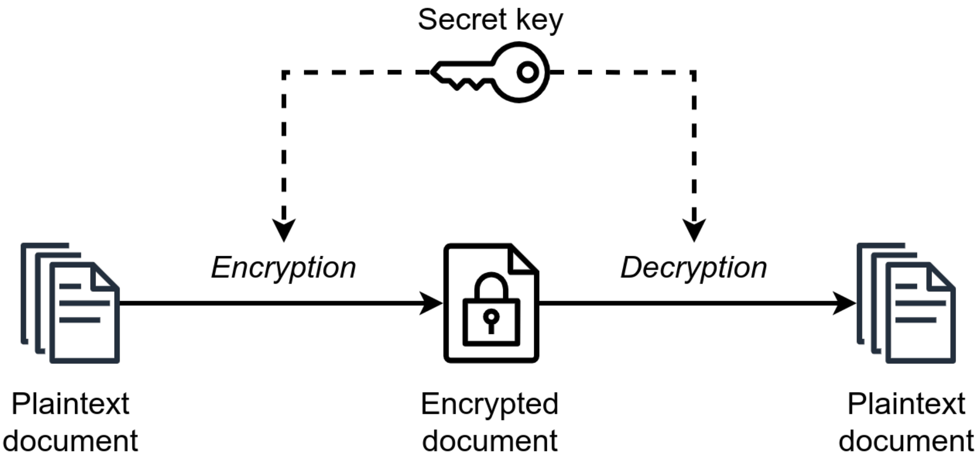
On Impossible Boomerangs Attacks

Xavier Bonnetain, Margarita Cordero, Virginie Lallemand, Marine Minier, María Naya-Plasencia

Université de Lorraine, CNRS, Inria, LORIA, Nancy, France

Journées C2
19/10/2023

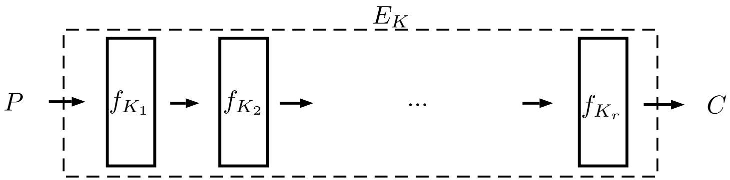
Symmetric Cryptography



Iterative Block Cipher

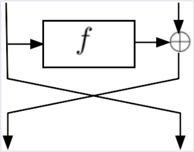
Block Cipher

Given a key $K \in \mathbb{F}_2^m$ and a message $M \in \mathbb{F}_2^N$, a block cipher of block size n is an **invertible** function E_K that encrypts the message M in blocks P of size n



Feistel Cipher

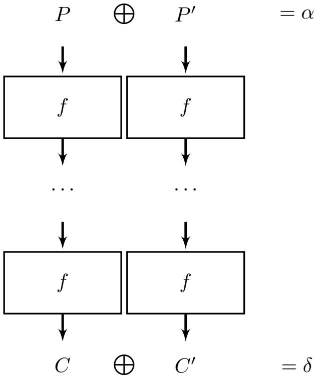
- $P = (x_0, y_0)$
- $y_i = x_{i-1}$
- $x_i = y_{i-i} \oplus f(x_{i-1}, K_i)$



Differential Distinguisher

Biham and Shamir at CRYPTO 1990

$$E_K(P) \oplus E_K(P \oplus \alpha) = \delta$$
$$p(\alpha \rightarrow \delta) \gg 1/2^n$$

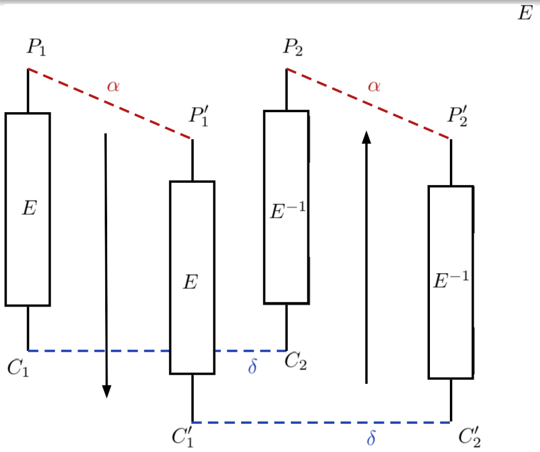


Related Key

$$E_K(P) \oplus E_{K \oplus \alpha_K}(P \oplus \alpha) = \delta$$

Boomerang Distinguisher

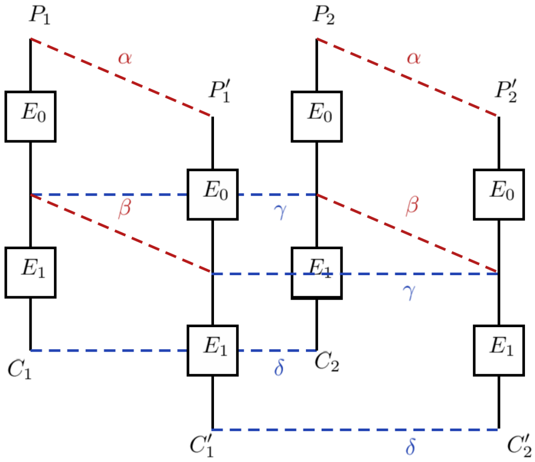
David Wagner. The boomerang attack. 1999



$$E^{-1}(E(P_1) \oplus \delta) \oplus E^{-1}(E(P_1 \oplus \alpha) \oplus \delta) = \alpha$$

David Wagner. The boomerang attack. 1999

- $E = E_1 \circ E_0$
- $p = p_{E_0}(\alpha \to \beta)$
- $q = p_{E_1}(\gamma \to \delta)$
- $p(P_2 \oplus P_2' = \Delta) = p^2 q^2$



Better Estimation of the Boomerang Probability

Dunkelman et al. Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony. 2014

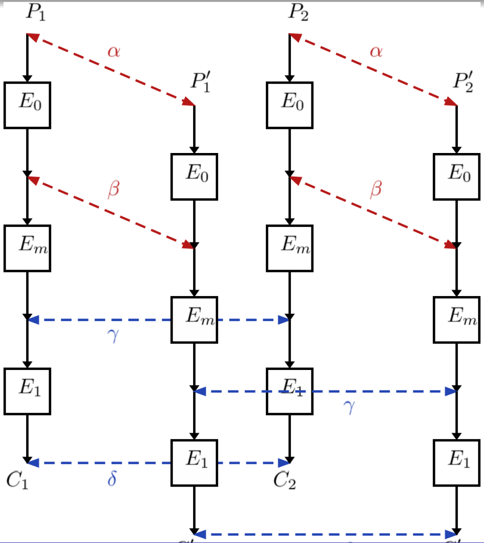
Sandwich Attack

$E = E_1 \circ E_m \circ E_0$

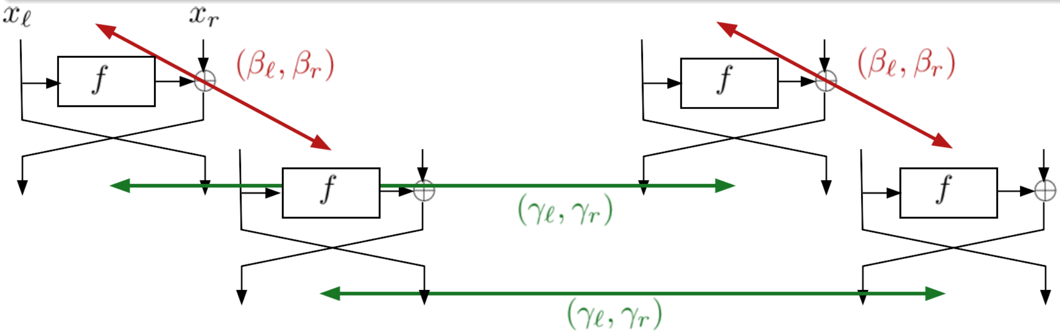
$p = p_{E_0}(\alpha \to \beta)$, $q = p_{E_1}(\gamma \to \delta)$,

$r = p_{E_m}(\beta \to \gamma \to \beta)$,

Boomerang probability $= p^2 q^2 r$

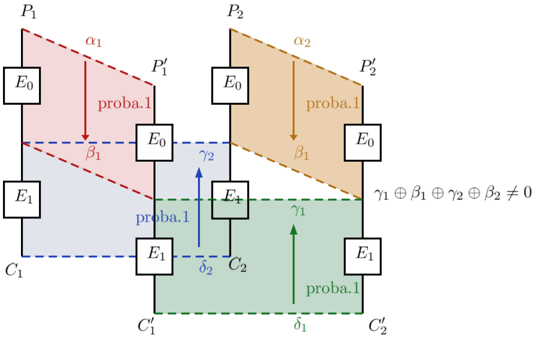


$$p = \frac{\#\{x \in \{0,1\}^n | f(x) \oplus f(x \oplus \beta) \oplus f(x \oplus \gamma) \oplus f(x \oplus \beta \oplus \gamma) = 0\}}{2^n}$$

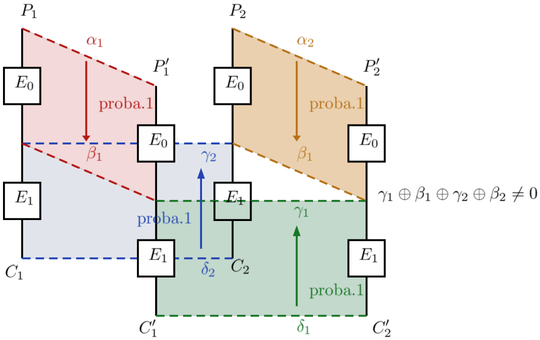


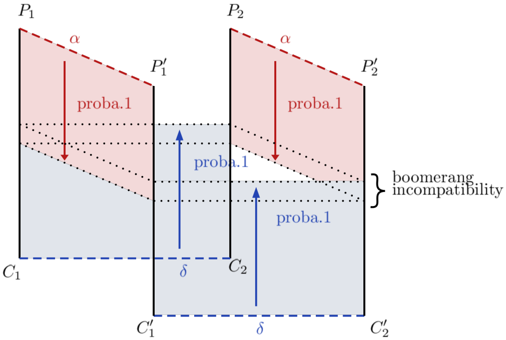
Jiqiang Lu's Impossible Boomerang Distinguisher

Jiqiang Lu. The (related-key) impossible boomerang attack and its application to the AES block cipher. 2011

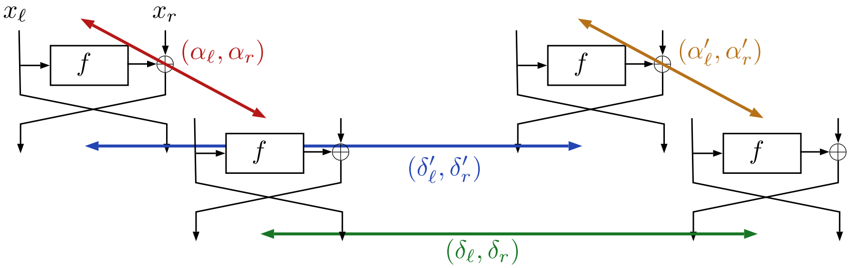


New Idea of Incompatibility





The Quadratic Feistel Ciphers Case

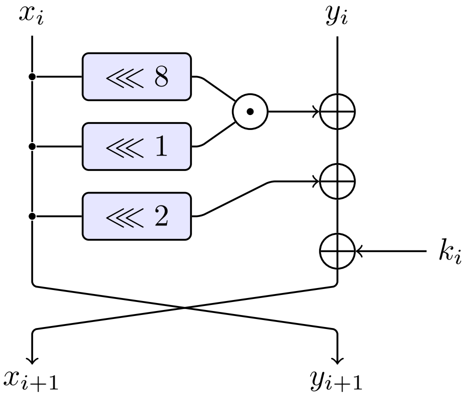


$$\begin{cases} f(x_\ell) \oplus f(x_\ell \oplus \delta'_r) \oplus f(x_\ell \oplus \alpha_\ell) \oplus f(x_\ell \oplus \alpha_\ell \oplus \delta_r) = \alpha_r \oplus \alpha'_r \oplus \delta_\ell \oplus \delta'_\ell, \\ \delta_r \oplus \delta'_r \oplus \alpha_\ell \oplus \alpha'_\ell = 0. \end{cases}$$

Simon32/64 Block Cipher

Beaulieu et al. The Simon and Speck Families of Lightweight Block Ciphers. 2013

- NSA 2013
- Different variants
- 32-bit block size
- 64-bit key size
- 32 rounds
- Linear key schedule



Simon32/64 Case

We want to be able to conclude without knowing the values of the internal state: $\delta'_r = \delta_r$

$$\begin{cases} (\delta_r \lll 1)(\alpha_\ell \lll 8) \oplus (\alpha_\ell \lll 1)(\delta_r \lll 8) \\ \qquad \oplus \alpha_r \oplus \alpha'_r \oplus \delta_\ell \oplus \delta'_\ell = 0 \\ \delta_r \oplus \delta'_r = 0 \\ \alpha_\ell \oplus \alpha'_\ell = 0 \end{cases} \tag{1}$$

Preliminary Results

Distinguisher

Technique	single key	related key
Rounds	7	17

State-of-the-Art

Technique	Rounds	Prob.	Ref.
RK Boomerang	17	$2^{-23.6}$	[BL23]
RX Rectangle	19	$2^{-29.5}$	[BL23]