Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Block-Cipher Cascading Strikes Back: Tight Bounds for Security Amplification

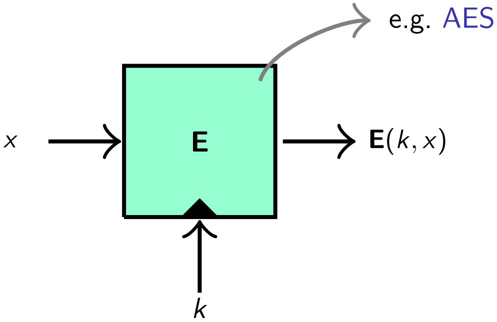
Stefano Tessaro

ETH Zurich

Rump Session EUROCRYPT 2010

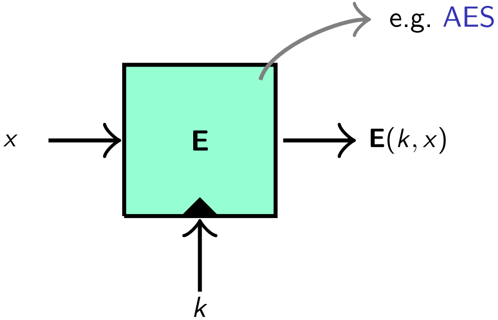
Motivation: Block Ciphers

Block Cipher



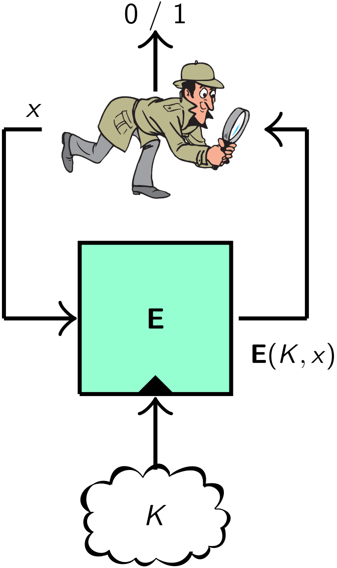
Motivation: Block Ciphers

Block Cipher

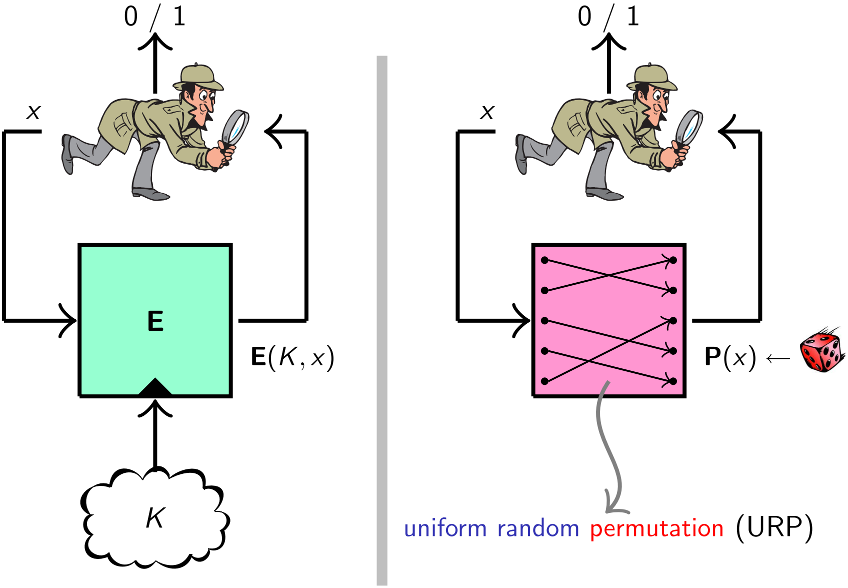


Security notion: **Pseudorandom Permutation**

Motivation: Block Ciphers – Pseudorandom Permutations

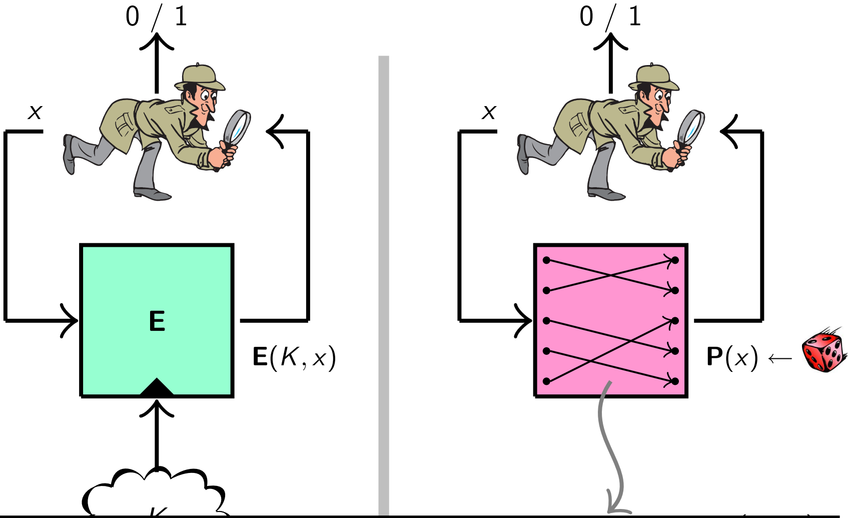


Motivation: Block Ciphers – Pseudorandom Permutations



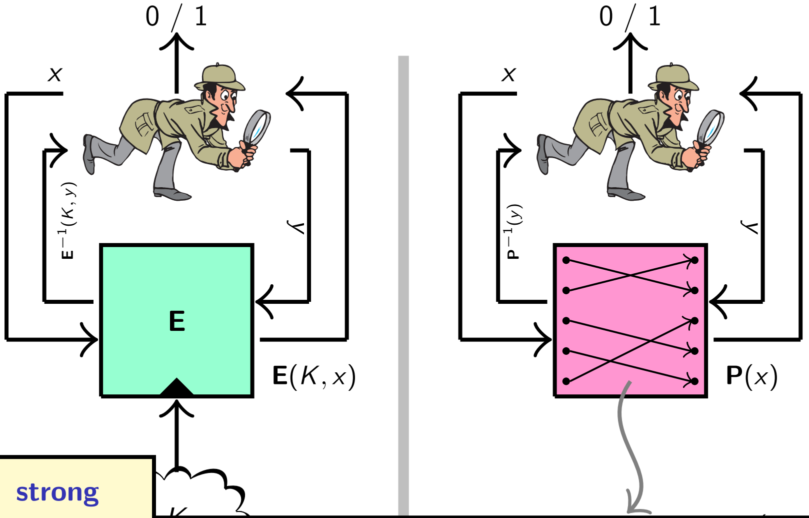
uniform random permutation (URP)

Motivation: Block Ciphers – Pseudorandom Permutations



E **PRP** $\Longleftrightarrow$ $\forall$ eff. : distinguishing advantage is **negligible**.

Motivation: Block Ciphers – Strong Pseudorandom Permutations

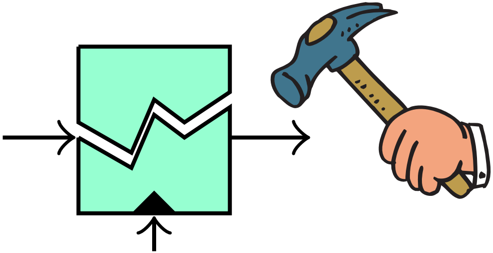


strong

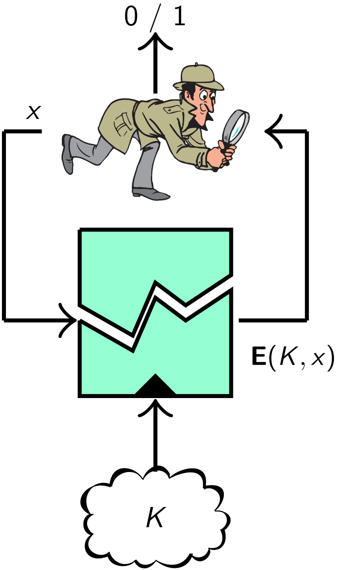
E **PRP** $\Longleftrightarrow$ $\forall$ eff. : distinguishing advantage is **negligible**.

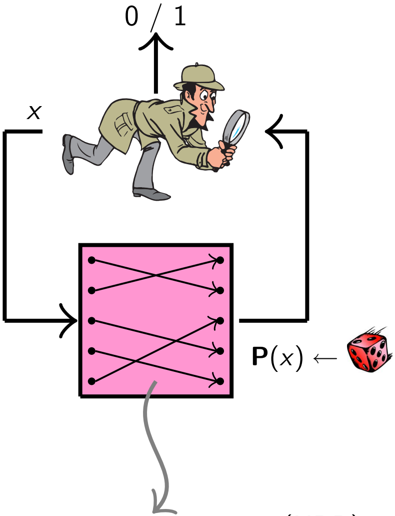
Cryptanalysis

Block Ciphers get broken!



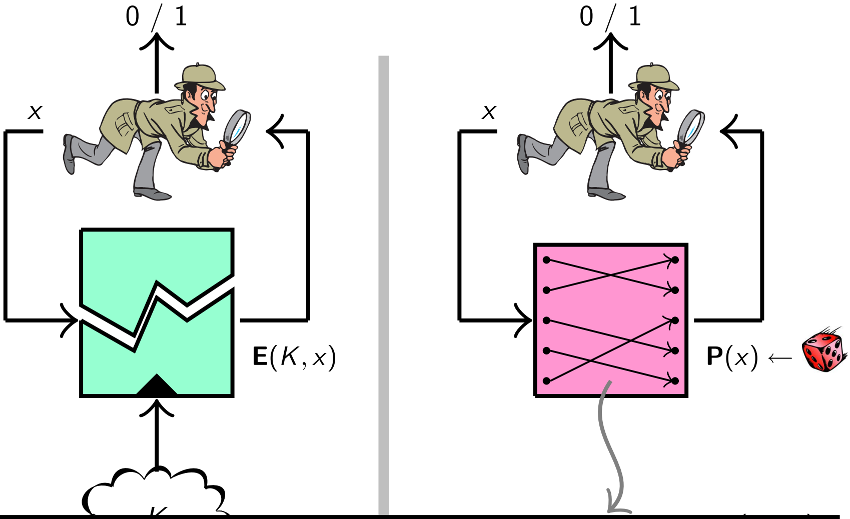
Weak Block Ciphers





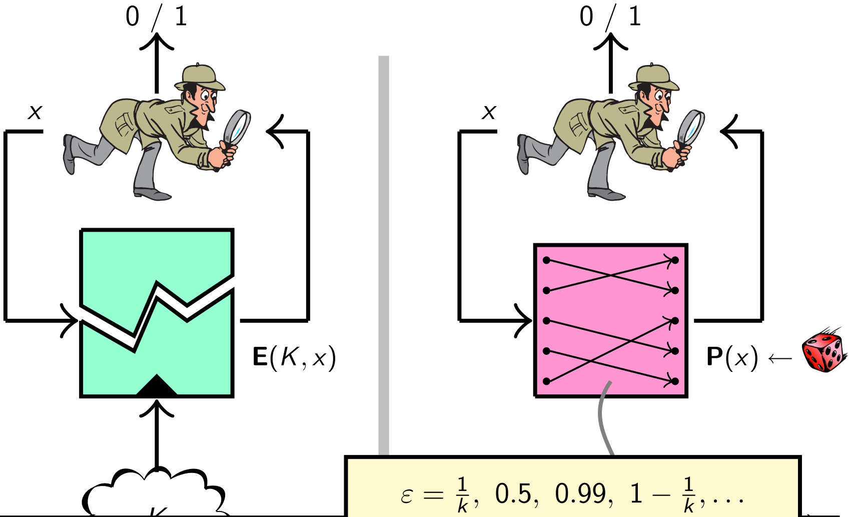
uniform random permutation (URP)

Weak Block Ciphers



E $\mathcal{E}$-**PRP** $\iff \forall$ eff. : distinguishing advantage is $\leq \mathcal{E}$.

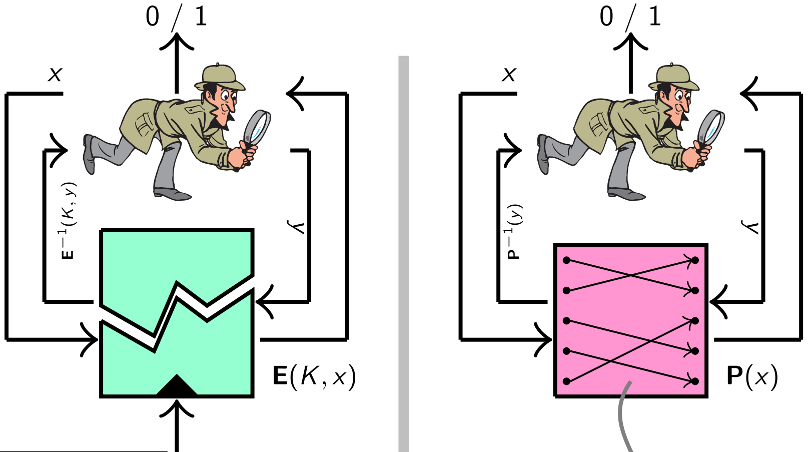
Weak Block Ciphers



$\varepsilon = \frac{1}{k},\ 0.5,\ 0.99,\ 1 - \frac{1}{k}, \ldots$

E $\mathcal{E}$-**PRP** $\iff \forall$ eff. : distinguishing advantage is $\leq \mathcal{E}$.

Weak Block Ciphers

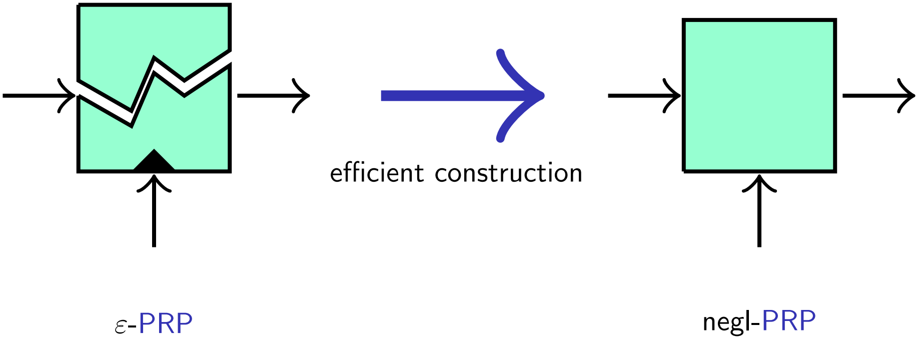


strong

$\varepsilon = \frac{1}{k},\ 0.5,\ 0.99,\ 1 - \frac{1}{k}, \ldots$

E ε-**PRP** $\iff \forall$ eff. : distinguishing advantage is $\leq \varepsilon$.

Security Amplification

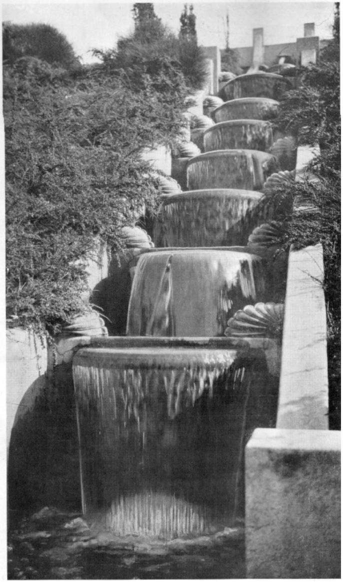


efficient construction

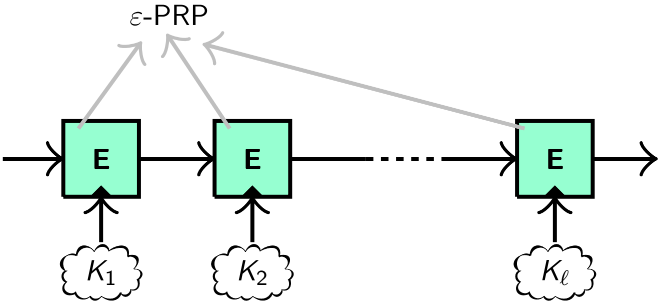
ε-PRP

negl-PRP

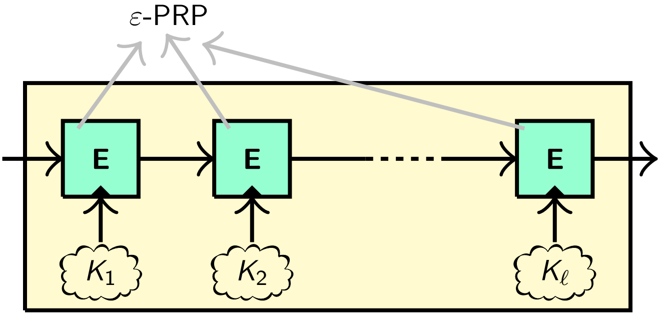
Cascades of Block Ciphers



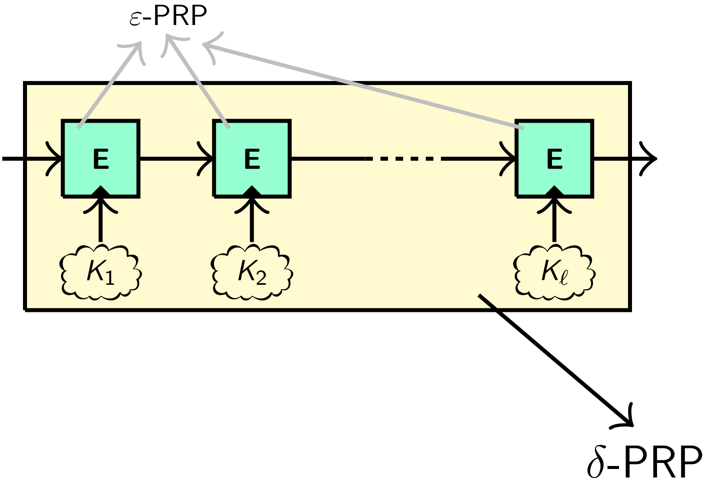
Cascades of Block Ciphers



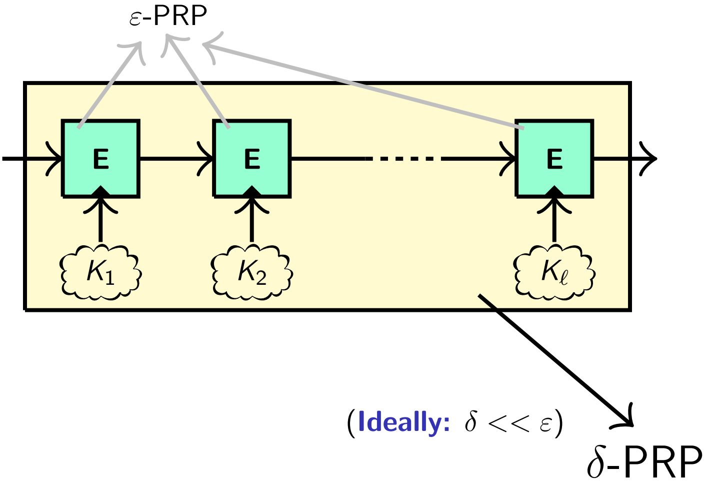
Cascades of Block Ciphers



Cascades of Block Ciphers

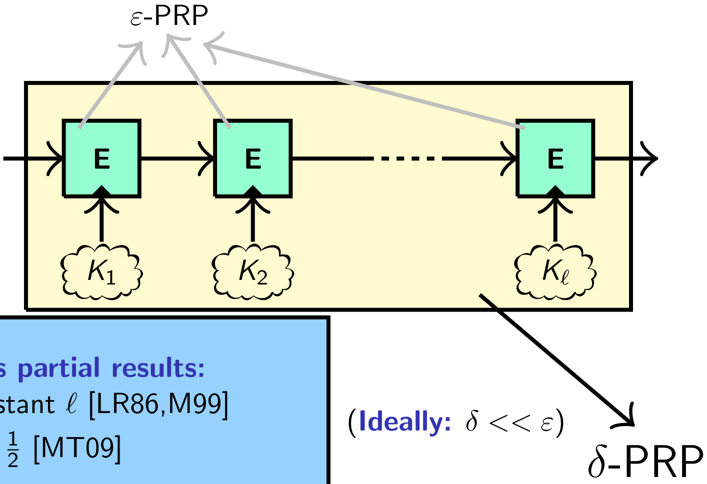


Cascades of Block Ciphers



(**Ideally:** $\delta << \varepsilon$)

Cascades of Block Ciphers

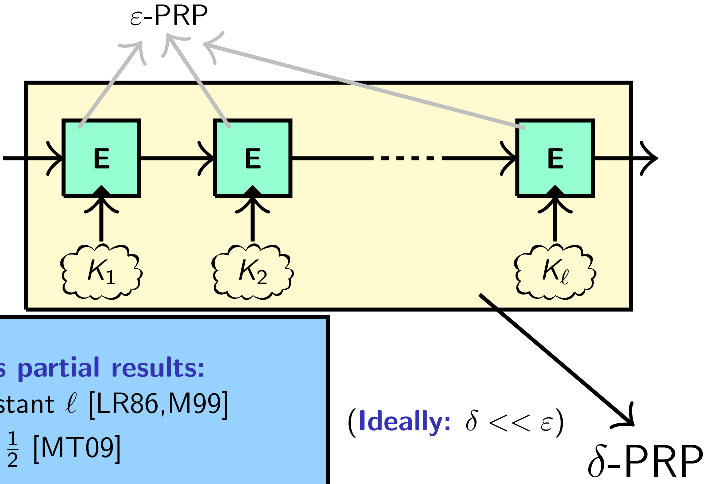


(**Ideally:** $\delta << \varepsilon$)

Previous partial results:

- constant ℓ [LR86,M99]
- $\varepsilon < \frac{1}{2}$ [MT09]

Our new bound: ℓ-cascade is $(\varepsilon^{\ell}(\ell-(\ell-1)\varepsilon)+\text{negl})$-PRP

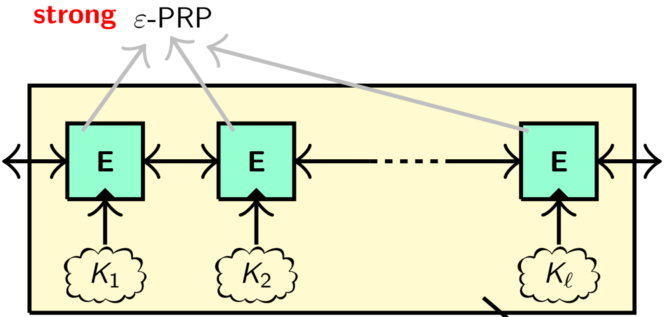


(**Ideally:** $\delta << \varepsilon$)

Previous partial results:

- constant ℓ [LR86,M99]
- $\varepsilon < \frac{1}{2}$ [MT09]

Our new bound: ℓ-cascade is $(\varepsilon^{\ell}(\ell-(\ell-1)\varepsilon)+\text{negl})$-PRP



strong ε-PRP

(**Ideally:** $\delta << \varepsilon$)

δ-PRP

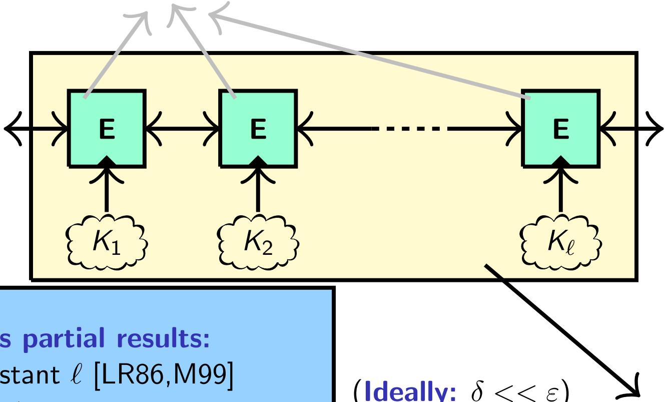
Previous partial results:

- constant ℓ [LR86,M99]
- $\varepsilon < \frac{1}{2}$ [MT09]

Our new bound: ℓ-cascade is $(\varepsilon^{\ell}(\ell-(\ell-1)\varepsilon)+\mathrm{negl})$-PRP

strong

strong ε-PRP



(**Ideally:** $\delta << \varepsilon$)

δ-PRP

Previous partial results:

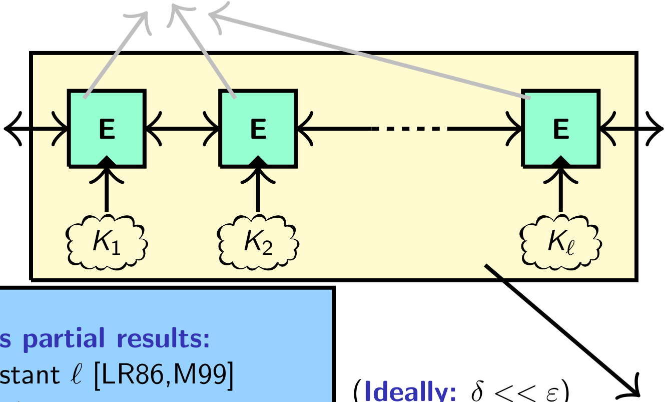
- constant ℓ [LR86,M99]
- $\varepsilon < \frac{1}{2}$ [MT09]

Our new bound: ℓ-cascade is $(\varepsilon^{\ell}(\ell - (\ell - 1)\varepsilon) + \text{negl})$-PRP

strong

Security amplification $\forall\ \varepsilon < 1 - \frac{1}{|\text{Domain}|}$

strong ε-PRP



(**Ideally:** $\delta << \varepsilon$)

δ-PRP

Previous partial results:

- constant ℓ [LR86,M99]
- $\varepsilon < \frac{1}{2}$ [MT09]

Conclusions

Final Remarks

- Bounds are **tight**
- **New technique** based on **interactive Hardcore Lemma**

Conclusions

Final Remarks

- Bounds are **tight**
- **New technique** based on **interactive Hardcore Lemma**

Paper

"Security Amplification for the Cascade of Arbitrarily Weak PRPs:
Tight Bounds via the Interactive Hardcore Lemma"
`www.crypto.ethz.ch/publications/`