There and back again: a tale of boomerang attacks

Paul HUYNH

Advisor: Marine MINIER

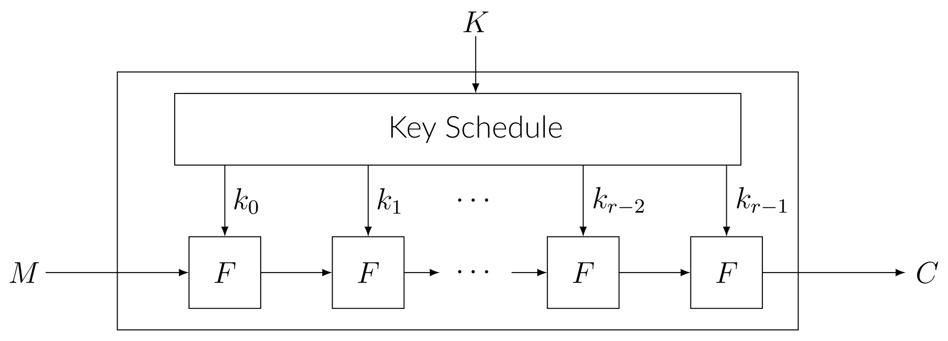
Team Caramba, LORIA, Université de Lorraine

Block Ciphers

Family of n-bit permutations parameterized by a key K used for data encryption i.e. turning a message M into a ciphertext C.

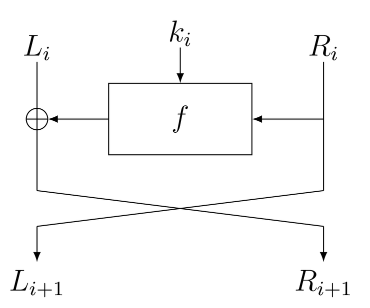
Iterative structure

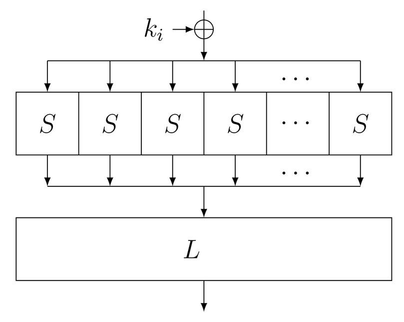
$E_K(M) = F_{k_{r-1}} \circ F_{k_{r-2}} \circ \cdots \circ F_{k_0}(M) = C$



Two major constructions for F

- Feistel
- SPN





Both constructions include non-linear components. In most cases, boolean mappings called substitution boxes (or *Sboxes*) are used.

A good block cipher must behave like a random permutation !

Attacking block ciphers

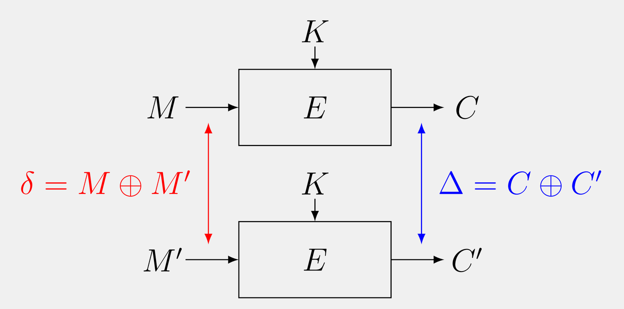
Differential Cryptanalysis of DES-like Cryptosystems, Biham and Shamir, 1990

For a random permutation π of $\mathbb{F}_2^n$ and for any differences $\delta, \Delta \in \mathbb{F}_2^n \setminus \{0\}$

$$Pr_X[\pi(X+\delta) + \pi(X) = \Delta] = \frac{1}{2^n - 1}$$

Core idea

Exploiting a bias in the difference distribution of the cipher



The cipher is weak if one can exhibit a path from an input difference δ to an output difference Δ (i.e. a *differential characteristic*) with high probability.

Consequences

Defending against differential cryptanalysis becomes a design goal: no differentials of high probability must exist in the designs

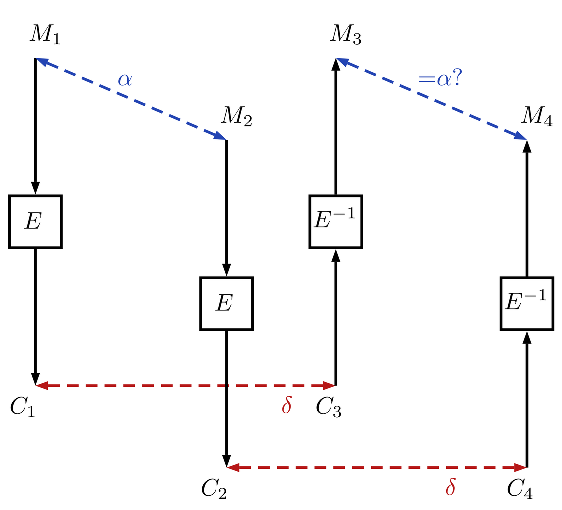
But...

The Boomerang Attack, David Wagner, FSE 1999:

- No need of high-probability differentials on the cipher to attack it, only on both halves of it

Basic Boomerang Distinguisher

- Pick M_1 at random, ask for its ciphertext C_1
- Ask for C_2, the ciphertext of $M_2 = M_1 \oplus \alpha$
- Compute $C_3 = C_1 \oplus \delta$, $C_4 = C_2 \oplus \delta$
- Ask for their decryption (M_3, M_4)
- Check if $M_3 \oplus M_4 = \alpha$.



We have a distinguisher if α 'comes back' more often than for a random permutation.

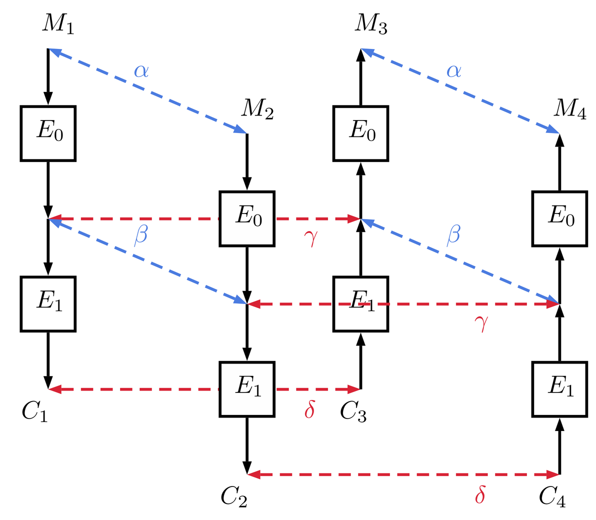
The Sandwich Attack

A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony: Dunkelman, Keller, Shamir, 2010

Basic distinguisher

- Rewrite $E = E_1 \circ E_0$
- Find good differentials over E_0 and E_1:
  - $\mathbb{P}(\alpha \longrightarrow_{E_0} \beta) = p$
  - $\mathbb{P}(\gamma \longrightarrow_{E_1} \delta) = q$

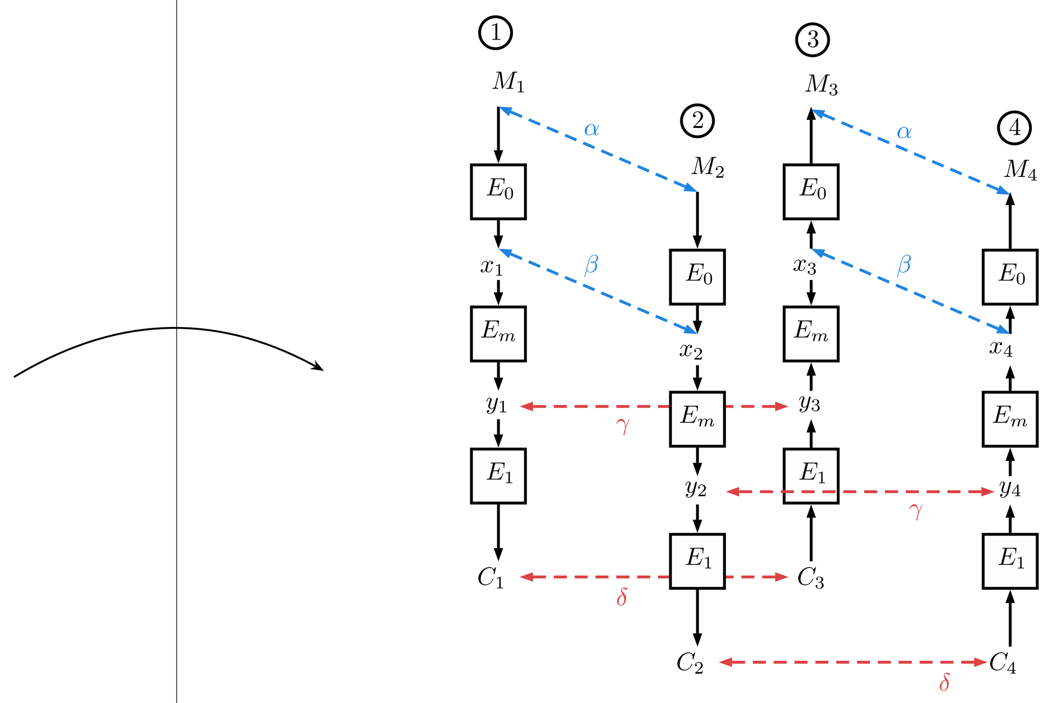
Expected probability of p^2q^2



- Incompatibilities can occur $\rightarrow$ probability 0 instead of p^2q^2
- The problems come from interactions at the junction of the two trails

The sandwich attack

- $E = E_1 \circ E_m \circ E_0$
- E_m of 1 round



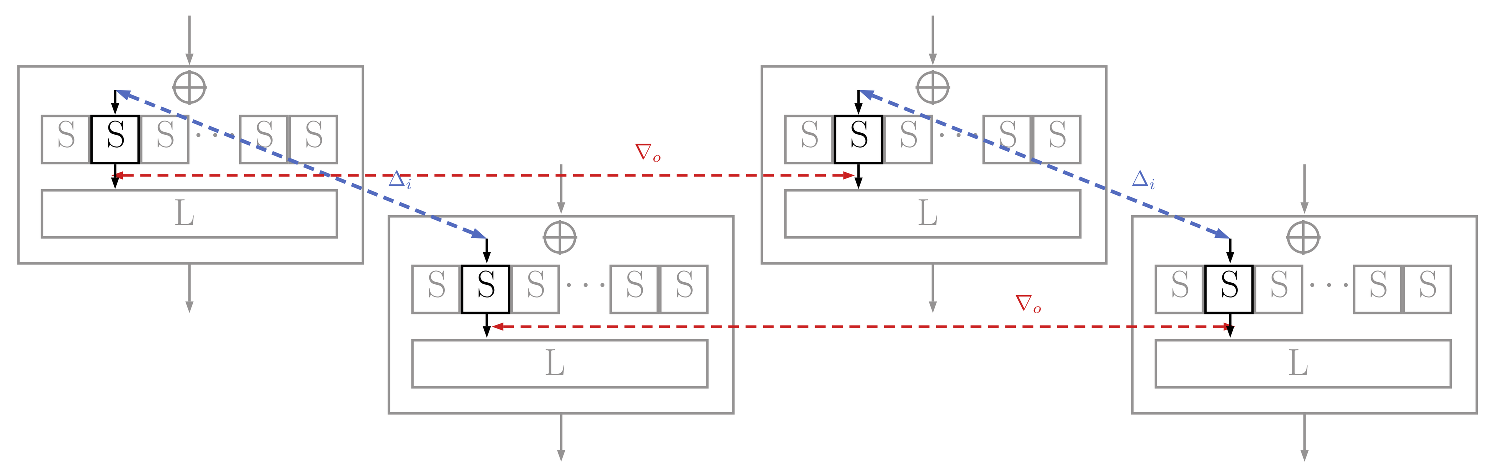
- Distinguisher in p^2q^2r

$\rightarrow$ how to compute r ?

The BCT: Automation of the Analysis of 1-round E_m for SPN

Boomerang Connectivity Table: A New Cryptanalysis Tool: Cid, Huang, Peyrin, Sasaki, Song, 2018.

Probability over 1 round of E_m = product of the probabilities over each Sbox S



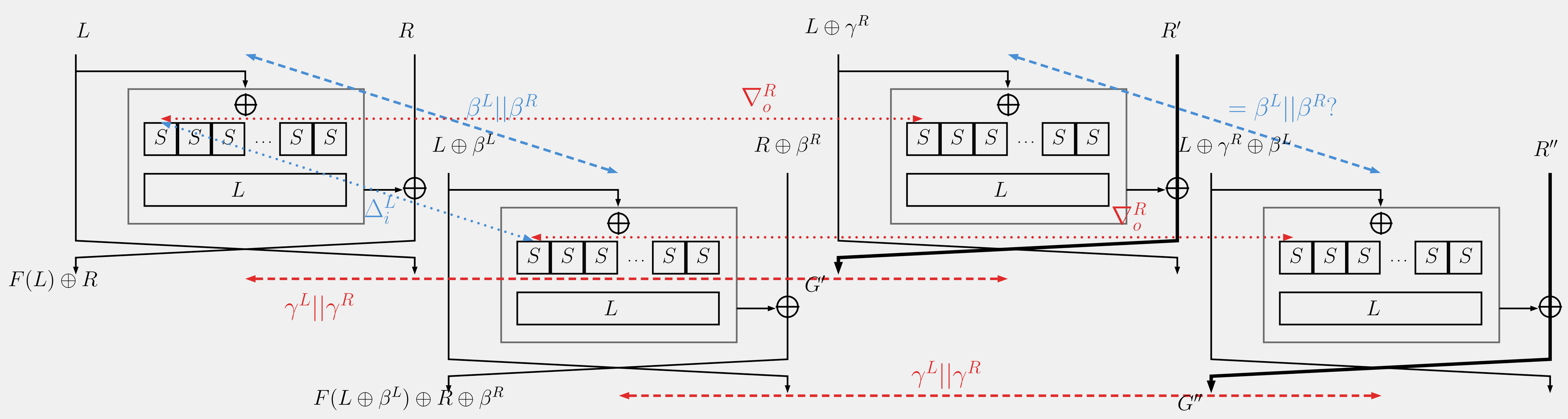
$$p = \frac{\mathtt{BCT}(\Delta_i, \nabla_o)}{2^s} = \frac{\#\{x | S^{-1}(S(x)\oplus\nabla_o)\oplus S^{-1}(S(x\oplus\Delta_i)\oplus\nabla_o)=\Delta_i\}}{2^s}$$

The problem we have solved [1]

The theory of Cid et al. is only valid for SPN ciphers, quid of Feistel constructions?

- Introduction of the **FBCT** (**F**eistel **B**oomerang **C**onnectivity **T**able)
- Generic formula for a middle part made of an arbitrary number of rounds: the **FBET**
- Proof that a former boomerang attack on LBlock was incorrect
- 16-round boomerang distinguisher on LBlock-s with E_m variying from 2 to 8 rounds Interesting probability of $2^{-56.14}$ found in the 8-round case.

The FBCT: overview



$$\mathtt{FBCT}(\Delta_i^L, \nabla_o^R) = \#\{x | S(x) \oplus S(x \oplus \Delta_i^L) \oplus S(x \oplus \nabla_o^R) \oplus S(x \oplus \Delta_i^L \oplus \nabla_o^R) = 0\}$$

$\rightarrow$ Number of times the second order derivative at points (Δ_i, ∇_o) cancels out

Properties

Symmetry $\mathtt{FBCT}(\Delta_i, \nabla_o) = \mathtt{FBCT}(\nabla_o, \Delta_i)$

Diagonal $\mathtt{FBCT}(\Delta_i, \Delta_i) = 2^n$

Multiplicity $\mathtt{FBCT}(\Delta_i, \nabla_o) \equiv 0 \mod 4$

Equalities $\mathtt{FBCT}(\Delta_i, \nabla_o) = \mathtt{FBCT}(\Delta_i, \Delta_i \oplus \nabla_o)$

What's next ?

- Automation of the search of the best parameters for a Boomerang attack taking into account the FBET
- Application to DES and other important Feistel ciphers: CLEFIA, Twine ...
- Related-key case (differences in the key as well)

References

[1] On the Feistel Counterpart of the Boomerang Connectivity Table - Introduction and Analysis of the FBCT
Hamid Boukerrou, Paul Huynh, Virginie Lallemand, Bimal Mandal and Marine Minier
Submitted to FSE 2020