Security Amplification against Meet-in-the-Middle Attacks Using Whitening

Pierre-Alain Fouque[†] **Pierre Karpman**[⋆]

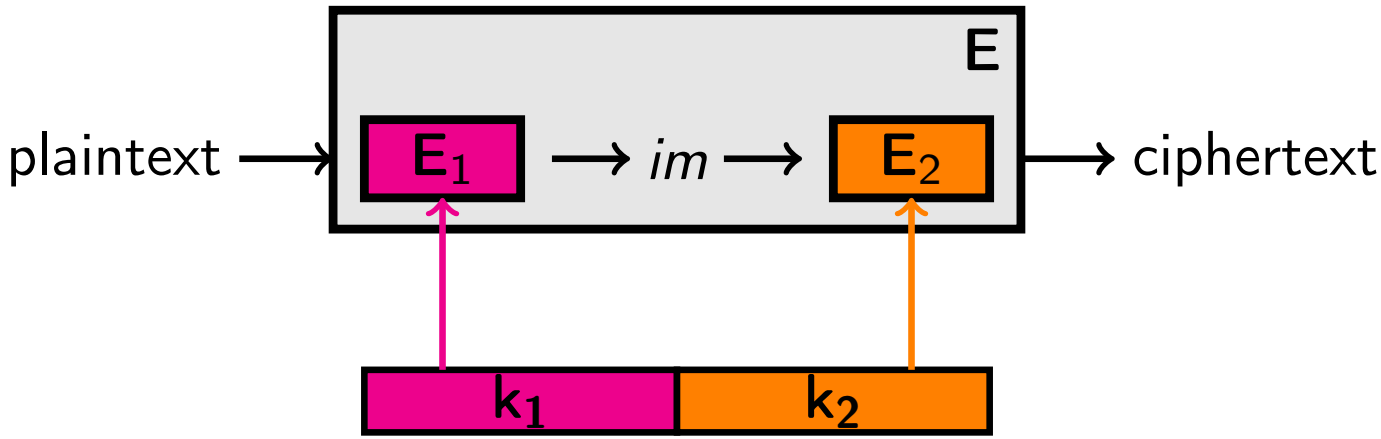
[†]Université de Rennes 1 & Institut universitaire de France
[⋆]École normale supérieure de Rennes

14th IMA Conference on Cryptography & Coding, Oxford
2013–12–18

The standard Meet-in-the-Middle (MiTM) attack

Idea

- decomposition $\mathbf{E}(k,\cdot) = \mathbf{E}_2(k_2) \circ \mathbf{E}_1(k_1)(\cdot)$ with $k_1 \cap k_2 = \emptyset$
- use $im = \mathbf{E}_1(k_1, p) = \mathbf{E}_2^{-1}(k_2, c)$ to filter wrong guesses

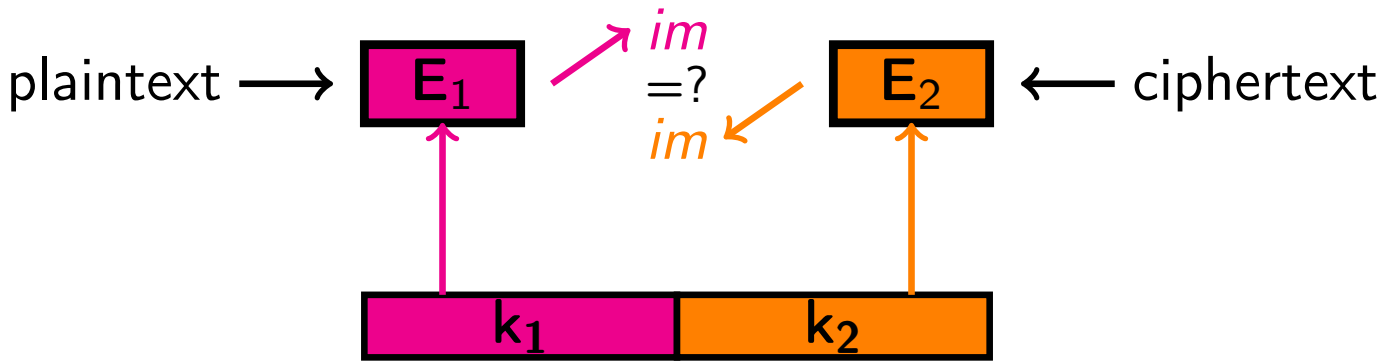


- Time complexity: $\sim \max(2^{\kappa_1}, 2^{\kappa_2})$ instead of $\sim 2^{\kappa_1+\kappa_2}$
- Memory complexity: $\sim \min(2^{\kappa_1}, 2^{\kappa_2})$ instead of ~ 1
- Data complexity: ~ 1

The standard Meet-in-the-Middle (MiTM) attack

Idea

- decomposition $\mathbf{E}(k,\cdot) = \mathbf{E}_2(k_2) \circ \mathbf{E}_1(k_1)(\cdot)$ with $k_1 \cap k_2 = \emptyset$
- use $im = \mathbf{E}_1(k_1, p) = \mathbf{E}_2^{-1}(k_2, c)$ to filter wrong guesses

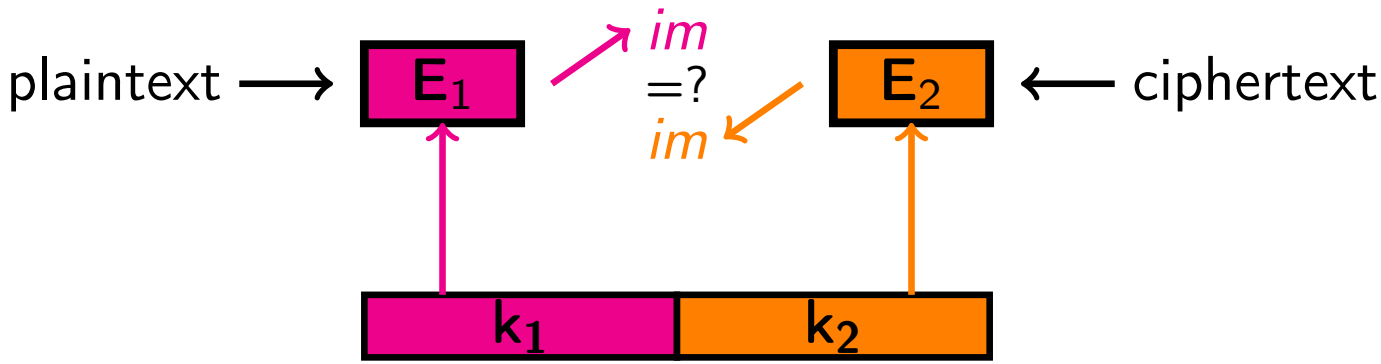


- Time complexity: $\sim \max(2^{\kappa_1}, 2^{\kappa_2})$ instead of $\sim 2^{\kappa_1+\kappa_2}$
- Memory complexity: $\sim \min(2^{\kappa_1}, 2^{\kappa_2})$ instead of ~ 1
- Data complexity: ~ 1

The standard Meet-in-the-Middle (MiTM) attack

Idea

- decomposition $\mathbf{E}(k,\cdot) = \mathbf{E}_2(k_2) \circ \mathbf{E}_1(k_1)(\cdot)$ with $k_1 \cap k_2 = \emptyset$
- use $im = \mathbf{E}_1(k_1, p) = \mathbf{E}_2^{-1}(k_2, c)$ to filter wrong guesses



- Time complexity: $\sim \max(2^{\kappa_1}, 2^{\kappa_2})$ instead of $\sim 2^{\kappa_1+\kappa_2}$
- Memory complexity: $\sim \min(2^{\kappa_1}, 2^{\kappa_2})$ instead of ~ 1
- Data complexity: ~ 1

(Recent) MiTM attacks in practice

- Best attacks on reduced AES (Demirci, Selçuk, FSE2008; DKS, ASIACRYPT2010; DFJ, EUROCRYPT2013)
- Best attacks on reduced IDEA (Biham, Dunkelman, Keller, Shamir, 2011)
- Best attacks on full GOST (Isobe, FSE2011; Dinur Dunkelman, Shamir, FSE2012)

- Preimages on the MD4 family, Splice & cut and Initial structures (Sasaki, Aoki, EUROCRYPT2009, CRYPTO2009)

- Biclique attacks on AES & IDEA (Bogdanov, Khovratovich, Rechberger, ASIACRYPT2011; KLR, EUROCRYPT2012)

Making MiTM attacks less efficient

Context

- No theory behind key schedule design (linear, non-linear, heavy, light?)
- Hard to go beyond ad hoc analysis

Requirements

- Be generic ⇒ Black box construction

Objective

- Resulting cipher is more secure w.r.t. (standard) MiTM attacks

Black box constructions aren't new

Usual objective

- Increase equivalent key-length

In our case

- Don't introduce new key material!
  - Don't redefine security parameters
  - Start by fully using the existing key!
- (Low overhead)

Example black boxes

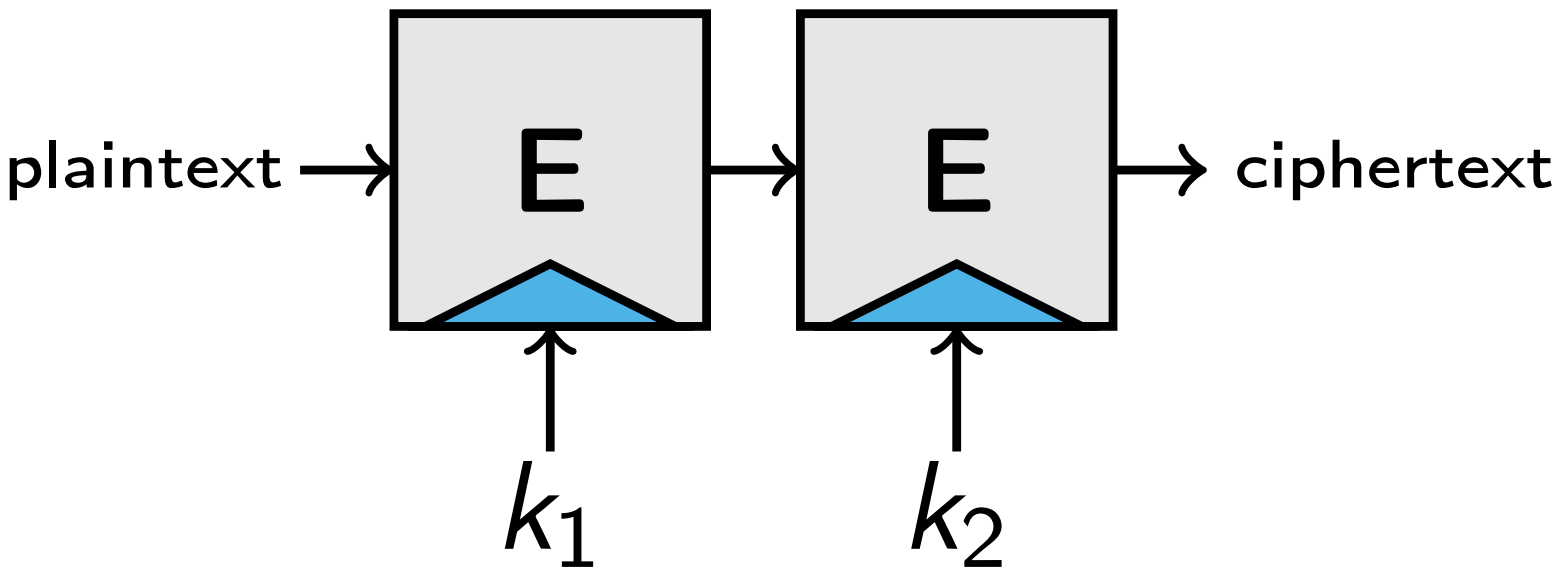


Figure : Cascade encryption (Diffie, Hellman, 1977, & Others)

Example black boxes

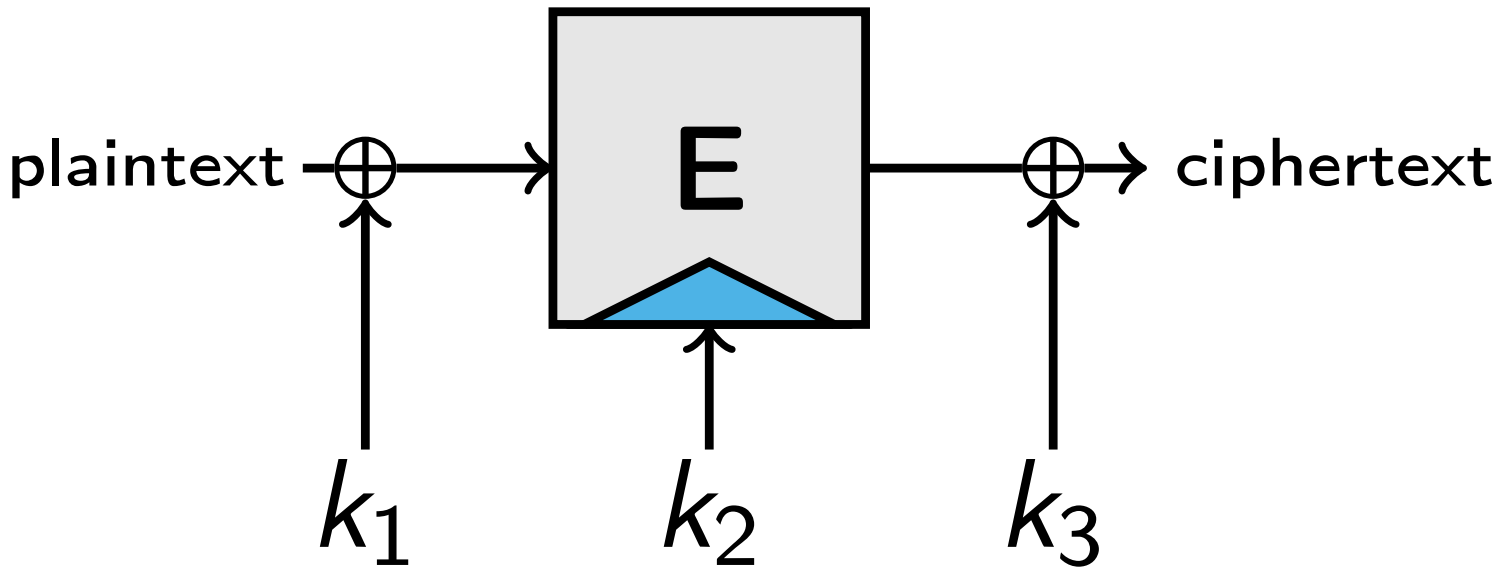


Figure : DESX/FX (Rivest, 1995; Kilian, Rogaway, CRYPTO1996)

Example black boxes

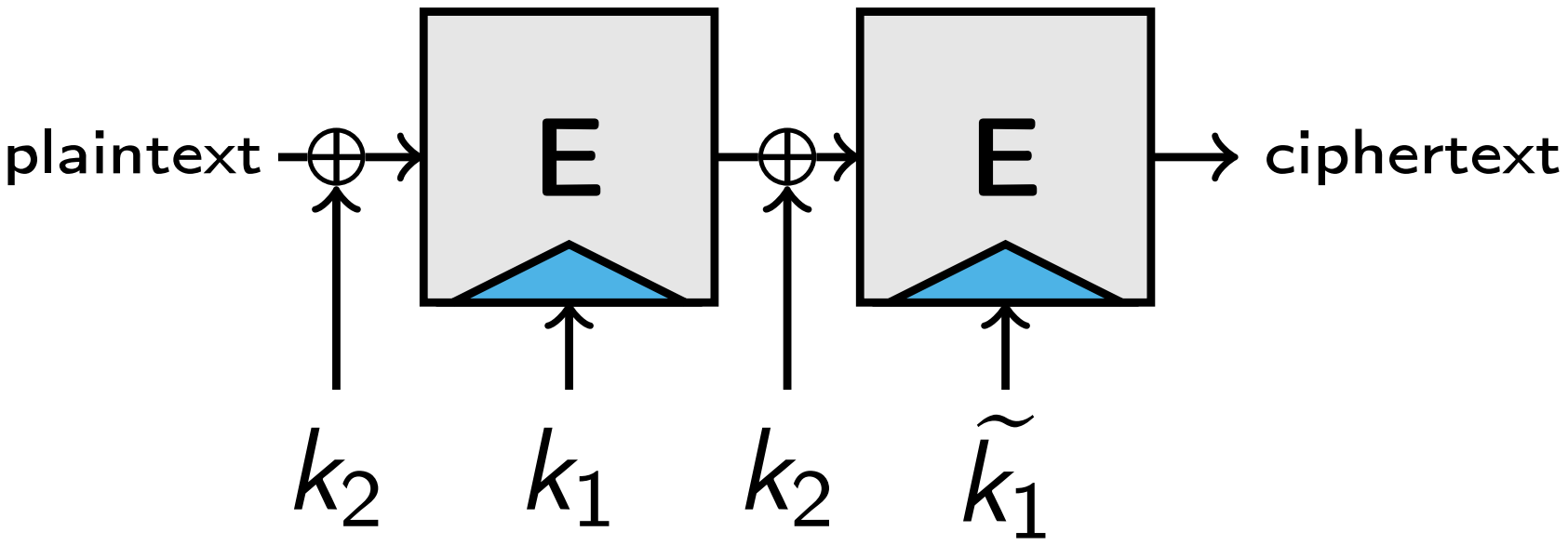
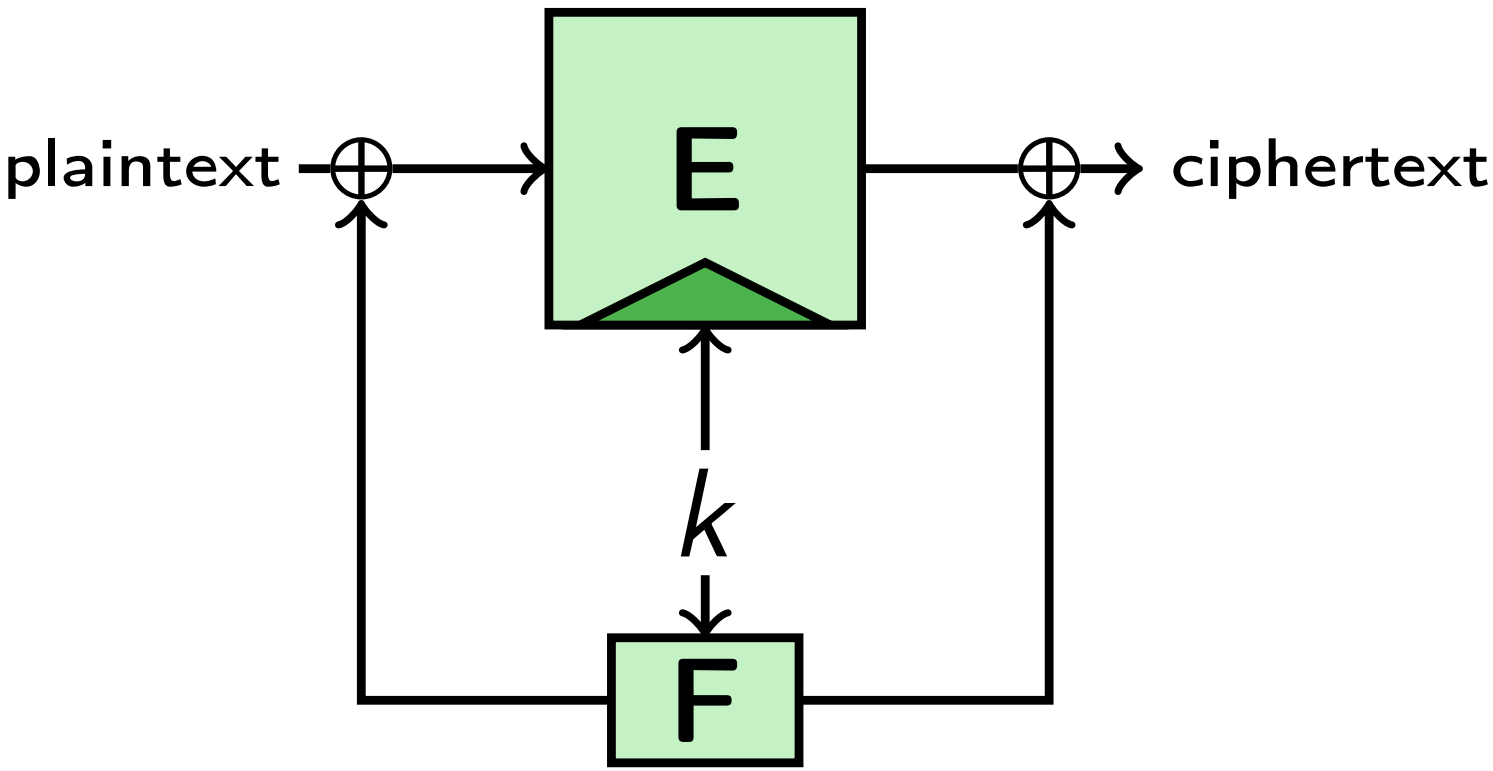
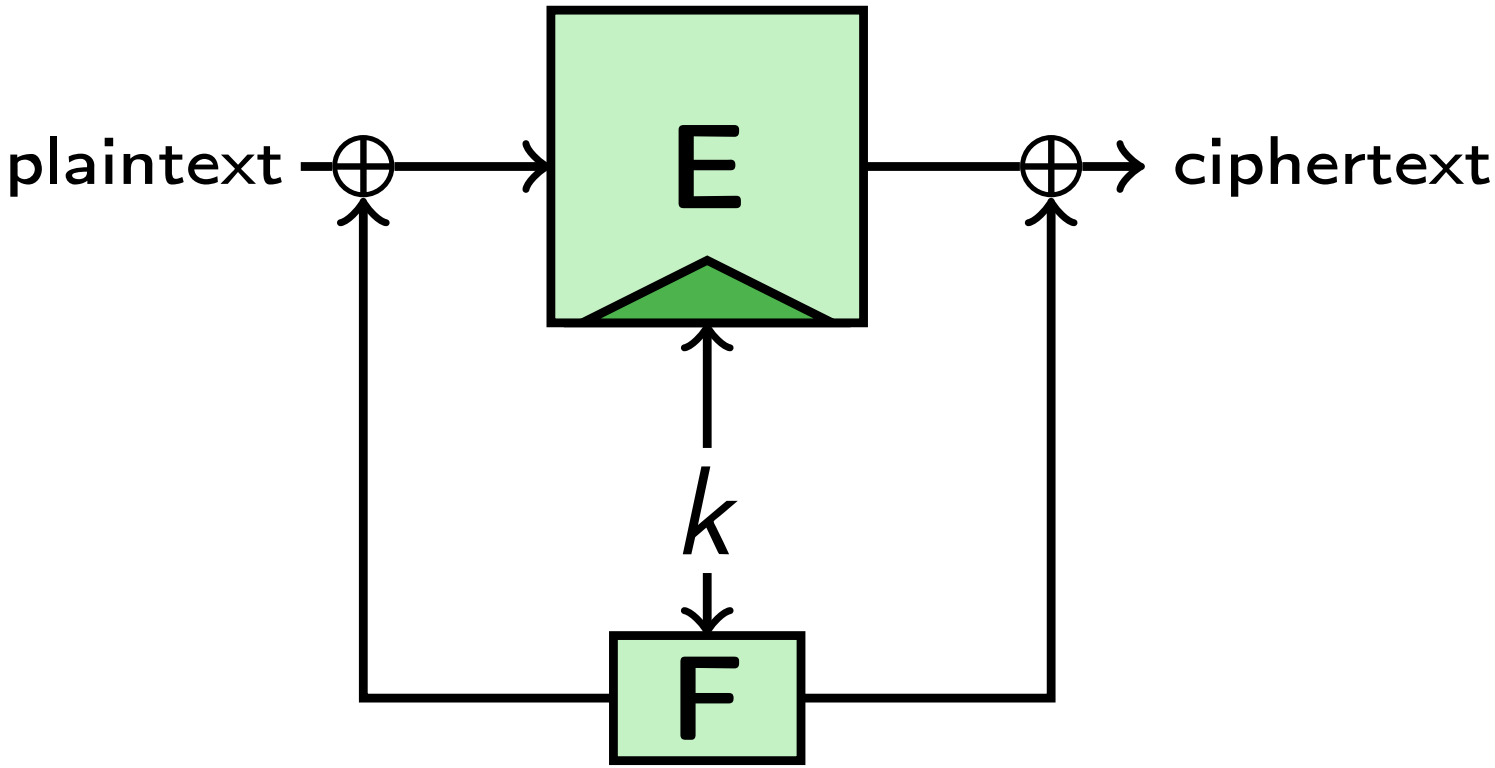


Figure : XOR Cascade (Gaži, Tessaro, EUROCRYPT2012)

Our black box proposal



Our black box proposal



Intuition

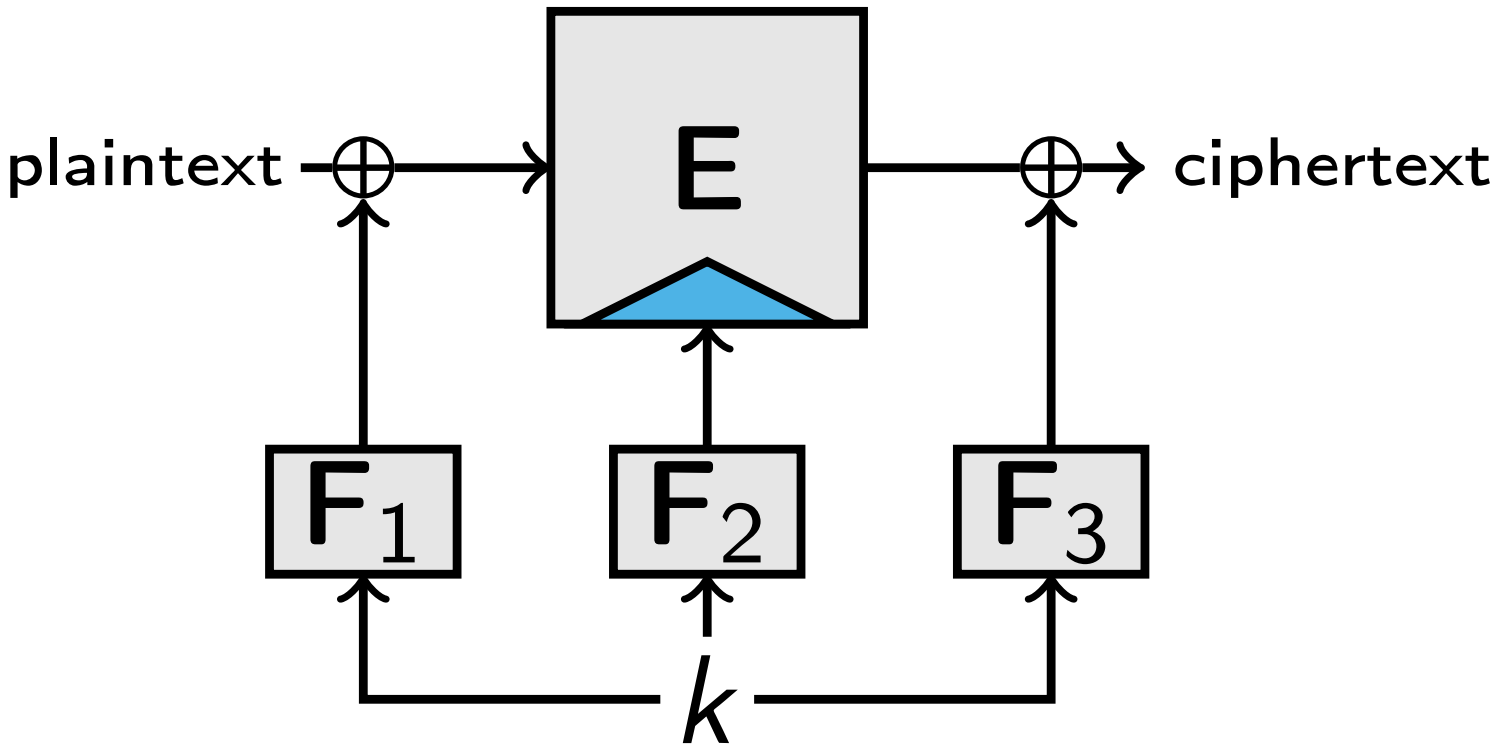
- Attacker has to commit to a value for k
- Or he has to work with more 'key material'

Requirements for **F**

- Objective: $\mathbf{F}(x)$ 'thoroughly depends on x'
- Not knowing part of $x \Rightarrow \mathbf{F}(x)$ seems random
- $\Rightarrow$ **F** is an exposure resilient function (ERF) (CDHKS, EUROCRYPT2000)
  - Related to all-or-nothing transformation (AONT) (Rivest, FSE1997)
- The k-bit output of an $\ell - ERF$ is indistinguishable from random when ℓ input bits are unknown
- Perfect $\ell - ERF$s can be built from linear codes if $\ell \geq k$
- Most secure symmetric primitives are computational $0/1 - ERF$s

Sidenote on DESX

Nicer key-length for DESX/FX (Kilian, Rogaway, CRYPTO1996):

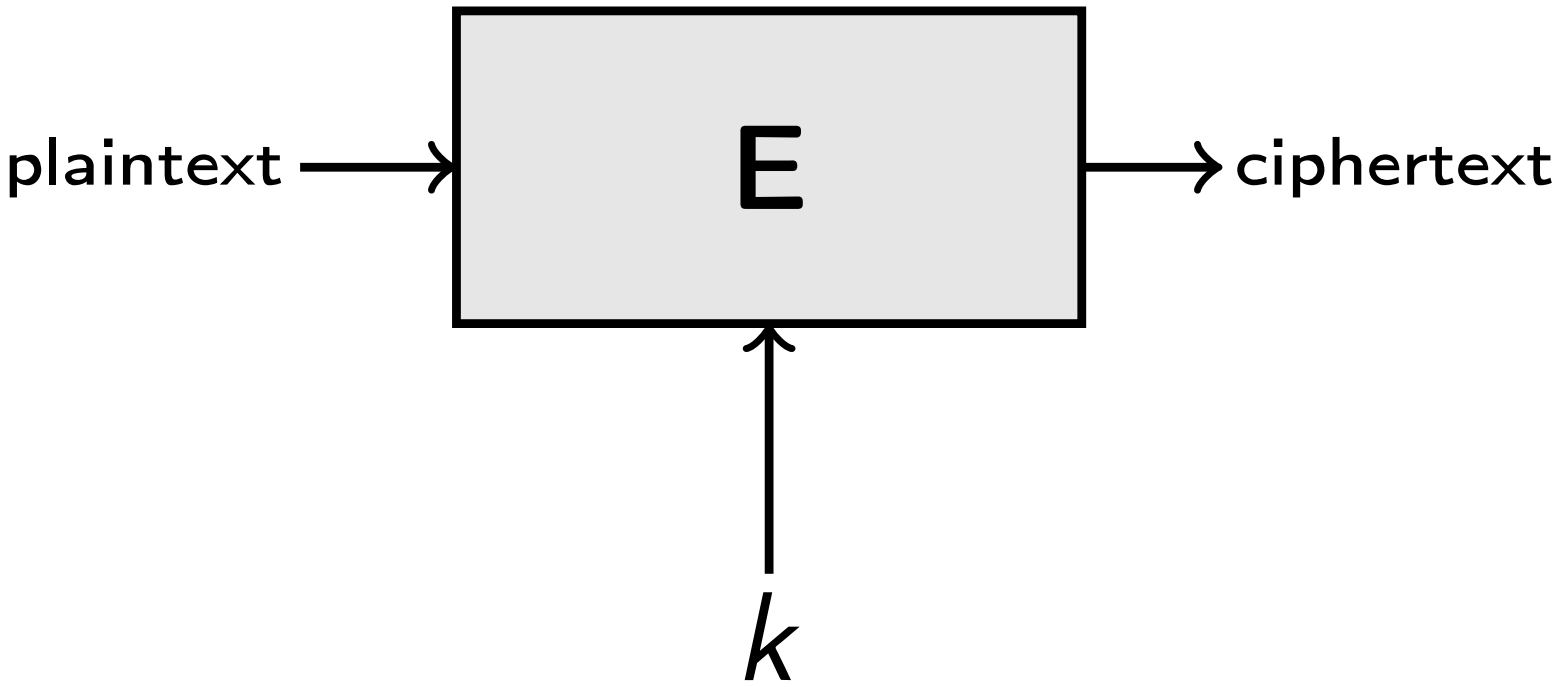


A model for MitM attacks

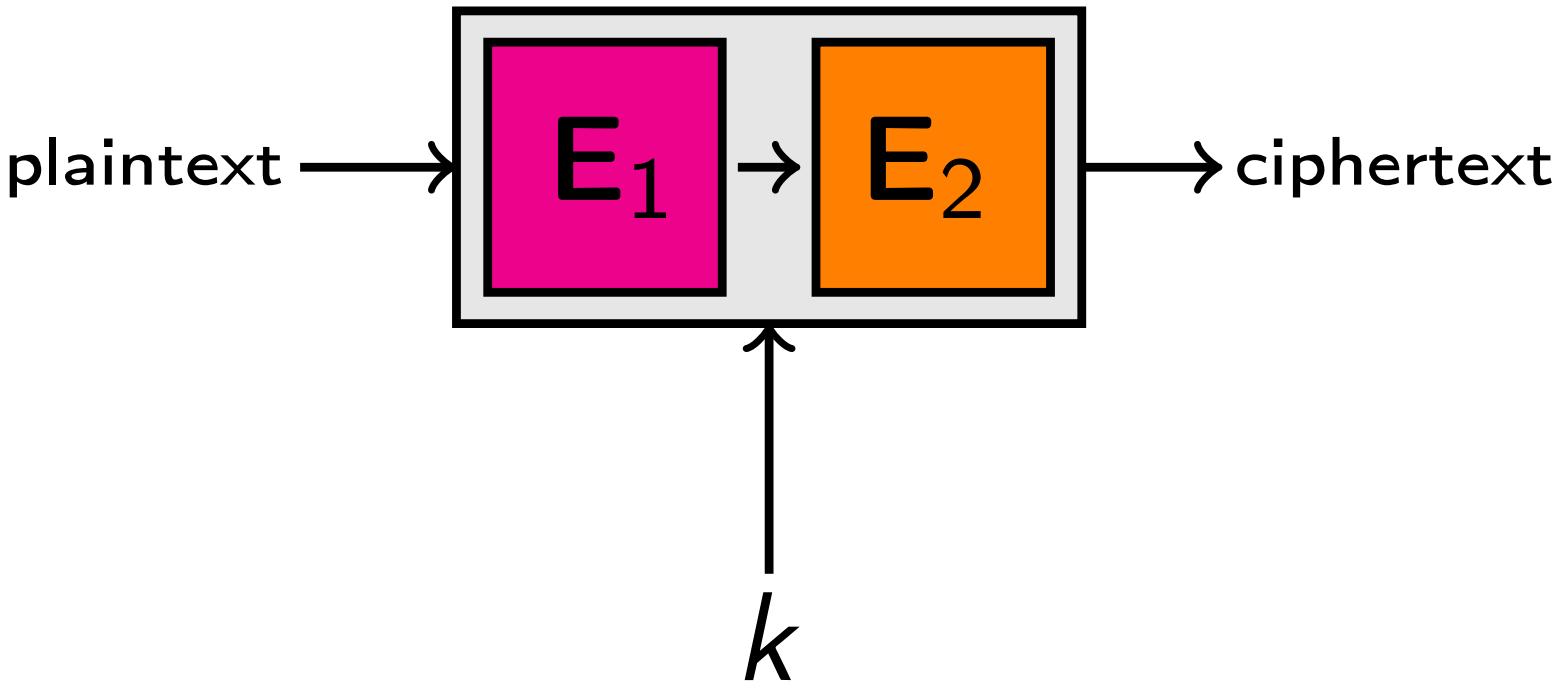
Idea

- MiTM attacks are most effective when
  - meeting on the whole block
  - $\kappa_1 = \kappa_2$
- $\Rightarrow$ Equivalent to attacking a 2-Cascade
- $\Rightarrow$ Make 2-Cascade more secure
- $\Rightarrow$ Apply the technique to a single cipher

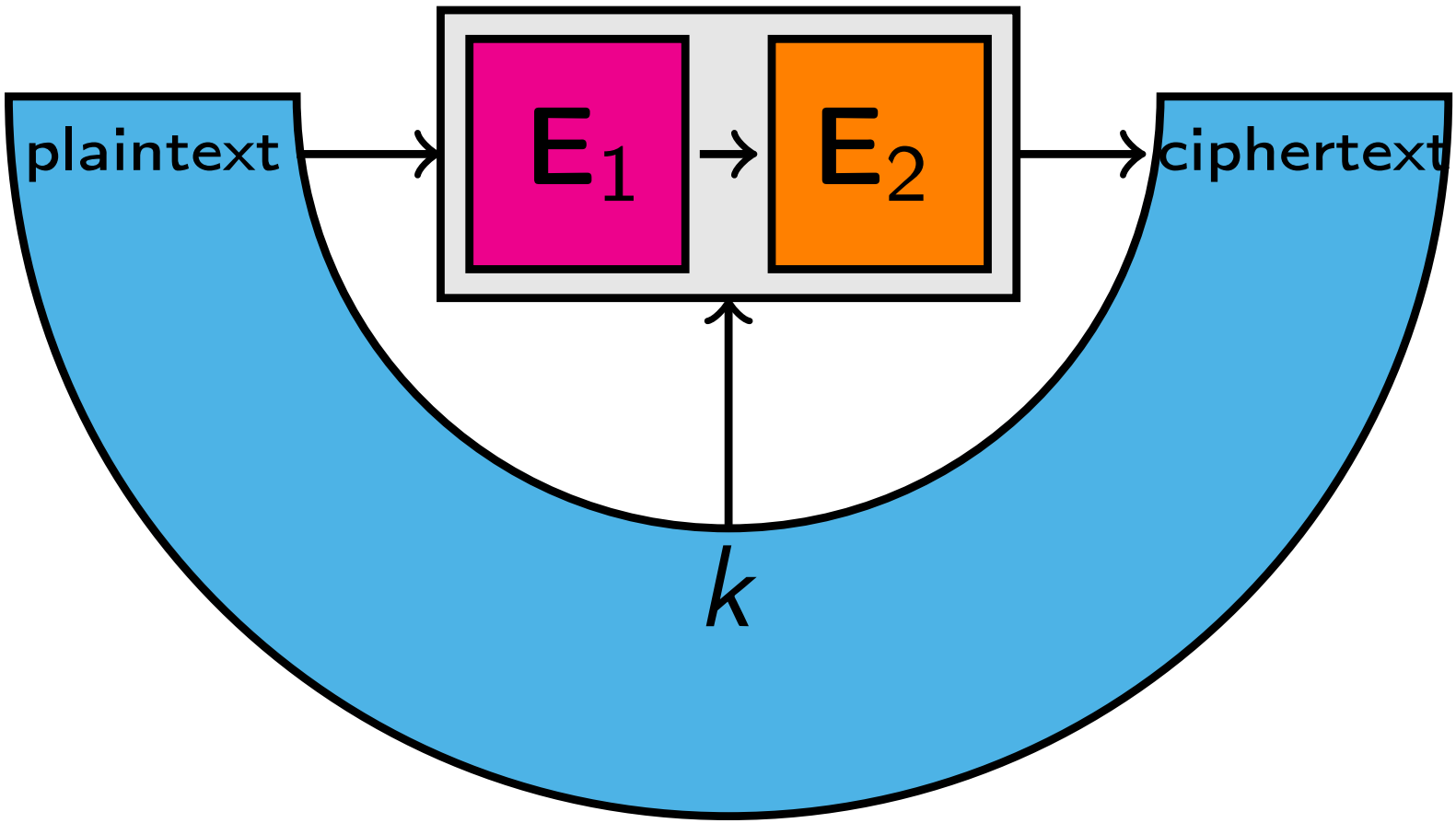
In a picture



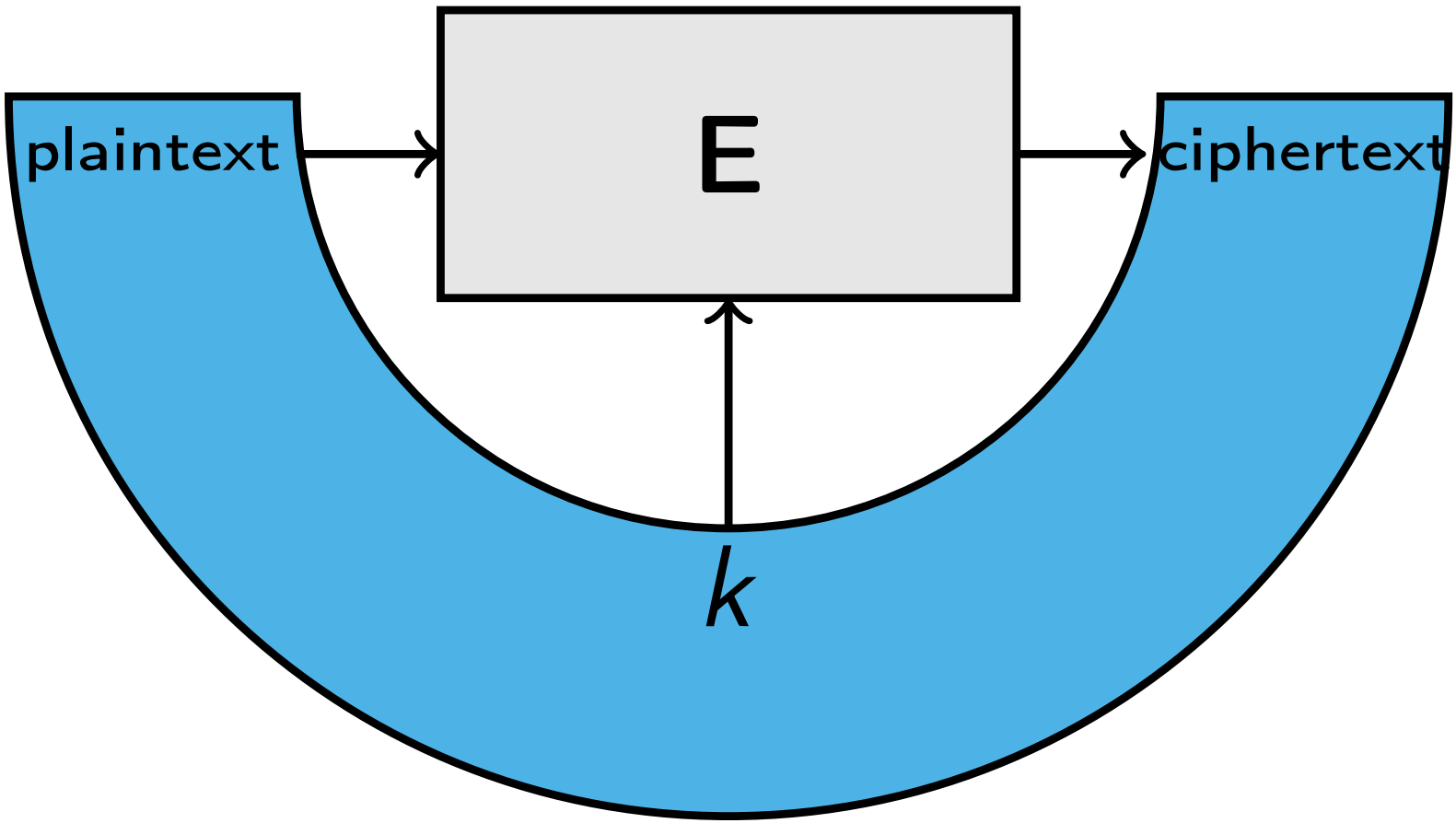
In a picture



In a picture



In a picture



More security for the 2-Cascade

- Natural attack is MiTM
- Advantage of an adversary with t queries is $\leq t^2/2^{2\kappa}$ (ABCV, CRYPTO1998) and tight $\Rightarrow$ only $\sim 2^{\kappa}$ queries for an advantage of one
- Apply a construction $\mathbf{C}$ $\Rightarrow$ success if advantage on $\mathbf{C}$ is $\ll t^2/2^{2\kappa}$

Our result for the 2-Cascade

For $\mathbf{C}(\mathbf{E}_2 \circ \mathbf{E}_1(k_1||k_2, x)) \triangleq \mathbf{E}_2 \circ \mathbf{E}_1(k_1||k_2, x \oplus \mathbf{F}(k_1||k_2)) \oplus \mathbf{F}(k_1||k_2)$ with $\mathbf{F}$ an ℓ-ERF:

- $\mathrm{Advantage}(\ell, D, q_1, q_2, q_f)$
  $\leq 2^{-2\kappa} \max\left(2^{\ell}\binom{n}{\ell} \cdot q_f, \quad 2^{-n} \cdot D \cdot \sum_{k_1', k_2'} \min(q_1(k_1'), q_2(k_2'))\right)$
- For an advantage of one $\Rightarrow 2^{2\kappa}/2^{\ell}\binom{n}{\ell}$ or $2^{\kappa+n}/D$ queries to the oracles $\underset{(\ell=0,\ n=\kappa,\ D=1)}{=} 2^{2\kappa}$ (instead of 2^{κ})

Summary

- For $D \ll 2^n$, advantage on $\mathbf{C} \ll$ advantage on the 2-Cascade
- Not true if $D \sim 2^n$
- Much more data needed for (theoretical) advantage comparable to 2-Cascade (not tight)
- Result carries on to a single cipher

About the proof

- Ideal cipher model
- Similar to DESX (Kilian, Rogaway, CRYPTO1996)
- Bound the probability of distinguishing the construction from a random permutation

Instantiating $\mathbf{F}$

Some possibilities among many

- Use a stand-alone hash function
- Build the 'hash function' from $\mathbf{E}$ or $\widetilde{\mathbf{E}}$: $\mathbf{F}(x) = \widetilde{\mathbf{E}}(x) \oplus x$
  $\Rightarrow$ compact implementation
- $\Rightarrow$ low amortized cost

Conclusion

- A model for standard MiTM on block ciphers
- A versatile and generic construction to increase the security of ciphers w.r.t MiTM attack
- Easy and efficient instantiations possible