THE BOOMERANG ATTACK

Halil İbrahim Kaplan

2021

TÜBİTAK BİLGEM

Overview

- The Boomerang Attack: A Generic View
- Structure of COCONUT98
- Boomerang Attack on COCONUT98
- Meet-in-the-Middle Attack on COCONUT98

The Boomerang Attack: A Generic View

The boomerang attack is a differential attack that attempts to generate a quartet structure at an intermediate value halfway through the cipher.

Plaintexts : P , P ′, Q , Q′ (quartet)

Respective ciphertexts : C , C′ , D , D′

Encryption : $E(\quad)$ *can be decomposed as* $E = E_0 \circ E_1$

Differential characteristic for $\boldsymbol{E_0}$: $\Delta \rightarrow \Delta^*$

Differential characteristic for $\boldsymbol{E_1^{-1}}$: $\nabla \rightarrow \nabla^*$

The Boomerang Attack: A Generic View

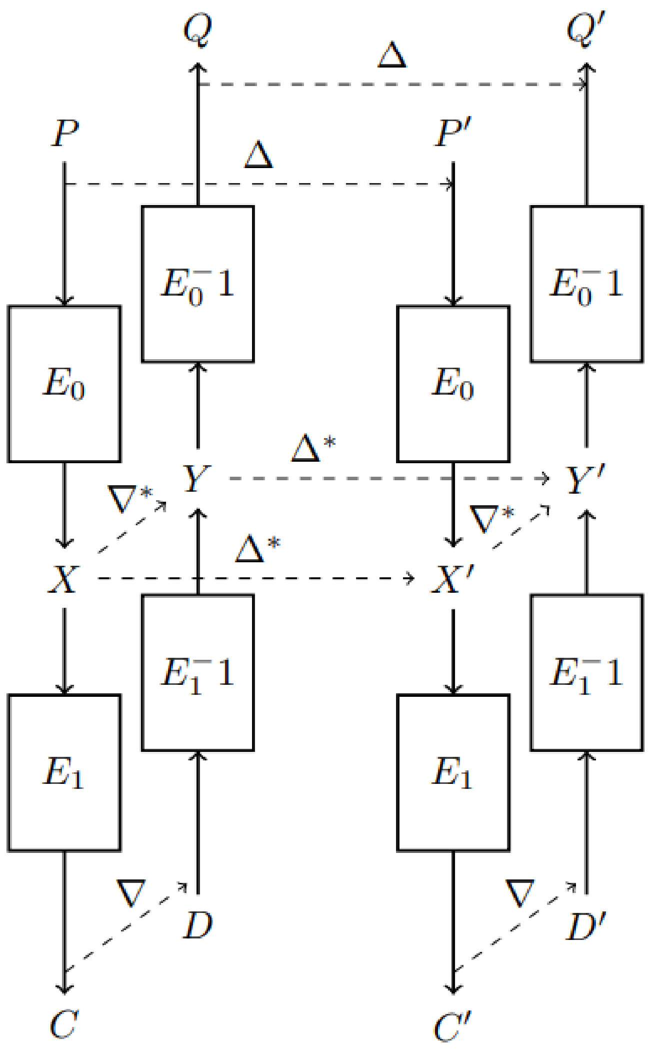
Generate

$P' = P \oplus \Delta$

$C = E(P)$, $C' = E(P')$

$D = C \oplus \nabla$, $D' = C' \oplus \nabla$

$Q = E^{-1}(D)$, $Q' = E^{-1}(D')$



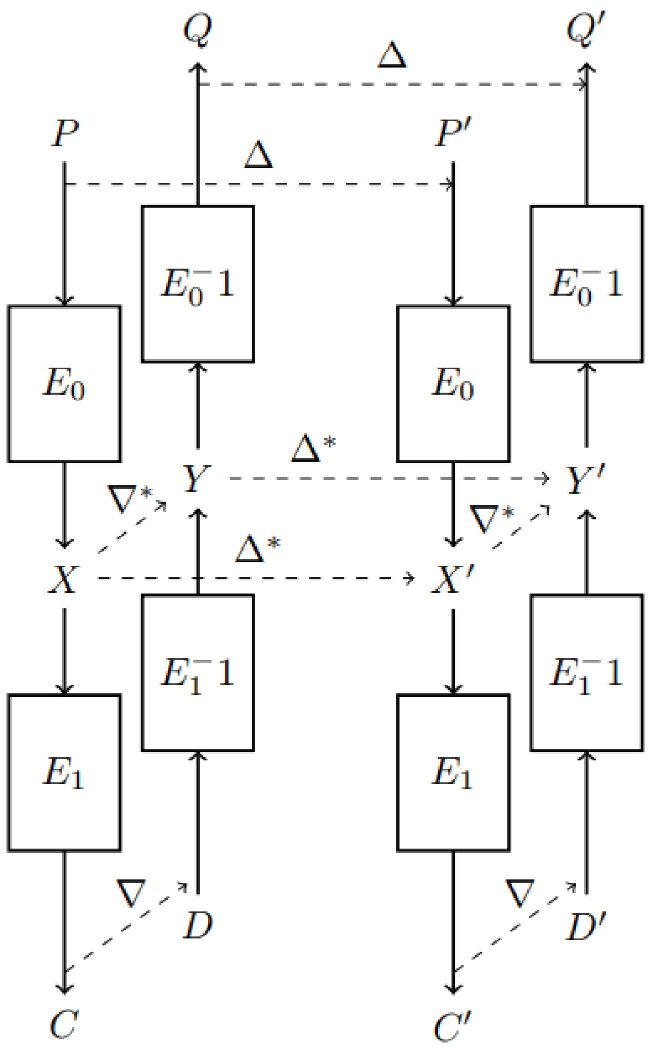
The Boomerang Attack: A Generic View

We will

Cover the pair P , P ′ with the characteristic for E_0 ($\Delta \rightarrow \Delta^*$)

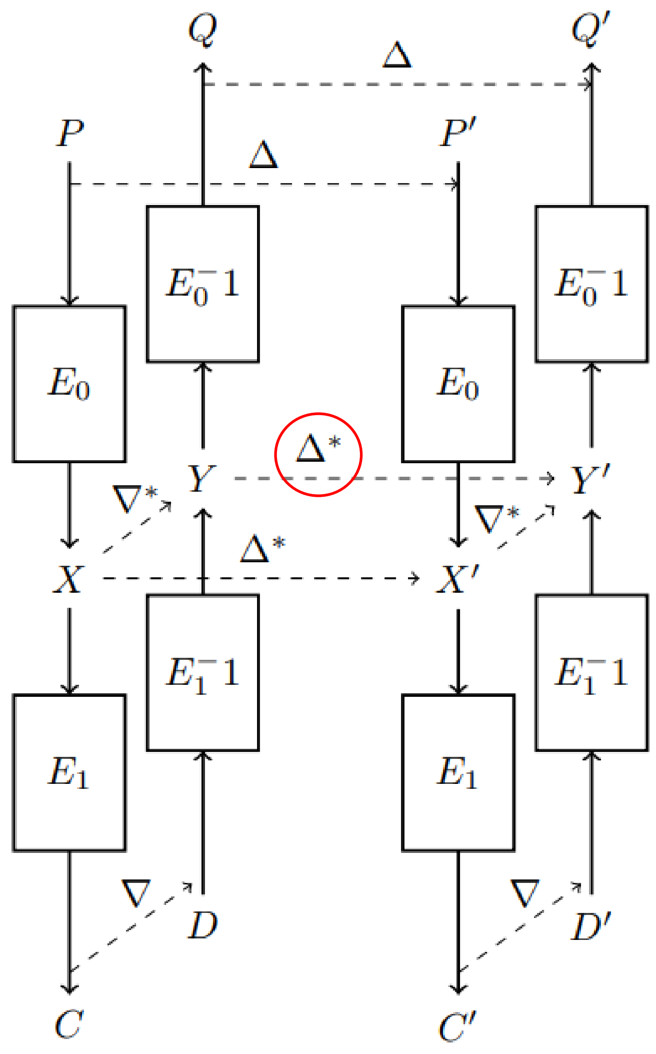
Cover the pairs P , Q and P ′, Q′ with the characteristic for E_1^{-1} ($\nabla \rightarrow \nabla^*$)

Then the pair Q , Q′ is perfectly set up to use the characteristic $\Delta^* \rightarrow \Delta$ for E_0^{-1} .



The Boomerang Attack: A Generic View

$$
\begin{aligned}
E_0(Q) \oplus E_0(Q') &= E_0(P) \oplus E_0(P') \oplus E_0(P) \oplus E_0(Q) \oplus E_0(P') \oplus E_0(Q') \\
&= E_0(P) \oplus E_0(P') \oplus E_1^{-1}(C) \oplus E_1^{-1}(D) \oplus E_1^{-1}(C') \oplus E_1^{-1}(D') \\
&= \Delta^* \oplus \nabla^* \oplus \nabla^* = \Delta^*,
\end{aligned}
$$



If the following conditions are fulfilled, (P, P ′ , Q, Q ′) is called a **right quartet**

$$
\begin{aligned}
P \oplus P' &= Q \oplus Q' = \Delta \\
X \oplus X' &= Y \oplus Y' = \Delta^* \\
X \oplus Y &= X' \oplus Y' = \nabla^* \\
C \oplus D &= C' \oplus D' = \nabla.
\end{aligned}
$$

Structure of COCONUT98

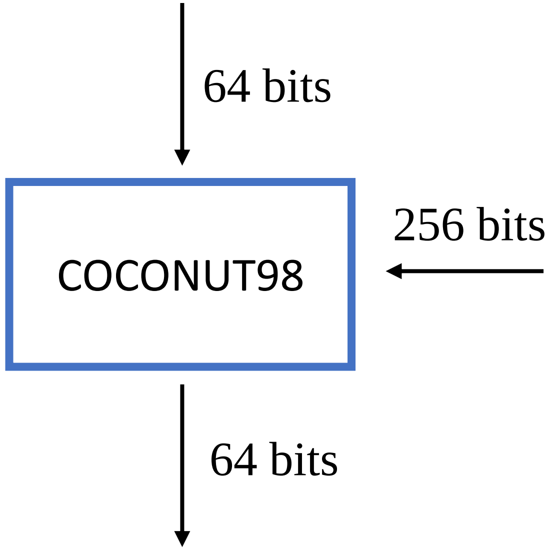
COCONUT98 is defined as : $\psi_1 \ o \ M \ o \ \psi_0$ where

$$\phi(x) = x + 256 \cdot S(x \bmod 256) \bmod 2^{32}$$

$$F_i((x,y)) = (y, x \oplus \phi(ROL_{11}(\phi(y \oplus k_i)) + c \bmod 2^{32}))$$

$$\Psi_i = F_{4i+4} \circ F_{4i+3} \circ F_{4i+2} \circ F_{4i+1}$$

$$M(xy) = (xy \oplus K_5K_6) \times K_7K_8 \bmod \mathrm{GF}(2^{64})$$



$\boldsymbol{ROL_{11}}(\,)$: Left rotation by 11 bits

c : Public 32-bit constant

S : $Z_2^8 \rightarrow Z_2^{24}$ is a fixed S-box

Structure of COCONUT98

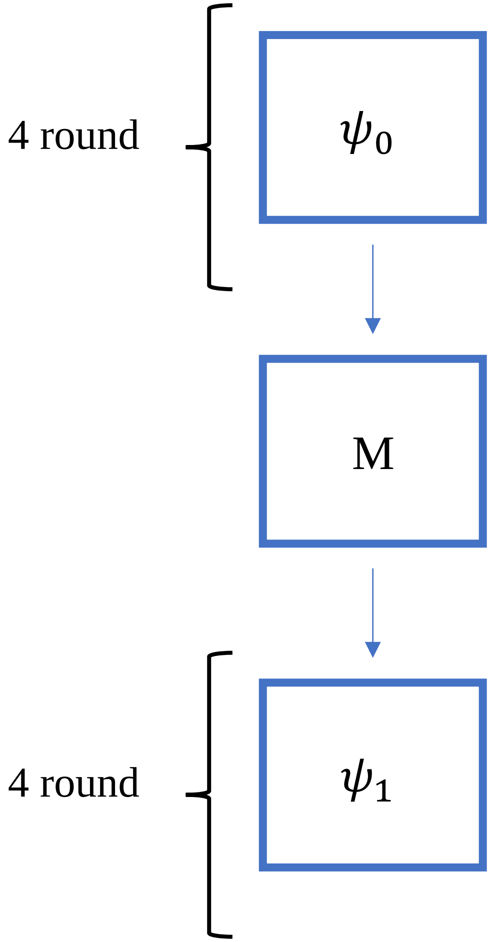
COCONUT98 is defined as : $\psi_1 \, o \, M \, o \, \psi_0$ where

$$\phi(x) = x + 256 \cdot S(x \bmod 256) \bmod 2^{32}$$

$$F_i((x, y)) = (y, x \oplus \phi(ROL_{11}(\phi(y \oplus k_i)) + c \bmod 2^{32}))$$

$$\Psi_i = F_{4i+4} \circ F_{4i+3} \circ F_{4i+2} \circ F_{4i+1}$$

$$M(xy) = (xy \oplus K_5K_6) \times K_7K_8 \bmod \mathrm{GF}(2^{64})$$



$\boldsymbol{ROL_{11}}()$: Left rotation by 11 bits

c : Public 32-bit constant

S : $Z_2^8 \rightarrow Z_2^{24}$ is a fixed S-box

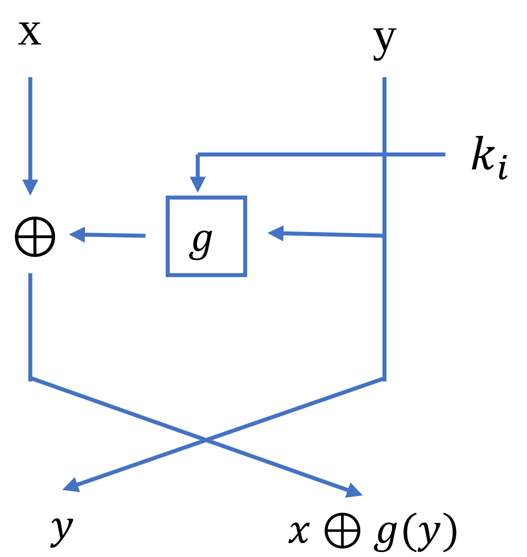
COCONUT98 is defined as : $\psi_1 \; o \; M \; o \; \psi_0$ where

$$\phi(x) = x + 256 \cdot S(x \bmod 256) \bmod 2^{32}$$

$$F_i((x,y)) = (y, x \oplus \phi(ROL_{11}(\phi(y \oplus k_i)) + c \bmod 2^{32}))$$

$$\Psi_i = F_{4i+4} \circ F_{4i+3} \circ F_{4i+2} \circ F_{4i+1}$$

$$M(xy) = (xy \oplus K_5K_6) \times K_7K_8 \bmod \mathrm{GF}(2^{64})$$



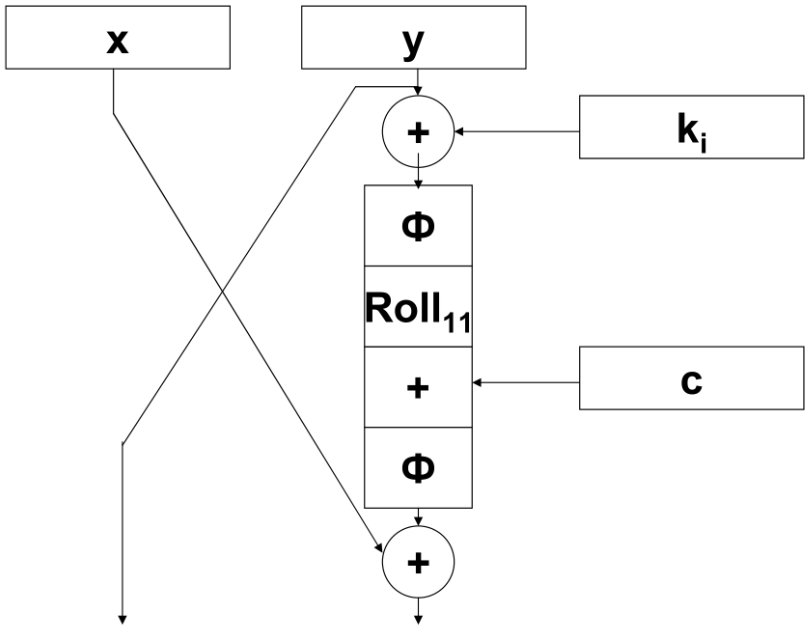
$\boldsymbol{ROL_{11}}(\,)$: Left rotation by 11 bits

where $g(y) = \phi(ROL_{11}(\phi(y \oplus ki)) + c \; mod \; 2^{32})$

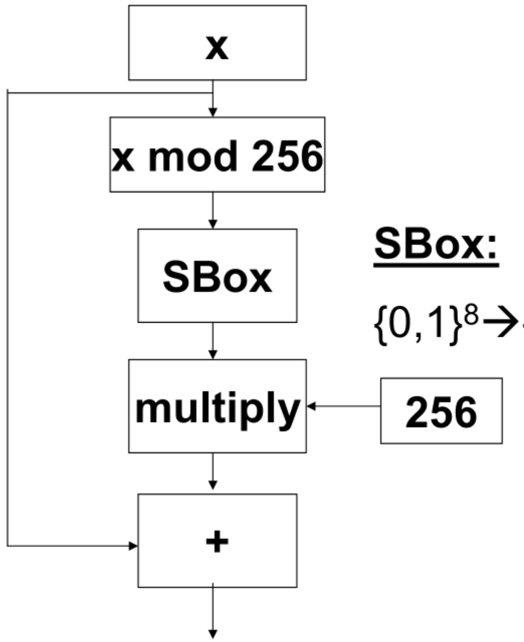
c : Public 32-bit constant

S : $Z_2^8 \rightarrow Z_2^{24}$ is a fixed S-box

Feistel Rounds of COCONUT98



The Phi Function



SBox:

$\{0,1\}^8 \rightarrow \{0,1\}^{24}$

$$\phi(x) = x + 256 \cdot S(x \bmod 256) \bmod 2^{32}$$

$$F_i((x,y)) = (y, x \oplus \phi(ROL_{11}(\phi(y \oplus k_i)) + c \bmod 2^{32}))$$

$$\Psi_i = F_{4i+4} \circ F_{4i+3} \circ F_{4i+2} \circ F_{4i+1}$$

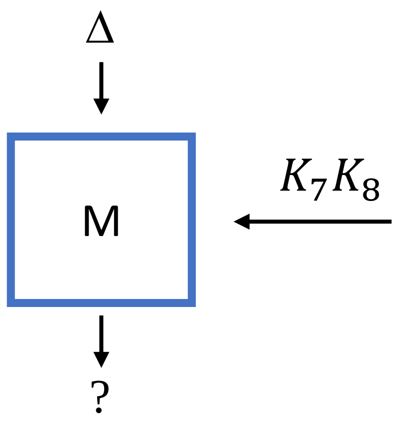
THE M LAYER

$$M(xy) = (xy \oplus K_5K_6) \times K_7K_8 \bmod \mathrm{GF}(2^{64})$$

- Uses irreducible polynomial $p(x) = x^{64} + x^{11} + x^2 + x + 1$
- Design is based on decorrelation theory.
- If K_7K_8 are unknown then the probability of a non-zero input differential to produce an output differential is $\frac{1}{2^{64}-1}$
- Decorrelation module prevents us from pushing a differential characteristic past M

THE M LAYER

$$M(xy) = (xy \oplus K_5K_6) \times K_7K_8 \bmod \mathrm{GF}(2^{64})$$



$$M(xy) \oplus M(x'y') = (xy \oplus K_5K_6) * K_7K_8 \oplus (x'y' \oplus K_5K_6) * K_7K_8$$

$$= (xy \oplus x'y') * K_7\, K_8$$

$$2^{64}\ possible\ differential\ outcome$$

The COCONUT98 Algorithm :

COCONUT98 uses a 256-bit key K = (K1, . . . , K8). The key schedule generates eight round subkeys k1, . . . , k8 as

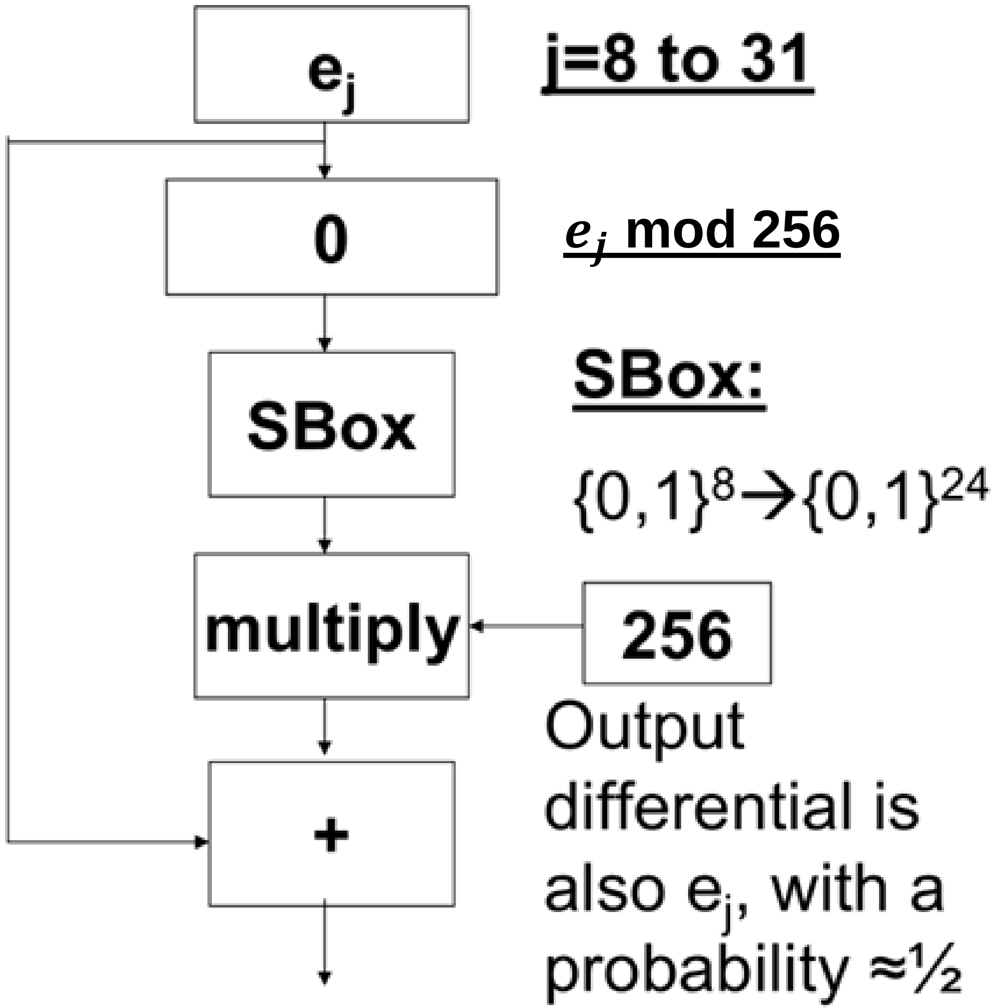
i	1	2	3	4
k_i	K_1	$K_1 \oplus K_3$	$K_1 \oplus K_3 \oplus K_4$	$K_1 \oplus K_4$

i	5	6	7	8
k_i	K_2	$K_2 \oplus K_3$	$K_2 \oplus K_3 \oplus K_4$	$K_2 \oplus K_4$

Differential Characteristics for COCONUT98 :

Let $e_j = 2^j$ be the 32-bit xor difference with just the j-th bit flipped.

$e_j \rightarrow e_{j+11}$ by the Feistel function with probability 1/2 when j ∈ J = {8, 9, . . . , 19, 20, 29, 30, 31}



Boomerang Attack on COCONUT98

Differential Characteristics for COCONUT98 :

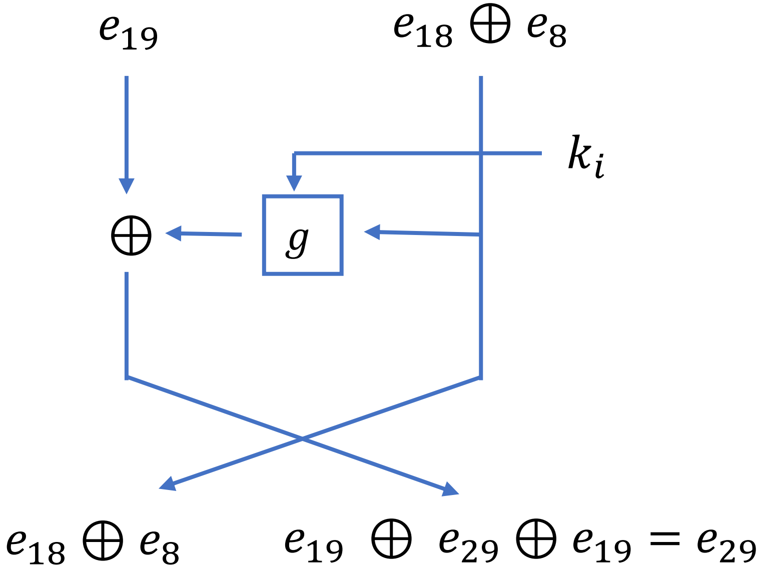
Similarly, $e_j \oplus e_k \rightarrow e_{j+11} \oplus e_{k+11}$ with probability 1/4 when j, k ∈ J (j ≠ k).

Using this idea,
we can build many good characteristics for four rounds of COCONUT98.

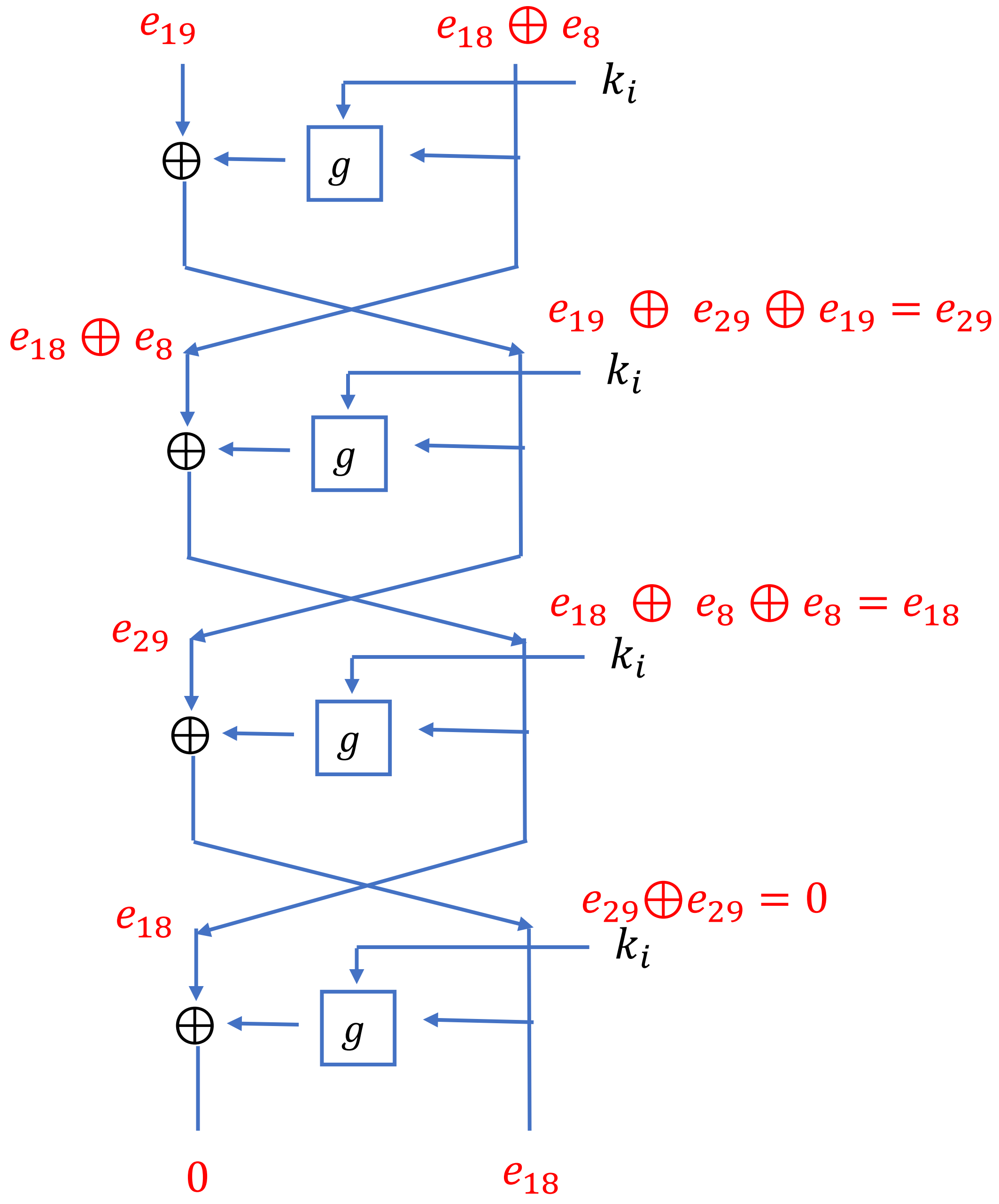
For example, the characteristic

$(e_{19}, e_{18} \oplus e_8) \rightarrow (e_{18} \oplus e_8, e_{29}) \rightarrow (e_{29}, e_{18}) \rightarrow (e_{18}, 0) \rightarrow (0, e_{18})$

for ψ has probability $\approx \frac{1}{2} * \frac{1}{2} * \frac{1}{2} * \frac{1}{2} = 2^{-4}$

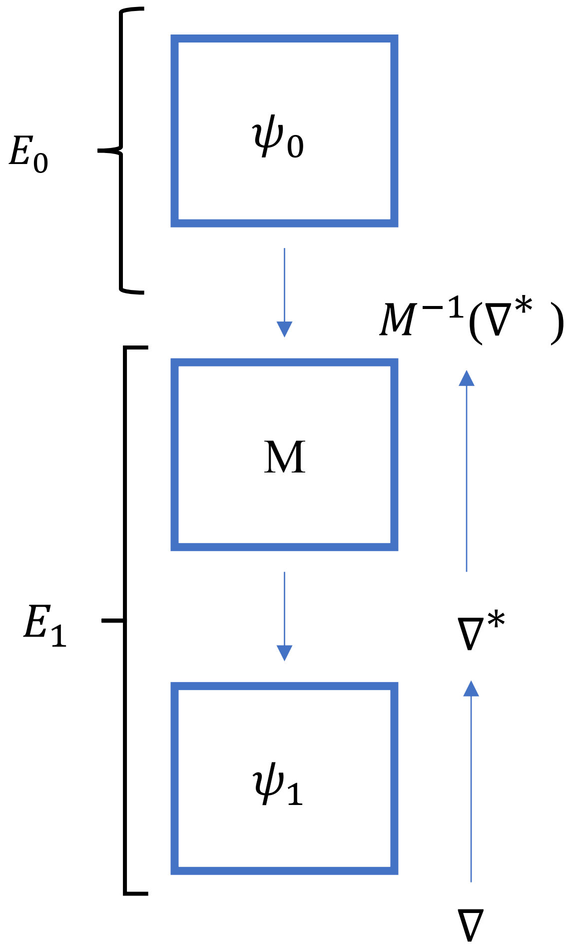


Probability $\approx \frac{1}{4} * \frac{1}{2} * \frac{1}{2} = 2^{-4}$



Differential Characteristics for COCONUT98 :

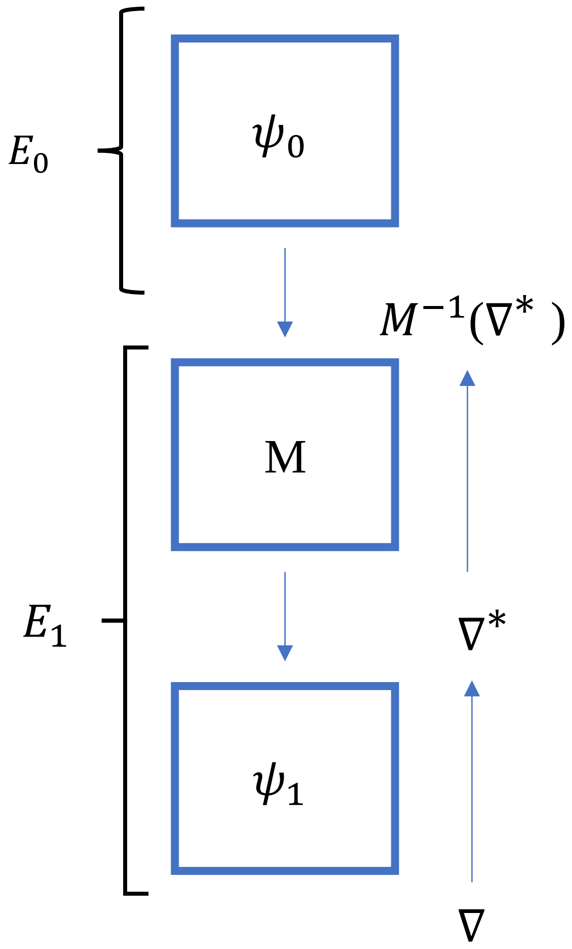
$M \text{ is affine } \Longrightarrow \text{For fixed key}, \nabla^* \rightarrow M^{-1}(\nabla^*) \text{ holds with probability } 1$



Boomerang Attack on COCONUT98

Differential Characteristics for COCONUT98 :

$$M \text{ is affine } \Longrightarrow For\ fixed\ key\ , \nabla^* \rightarrow M^{-1}(\nabla^*)\ holds\ with\ probability\ 1$$



Simple Ex:

$$M(x) = 3x + 2$$

M(1) = 5
M(3) = 11

M(5) = 17
M(7) = 23

Differential Characteristics for COCONUT98 :

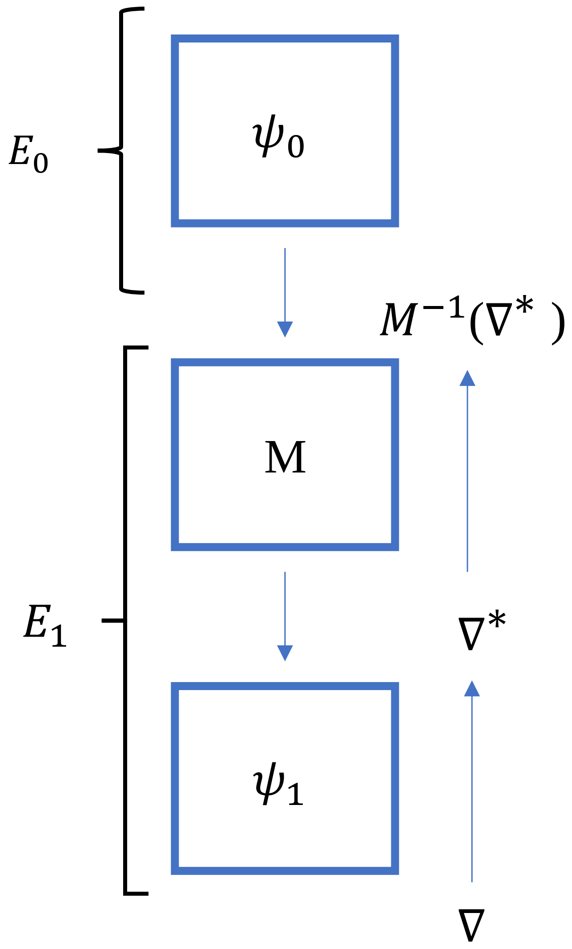
$M \; is \; affine \;\; \Longrightarrow \; For \; fixed \; key \, , \nabla^* \rightarrow M^{-1}(\nabla^*) \; holds \; with \; probability \; 1$

Take $E_0 = \psi_0$ and $E_1 = \psi_1 \; o \; M$

$\nabla \rightarrow \nabla^*$ is a good characteristic for ψ_1^{-1}

$$\Downarrow$$

we will obtain a good characteristic $\nabla^* \rightarrow M^{-1}(\nabla^* \,)$ for E_1^{-1}

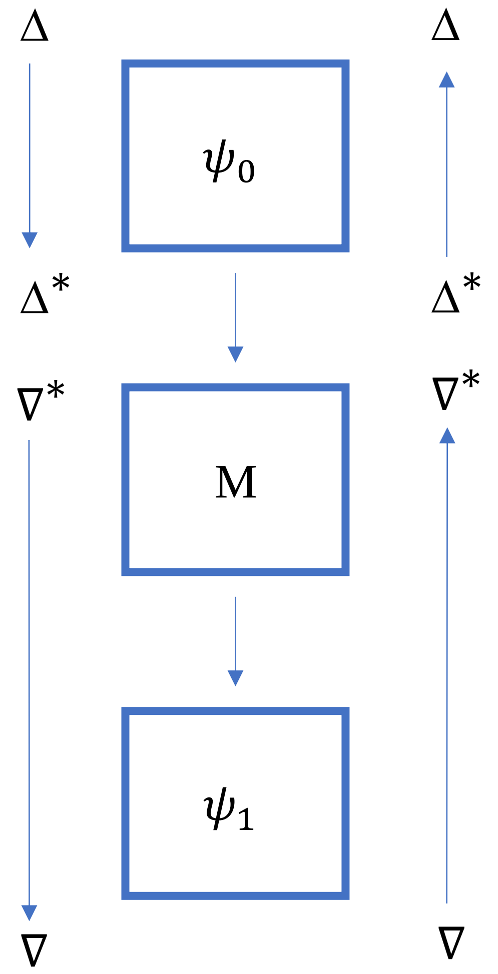


Boomerang Attack on COCONUT98

Probability:

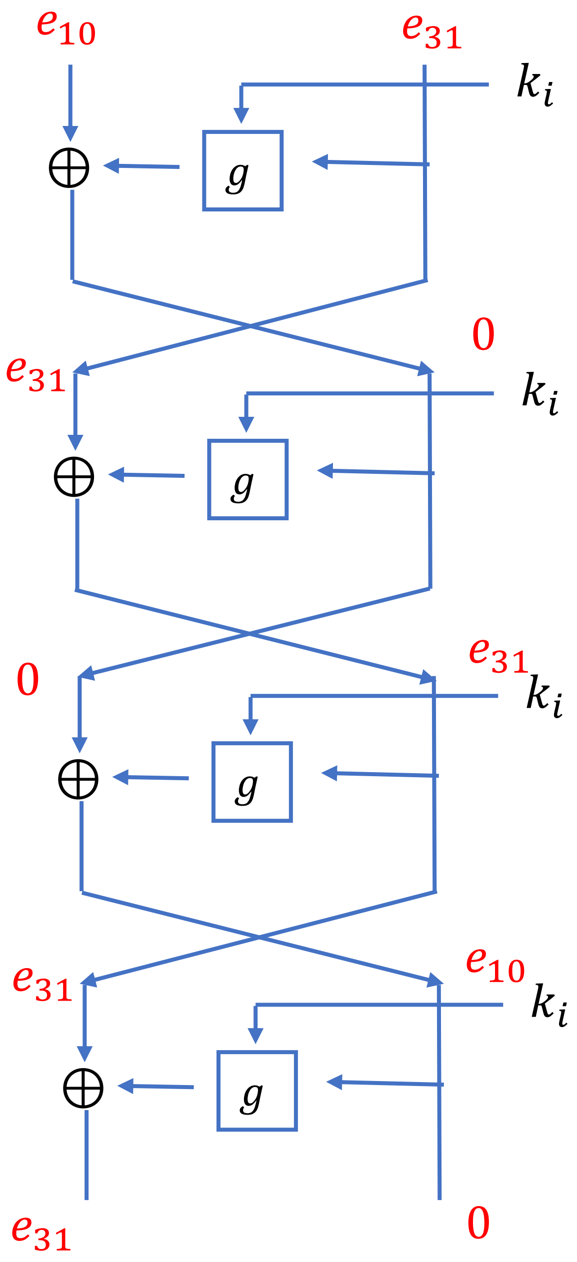
$$p \approx \sum_{\Delta^*} \Pr[\Delta \to \Delta^* \text{ by } \Psi_0]^2 \cdot \sum_{\nabla^*} \Pr[\nabla \to \nabla^* \text{ by } \Psi_1^{-1}]^2.$$

For COCONUT98, this can be used to significantly increase the probability of attack. Empirically, we find that $\Delta = \nabla = (e_{10}, e_{31})$ provides $p \approx 0.023 \cdot 0.023 \approx 1/1900$.



$$\textbf{Probability} \approx \frac{1}{2} * 1 * \frac{1}{2} * \frac{1}{2} = 2^{-3}$$

$$\mathbf{p} \approx 2^{-3*2} = 2^{-6} = 0.016$$



Boomerang Attack on COCONUT98

DISTINGUISHED ATTACK:

Let $Q \oplus Q' = (?, e_{31})$ where ? represents an arbitrary word $\qquad \boldsymbol{probability} = \frac{1}{1900} * 2 = \frac{1}{950}$

- With $950 * 4 = 3800$ adaptive chosen plaintext-ciphertext queries, we can get 1 right quartet.
- COCONUT98 can be easily distinguished from an ideal cipher with using right quartet.

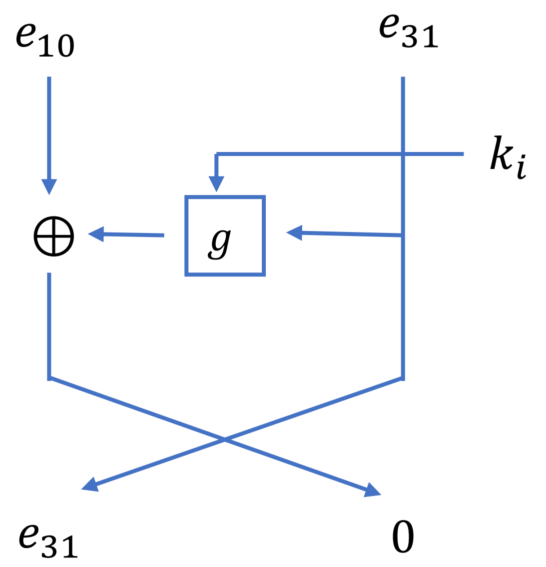
Boomerang Attack on COCONUT98

KEY RECOVERY ATTACK:

Let $Q \oplus Q' = (?, e_{31})$ where ? represents an arbitrary word

$$\boldsymbol{probability} = \frac{1}{1900} * 2 = \frac{1}{950}$$

- From $16 * 950 * 4$ adaptive choosen plaintext-ciphertext queries, we generate 16 right quartet.
- Guess K_1 and peel off the first round.
- Xor difference after one round must be (e_{31},0) for both P , P′ and Q,Q′
- This condition holds for 1/2 of the wrong key values.Therefore each quartet gives one bit of information on K_1 from the P, P ′ pair and another bit of information from the Q, Q′ pair.



Boomerang Attack on COCONUT98

For each K_1 candidate (2^{32})

For each Right quartets (16)

Encrypt P , P′, Q , Q′ 1 round
Xor difference after one round must be (e_{31},0) for both P , P′ and Q , Q′

If all Right quartets gives correct xor difference

Key candidate is correct

If not

Key candidate is wrong

Boomerang Attack on COCONUT98

- Next, we recover $K_2 \oplus K_4$ by decrypting up one round and examining the xor difference in the C, D pair and in the C′, D′ pair.

- Then we repeat the attack on the reduced cipher. For instance, we can use about $8 * 144 * 4$ more adaptive chosen plaintext/ciphertext queries to generate about 8 useful quartets for the reduced cipher if we use the same settings for Δ, ∇, since then the success probability p increases to about $\frac{1}{144}$.

- Using these 8 useful quartets for the reduced cipher we learn K_3

- We repeat the attack iteratively until the entire key is known.

Boomerang Attack on COCONUT98

In all, the complexity of the attack is about $16 * 950 * 4 + 8 * 144 * 4 + \ldots \approx 2^{16}$

The attack requires $8 * 2 * 32 * 2^{32} = 2^{41}$ offline computations of the F function

$$\text{time} = 2^{32}(16 * 4 * 2) + 2^{32}(8 * 4 * 2) + 2^{32}(4 * 4 * 2) + 2^{32}(2 * 4 * 2) + 2^{32}(1 * 4 * 2)$$

$$= 2^{32}(16 * 4 * 2 + 8 * 4 * 2 + 4 * 4 * 2 + 2 * 4 * 2 + 1 * 4 * 2)$$

$$= 2^{32} * 8 * (16 + 8 + 4 + 2 + 1)$$

$$\approx 2^{32} * 8 * 32$$

Meet-in-the-Middle Attack on COCONUT98

- The very simple key schedule used in COCONUT98 exposes it to meet-in-the-middle attacks.

- The problem is that there are only 96 bits of entropy in the first four round subkeys, and a similar property holds for the last four round subkeys.

i	1	2	3	4
k_i	K_1	$K_1 \oplus K_3$	$K_1 \oplus K_3 \oplus K_4$	$K_1 \oplus K_4$

i	5	6	7	8
k_i	K_2	$K_2 \oplus K_3$	$K_2 \oplus K_3 \oplus K_4$	$K_2 \oplus K_4$

Meet-in-the-Middle Attack on COCONUT98

ATTACK FOR ONE PAIR :

1. Obtain known text pairs P , C
2. Guess K_2 and K_3
3. For each possibility for K_1 , store $\psi_0(P)$ in the look-up table
4. For each possibility for K_4 , compute $\psi_1^{-1}\ (C)$
5. Look mach in the lookup table.

$\psi_0(P)$= z

(z_1, l_1)
(z_2, l_2)
….
$(z_{2^{32}}, l_{2^{32}})$

$\psi_1^{-1}\ (C)$= l

Meet-in-the-Middle Attack on COCONUT98

ATTACK:

1. Obtain four known text pairs $P_{j\,,}\, C_j$ for j = 0,1,2,3.
2. Guess K_2 *and* K_3
3. For each possibility for K_1, store $(\psi_0(P_0) - \psi_0(P_1))$ / $(\psi_0(P_2) - \psi_0(P_3))$ in the look-up table.
4. For each possibility for K_2 , compute $(\psi_1^{-1}\,(C_0) - \psi_1^{-1}\,(C_0))$ / $(\psi_1^{-1}\,(C_0) - \psi_1^{-1}\,(C_0))$
5. Look mach in the lookup table.

Therefore, with just four known texts and about $\mathbf{2^{96}}$ offline work, one can break COCONUT98 using standard meet-in-the-middle techniques

References

1) S. Vaudenay, “Provable Security for Block Ciphers”

2) D. Wagner, “The Boomerang Attack”, FSE 99