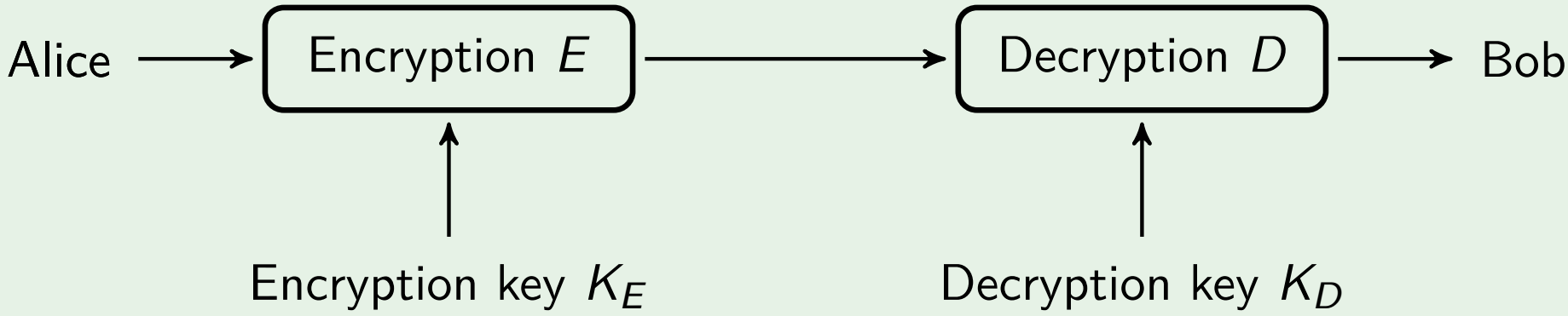
Proprietà crittografiche di funzioni Booleane nei block cipher

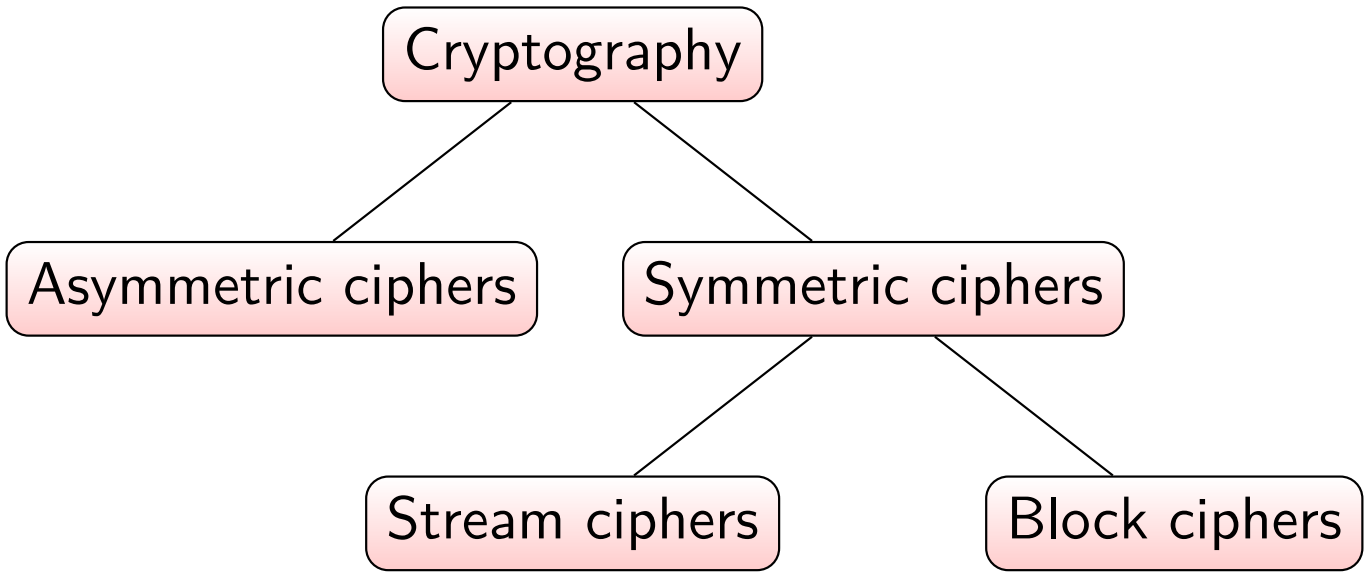
Irene Villa

Università di Trento

CrypTO Conference 2023 - 25/26 Maggio, Torino

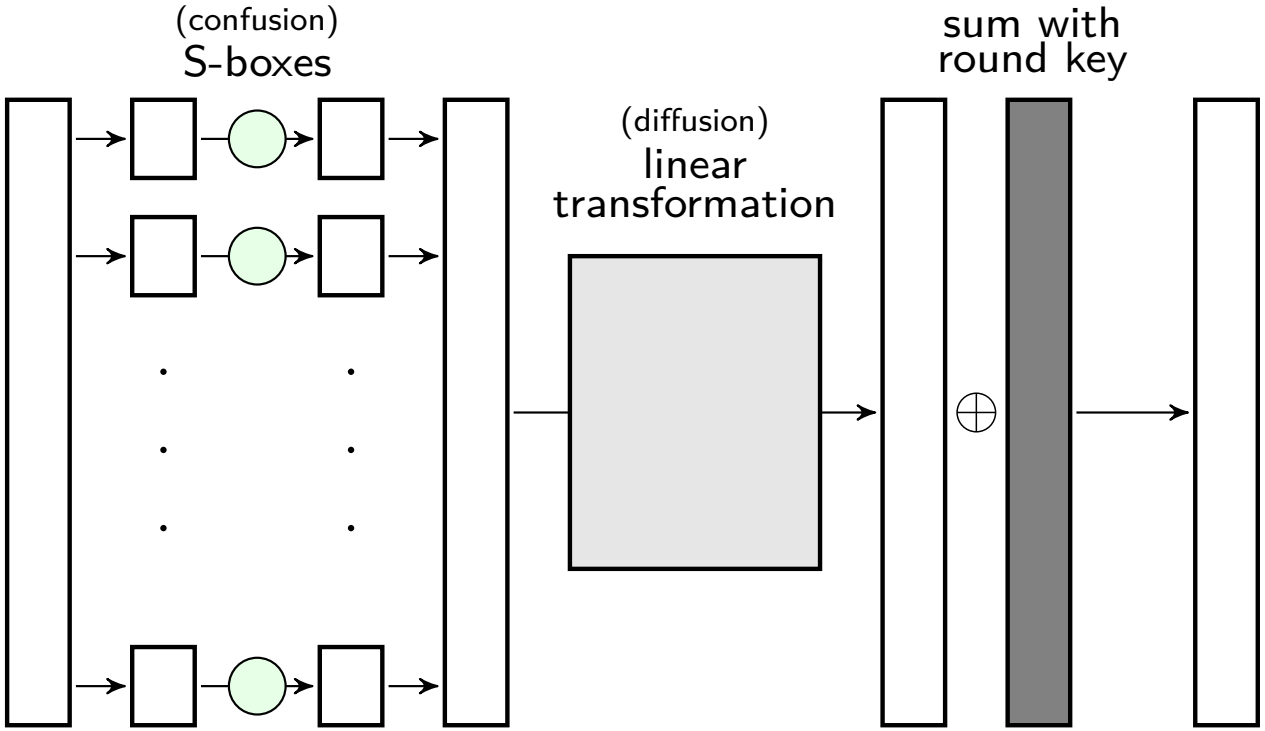
Cryptography



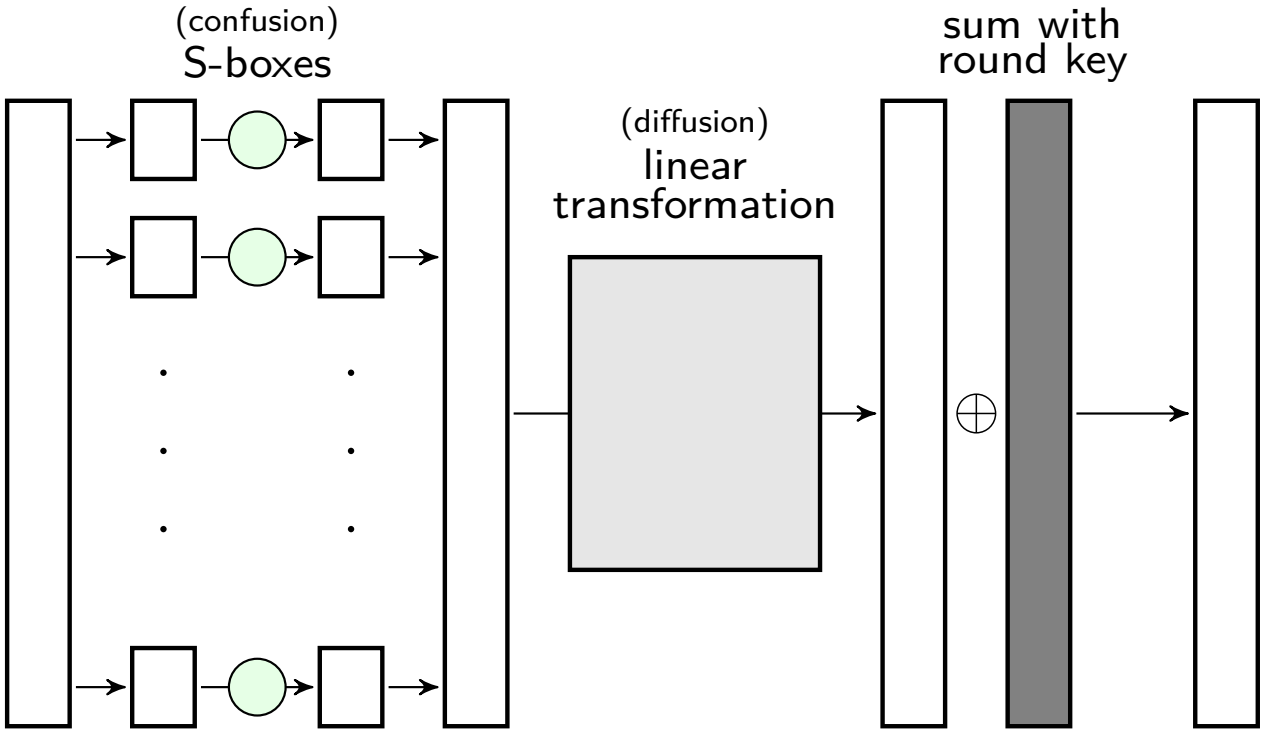


Typical round of a block cipher

Typical round of a block cipher



Typical round of a block cipher



Substitution box (S-box)

- vectorial Boolean function
- nonlinear
- often invertible
- cryptographic properties

Cryptographic Properties

Cryptographic Properties

- Attacks on block ciphers
  - **Black box attacker model** (cryptanalysis)
    knowledge about the algorithm + several inputs and/or outputs
- Mathematical properties (of the components of the block cipher) defined to measure the resistance of the block cipher to some specific attacks

The message, the key and the ciphertext are sequences of zeroes and ones.

Notation

- $\mathbb{F}_2 = \{0, 1\}$
- $\mathbb{F}_2^n = \{(a_1, \ldots, a_n) : a_i \in \mathbb{F}_2\}$
- $\mathbb{F}_{2^n}$ finite field with 2^n elements

The message, the key and the ciphertext are sequences of zeroes and ones.

Notation

- $\mathbb{F}_2 = \{0, 1\}$
- $\mathbb{F}_2^n = \{(a_1, \ldots, a_n) : a_i \in \mathbb{F}_2\}$
- $\mathbb{F}_{2^n}$ finite field with 2^n elements

Vectorial Boolean function

Given n and m integers, an (n, m)-function F is a map

$$F : \mathbb{F}_2^n \to \mathbb{F}_2^m.$$

If $m = n$ equivalently $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

Usually we deal with (n, n)-functions.

Vectorial Boolean function

Representations

Algebraic Normal Form (ANF) of $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$F(x_1, \ldots, x_n) = \sum_{I \subseteq \{1,\ldots,n\}} a_I \prod_{i \in I} x_i, \qquad a_I \in \mathbb{F}_2^m$$

Examples

$$F(x_1, x_2, x_3, x_4) = \begin{bmatrix} x_1x_2x_3 + x_3 \\ x_1x_2x_3 + x_2x_3 + 1 \\ x_2x_3 + x_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} x_1x_2x_3 + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} x_2x_3 + \cdots$$

Differential attack

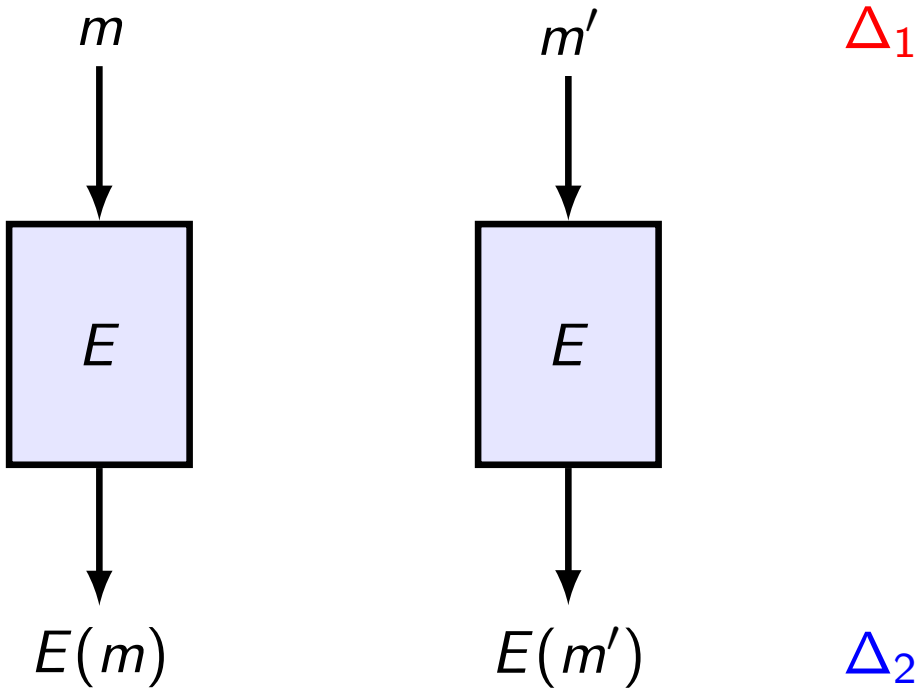
- well known attack to block ciphers
- introduced by Biham and Shamir in 1990

Δ_1

Δ_2

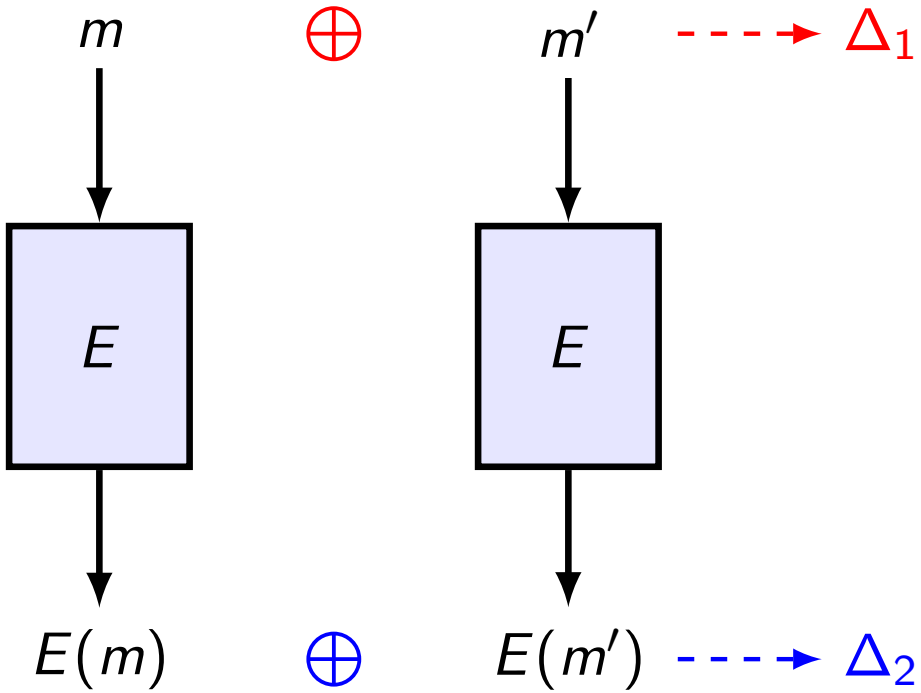
Differential attack

- well known attack to block ciphers
- introduced by Biham and Shamir in 1990

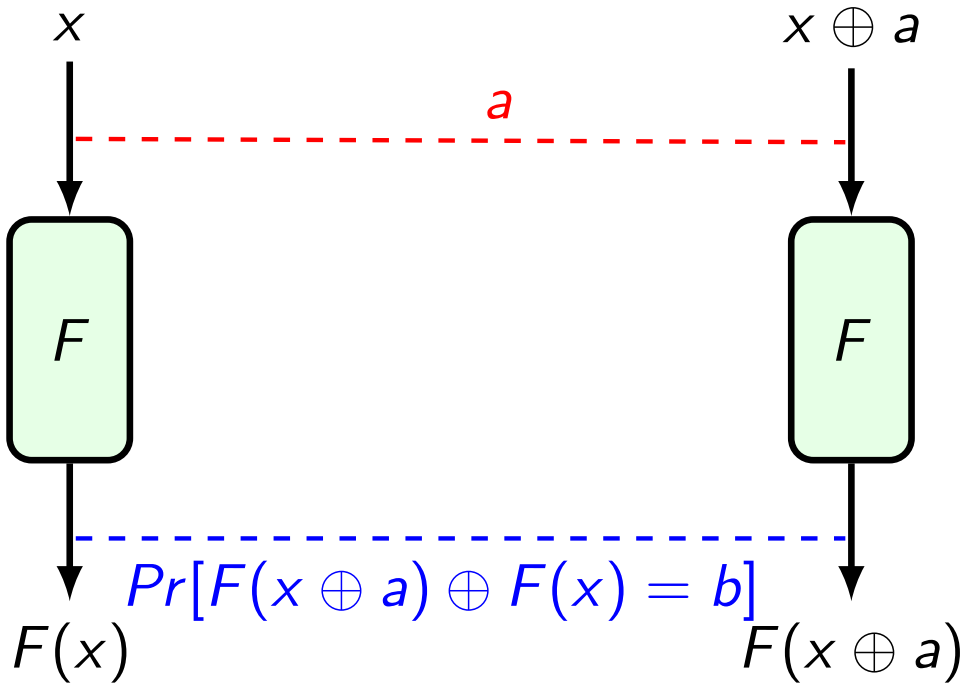


Differential attack

- well known attack to block ciphers
- introduced by Biham and Shamir in 1990



Differential attack at the S-box level



Differential uniformity

- Cryptographic property related to the differential attack
- introduced by Nyberg in 1993

Differentially δ-uniform

For $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$

$$\delta_F = \max_{\substack{a,b \in \mathbb{F}_2^n \\ a \neq 0}} |\{x \in \mathbb{F}_{2^n} : F(x+a) + F(x) = b\}|$$

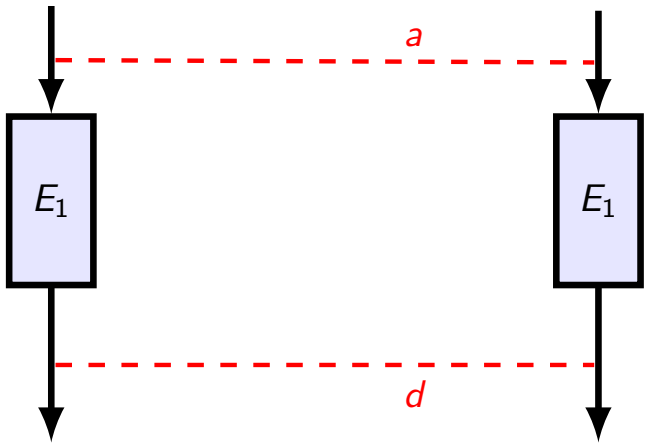
F is called almost perfect nonlinear (APN) if $\delta_F = 2$

Boomerang attack $E = E_1 \circ E_2$

- introduced by Wagner in 1999

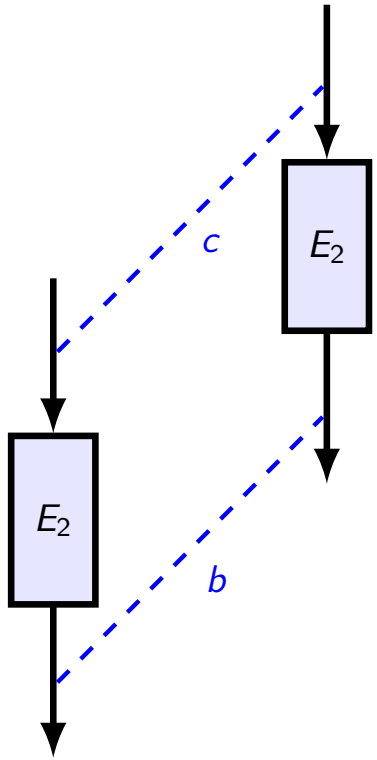
Boomerang attack $E = E_1 \circ E_2$

- introduced by Wagner in 1999



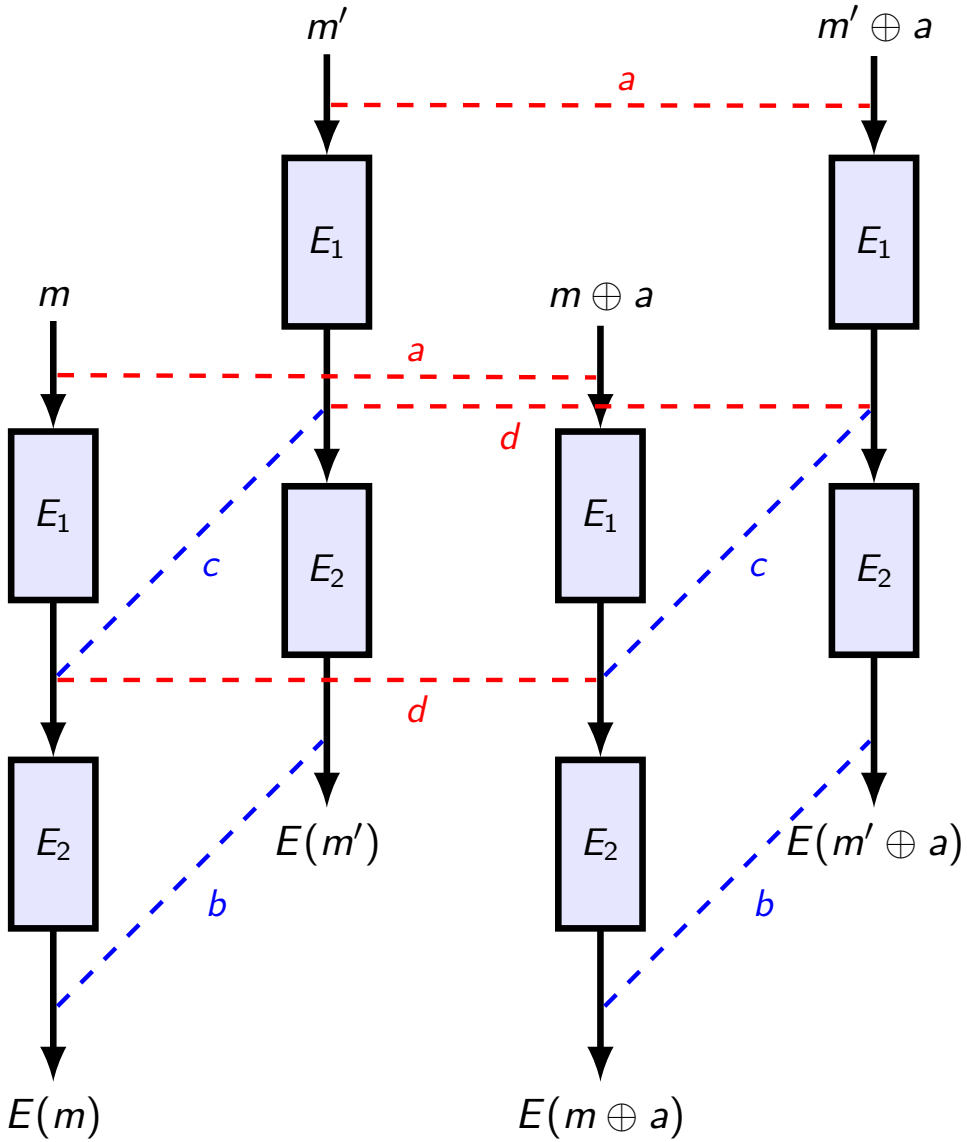
Boomerang attack $E = E_1 \circ E_2$

- introduced by Wagner in 1999



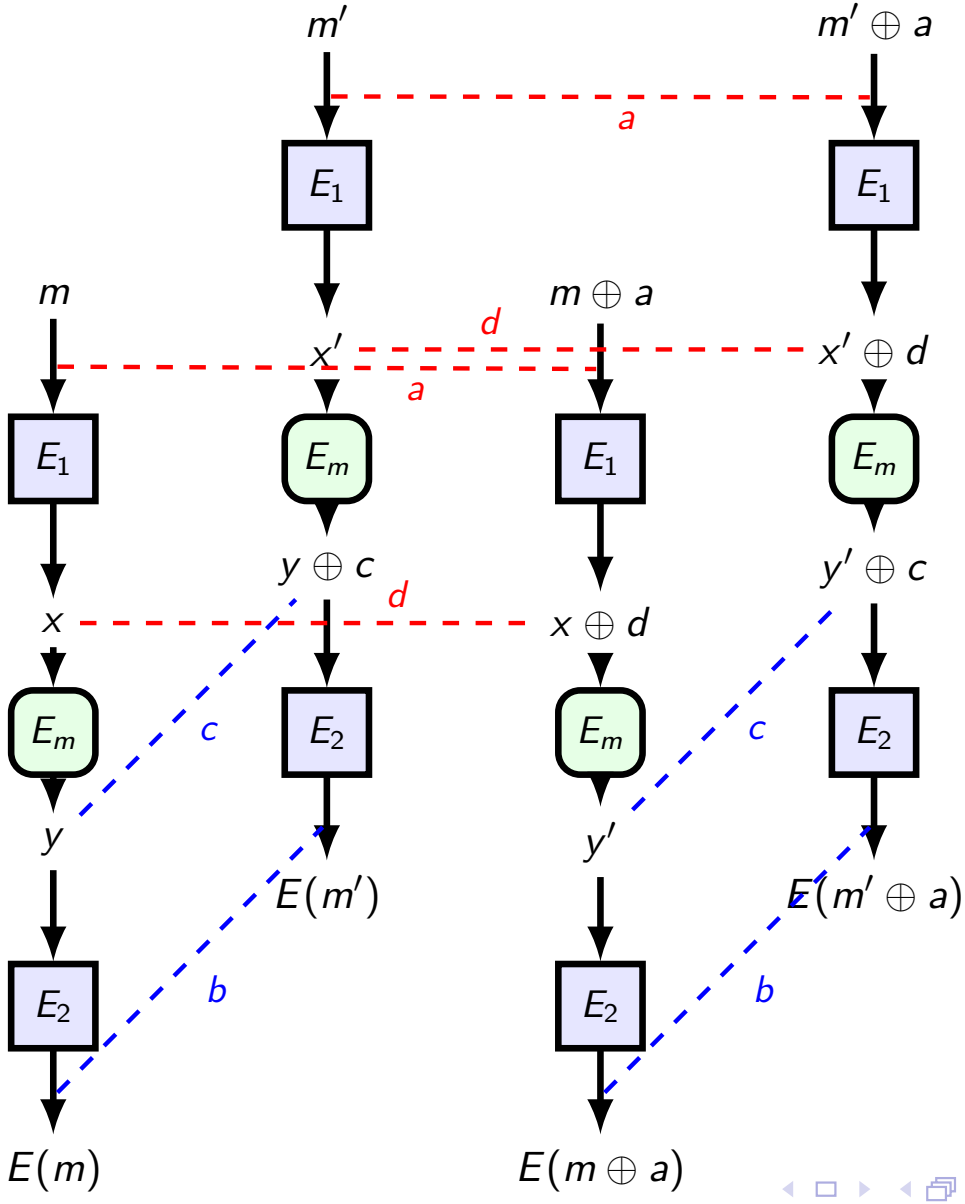
Boomerang attack $E = E_1 \circ E_2$

- introduced by Wagner in 1999

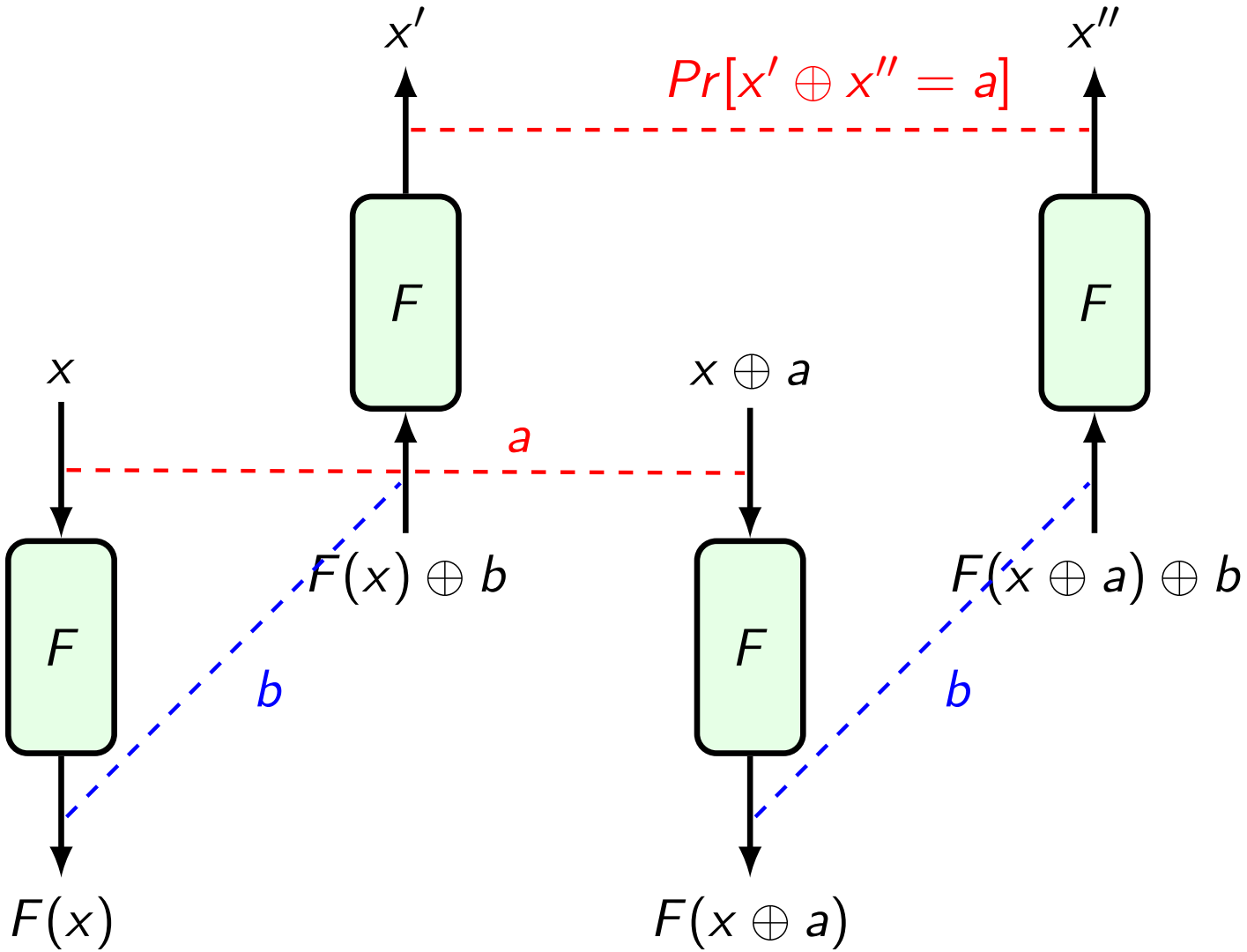


Sandwich attack $E = E_1 \circ E_m \circ E_2$

- proposed in 2014 by Dunkelman et al.



Boomerang-like attack at the S-box level



Boomerang uniformity

- cryptographic property related to boomerang-like attacks
- introduced in 2018 by Cid et al. and further formalized by Boura and Canteaut in 2018

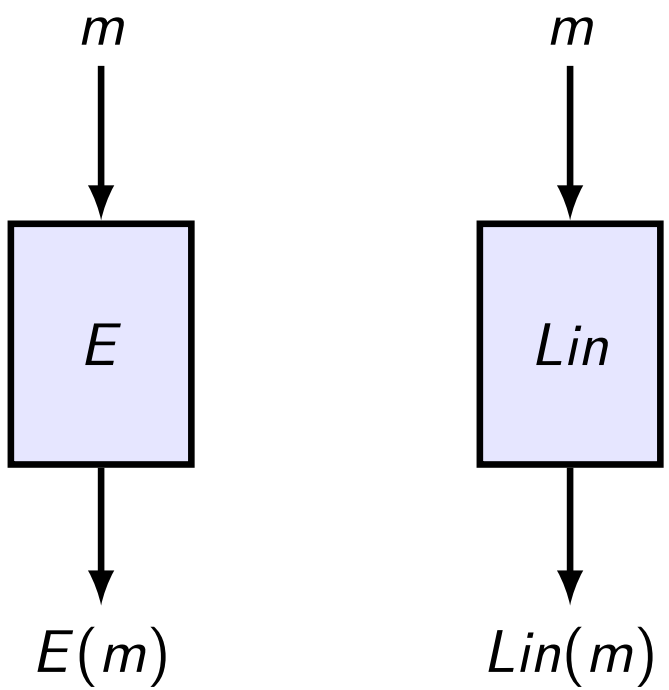
Boomerang uniformity

For $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ invertible,

$$\beta_F = \max_{\substack{a,b \in \mathbb{F}_2^n \\ a,b \neq 0}} |\{x \in \mathbb{F}_{2^n} : F^{-1}(F(x)+b) + F^{-1}(F(x+a)+b) = a\}|$$

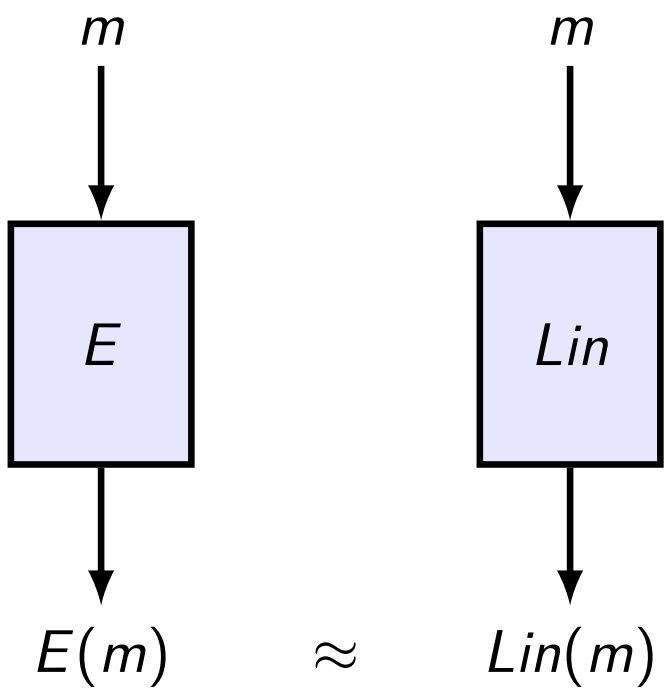
Linear attack

- introduced by Matsui in 1993
- idea: find a good linear approximation of the cipher

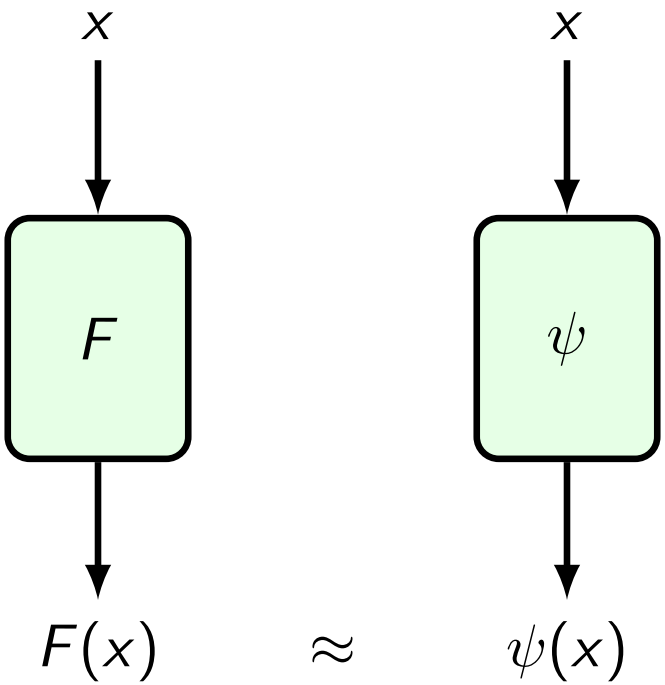


Linear attack

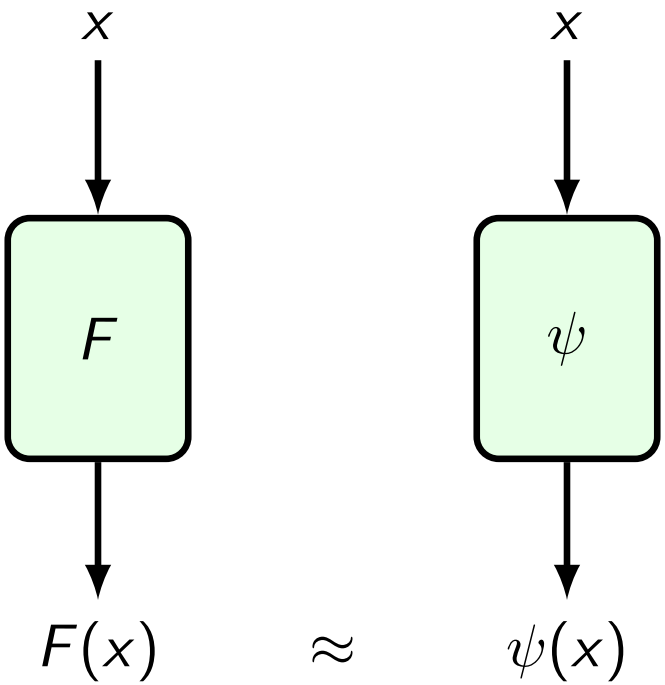
- introduced by Matsui in 1993
- idea: find a good linear approximation of the cipher



Linear attack at the S-box level



Linear attack at the S-box level



$$dist(F, \psi) = |\{x \in \mathbb{F}_2^n : F(x) \neq \psi(x)\}|$$

Nonlinearity

To resist the linear attack, the S-box F must have a high nonlinearity $\mathcal{NL}_F$.

Nonlinearity

For $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$

$$\mathcal{NL}_F = \min_{\substack{\lambda \in \mathbb{F}_2^n \\ \lambda \neq \mathbf{0}}} \min_{\phi \in \mathcal{A}_n} dist(F_\lambda, \phi),$$

where $F_\lambda = \lambda \cdot F : \mathbb{F}_2^n \to \mathbb{F}_2$ and $\mathcal{A}_n$ is the set of affine functions $\phi : \mathbb{F}_2^n \to \mathbb{F}_2$.

F is called almost bent (AB) if $\mathcal{NL}_F = 2^{n-1} - 2^{\frac{n-1}{2}}$.

To reach the upper bound (AB), n must be odd.

Good S-box

We want the S-box F

- (usually) invertible/permutation $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$,
- low differential uniformity,
- low boomerang uniformity,
- high nonlinearity,
- (for implementation reasons) n even (power of 2),
- ...

What we know:

- F permutation: $\delta_F \leq \beta_F$
- If APN ($\delta_F = 2$) then $\beta_F = 2$
- For n odd, if AB then APN
- Known many APN permutation for n odd
- For n even only one APN permutation known with $n = 6$
- Known many APN (non-permutations) for n even, but they have degree 2
- Known permutations with $\delta_F = 4$ for n even
- ...

Research directions

- **Big APN problem**: construct (other) APN permutations in even dimension
- Construct other (infinite families of) APN functions
- Find APN functions with degree greater than 2
- Increase the lists of known (inequivalent) APN functions
- Study the β_F for known permutations with $\delta_F = 4$
- ...

Combination of theoretical analysis with computational results

Grazie per l'attenzione!