \mathbf{F}) := \max_{\mathbf{A}: t_{\mathbf{A}} \leq t, q_{\mathbf{A}} \leq q} \mathbf{Guess}^{\mathbf{A}}(B \mid \mathbf{F})$$

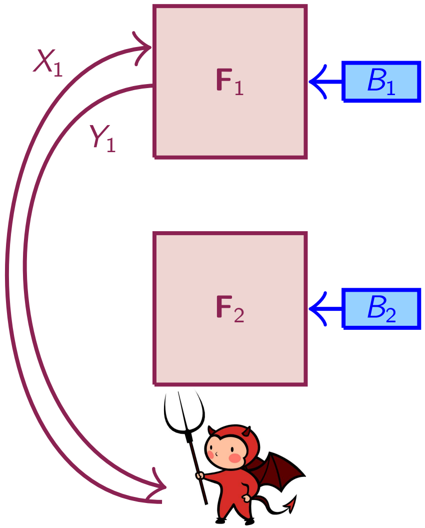
Generalized XOR Lemma



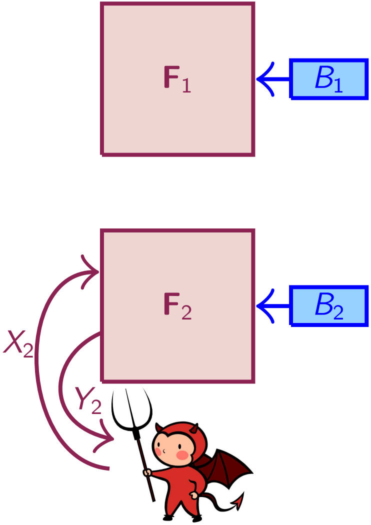
Generalized XOR Lemma



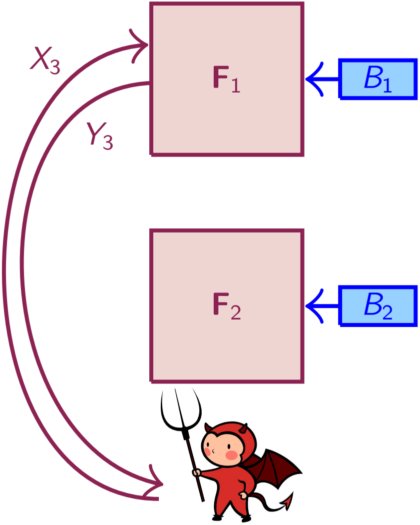
Generalized XOR Lemma



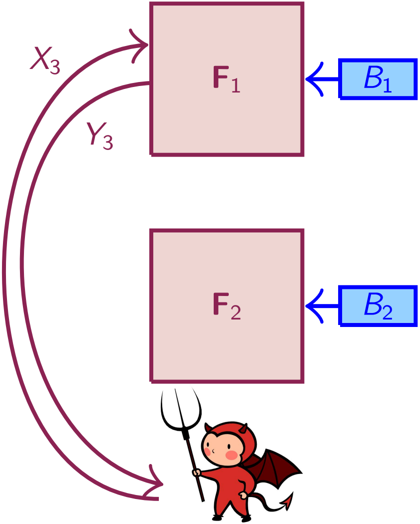
Generalized XOR Lemma



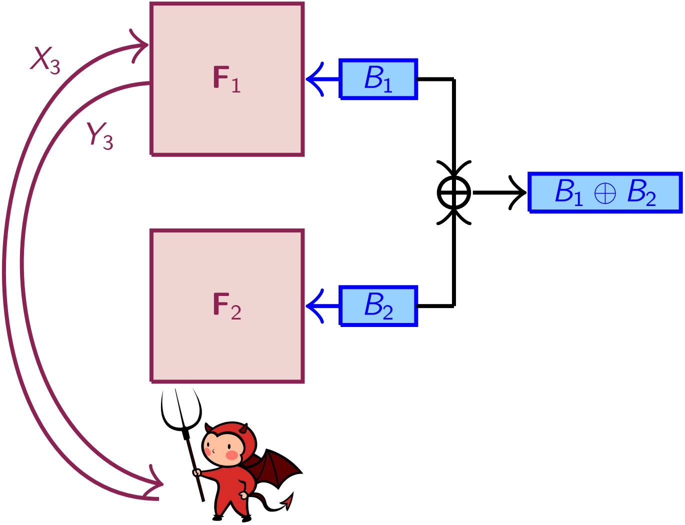
Generalized XOR Lemma



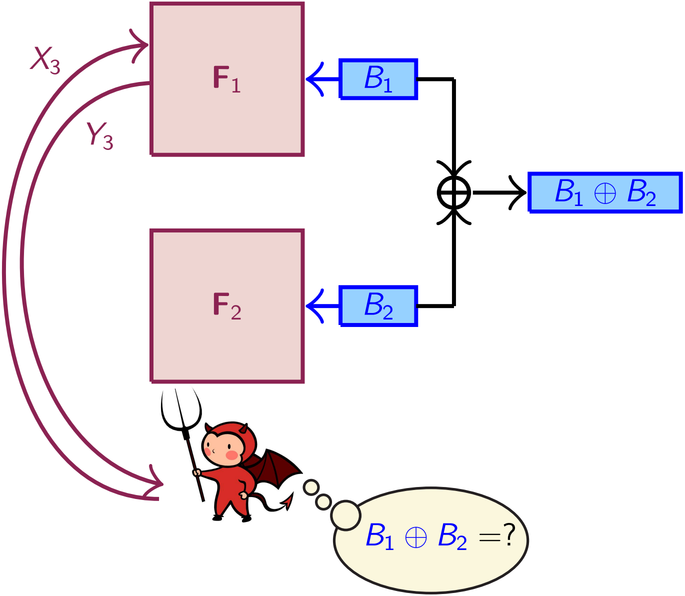
Generalized XOR Lemma



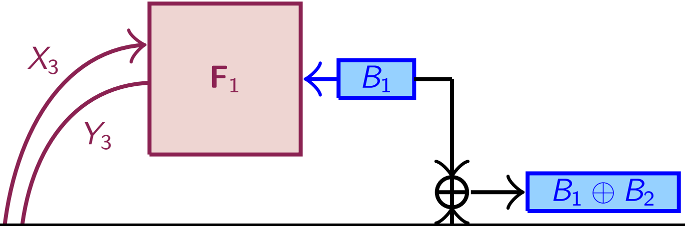
Generalized XOR Lemma



Generalized XOR Lemma



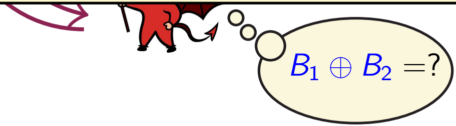
Generalized XOR Lemma



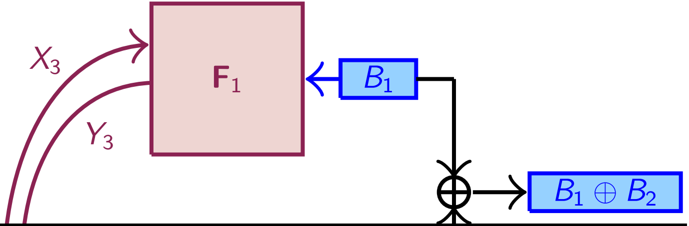
Theorem. $\forall$ cc-stateless $(\mathbf{F}_1, B_1), \ldots, (\mathbf{F}_m, B_m)$, $\forall\ \gamma > 0$

$$\mathbf{Guess}_{t,q}(B_1 \oplus \cdots \oplus B_m \mid \mathbf{F}_1 \| \ldots \| \mathbf{F}_m) \leq \prod_{i=1}^{m} \mathbf{Guess}_{t',q'}(B_i \mid \mathbf{F}_i) + \gamma,$$

with $t' = \mathcal{O}(\frac{t}{\gamma^2})$ and $q' = \mathcal{O}(\frac{q}{\gamma^2})$.



Generalized XOR Lemma

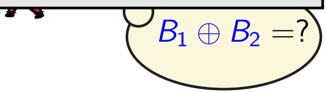


Theorem. $\forall$ cc-stateless $(\mathbf{F}_1, B_1), \ldots, (\mathbf{F}_m, B_m)$, $\forall\ \gamma > 0$

$$\mathbf{Guess}_{t,q}(B_1 \oplus \cdots \oplus B_m \mid \mathbf{F}_1 \| \ldots \| \mathbf{F}_m) \leq \prod_{i=1}^{m} \mathbf{Guess}_{t',q'}(B_i \mid \mathbf{F}_i) + \gamma,$$

with $t' = \mathcal{O}(\frac{t}{\gamma^2})$ and $q' = \mathcal{O}(\frac{q}{\gamma^2})$.

[HR08]: sequential access (not sufficient here)



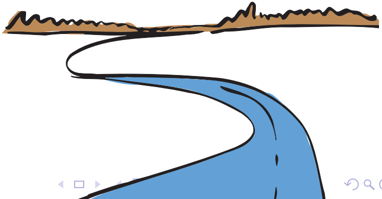
Outline

1. Generalizing Yao's XOR Lemma

2. Neutralizing Constructions

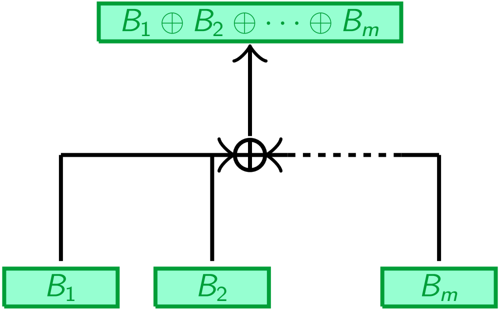
3. Strong Indistinguishability Amplification

4. Concluding Remarks



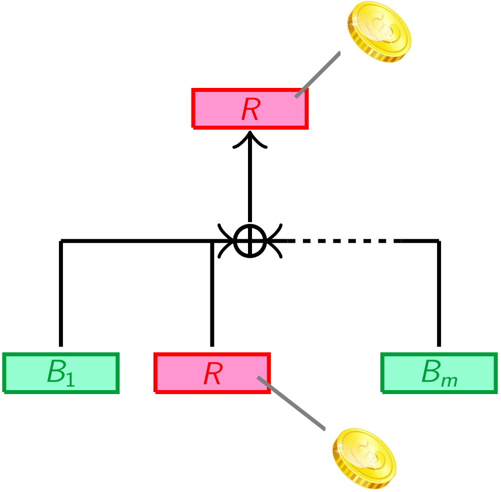
XOR of Random Bits

$B_1, \ldots, B_m$: independent (biased) random bits



XOR of Random Bits

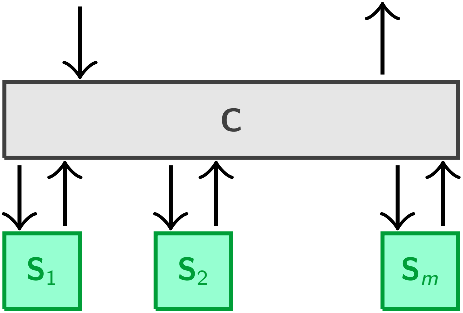
$B_1, \ldots, B_m$: independent (biased) random bits



Neutralizing Constructions [MPR07]

$\mathbf{C}(\cdot)$ **neutralizing** for $\mathcal{F}$ and ideal $\mathbf{I}_1, \ldots, \mathbf{I}_m \in \mathcal{F}$

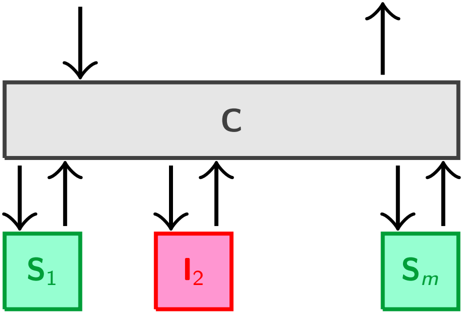
$$\forall \mathbf{S}_1, \ldots, \mathbf{S}_m \in \mathcal{F} : (\exists i : \mathbf{S}_i \equiv \mathbf{I}_i) \implies \mathbf{C}(\mathbf{S}_1, \ldots, \mathbf{S}_m) \equiv \mathbf{C}(\mathbf{I}_1, \ldots, \mathbf{I}_m)$$



Neutralizing Constructions [MPR07]

$\mathbf{C}(\cdot)$ **neutralizing** for $\mathcal{F}$ and ideal $\mathbf{I}_1, \ldots, \mathbf{I}_m \in \mathcal{F}$

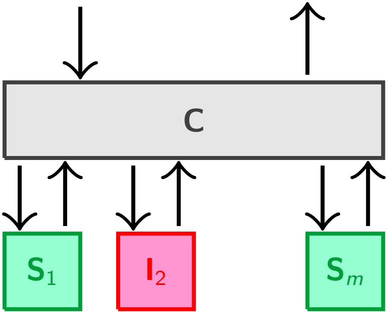
$$\forall \mathbf{S}_1, \ldots, \mathbf{S}_m \in \mathcal{F} : (\exists i : \mathbf{S}_i \equiv \mathbf{I}_i) \implies \mathbf{C}(\mathbf{S}_1, \ldots, \mathbf{S}_m) \equiv \mathbf{C}(\mathbf{I}_1, \ldots, \mathbf{I}_m)$$



Neutralizing Constructions [MPR07]

$\mathbf{C}(\cdot)$ **neutralizing** for $\mathcal{F}$ and ideal $\mathbf{I}_1, \ldots, \mathbf{I}_m \in \mathcal{F}$

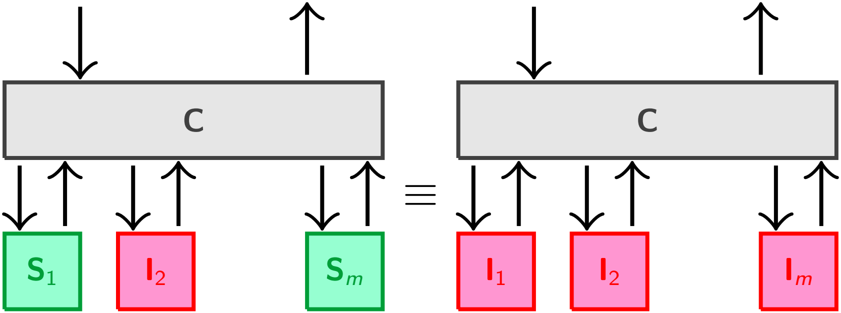
$$\forall \mathbf{S}_1, \ldots, \mathbf{S}_m \in \mathcal{F} : (\exists i : \mathbf{S}_i \equiv \mathbf{I}_i) \implies \mathbf{C}(\mathbf{S}_1, \ldots, \mathbf{S}_m) \equiv \mathbf{C}(\mathbf{I}_1, \ldots, \mathbf{I}_m)$$



Neutralizing Constructions [MPR07]

$\mathbf{C}(\cdot)$ **neutralizing** for $\mathcal{F}$ and ideal $\mathbf{I}_1, \ldots, \mathbf{I}_m \in \mathcal{F}$

$$\forall \mathbf{S}_1, \ldots, \mathbf{S}_m \in \mathcal{F} : (\exists i : \mathbf{S}_i \equiv \mathbf{I}_i) \implies \mathbf{C}(\mathbf{S}_1, \ldots, \mathbf{S}_m) \equiv \mathbf{C}(\mathbf{I}_1, \ldots, \mathbf{I}_m)$$

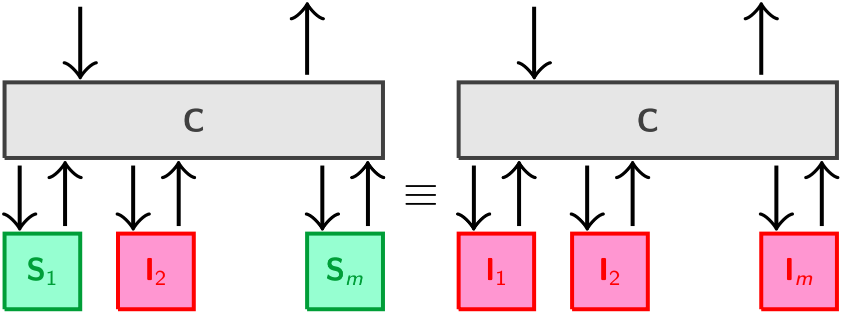


Neutralizing Constructions [MPR07]

C$(\cdot)$ **neutralizing** for $\mathcal{F}$ and ideal $\mathbf{I}_1, \ldots, \mathbf{I}_m \in \mathcal{F}$

$$\forall \mathbf{S}_1, \ldots, \mathbf{S}_m \in \mathcal{F} : (\exists i : \mathbf{S}_i \equiv \mathbf{I}_i) \implies \mathbf{C}(\mathbf{S}_1, \ldots, \mathbf{S}_m) \equiv \mathbf{C}(\mathbf{I}_1, \ldots, \mathbf{I}_m)$$

combiner



Security Amplification for All Neutralizing Constructions

First Product Theorem

Given: $\mathbf{C}(\cdot)$ neutralizing for $\mathcal{F}$ and cc-stateless $\mathbf{I}_1, \ldots, \mathbf{I}_m$

Then: $\forall$ cc-stateless $\mathbf{F}_1, \ldots, \mathbf{F}_m \in \mathcal{F}$ and $\forall\ \gamma > 0$

$$\Delta_{t,q}(\mathbf{C}(\mathbf{F}_1, \ldots, \mathbf{F}_m), \mathbf{C}(\mathbf{I}_1, \ldots, \mathbf{I}_m))$$

Security Amplification for All Neutralizing Constructions

First Product Theorem

Given: $\mathbf{C}(\cdot)$ neutralizing for $\mathcal{F}$ and cc-stateless $\mathbf{I}_1, \ldots, \mathbf{I}_m$

Then: $\forall$ cc-stateless $\mathbf{F}_1, \ldots, \mathbf{F}_m \in \mathcal{F}$ and $\forall\ \gamma > 0$

$$\Delta_{t,q}(\mathbf{C}(\mathbf{F}_1, \ldots, \mathbf{F}_m), \mathbf{C}(\mathbf{I}_1, \ldots, \mathbf{I}_m)) \leq 2^{m-1} \prod_{i=1}^{m} \Delta_{t',q'}(\mathbf{F}_i, \mathbf{I}_i) + \gamma,$$

with $t' = \mathcal{O}(\frac{t}{\gamma^2})$ and $q' = \mathcal{O}(\frac{q}{\gamma^2})$.

Security Amplification for All Neutralizing Constructions

First Product Theorem

Given: $\mathbf{C}(\cdot)$ neutralizing for $\mathcal{F}$ and cc-stateless $\mathbf{I}_1, \ldots, \mathbf{I}_m$

Then: $\forall$ cc-stateless $\mathbf{F}_1, \ldots, \mathbf{F}_m \in \mathcal{F}$ and $\forall\ \gamma > 0$

$$\Delta_{t,q}(\mathbf{C}(\mathbf{F}_1, \ldots, \mathbf{F}_m), \mathbf{C}(\mathbf{I}_1, \ldots, \mathbf{I}_m)) \leq 2^{m-1} \prod_{i=1}^{m} \Delta_{t',q'}(\mathbf{F}_i, \mathbf{I}_i) + \gamma,$$

with $t' = \mathcal{O}(\frac{t}{\gamma^2})$ and $q' = \mathcal{O}(\frac{q}{\gamma^2})$.

Remarks

- Security amplification for all combiners!
- Matches tight IT-bounds [MPR07]

Security Amplification for All Neutralizing Constructions

First Product Theorem

Given: $\mathbf{C}(\cdot)$ neutralizing for $\mathcal{F}$ and cc-stateless $\mathbf{I}_1, \ldots, \mathbf{I}_m$

Then: $\forall$ cc-stateless $\mathbf{F}_1, \ldots, \mathbf{F}_m \in \mathcal{F}$ and $\forall\, \gamma > 0$

$$\Delta_{t,q}(\mathbf{C}(\mathbf{F}_1, \ldots, \mathbf{F}_m), \mathbf{C}(\mathbf{I}_1, \ldots, \mathbf{I}_m)) \leq 2^{m-1} \prod_{i=1}^{m} \Delta_{t',q'}(\mathbf{F}_i, \mathbf{I}_i) + \gamma,$$

with $t' = \mathcal{O}(\frac{t}{\gamma^2})$ and $q' = \mathcal{O}(\frac{q}{\gamma^2})$.

Remarks

- Security amplification for all combiners!
- Matches tight IT-bounds [MPR07]

Security Amplification for All Neutralizing Constructions

First Product Theorem

Given: $\mathbf{C}(\cdot)$ neutralizing for $\mathcal{F}$ and cc-stateless $\mathbf{I}_1, \ldots, \mathbf{I}_m$

Then: $\forall$ cc-stateless $\mathbf{F}_1, \ldots, \mathbf{F}_m \in \mathcal{F}$ and $\forall\ \gamma > 0$

$$\Delta_{t,q}(\mathbf{C}(\mathbf{F}_1, \ldots, \mathbf{F}_m), \mathbf{C}(\mathbf{I}_1, \ldots, \mathbf{I}_m)) \leq 2^{m-1} \prod_{i=1}^{m} \Delta_{t',q'}(\mathbf{F}_i, \mathbf{I}_i) + \gamma,$$

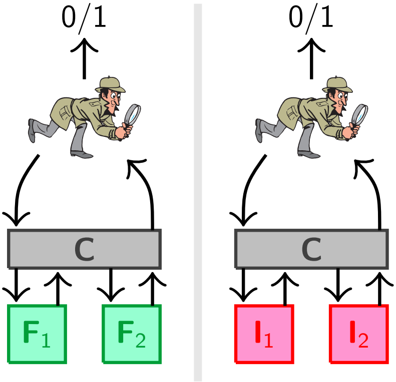
with $t' = \mathcal{O}(\frac{t}{\gamma^2})$ and $q' = \mathcal{O}(\frac{q}{\gamma^2})$.

$< \frac{1}{2}$

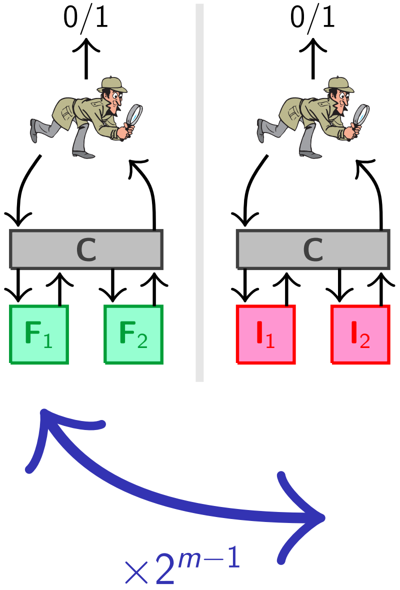
Remarks

- Security amplification for all combiners!
- Matches tight IT-bounds [MPR07]

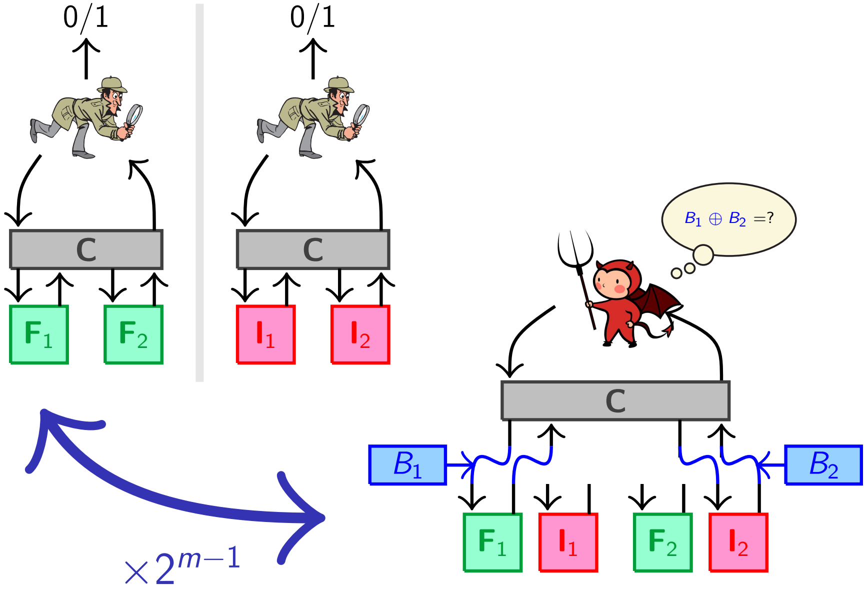
Proof Idea: Reduction to the XOR Lemma



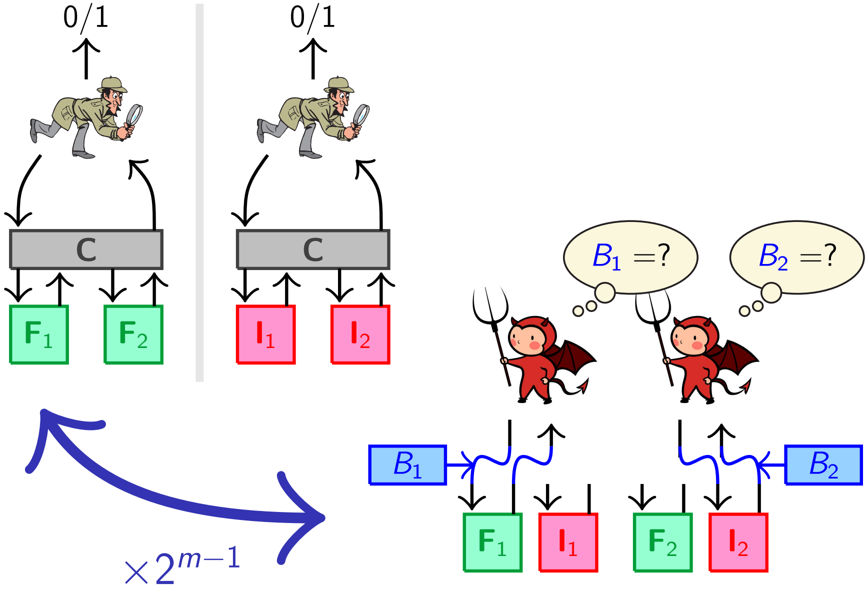
Proof Idea: Reduction to the XOR Lemma



Proof Idea: Reduction to the XOR Lemma

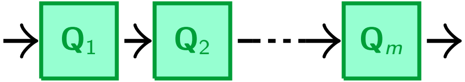


Proof Idea: Reduction to the XOR Lemma



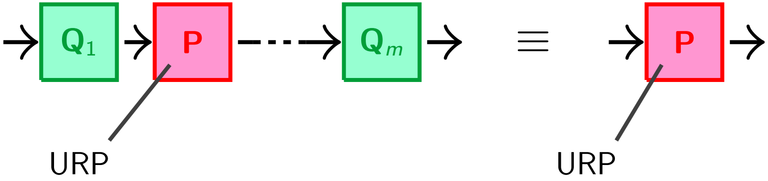
Example – Cascade of PRPs

$\mathbf{Q}_1, \ldots, \mathbf{Q}_m$: permutations $D \longrightarrow D$ (e.g. $\mathbf{E}_K$)



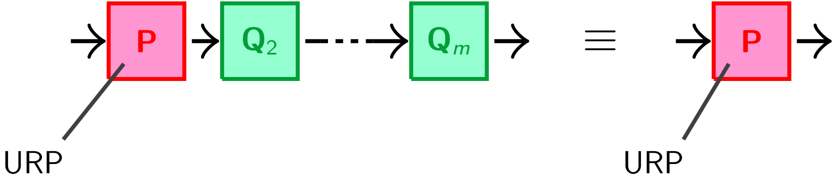
Example – Cascade of PRPs

$\mathbf{Q}_1, \ldots, \mathbf{Q}_m$: permutations $D \to D$ (e.g. $\mathbf{E}_K$)



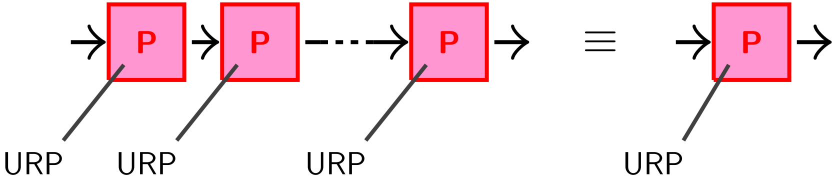
Example – Cascade of PRPs

$\mathbf{Q}_1, \ldots, \mathbf{Q}_m$: permutations $D \to D$ (e.g. $\mathbf{E}_K$)



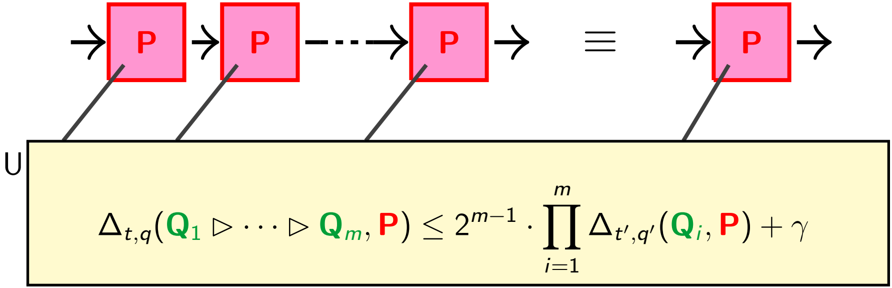
Example – Cascade of PRPs

$\mathbf{Q}_1, \ldots, \mathbf{Q}_m$: permutations $D \longrightarrow D$ (e.g. $\mathbf{E}_K$)



Example – Cascade of PRPs

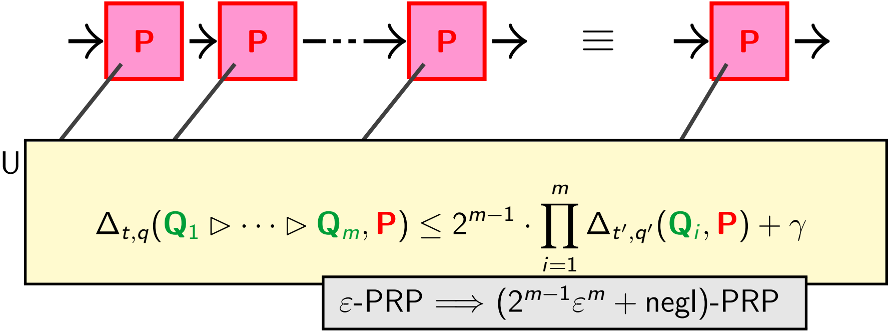
$\mathbf{Q}_1, \ldots, \mathbf{Q}_m$: permutations $D \rightarrow D$ (e.g. $\mathbf{E}_K$)



$$\Delta_{t,q}(\mathbf{Q}_1 \triangleright \cdots \triangleright \mathbf{Q}_m, \mathbf{P}) \leq 2^{m-1} \cdot \prod_{i=1}^{m} \Delta_{t',q'}(\mathbf{Q}_i, \mathbf{P}) + \gamma$$

Example – Cascade of PRPs

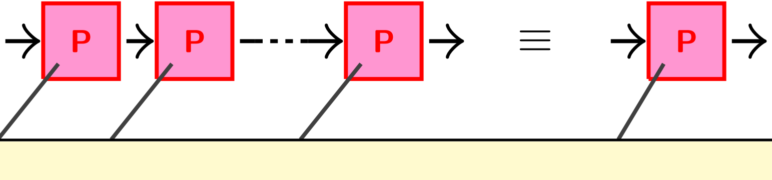
$\mathbf{Q}_1, \ldots, \mathbf{Q}_m$: permutations $D \to D$ (e.g. $\mathbf{E}_K$)



Example – Casca

two-sided

$\mathbf{Q}_1, \ldots, \mathbf{Q}_m$: permutations $D \to D$ (e.g. $\mathbf{E}_K$)

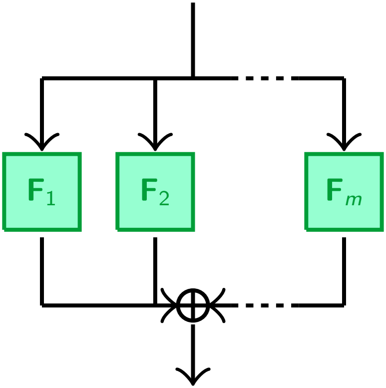


$$\Delta_{t,q}(\mathbf{Q}_1 \triangleright \cdots \triangleright \mathbf{Q}_m, \mathbf{P}) \leq 2^{m-1} \cdot \prod_{i=1}^{m} \Delta_{t',q'}(\mathbf{Q}_i, \mathbf{P}) + \gamma$$

ε-PRP $\Longrightarrow$ $(2^{m-1}\varepsilon^m + \text{negl})$-PRP

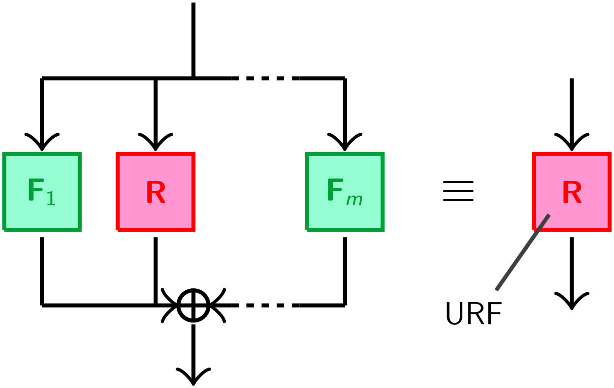
Examples — Sum of PRFs

$\mathbf{F}_1, \ldots, \mathbf{F}_m$: functions $D \to R$ (e.g. $\mathbf{E}_K$)



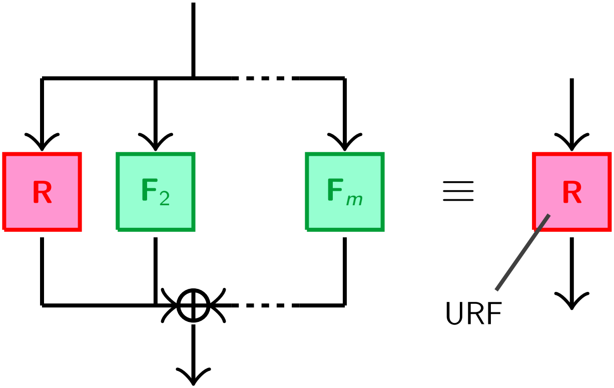
Examples — Sum of PRFs

$\mathbf{F}_1, \ldots, \mathbf{F}_m$: functions $D \to R$ (e.g. $\mathbf{E}_K$)



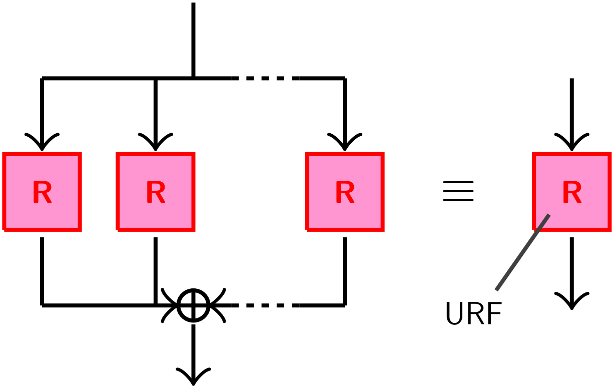
Examples — Sum of PRFs

$\mathbf{F}_1, \ldots, \mathbf{F}_m$: functions $D \rightarrow R$ (e.g. $\mathbf{E}_K$)



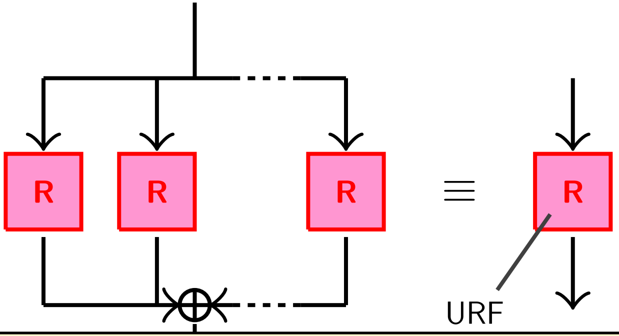
Examples — Sum of PRFs

$\mathbf{F}_1, \ldots, \mathbf{F}_m$: functions $D \rightarrow R$ (e.g. $\mathbf{E}_K$)



Examples — Sum of PRFs

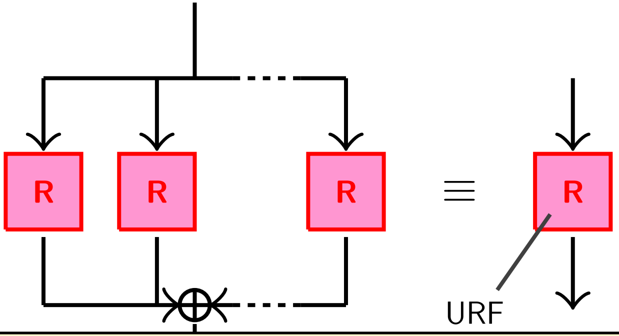
$\mathbf{F}_1, \ldots, \mathbf{F}_m$: functions $D \to R$ (e.g. $\mathbf{E}_K$)



$$\Delta_{t,q}(\mathbf{F}_1 \oplus \cdots \oplus \mathbf{F}_m, \mathbf{R}) \leq 2^{m-1} \cdot \prod_{i=1}^{m} \Delta_{t',q'}(\mathbf{F}_i, \mathbf{R}) + \gamma$$

Examples — Sum of PRFs

$\mathbf{F}_1, \ldots, \mathbf{F}_m$: functions $D \to R$ (e.g. $\mathbf{E}_K$)

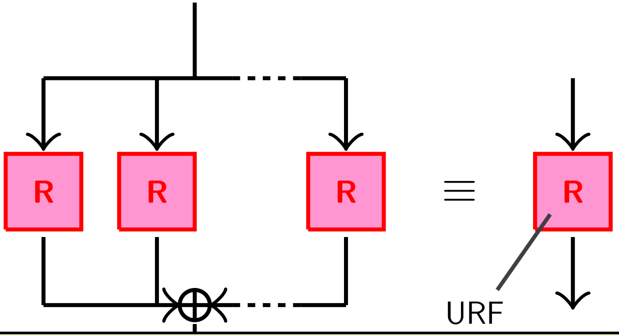


$$\Delta_{t,q}(\mathbf{F}_1 \oplus \cdots \oplus \mathbf{F}_m, \mathbf{R}) \leq 2^{m-1} \cdot \prod^{m} \Delta_{t',q'}(\mathbf{F}_i, \mathbf{R}) + \gamma$$

ε-PRF $\Longrightarrow$ $(2^{m-1}\varepsilon^m + \text{negl})$-PRF

Examples — Sum of PRFs

$\mathbf{F}_1, \ldots, \mathbf{F}_m$: functions $D \to R$ (e.g. $\mathbf{E}_K$)



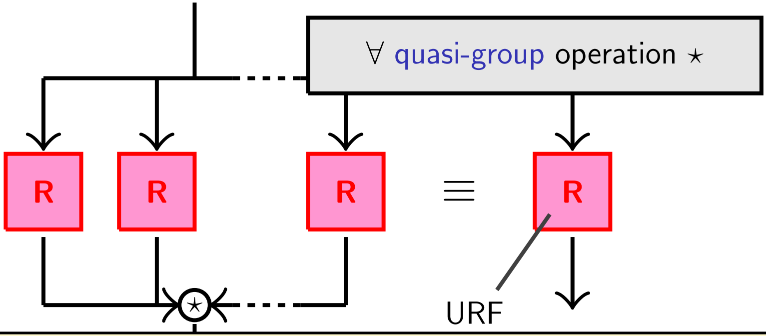
$$\Delta_{t,q}(\mathbf{F}_1 \oplus \cdots \oplus \mathbf{F}_m, \mathbf{R}) \leq 2^{m-1} \cdot \prod^{m} \Delta_{t',q'}(\mathbf{F}_i, \mathbf{R}) + \gamma$$

ε-PRF $\Longrightarrow$ $(2^{m-1}\varepsilon^m + \text{negl})$-PRF

Improves bounds of [DIJK09]

Examples — Sum of PRFs

$\mathbf{F}_1, \ldots, \mathbf{F}_m$: functions $D \to R$ (e.g. $\mathbf{E}_K$)



$$\Delta_{t,q}(\mathbf{F}_1 \star \cdots \star \mathbf{F}_m, \mathbf{R}) \leq 2^{m-1} \cdot \prod^{m} \Delta_{t',q'}(\mathbf{F}_i, \mathbf{R}) + \gamma$$

ε-PRF $\Longrightarrow$ $(2^{m-1}\varepsilon^m + \text{negl})$-PRF

Improves bounds of [DIJK09]

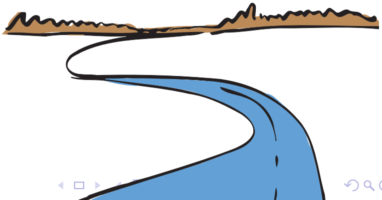
Outline

1. Generalizing Yao's XOR Lemma

2. Neutralizing Constructions

3. Strong Indistinguishability Amplification

4. Concluding Remarks



Security Amplification for Neutralizing Constructions

First Product Theorem

Given: $\mathbf{C}(\cdot)$ neutralizing for $\mathcal{F}$ and cc-stateless $\mathbf{I}_1, \ldots, \mathbf{I}_m$

Then: $\forall$ cc-stateless $\mathbf{F}_1, \ldots, \mathbf{F}_m \in \mathcal{F}$ and $\forall\ \gamma > 0$

$$\Delta_{t,q}(\mathbf{C}(\mathbf{F}_1, \ldots, \mathbf{F}_m), \mathbf{C}(\mathbf{I}_1, \ldots, \mathbf{I}_m)) \leq 2^{m-1} \prod_{i=1}^{m} \Delta_{t',q'}(\mathbf{F}_i, \mathbf{I}_i) + \gamma,$$

with $t' = \mathcal{O}(\frac{t}{\gamma^2})$ and $q' = \mathcal{O}(\frac{q}{\gamma^2})$.

$< \frac{1}{2}$

+ η-self independence

First Product Theorem

Given: $\mathbf{C}(\cdot)$ neutralizing for $\mathcal{F}$ and cc-stateless $\mathbf{I}_1, \ldots, \mathbf{I}_m$

Then: $\forall$ cc-stateless $\mathbf{F}_1, \ldots, \mathbf{F}_m \in \mathcal{F}$ and $\forall\ \gamma > 0$

$$\Delta_{t,q}(\mathbf{C}(\mathbf{F}_1, \ldots, \mathbf{F}_m), \mathbf{C}(\mathbf{I}_1, \ldots, \mathbf{I}_m)) \leq 2^{m-1} \prod_{i=1}^{m} \Delta_{t',q'}(\mathbf{F}_i, \mathbf{I}_i) + \gamma,$$

with $t' = \mathcal{O}(\frac{t}{\gamma^2})$ and $q' = \mathcal{O}(\frac{q}{\gamma^2})$.

$< \frac{1}{2}$

+ η-self independence

Second

~~First~~ Product Theorem

Given: $\mathbf{C}(\cdot)$ neutralizing for $\mathcal{F}$ and cc-stateless $\mathbf{I}_1, \ldots, \mathbf{I}_m$

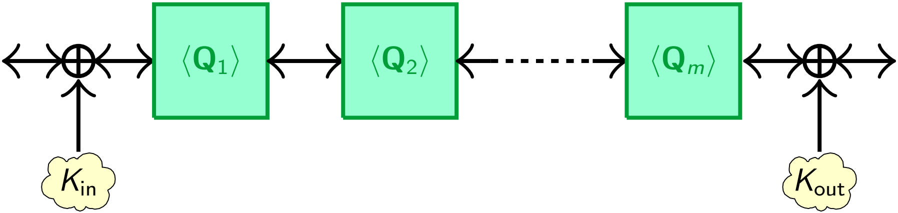
Then: $\forall$ cc-stateless $\mathbf{F}_1, \ldots, \mathbf{F}_m \in \mathcal{F}$ and $\forall\ \gamma > 0$

$$\Delta_{t,q}(\mathbf{C}(\mathbf{F}_1, \ldots, \mathbf{F}_m), \mathbf{C}(\mathbf{I}_1, \ldots, \mathbf{I}_m)) \leq \cancel{2^{m-1}} \prod_{i=1}^{m} \Delta_{t',q'}(\mathbf{F}_i, \mathbf{I}_i) + m \cdot \eta\left(q, \frac{1}{\gamma^2}\right) + \gamma,$$

with $t' = \mathcal{O}(\frac{t}{\gamma^2})$ and $q' = \mathcal{O}(\frac{q}{\gamma^2})$.

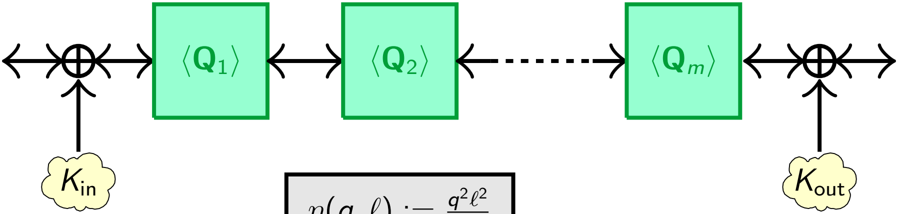
Example — Randomized Cascade of ↔PRPs

$\langle \mathbf{Q}_1 \rangle, \ldots, \langle \mathbf{Q}_m \rangle$: two-sided permutations $D \rightarrow D$ (e.g. $\langle \mathbf{E}_K \rangle$)



Example — Randomized Cascade of ↔PRPs

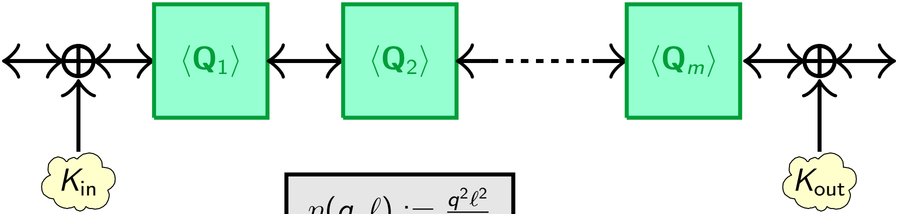
$\langle \mathbf{Q}_1 \rangle, \ldots, \langle \mathbf{Q}_m \rangle$: two-sided permutations $D \to D$ (e.g. $\langle \mathbf{E}_K \rangle$)



$$\eta(q, \ell) := \frac{q^2 \ell^2}{|D|}$$

Example — Randomized Cascade of ↔PRPs

$\langle \mathbf{Q}_1 \rangle, \ldots, \langle \mathbf{Q}_m \rangle$: two-sided permutations $D \to D$ (e.g. $\langle \mathbf{E}_K \rangle$)



$$\eta(q, \ell) := \frac{q^2 \ell^2}{|D|}$$

$$\Delta_{t,q}(\langle \mathbf{Q}_1 \rangle \triangleright \cdots \triangleright \langle \mathbf{Q}_m \rangle, \langle \mathbf{P} \rangle) \leq \prod_{i=1}^{m} \Delta_{t',q'}(\langle \mathbf{Q}_i \rangle, \langle \mathbf{P} \rangle) + \frac{mq^2}{|D|\gamma^4} + \gamma$$

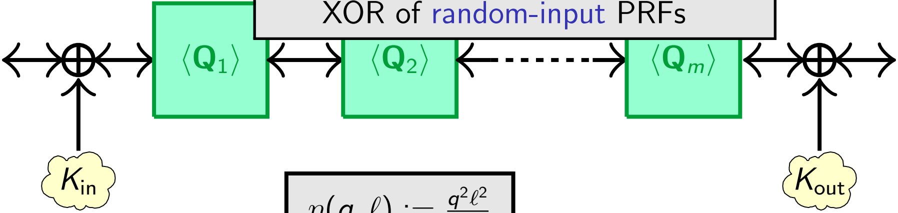
ε-↔PRP $\Longrightarrow$ (ε^m + negl)-↔PRP

Example — Randomized Cascade of ↔PRPs

Further Applications:

- Strong security amplification of PRFs [M03]
- Strong security amplification for XOR of random-input PRFs

$\langle \mathbf{Q}_1 \rangle, \ldots, \langle \mathbf{Q}_m \rangle$: … $\mathbf{E}_K \rangle)$



$$\eta(q, \ell) := \frac{q^2 \ell^2}{|D|}$$

$$\Delta_{t,q}(\langle \mathbf{Q}_1 \rangle \triangleright \cdots \triangleright \langle \mathbf{Q}_m \rangle, \langle \mathbf{P} \rangle) \leq \prod_{i=1}^{m} \Delta_{t',q'}(\langle \mathbf{Q}_i \rangle, \langle \mathbf{P} \rangle) + \frac{mq^2}{|D|\gamma^4} + \gamma$$

ε-↔PRP $\Longrightarrow$ $(\varepsilon^m + \text{negl})$-↔PRP

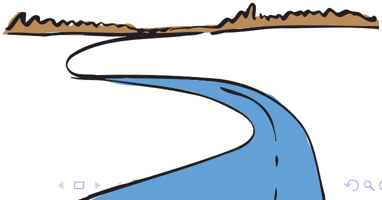
Outline

1. Generalizing Yao's XOR Lemma

2. Neutralizing Constructions

3. Strong Indistinguishability Amplification

4. Concluding Remarks



General Framework

- Improves all existing computational indistinguishability amplification results
- First standard-model analysis of cascaded encryption
- Strong security amplification for PRPs

Open Problems

- Further applications
- Specialized product theorems

Thank you!

Full Version: e-print 2009/396