The Retracing Boomerang Attack

Gautam Singh

Indian Institute of Technology Hyderabad

April 28, 2025

Introduction

1. Broke the record for 5-round AES when it was published.

Introduction

1. Broke the record for 5-round AES when it was published.
2. Brings the attack complexity down to $2^{16.5}$ encryptions.

Introduction

1. Broke the record for 5-round AES when it was published.
2. Brings the attack complexity down to $2^{16.5}$ encryptions.
3. Uncovers a hidden relationship between boomerang attacks and two other cryptanalysis techniques: yoyo game and mixture differentials.

The Boomerang Attack

1. Typically split the encryption function as $E = E_1 \circ E_0$, with differential trails for each sub-cipher.

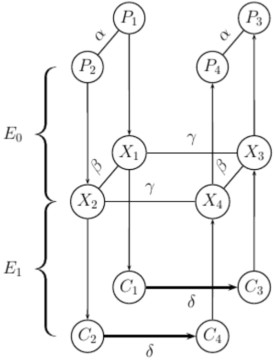

Figure 1: The boomerang attack.

The Boomerang Attack

1. Typically split the encryption function as $E = E_1 \circ E_0$, with differential trails for each sub-cipher.
2. We can build a distinguisher that can distinguish E from a truly random permutation in $\mathcal{O}((pq)^{-2})$ plaintext pairs.

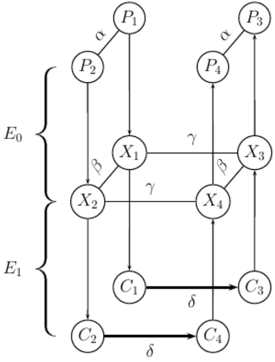

Figure 1: The boomerang attack.

The Boomerang Distinguisher

Algorithm 1 The Boomerang Attack Distinguisher

Initialize a counter $ctr \leftarrow 0$.
Generate $(pq)^{-2}$ plaintext pairs (P_1, P_2) such that $P_1 \oplus P_2 = \alpha$.
for all pairs (P_1, P_2) **do**
    Ask for the encryption of (P_1, P_2) to (C_1, C_2).
    Compute $C_3 = C_1 \oplus \delta$ and $C_4 = C_2 \oplus \delta$. ▷ *δ-shift*
    Ask for the decryption of (C_3, C_4) to (P_3, P_4).
    if $P_3 \oplus P_4 = \alpha$ **then**
        Increment *ctr*
if $ctr > 0$ **then**
    return This is the cipher E
else
    return This is a random permutation

Boomerang Switches

1. Gain 1-2 middle rounds for free by choosing differentials carefully. Here, we discuss the *S-box switch*.

Boomerang Switches

1. Gain 1-2 middle rounds for free by choosing differentials carefully. Here, we discuss the *S-box switch*.
2. Suppose the last operation in E_0 is a layer of S-boxes where $S(\rho_1 \| \rho_2 \| \dots \| \rho_t) = (f_1(\rho_1) \| f_2(\rho_2) \| \dots \| f_t(\rho_t))$ for t independent keyed functions f_i. Suppose the difference for both β and γ corresponding to the output of some f_j is equal to Δ.

Boomerang Switches

1. Gain 1-2 middle rounds for free by choosing differentials carefully. Here, we discuss the *S-box switch*.
2. Suppose the last operation in E_0 is a layer of S-boxes where $S(\rho_1\|\rho_2\|\ldots\|\rho_t) = (f_1(\rho_1)\|f_2(\rho_2)\|\ldots\|f_t(\rho_t))$ for t independent keyed functions f_i. Suppose the difference for both β and γ corresponding to the output of some f_j is equal to Δ.
3. Denoting this part of the intermediate state by X_j,

$$(X_1)_j \oplus (X_2)_j = (X_1)_j \oplus (X_3)_j = (X_2)_j \oplus (X_4)_j = \Delta \tag{1}$$

which shows $(X_1)_j = (X_4)_j$ and $(X_2)_j = (X_3)_j$.

Boomerang Switches

1. Gain 1-2 middle rounds for free by choosing differentials carefully. Here, we discuss the *S-box switch*.
2. Suppose the last operation in E_0 is a layer of S-boxes where $S(\rho_1 \| \rho_2 \| \dots \| \rho_t) = (f_1(\rho_1) \| f_2(\rho_2) \| \dots \| f_t(\rho_t))$ for t independent keyed functions f_i. Suppose the difference for both β and γ corresponding to the output of some f_j is equal to Δ.
3. Denoting this part of the intermediate state by X_j,

$$(X_1)_j \oplus (X_2)_j = (X_1)_j \oplus (X_3)_j = (X_2)_j \oplus (X_4)_j = \Delta \tag{1}$$

   which shows $(X_1)_j = (X_4)_j$ and $(X_2)_j = (X_3)_j$.
4. If the differential characteristic in f_j^{-1} holds for (X_1, X_2), then it will hold for (X_3, X_4). *We pay for probability in one direction.*

Boomerang Switches

1. Gain 1-2 middle rounds for free by choosing differentials carefully. Here, we discuss the *S-box switch*.
2. Suppose the last operation in E_0 is a layer of S-boxes where $S(\rho_1 \| \rho_2 \| \dots \| \rho_t) = (f_1(\rho_1) \| f_2(\rho_2) \| \dots \| f_t(\rho_t))$ for t independent keyed functions f_i. Suppose the difference for both β and γ corresponding to the output of some f_j is equal to Δ.
3. Denoting this part of the intermediate state by X_j,
$$(X_1)_j \oplus (X_2)_j = (X_1)_j \oplus (X_3)_j = (X_2)_j \oplus (X_4)_j = \Delta \tag{1}$$
which shows $(X_1)_j = (X_4)_j$ and $(X_2)_j = (X_3)_j$.
4. If the differential characteristic in f_j^{-1} holds for (X_1, X_2), then it will hold for (X_3, X_4). *We pay for probability in one direction.*
5. Distinguisher probability increases by a factor of $(q')^{-1}$, where q' is the probability of the differential characteristic in f_j.

The Yoyo Game

1. Similar to boomerang, starts by encrypting (P_1, P_2) to (C_1, C_2), then modifying them to (C_3, C_4) and decrypting them.

The Yoyo Game

1. Similar to boomerang, starts by encrypting (P_1, P_2) to (C_1, C_2), then modifying them to (C_3, C_4) and decrypting them.
2. *Unlike* the boomerang attack, this process continues in the yoyo game.

The Yoyo Game

1. Similar to boomerang, starts by encrypting (P_1, P_2) to (C_1, C_2), then modifying them to (C_3, C_4) and decrypting them.
2. *Unlike* the boomerang attack, this process continues in the yoyo game.
3. *All* pairs of intermediate values (X_{2l+1}, X_{2l+2}) satisfy some property (such as zero difference in some part).

The Yoyo Game

1. Similar to boomerang, starts by encrypting (P_1, P_2) to (C_1, C_2), then modifying them to (C_3, C_4) and decrypting them.
2. *Unlike* the boomerang attack, this process continues in the yoyo game.
3. *All* pairs of intermediate values (X_{2l+1}, X_{2l+2}) satisfy some property (such as zero difference in some part).
4. Probabilities are low with large l. Still, the yoyo technique has been used to attack AES reduced to 5 rounds.

Mixture

Definition 1 (Mixture)

Suppose $P_i \triangleq (\rho_1^i, \rho_2^i, \ldots, \rho_t^i)$. Given a plaintext pair (P_1, P_2), we say (P_3, P_4) is a *mixture counterpart* of (P_1, P_2) if for each $1 \leq j \leq t$, the quartet $(\rho_j^1, \rho_j^2, \rho_j^3, \rho_j^4)$ consists of two pairs of equal values or of four equal values. The quartet (P_1, P_2, P_3, P_4) is called a *mixture*.

Mixture

Definition 1 (Mixture)

Suppose $P_i \triangleq (\rho_1^i, \rho_2^i, \ldots, \rho_t^i)$. Given a plaintext pair (P_1, P_2), we say (P_3, P_4) is a *mixture counterpart* of (P_1, P_2) if for each $1 \leq j \leq t$, the quartet $(\rho_j^1, \rho_j^2, \rho_j^3, \rho_j^4)$ consists of two pairs of equal values or of four equal values. The quartet (P_1, P_2, P_3, P_4) is called a *mixture*.

1. If (P_1, P_2, P_3, P_4) is a mixture, then XOR of the intermediate values (X_1, X_2, X_3, X_4) is zero.

Mixture

Definition 1 (Mixture)

Suppose $P_i \triangleq (\rho^i_1, \rho^i_2, \ldots, \rho^i_t)$. Given a plaintext pair (P_1, P_2), we say (P_3, P_4) is a *mixture counterpart* of (P_1, P_2) if for each $1 \leq j \leq t$, the quartet $(\rho^1_j, \rho^2_j, \rho^3_j, \rho^4_j)$ consists of two pairs of equal values or of four equal values. The quartet (P_1, P_2, P_3, P_4) is called a *mixture*.

1. If (P_1, P_2, P_3, P_4) is a mixture, then XOR of the intermediate values (X_1, X_2, X_3, X_4) is zero.
2. $X_1 \oplus X_3 = \gamma \implies X_2 \oplus X_4 = \gamma$. Hence, for $\gamma \xrightarrow{q} \delta$ in E_1, $C_1 \oplus C_3 = C_2 \oplus C_4 = \delta$ with probability q^2.

Mixture

Definition 1 (Mixture)

Suppose $P_i \triangleq (\rho_1^i, \rho_2^i, \ldots, \rho_t^i)$. Given a plaintext pair (P_1, P_2), we say (P_3, P_4) is a *mixture counterpart* of (P_1, P_2) if for each $1 \leq j \leq t$, the quartet $(\rho_j^1, \rho_j^2, \rho_j^3, \rho_j^4)$ consists of two pairs of equal values or of four equal values. The quartet (P_1, P_2, P_3, P_4) is called a *mixture*.

1. If (P_1, P_2, P_3, P_4) is a mixture, then XOR of the intermediate values (X_1, X_2, X_3, X_4) is zero.
2. $X_1 \oplus X_3 = \gamma \implies X_2 \oplus X_4 = \gamma$. Hence, for $\gamma \xrightarrow{q} \delta$ in E_1, $C_1 \oplus C_3 = C_2 \oplus C_4 = \delta$ with probability q^2.
3. Has been applied to AES reduced up to 6 rounds. E_0 is taken to be the first 1.5 rounds of AES, which can be treated as four parallel super S-boxes.

The Retracing Boomerang Framework

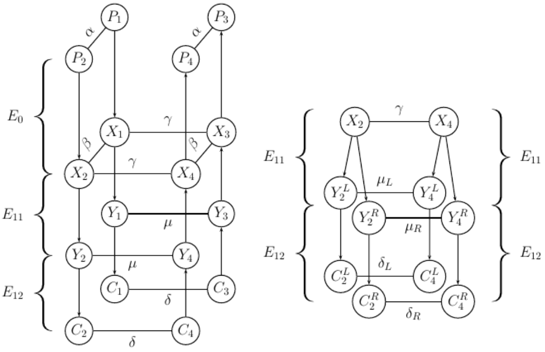

Figure 2: The retracing boomerang attack.

The Retracing Boomerang Attack

1. The *retracing boomerang* framework consists of a *shifting* type and a *mixing* type.

The Retracing Boomerang Attack

1. The *retracing boomerang* framework consists of a *shifting* type and a *mixing* type.
2. Both attacks use the setup shown in Figure 2.

The Retracing Boomerang Attack

1. The *retracing boomerang* framework consists of a *shifting* type and a *mixing* type.
2. Both attacks use the setup shown in Figure 2.
3. Although the additional split looks restrictive, it applies for a wide class of block ciphers such as SASAS constructions.

The Retracing Boomerang Attack

1. The *retracing boomerang* framework consists of a *shifting* type and a *mixing* type.
2. Both attacks use the setup shown in Figure 2.
3. Although the additional split looks restrictive, it applies for a wide class of block ciphers such as SASAS constructions.
4. Further, we assume that E_{12} can be split into two parts of size b and $n - b$ bits, call these functions E_{12}^L and E_{12}^R, with characteristic probabilities q_2^L and q_2^R respectively.