Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Computational Indistinguishability Amplification:

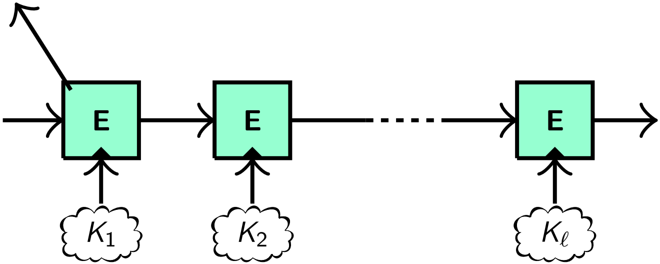
Provable Security Amplification by Cascade Encryption

Ueli Maurer **Stefano Tessaro**

ETH Zurich

Rump Session EUROCRYPT 2009

Cascade Encryption

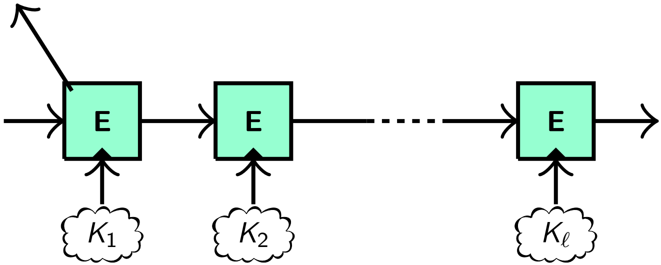


Block-Cipher (e.g. AES)

Cascade Encryption

security cascade $\geq$ security of **E**

Block-Cipher (e.g. AES)

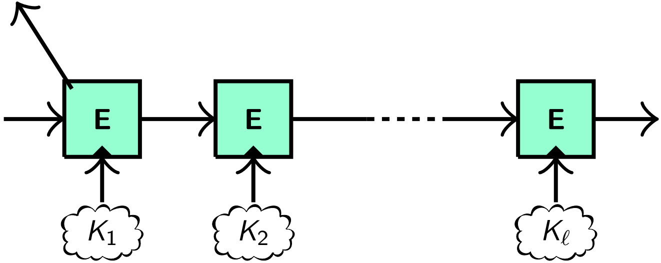


Cascade Encryption

???

security cascade $\gg$ security of **E**

Block-Cipher (e.g. AES)

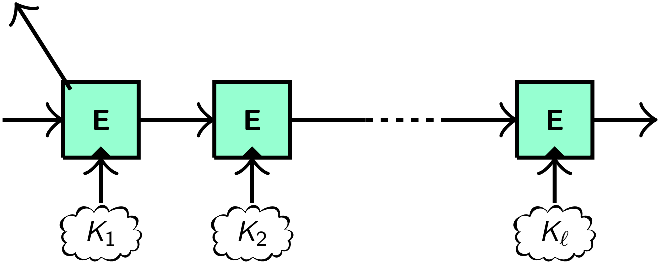


Cascade Encryption

???

security cascade $\gg$ security of **E**

Block-Cipher (e.g. AES)



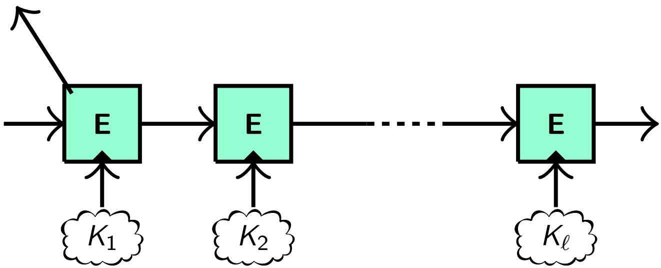
Previously: information-theoretic/ideal model [V99,BR06,MPR07,GM08]

Cascade Encryption

???

security cascade $\gg$ security of **E**

Block-Cipher (e.g. AES)



BUT: AES is only **computationally** secure

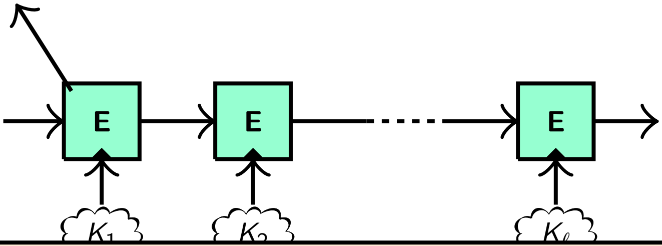
Previously: information-theoretic/ideal model [V99,BR06,MPR07,GM08]

Cascade Encryption

???

security cascade $\gg$ security of **E**

Block-Cipher (e.g. AES)

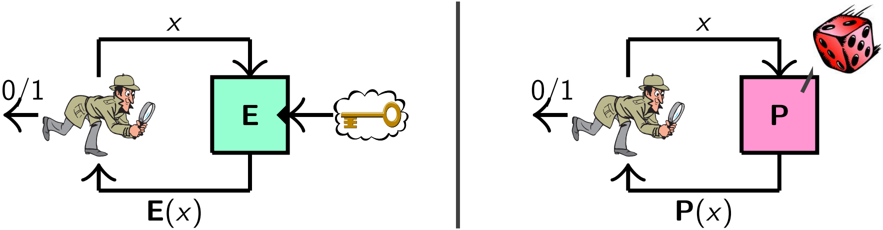


Our work: Computational security amplification (and more)

BUT: AES is only **computationally** secure

Previously: information-theoretic/ideal model [V99,BR06,MPR07,GM08]

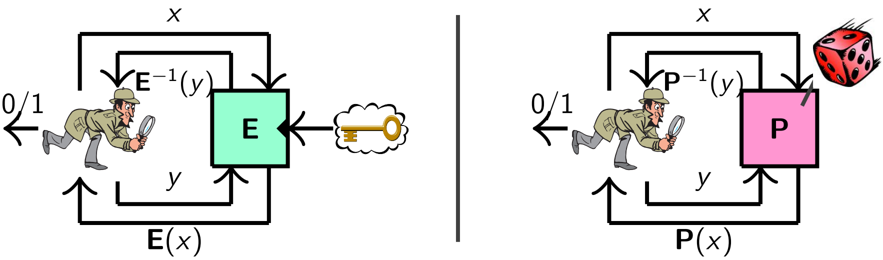
Pseudorandom Permutations (PRPs)



E PRP ⇔ ∀ PPT distinguishers **D** :

$$\mathbf{Adv} = |\Pr[\mathbf{D} = 1|\mathit{left}] = 1] - \Pr[\mathbf{D} = 1|\mathit{right}]| \;= \textbf{negligible}$$

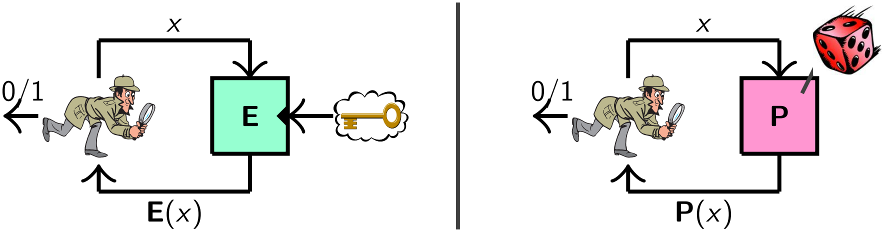
Pseudorandom Permutations (PRPs)



E **strong** PRP ⇔ ∀ PPT distinguishers **D** :

$\mathbf{Adv} = |\Pr[\mathbf{D} = 1|\mathit{left}] = 1] - \Pr[\mathbf{D} = 1|\mathit{right}]| =$ **negligible**

Pseudorandom Permutations (PRPs)

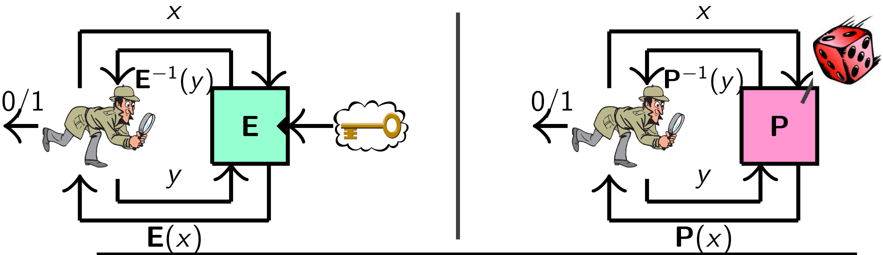


Examples: $\varepsilon = \text{negl}$, $\varepsilon = \frac{3}{4}$, $\varepsilon = 1 - \frac{1}{\text{poly}}$, ...

E $\mathcal{E}$-PRP ⇔ ∀ PPT distinguishers **D** :

$$\mathbf{Adv} = |\Pr[\mathbf{D} = 1|\textit{left}] = 1] - \Pr[\mathbf{D} = 1|\textit{right}]| \le \varepsilon$$

Pseudorandom Permutations (PRPs)

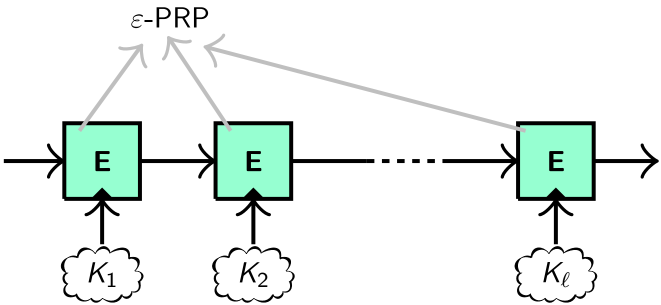


Examples: $\varepsilon = \text{negl}$, $\varepsilon = \frac{3}{4}$, $\varepsilon = 1 - \frac{1}{\text{poly}}$, ...

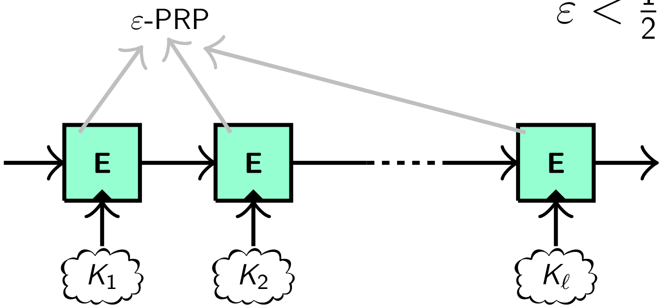
E **strong** $\mathcal{E}$-PRP $\Leftrightarrow \forall$ PPT distinguishers **D** :

$$\mathbf{Adv} = |\Pr[\mathbf{D} = 1|\mathit{left}] = 1] - \Pr[\mathbf{D} = 1|\mathit{right}]| \leq \varepsilon$$

Security of Cascades [MT09]



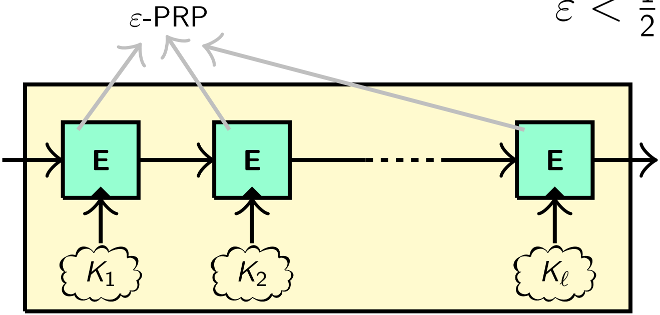
Security of Cascades [MT09]



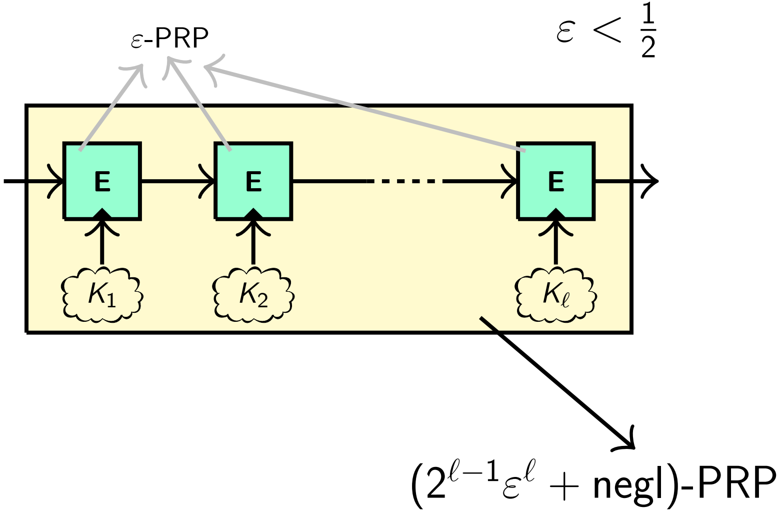
$$\varepsilon < \frac{1}{2}$$

Security of Cascades [MT09]

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

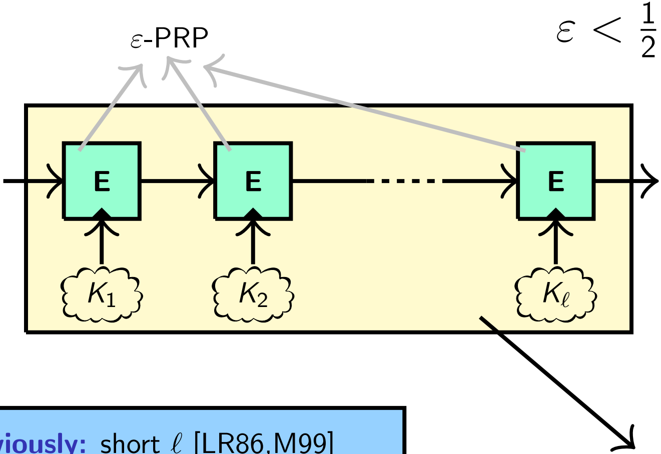


Security of Cascades [MT09]


ε-PRP
$\varepsilon < \frac{1}{2}$
E
E
E
K_1
K_2
K_ℓ
$(2^{\ell-1}\varepsilon^{\ell} + \text{negl})$-PRP

Cascades of Block-Ciphers

Security of Cascades [MT09]



$(2^{\ell-1}\varepsilon^{\ell} + \text{negl})$-PRP

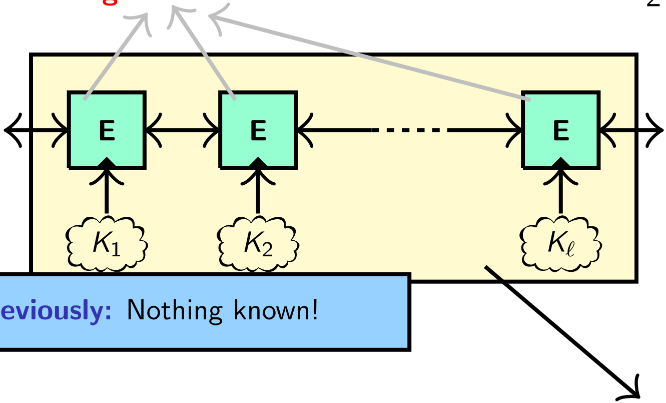
Previously: short ℓ [LR86,M99]

Cascades of Block-Ciphers

Security of Cascades [MT09]

strong ε-PRP

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



Previously: Nothing known!

strong $(2^{\ell-1}\varepsilon^{\ell} + \text{negl})$-PRP

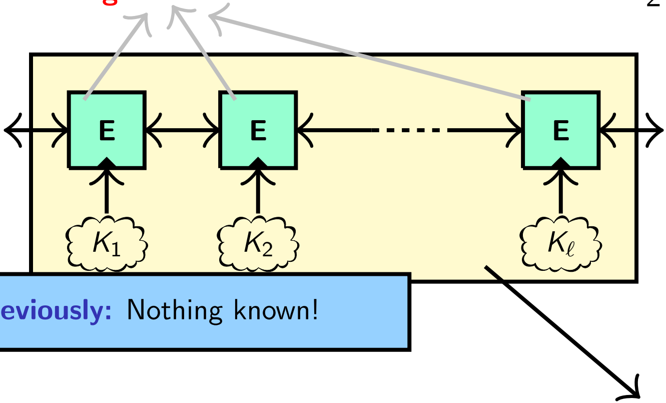
Cascades of Block-Ciphers

Security of Cascades [MT09]

Question: What if $\varepsilon \geq \frac{1}{2}$?

strong ε-PRP

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

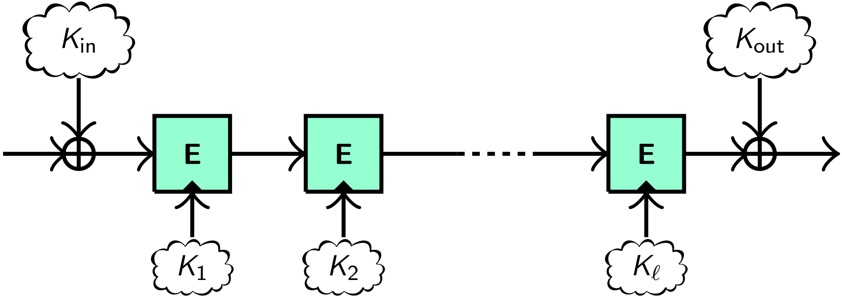


Previously: Nothing known!

strong $(2^{\ell-1}\varepsilon^{\ell} + \text{negl})$-PRP

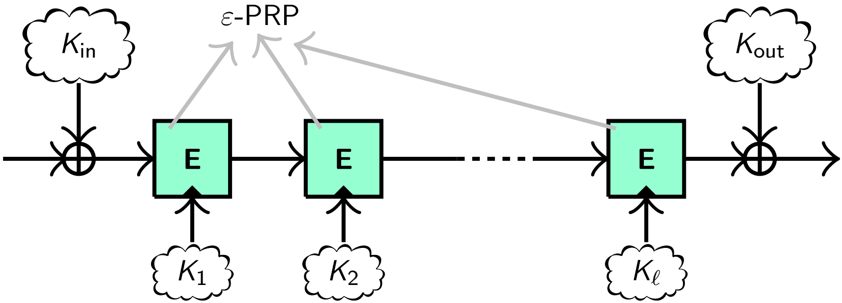
Cascades of Block-Ciphers

Randomized Cascade [MT09]



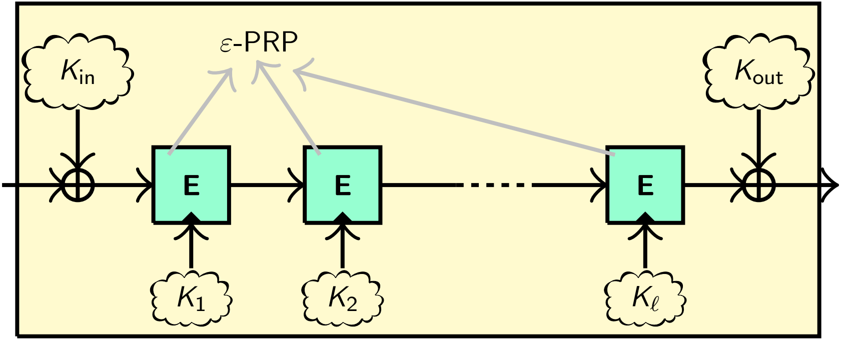
Cascades of Block-Ciphers

Randomized Cascade [MT09]



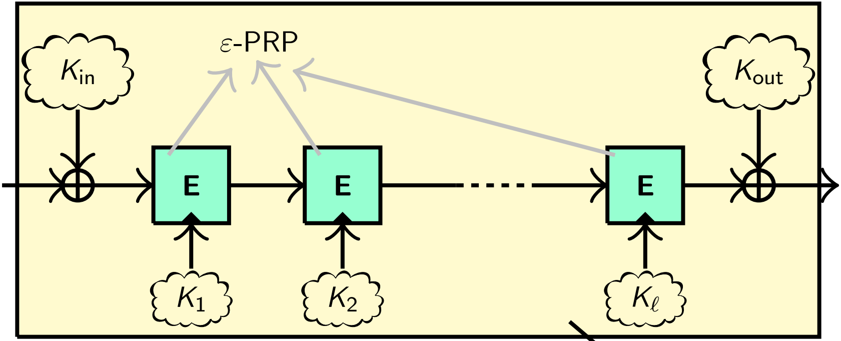
Cascades of Block-Ciphers

Randomized Cascade [MT09]



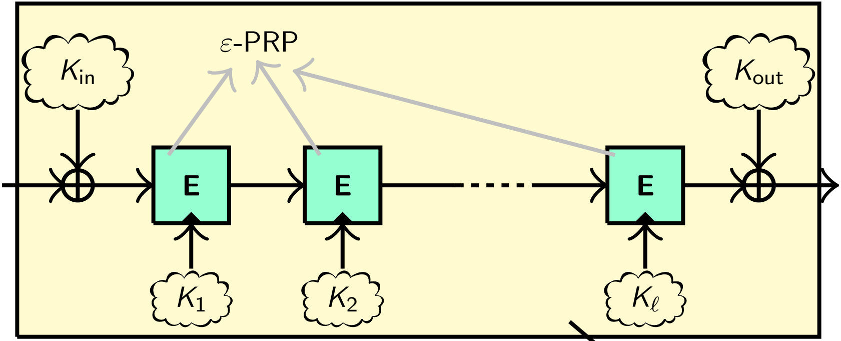
Cascades of Block-Ciphers

Randomized Cascade [MT09]



$(\varepsilon^\ell + \text{negl})$-PRP

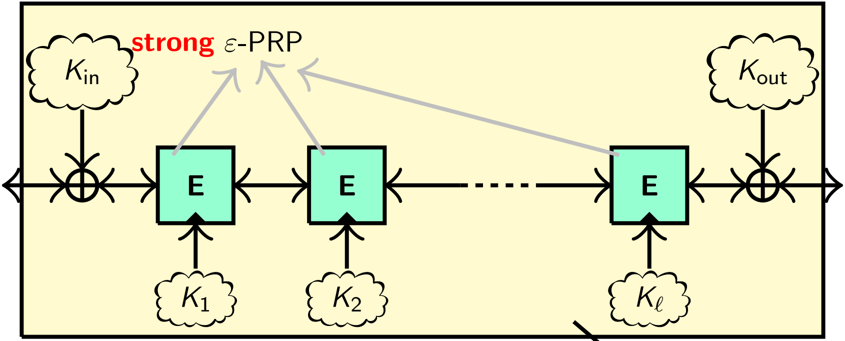
Randomized Cascade [MT09]



$(\varepsilon^\ell + \text{negl})$-PRP

Cascades of Block-Ciphers

Randomized Cascade [MT09]



strong $(\varepsilon^\ell + \text{negl})$-PRP

Conclusions

- **General framework** for **computational indistinguishability amplification**
- Further results on composition of **PRGs**, **PRFs**, **random-input-secure PRFs (WPRFs)**, ...

Conclusions

- **General framework** for **computational indistinguishability amplification**
- Further results on composition of **PRGs**, **PRFs**, **random-input-secure PRFs (WPRFs)**, ...

Coming soon ...