CS5760: Topics in Cryptanalysis **24 March 2025**

Lecture 5: The Boomerang Attack

Instructors: Maria Francis and M. V. Panduranga Rao *Scribe: Gautam Singh*

This set of notes explains the original boomerang attack described in David Wagner's 1999 paper.

5.1 Introduction

The boomerang attack is based on differential cryptanalysis. The main strength of this attack is in the fact that preventing high probability differentials does not make a cipher secure. According to the authors, symmetric ciphers at the time were designed to restrict high probability differentials. Designers would appeal to a "folk theorem", which states that if p is an upper bound on the probability of any differential characteristic of the cipher, then $\frac{1}{p}$ texts are required to break it.

However, the boomerang attack disproves this theorem. In particular, if the best characteristic for half of the rounds of the cipher has probability q, then the boomerang attack requires $\mathcal{O}(q^{-4})$ chosen texts. The bound would then be surpassed if $q^{-4} << p^{-1}$. It is worth mentioning that the (unrelated) technique of *impossible differentials* also disproves this "folk theorem".

5.2 An Overview of the Boomerang Attack

The boomerang attack aims to generate a quartet halfway though the cipher as shown in Figure 5.1. Suppose E represents the encryption operation. Then, we decompose the cipher into two halves $E = E_1 \circ E_0$. Let $\Delta \to \Delta^*$ be a differential characteristic for E_0 and $\nabla \to \nabla^*$ be a differential characteristic for E_1^{-1}.

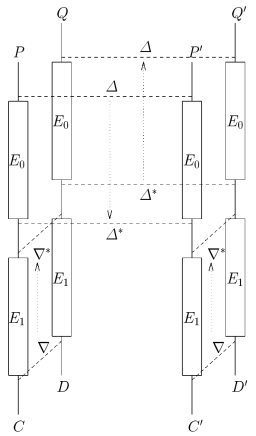

Figure 5.1: A schematic of the basic boomerang attack.

The basic idea of the boomerang attack is to generate a quartet P, P', Q, Q' with ciphertexts C, C', D, D' respectively such that P, P' follow the characteristic for E_0 and the pairs P, Q and P', Q' follow the charac-

teristic for E_1^{-1}. Then, the authors claim the pair Q, Q' is set up to use the characteristic $\Delta^* \to \Delta$ for E_0^{-1}. This is because

$$E_0(Q) \oplus E_0(Q') = E_0(P) \oplus E_0(P') \oplus E_0(P) \oplus E_0(Q) \oplus E_0(P') \oplus E_0(Q') \tag{5.1}$$
$$= E_0(P) \oplus E_0(P') \oplus E_1^{-1}(C) \oplus E_1^{-1}(D) \oplus E_1^{-1}(C') \oplus E_1^{-1}(D') \tag{5.2}$$
$$= \Delta^* \oplus \nabla^* \oplus \nabla^* = \Delta^*. \tag{5.3}$$

From (5.3), we see that Q, Q' will also follow the same characteristic as P, P', which shows the "boomerang". A *right quartet* is one where all the four characteristics mentioned above hold for their respective pairs. To generate this quartet, one can choose an arbitrary P and set $P' = P \oplus \Delta$. After obtaining C, C' with two chosen-plaintext queries, we can generate $D = C \oplus \nabla$ and $D' = C' \oplus \nabla$. Finally, we obtain Q, Q' with two adaptive chosen-ciphertext queries. After generating sufficiently many right quartets, a suitable counting scheme may be used for cryptanalysis or an attack distinguishing the cipher from a truly random function may be carried out.

We will now describe the working of COCONUT98 and the boomerang attack on it.

5.3 Cryptanalysis of COCONUT98

The COCONUT98 cipher uses decorrelation techniques to admit no high probability differentials over the entire cipher. However, the boomerang attack still works and is able to break this cipher.

5.3.1 The COCONUT98 Algorithm

COCONUT98 uses a 256-bit key $K = (K_1, \ldots, K_8)$. The key schedule is shown in Table 5.1.

i	1	2	3	4	5	6	7	8
k_i	K_1	$K_1 \oplus K_3$	$K_1 \oplus K_3 \oplus K_4$	$K_1 \oplus K_4$	K_2	$K_2 \oplus K_3$	$K_2 \oplus K_3 \oplus K_4$	$K_2 \oplus K_4$

Table 5.1: Key schedule of COCONUT98.

The last four words of the key are used in the decorrelation module

$$M(xy) = (xy \oplus K_5K_6) \times K_7K_8 \bmod \mathrm{GF}(2^{64}) \tag{5.4}$$

where xy denotes the concatenation of the 32-bit words x and y and $\mathrm{GF}(2^{64})$ denotes the Galois Field of size 2^{64}.

Now, we can build the Feistel network. Suppose that c is a public 32 bit constant, $ROL_{11}(\cdot)$ represents left rotation by 11 bits and $S : \mathbb{Z}_2^8 \to \mathbb{Z}_2^{24}$ is a fixed S box. Then, the i-th round function F_i is given by

$$\phi(x) = x + 256 \cdot S(x \bmod 256) \bmod 2^{32} \tag{5.5}$$
$$F_i((x, y)) = (y, x \oplus \phi(ROL_{11}(\phi(y \oplus k_i)) + c \bmod 2^{32})) \tag{5.6}$$
$$\Psi_i = F_{4i+4} \circ F_{4i+3} \circ F_{4i+2} \circ F_{4i+1} \tag{5.7}$$

and COCONUT98 is defined as $\Psi_1 \circ M \circ \Psi_0$. Thus, there are four Feistel rounds before and after the decorrelation module.

5.3.2 Differential Characteristics of COCONUT98

Every differential $\delta \to \delta^*$ over M has an average probability of $\frac{1}{2^{64}-1}$, where $\delta, \delta^* \neq 0$. This is the reason why COCONUT98 does not admit high probability differentials. This makes it a perfect candidate to demonstrate the strength of the boomerang attack.

Suppose $e_j = 2^j$ for $0 \leq j < 32$ (we consider 0-based subscripts here to better model the left rotation). An important differential characteristic for one round of COCONUT98 is that $e_j \to e_{j+11}$ with probability approximately $\frac{1}{2}$ when $j \in J = \{8, 9, \ldots, 19, 20, 29, 30, 31\}$. To see how, we can write $x \overset{\phi}{\mapsto} (x + a \bmod 2^{32})$ and the overall effect of F is $x \overset{F}{\mapsto} (x + a \bmod 2^{32}) + b \bmod 2^{32}$ which can be written as $x + c \bmod 2^{32}$, where $c = a + b$. In other words, there is effectively only one carry happening for bits in J. Empirically, the probabilities are smaller than $\frac{1}{2}$ for some values of j. For instance, the probabilities are $0.47, 0.44, 0.38$ for $j = 18, 19, 20$ and $0.47, 0.44$ for $j = 29, 30$.

This observation enables us to write four-round characteristics for COCONUT98 such as

$$(e_{19}, e_{18} \oplus e_8) \to (e_{18} \oplus e_8, e_{29}) \to (e_{29}, e_{18}) \to (e_{18}, 0) \to (0, e_{18}) \tag{5.8}$$

with probability $0.83 \cdot 2^{-4} \approx 2^{-4.3}$.

We now have our differentials for the two halves of the cipher, but we have to account for the decorrelation module. The authors use the crucial idea that M is affine to make the boomerang attack work. For any fixed key, the decorrelation module M becomes affine (of the form $y = mx + c$) and thus has characteristics $\nabla^* \to M^{-1}(\nabla^*)$ with probability 1. Thus, by absorbing M in either E_0 or E_1, there will be no change in the probabilities of the respective characteristics over half the rounds. In other words, the attacker need not know the exact value of $M^{-1}(\nabla^*)$, since it depends only on the key.

An estimate of the success probability for this attack is

$$p \approx \sum_{\Delta^*} \Pr[\Delta \to \Delta^* \text{ by } \Psi_0]^2 \cdot \sum_{\nabla^*} \Pr[\nabla \to \nabla^* \text{ by } \Psi_1^{-1}]^2. \tag{5.9}$$

We do not need to know that value of ∇^* in advance because we only require that the difference after decrypting by Ψ_1 is same in the pairs P, Q and P', Q'. A similar argument holds for Δ^*. The authors find empiricially that $\Delta = \nabla = (e_{10}, e_{31})$ gives $p \approx 0.023 \cdot 0.023 \approx \frac{1}{1900}$.

5.3.3 The Boomerang Attack on COCONUT98

The authors use a 1-R attack on COCONUT98, where the success criterion is $Q \oplus Q' = (?, e_{31})$ with ? representing an arbitrary word. This doubles the success probability to $\frac{1}{950}$. Clearly, we can use $950 \cdot 4 = 3800$ adaptive chosen plaintext/ciphertext (ACPC) queries to distinguish COCONUT98 from an ideal cipher.

For a key recovery attack, notice that we can generate 16 right quartets in about $16 \cdot 950 \cdot 4$ ACPC. With a very high signal to noise ratio, the quartets should be filtered out effectively. To peel of the first (and last) rounds, we exhaustively search K_1. Notice that 16 quartets are enough since the XOR difference after one round will be $(e_{31}, 0)$, which holds for half of the wrong key values since the probability of this characteristic

is $\frac{1}{2}$. Using the 32 pairs from each of the 16 quartets should be enough to uniquely identify K_1 and similarly $K_2 \oplus K_4$. Now we can repeat this attack on the peeled-off cipher similarly with more ACPC to generate some more quartets. Notice that with each peel, the characteristic probability will increase and fewer ACPC are needed to get enough quartets.

The complexity of this attack is about $16 \cdot 950 \cdot 4 + 8 \cdot 144 \cdot 4 + \ldots \approx 2^{16}$ ACPC. Additionally, this attack requires $8 \cdot 2 \cdot 32 \cdot 2^{32} = 2^{41}$ offline computations of the F function. Converting this to a known-plaintext attack will increase the complexity to 2^{52} texts. Since offline computations are one-time, this attack is practical.

The authors propose a few ways to strengthen COCONUT98. One way is to use more rounds to weaken the characteristic probabilities over half the cipher (for instance, using 16 rounds instead of 4). Another approach could be to use the decorrelation module after each Feistel round.