New Exchanged Boomerang Distinguishers for 5-Round AES

Hanbeom Shin[1], Seonkyu Kim[1], Dongjae Lee[2], Deukjo Hong[3], Jaechul Sung[4], and Seokhie Hong[1]

[1] School of Cybersecurity, Korea University, South Korea
newonetiger@korea.ac.kr, kimsg125@korea.ac.kr, shhong@korea.ac.kr
[2] Department of Convergence Security, Kangwon National University, South Korea
dongjae.lee@kangwon.ac.kr
[3] Department of Information and Engineering, Jeonbuk National University, South Korea
deukjo.hong@jbnu.ac.kr
[4] Department of Mathematics, University of Seoul, South Korea
jcsung@uos.ac.kr

Abstract. In block ciphers, the attacker should not be able to distinguish a block cipher from a random permutation, making the existence of a distinguisher important. Cryptanalysis of the reduced-round variants of block ciphers is also important in cryptographic design. AES is the most widely used block cipher, and currently, the best-known distinguisher for 5-round AES has a data and time complexity of $2^{29.95}$ with a success probability of 55%. In this paper, we propose the fully active exchanged boomerang and multiple exchanged boomerang distinguishers for 5-round AES, based on the retracing boomerang key-recovery attack. The fully active exchanged boomerang distinguisher utilizes the probability that either each byte of the diagonal of the returned plaintext pair is fully active, or the diagonal is inactive for all diagonals. This probability is very high, but we enhance it using the friends pair technique to distinguish a block cipher from a random permutation. The multiple exchanged boomerang distinguisher utilizes the fact that there are three trails where the probability of one diagonal of the returned plaintext pair being inactive is higher than the random probability, and one trail where it is equal to the random probability. This 5-round distinguisher has a complexity of $2^{27.08}$ and a success probability of 82%, which represents a new best-known result for the secret-key distinguisher on 5-round AES.

Keywords: AES · Distinguisher · Boomerang · Exchanged Boomerang.

1 Introduction

A block cipher is a cryptographic algorithm that encrypts data in fixed-size units using a secret key. A block cipher primitive is typically designed by repeating a round function multiple times. While using many rounds ensures security, it also reduces efficiency. Therefore, to design a block cipher that is both secure

and efficient, it is important to calculate the number of rounds that are secure against various attacks through security analysis of reduced-round variants, and then select the appropriate number of rounds by adding margin rounds.

The security of a block cipher primitive is generally evaluated by demonstrating its resistance against various known attacks, which fall into two categories: distinguishing attacks and key recovery attacks. A distinguishing attack aims to distinguish a block cipher from a random permutation, and is referred to as a distinguisher. In particular, the secret-key distinguisher allows for the evaluation of the cipher's randomness for any given key.

Well-known attacks on block ciphers include differential cryptanalysis (DC) [9] and linear cryptanalysis (LC) [30]. These cryptanalysis techniques were initially introduced for the Data Encryption Standard (DES) and have since led to various variants. As these analysis techniques evolved and computing power increased, the National Institute of Standards and Technology (NIST) initiated a competition to develop a new block cipher standard.

DC has been utilized and extended in various attacks, including truncated differentials [27], impossible differential cryptanalysis [26], high-order differentials [27], boomerang attacks [37], differential-linear attacks [28], integral [17], meet-in-the-middle [14] and others. Most recently, variations of DC have been proposed, such as the subspace trail [21], the yoyo trick [33,31], the multiple-of-8 property [20], mixture-differential cryptanalysis [19,3], the exchange attacks [4], and the fixed property [34].

In particular, we focus on the boomerang attack [37] introduced at FSE 1999. The boomerang attack, proposed by Wagner, is a technique that combines two high-probability short differentials to achieve a higher overall probability boomerang trail in the adaptively chosen ciphertexts setting. A boomerang trail consisting of an upper-part differential with probability p and a lower-part differential with probability q has an overall probability of p^2q^2. If $p^2q^2 < 2^{-n}$ (where n is the block size), it can be used as a distinguisher.

The boomerang attack has been extended into various variants. Plaintext-only variants, the amplified boomerang [25] and the rectangle attacks [8], were presented shortly after. To further study the dependence and the connectivity of upper and lower differentials in the boomerang attack, Dunkelman et al. proposed the sandwich attack [15]. Cid et al. used the boomerang connectivity table (BCT) [11] to analyze the case where the middle round is a single s-box layer. In [13,35,38], researchers studied the case where the middle round is composed of several rounds. Yang et al. introduced the double boomerang connectivity table (DBCT) [40] and showed that the relation between neighboring rounds cannot be ignored. Murphy showed in 2011 that some boomerang characteristics were in fact impossible [32]. The truncated boomerang attack which utilizes truncated differentials with boomerang is presented in EUROCRYPT 2023. The exchanged boomerang attack is an attack that utilizes the mixing technique (exchange property [4]) from the retracing boomerang attack [16], and it has also been utilized in the re-boomerang and boomerang chain distinguishers [39].

Among block ciphers, the most widely used is the Advanced Encryption Standard (AES) [12], which has demonstrated its security over the last 25 years. AES is designed by Daemen and Rijmen in 1997 and standardized by the NIST in 2001. Due to its security, several block ciphers with structures similar to AES have been proposed, such as SKINNY [6] and MIDORI [1]. Additionally, many tweakable block ciphers, like KIASU-BC [23] and DEOXYS-BC [24], reuse the round function of AES in their designs and some block cipher use reduced-round AES as a core component, such as Hound [18] and WEM [10], which use 5-round AES, and TNT-AES [2], which uses 6-round AES. Therefore, analyzing reduced-round variants of AES is particularly important.

Our Contributions

We first propose the fully active exchanged boomerang distinguisher. It uses plaintext pairs with one active diagonal and checks whether each of the four diagonals of the returned plaintext pair is either fully active (i.e., all four bytes are active) or inactive in the exchanged boomerang. This is possible because the right pairs following the fully active exchanged boomerang trail have at most one active byte per column after the first round MC. The probability of the fully active exchanged boomerang is 2^{-22}. However, the random probability that each of the four diagonals of the returned plaintext pair is either fully active or inactive is very high, given by

$$((1-2^{-8})^4+2^{-32})^4 \approx 2^{-0.09}.$$

We utilize the friend pairs technique [7] and exchange active inverse diagonal technique to reduce this probability to

$$(((1-2^{-8})^4+2^{-32})^4)^{2^8} \approx 2^{-23.1},$$

which is lower than the boomerang probability of 2^{-22}. As a result, we can construct the fully active exchanged boomerang distinguisher. Although the boomerang probability is high, the use of friend pairs increases the complexity accordingly. The fully active exchanged boomerang distinguisher on 5-round AES has the data and time complexities of 2^{31} with a success probability of 70%. Although the fully active distinguisher does not provide better results than the existing distinguisher, it is significant because it introduces a new approach for distinguishing based on the pair being fully active, which, to the best of our knowledge, has not been proposed before.

Then, we propose the multiple exchanged boomerang distinguisher. It uses plaintext pairs with one active diagonal and checks whether the returned plaintext pair is inactive in one inverse diagonal. We use four exchanged boomerang trails which have same input truncated differences to increase the boomerang probability to

$$2^{-28}+2^{-27.4}+2^{-28}+2^{-30} \approx 2^{-26.08}.$$

Since the probability that the returned plaintext pair is inactive in one inverse diagonal is randomly given by $4 \cdot 2^{-32} = 2^{-30}$, we can construct the multiple

exchanged boomerang distinguisher. Although the boomerang probability is not as good as that of the fully active exchanged boomerang, it is more efficient since it does not require additional pairs. The multiple exchanged boomerang distinguisher on 5-round AES has the data and time complexities of $2^{27.08}$ with a success probability of 82%. The multiple exchanged boomerang distinguisher is, to the best of our knowledge, the best distinguisher for 5-round AES.

Comparison with Previous Work

The first secret-key distinguisher for 5-round AES, known as the multiple-of-8 distinguisher, was first presented by Grassi et al. at EUROCRYPT 2017 [20]. In [33], the 5-round and 6-round yoyo distinguishers in an adaptively chosen plaintexts and ciphertexts setting were presented by Rønjom et al. at ASIACRYPT 2017. However, there was an error in the complexity calculation in [33], and it was recomputed in [31]. In ASIACRYPT 2019, Bardeh et al. presented 5-round and 6-round distinguishers, known as exchange attacks [4]. The current secret-key distinguishers for 5-round AES are shown in Table 1. Data complexity is measured in chosen plaintexts (CP), adaptively chosen ciphertexts (ACC) or adaptively chosen plaintexts and ciphertexts (ACPC). Time complexity is measured in equivalent number of 5-round AES encryptions (E) or memory accesses (M).

Table 1. Secret-key distinguishers for 5-round AES

Property	Data	Time	Succ. Prob.	Ref.
Multiple-of-8	2^{32} CP	$2^{35.6}$ M	99%	[20]
Exchange	2^{30} CP	2^{30} E	63%	[4]
Yoyo	$2^{29.95}$ ACPC	$2^{29.95}$ M	55%	[31]
Yoyo	$2^{30.65}$ ACPC	$2^{29.95}$ M	81%	[31]
Fully active exchanged boomerang	2^{31} ACC	2^{31} M	70%	Sect. 3
Multiple exchanged boomerang	$2^{27.08}$ ACC	$2^{27.08}$ M	82%	Sect. 4

Organization

The remainder of the paper is organized as follows. Section 2 provides a brief introduction to AES and explains the exchanged boomerang attack. In Section 3, we introduce the fully active exchanged boomerang distinguisher for 5-round AES. In Section 4, we introduce the fully active exchanged boomerang distin-

guisher for 5-round AES. Finally, in Section 5, we conclude the paper. The source code for the experiments in this paper is available online.[5]

2 Preliminaries

2.1 Description of the AES

AES [12] was designed by Daemen and Rijmen in 1997. It is a Substitution-Permutation Network (SPN) block cipher with a block size of 128 bits. It supports key sizes of 128, 192, and 256 bits, and employs 10, 12, and 14 rounds for each respective key size. The internal state of AES is represented as a 4×4 array of bytes, with indexing done column-wise. The round function of AES consists of four operations performed in the following order and can be seen in Figure 1.

- *SubBytes* (SB) : The S-box operation is applied to each byte of the internal state.
- *ShiftRows* (SR) : The second, third, and fourth rows are rotated to the left by 1, 2, and 3 bytes, respectively.
- *MixColumns* (MC) : Each column is multiplied by a 4×4 MDS (Maximum Distance Separable) matrix.
- *AddRoundKey* (AK) : The state is XORed with a 128-bit round key.

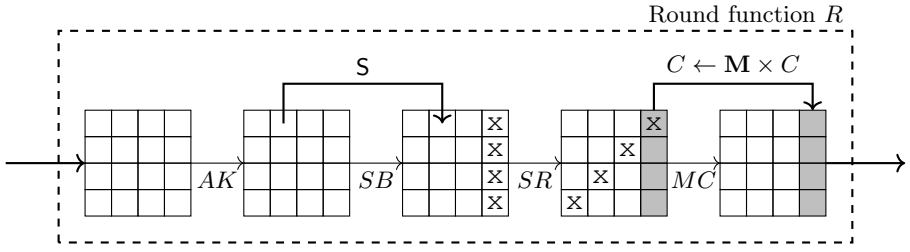

Fig. 1. Round function of AES

Before the first round, an additional AK is applied and in the final round the MC is omitted. For the reduced-round AES, the MC in the final round is omitted. The round are indexed from 1 to 14, with the initial whitening key AK as 0th round. The description of the key schedule is omitted in this paper because it is not utilized.

[5] We have submitted the source code as Supplementary Material. After the anonymous review, we will upload and make it publicly available on GitHub.

2.2 Differential and Truncated Differential Cryptanalysis

Differential cryptanalysis (DC) [9] is a well-known and powerful cryptanalysis technique for block ciphers. DC is a statistical attack on block ciphers that studies the development of differences between two encrypted plaintexts through the encryption process. A differential is defined by an input difference $\Delta_{\text{in}} \in \{0,1\}^n$ and output difference $\Delta_{\text{out}} \in \{0,1\}^n$, where n is the block size. We use the notation $\Delta_{\text{in}} \xrightarrow{E} \Delta_{\text{out}}$ with p when a differential exists with probability p, where the probability is defined over a random plaintext P:

$$p = \Pr[\Delta_{\text{in}} \xrightarrow{E} \Delta_{\text{out}}] = \Pr[E(P) \oplus E(P \oplus \Delta_{\text{in}}) = \Delta_{\text{out}}].$$

Since E is a permutation, we have $\Pr[\Delta_{\text{in}} \xrightarrow{E} \Delta_{\text{out}}] = \Pr[\Delta_{\text{out}} \xrightarrow{E^{-1}} \Delta_{\text{in}}]$.

A truncated differential [27] is defined by a set of input differences $\mathcal{D}_{\text{in}}$ and a set of output differences $\mathcal{D}_{\text{out}}$. We use the notation $\mathcal{D}_{\text{in}} \xrightarrow{E} \mathcal{D}_{\text{out}}$ to denote the existence of a truncated differential with probability $\overrightarrow{p}$, defined as (with Avg denoting the average):

$$\overrightarrow{p} = \Pr[\mathcal{D}_{\text{in}} \xrightarrow{E} \mathcal{D}_{\text{out}}] = \text{Avg}_{\Delta_{\text{in}} \in \mathcal{D}_{\text{in}}} \Pr[E(P) \oplus E(P \oplus \Delta_{\text{in}}) \in \mathcal{D}_{\text{out}}].$$

We also define the probability of the reverse truncated differential as

$$\overleftarrow{p} = \Pr[\mathcal{D}_{\text{out}} \xrightarrow{E^{-1}} \mathcal{D}_{\text{in}}] = \text{Avg}_{\Delta_{\text{out}} \in \mathcal{D}_{\text{out}}} \Pr[E^{-1}(C) \oplus E^{-1}(C \oplus \Delta_{\text{out}}) \in \mathcal{D}_{\text{in}}],$$

where C is a random ciphertext. In general, $\Pr(\mathcal{D}_{\text{in}} \xrightarrow{E} \mathcal{D}_{\text{out}})$ and $\Pr(\mathcal{D}_{\text{out}} \xrightarrow{E^{-1}} \mathcal{D}_{\text{in}})$ are different.

2.3 Boomerang Attacks

In 1999, Wagner introduced the boomerang attack [37], which combines two differential trails to construct a boomerang trail that uses longer rounds in the adaptive chosen ciphertext setting. In the boomerang attack, the encryption function E is divided into two parts, $E = E_1 \circ E_0$. For upper part E_0, there exists a differential trail $\Delta_{\text{in}} \xrightarrow{E_0} \Delta_{\text{out}}$ with probability $\overrightarrow{p}$ in the forward direction and a differential trail $\Delta_{\text{out}} \xrightarrow{E_0^{-1}} \Delta_{\text{in}}$ with probability $\overleftarrow{p}$ in the backward direction. For the lower part E_1, there exists a differential trail $\nabla_{\text{out}} \xrightarrow{E_1^{-1}} \nabla_{\text{in}}$ with probability $\overleftarrow{q}$. The boomerang process is as follows and is shown in Figure 2.

1. Choose plaintext pairs (P_1, P_2) such that $P \oplus P' = \Delta_{\text{in}}$, and ask for the corresponding ciphertext pairs (C_1, C_2).
2. Generate $C_3 = C_1 \oplus \nabla_{\text{out}}$ and $C_4 = C_2 \oplus \nabla_{\text{out}}$, and ask for the corresponding plaintext pairs (P_3, P_4).
3. Check if $P_3 \oplus P_4 = \Delta_{\text{in}}$.

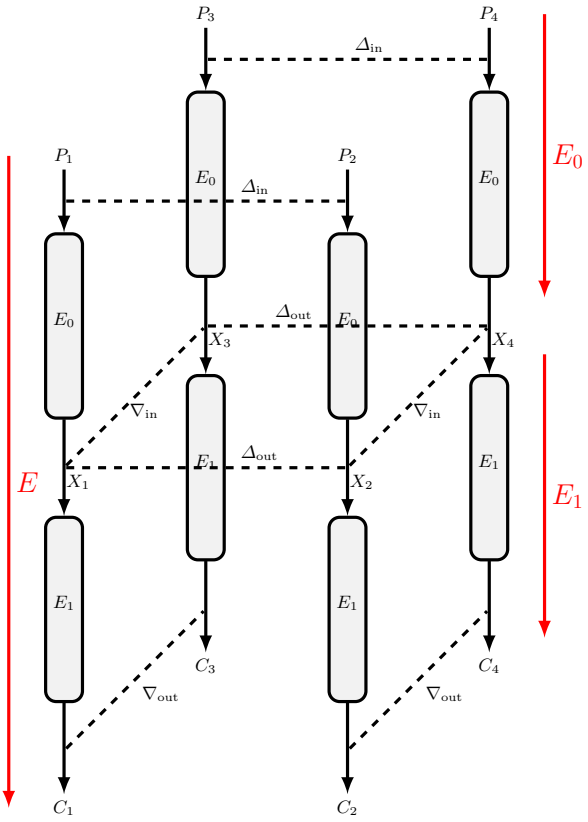

Fig. 2. The boomerang Attack

Denote $X_i = E_0(P_i)$ for $i = 1, 2, 3, 4$. Since $P_1 \oplus P_2 = \Delta_{\text{in}}$, it follows that $X_1 \oplus X_2 = \Delta_{\text{out}}$ with probability

$$\Pr[X_1 \oplus X_2 = \Delta_{\text{out}} \mid P_1 \oplus P_2 = \Delta_{\text{in}}] = \overrightarrow{p}.$$

Similarly, since $C_1 \oplus C_3 = \nabla_{\text{out}}$ and $C_2 \oplus C_4 = \nabla_{\text{out}}$, we have $X_1 \oplus X_3 = \nabla_{\text{in}}$ and $X_2 \oplus X_4 = \nabla_{\text{in}}$, each with probability

$$\Pr[X_1 \oplus X_3 = \nabla_{\text{in}} \mid C_1 \oplus C_3 = \nabla_{\text{out}}] = \Pr[X_2 \oplus X_4 = \nabla_{\text{in}} \mid C_2 \oplus C_4 = \nabla_{\text{out}}] = \overleftarrow{q}.$$

If $X_1 \oplus X_2 = \Delta_{\text{out}}$, $X_1 \oplus X_3 = \nabla_{\text{in}}$, and $X_2 \oplus X_4 = \nabla_{\text{in}}$, then

$$X_3 \oplus X_4 = X_1 \oplus X_2 \oplus X_1 \oplus X_3 \oplus X_2 \oplus X_4 = \Delta_{\text{out}} \oplus \nabla_{\text{in}} \oplus \nabla_{\text{in}} = \Delta_{\text{out}}.$$

If $X_3 \oplus X_4 = \Delta_{\text{out}}$, then $P_3 \oplus P_4 = \Delta_{\text{in}}$ holds with probability

$$\Pr[P_3 \oplus P_4 = \Delta_{\text{in}} \mid X_3 \oplus X_4 = \Delta_{\text{out}}] = \overleftarrow{p}.$$

Therefore, given that $P_1 \oplus P_2 = \Delta_{\text{in}}$, $C_1 \oplus C_3 = \nabla_{\text{out}}$ and $C_2 \oplus C_4 = \nabla_{\text{out}}$, the probability that $P_3 \oplus P_4 = \Delta_{\text{in}}$ is

$$\Pr[P_3 \oplus P_4 = \Delta_{\text{in}} \mid P_1 \oplus P_2 = \Delta_{\text{in}}] = \overrightarrow{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2.$$

If $\overrightarrow{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 > 2^{-n}$, then it can be used as a distinguisher.

2.4 Truncated Boomerang attack

In EUROCRYPT 2023, Bariant et al. replaced all differential trails in boomerang attaks by truncated differential trails to propose the truncated boomerang attacks [5]. The truncated boomerang attacks use structures on both plaintext and ciphertext sides, which can reduce the complexity effectively. The truncated boomerang attack consider two truncated differentials $\mathcal{D}^0_{\text{in}} \xrightarrow{E_0} \mathcal{D}^0_{\text{out}}$ and $\mathcal{D}^1_{\text{in}} \xrightarrow{E_1} \mathcal{D}^1_{\text{out}}$ with probabilities $\overrightarrow{p}, \overleftarrow{p}$ and $\overrightarrow{q}, \overleftarrow{q}$ on E_0 and E_1. The truncated boomerang attack proceeds as follows.

1. Choose a plaintext structure $P_0 \oplus \mathcal{D}^0_{\text{in}}$. For each $i \in \mathcal{D}^0_{\text{in}}$, we define $P_i = P_0 \oplus i$ and ask for the corresponding $C_i = E(P_i)$.
2. Generate cipher structures $C_i \oplus \mathcal{D}^1_{\text{out}}$ for each ciphertext C_i. For each $j \in \mathcal{D}^1_{\text{out}}$, we define $\bar{C_i}^j = C_i \oplus j$ and ask for the corresponding $\bar{P_i}^j = E^{-1}(\bar{C_i}^j)$.
3. Check if there exists a pair such that $\bar{P_i}^j \oplus \bar{P_i}^{j'} \in \mathcal{D}^0_{\text{in}}$.

Similarly to the boomerang attack,

$$\begin{aligned}
\Pr[X_1 \oplus X_2 \in \mathcal{D}^0_{\text{out}} \mid P_1 \oplus P_2 \in \mathcal{D}^0_{\text{in}}] &= \overrightarrow{p}, \\
\Pr[X_1 \oplus X_3 \in \mathcal{D}^1_{\text{in}} \mid C_1 \oplus C_3 \in \mathcal{D}^1_{\text{out}}] &= \overleftarrow{q}, \\
\Pr[X_2 \oplus X_4 \in \mathcal{D}^1_{\text{in}} \mid C_2 \oplus C_4 \in \mathcal{D}^1_{\text{out}}] &= \overleftarrow{q}.
\end{aligned}$$

However, like in sandwich attack analysis, there is a connection probability

$$r = \Pr[X_3 \oplus X_4 \in \mathcal{D}^0_{\text{out}} \mid (X_1 \oplus X_2 \in \mathcal{D}^0_{\text{out}}) \wedge (X_1 \oplus X_3 \in \mathcal{D}^1_{\text{in}}) \wedge (X_2 \oplus X_4 \in \mathcal{D}^1_{\text{in}})].$$

And again, similarly to the boomerang attack,

$$\Pr[P_3 \oplus P_4 \in \mathcal{D}^0_{\text{in}} \mid X_3 \oplus X_4 \in \mathcal{D}^0_{\text{out}}] = \overrightarrow{p}.$$

Therefore, the probability that a pair follows truncated boomerang trail is

$$\Pr[P_3 \oplus P_4 \in \mathcal{D}^0_{\text{in}} \mid P_1 \oplus P_2 \in \mathcal{D}^0_{\text{in}}] = \overrightarrow{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r.$$

2.5 Exchanged Boomerangs for 5-round AES

The authors of [16] and [39] utilized the exchange technique to construct a new boomerang attack on reduced-round AES. We call it as the exchanged

boomerang attack. The exchange boomerang attacks use truncated differential trails in the forward characteristic, and differential trail in the backward characteristic. Thus it can use structures on plaintext side, but can not use structures on ciphertext side.

We consider only 5-round AES and decompose it into two parts, $E_1 \circ E_0$, where

$$E_0 = SR \circ SB \circ AK \circ MC \circ SR \circ SB \circ AK \circ MC \circ SR \circ SB \circ AK$$

is the upper 2.5 rounds before MC of the third round, and

$$E_1 = AK \circ SR \circ SB \circ AK \circ MC \circ SR \circ SB \circ AK \circ MC$$

is the final 2 rounds. Let (P_1, P_2) be a pair of plaintexts and (C_1, C_2) be the corresponding pair of ciphertexts. The exchanged boomerang generates the new ciphertext pair (C_3, C_4) by exchanging the active inverse diagonal. For each inverse diagonal $1 \leq j \leq 4$, let the ciphertext pair generated by exchanging the j-th inverse diagonal be denoted as (C_3^j, C_4^j). Denote the intermediate value after E_0 as X. We decompose E_1 as $E_1 = E_{1,1} \circ E_{1,0}$, where

$$E_{1,0} = AK \circ MC$$

and

$$E_{1,1} = AK \circ SR \circ SB \circ AK \circ MC \circ SR \circ SB.$$

Denote the intermediate value after $E_{1,0}$ as Y.

(C_3^j, C_4^j) is obtained by exchanging the active inverse diagonal of (C_1, C_2), and since $E_{1,1}$ can be computed in 32-bit super box units, (Y_3^j, Y_4^j) is obtained by exchanging the active diagonal of (Y_1, Y_2). (Y_3^j, Y_4^j) is obtained by exchanging the active diagonal of (Y_1, Y_2), and since $E_{1,0} = AK \circ MC$, (X_3^j, X_4^j) and (X_1, X_2) have the same zero difference pattern with probability 1. It can be used to construct an efficient boomerang trail.

3 Fully active exchanged boomerang distinguisher

In this section, we propose the fully active exchanged boomerang distinguisher by increasing the probability that the diagonal of the returned plaintext pair (P_3^j, P_4^j) in the exchanged boomerang trail is either fully active or inactive in each diagonal, using friend pairs. As far as we know, this is the first time that a block cipher and a random permutation have been distinguished using fully active pairs. The fully active exchanged boomerang distinguisher for 5-round AES has a complexity of 2^{31} with a success probability of 70%. We first present the fully active exchanged boomerang distinguisher algorithm, followed by an analysis of the distinguisher's complexity and success probability. Then, we provide experimentally verified data and consider key recovery attack.

The idea of the fully active exchanged boomerang distinguisher is that if each column of returned pair has only one active byte after the first round MC, then

the plaintext pair must be fully active because the MC and MC^{-1} is an MDS matrix. The probability that a returned plaintext pair is fully active at random is very high, but we can reduce it using the friend pairs technique. Additionally, by using a backward trail with probability 1 in the exchanged boomerang trail, we ensure that all pairs obtained by exchanging the active inverse diagonal of a right pair's ciphertext pair remain right pairs, further reducing the random probability. We utilize these two techniques to reduce the random probability to be lower than the boomerang probability, thereby constructing the fully active boomerang distinguisher.

We introduce the fully active exchanged boomerang trail. For the upper part E_0, the input truncated difference $\mathcal{D}_{\text{in}}$ is active only in the 0th diagonal, the output truncated difference $\mathcal{D}_{\text{out}}$ is active only in one inverse diagonal, and the truncated difference for returned plaintext pairs $\mathcal{D}'_{\text{in}}$ is either inactive or all bytes of the diagonal are active for all diagonals. Since $\mathcal{D}_{\text{in}} \xrightarrow{E_0} \mathcal{D}_{\text{out}}$ is equivalent to the condition where only one byte is active after the first round MC, the probability of $\mathcal{D}_{\text{in}} \xrightarrow{E_0} \mathcal{D}_{\text{out}}$ is

$$\Pr[\mathcal{D}_{\text{in}} \xrightarrow{E_0} \mathcal{D}_{\text{out}}] = \overrightarrow{p} = 4 \cdot 2^{-24} = 2^{-22}.$$

$\mathcal{D}_{\text{out}} \xrightarrow{E_0^{-1}} \mathcal{D}'_{\text{in}}$ holds with probability

$$\Pr[\mathcal{D}_{\text{out}} \xrightarrow{E_0^{-1}} \mathcal{D}'_{\text{in}}] = \overleftarrow{p} = 1.$$

If there are no inactive bytes before the second round MC, there will be no inactive bytes (fully active) in the plaintext pair. If there are n inactive bytes before the second round MC, there will be n inactive diagonals in the plaintext pair.

For the lower part E_1, one of the inverse diagonals of (C_1, C_2) is exchanged to obtain ciphertext pairs (C_3^j, C_4^j) for $j \in \{1, 2, 3, 4\}$. Then, the probability that $X_3^j \oplus X_4^j \in \mathcal{D}_{\text{out}}$ is

$$\Pr[X_3^j \oplus X_4^j \in \mathcal{D}_{\text{out}}] = 1$$

by the exchange boomerang. Therefore, the probability of satisfying the fully active exchanged boomerang trail is 2^{-22}. The fully active exchanged boomerang trail can be seen in Figure 3. In the figure, white boxes represent inactive bytes, gray boxes represent active bytes, and hatched boxes represent exchanged bytes.

Since the probability of a single byte being active is $1 - 2^{-8}$, the probability of an entire diagonal being active is $(1 - 2^{-8})^4$. Since the probability of a diagonal being inactive is 2^{-32}, the probability that one returned plaintext pair is randomly either fully active or inactive in each diagonal is $((1 - 2^{-8})^4 + 2^{-32})^4$. Therefore, the probability that all four returned plaintext pairs are randomly either fully active or inactive in each diagonal is

$$(((1 - 2^{-8})^4 + 2^{-32})^4)^4 \approx 2^{-0.36}.$$

It is a very high probability for distinguishing using the fully active exchanged boomerang trail, so we reduce it by using friend pairs. For the right pair (P_1, P_2)

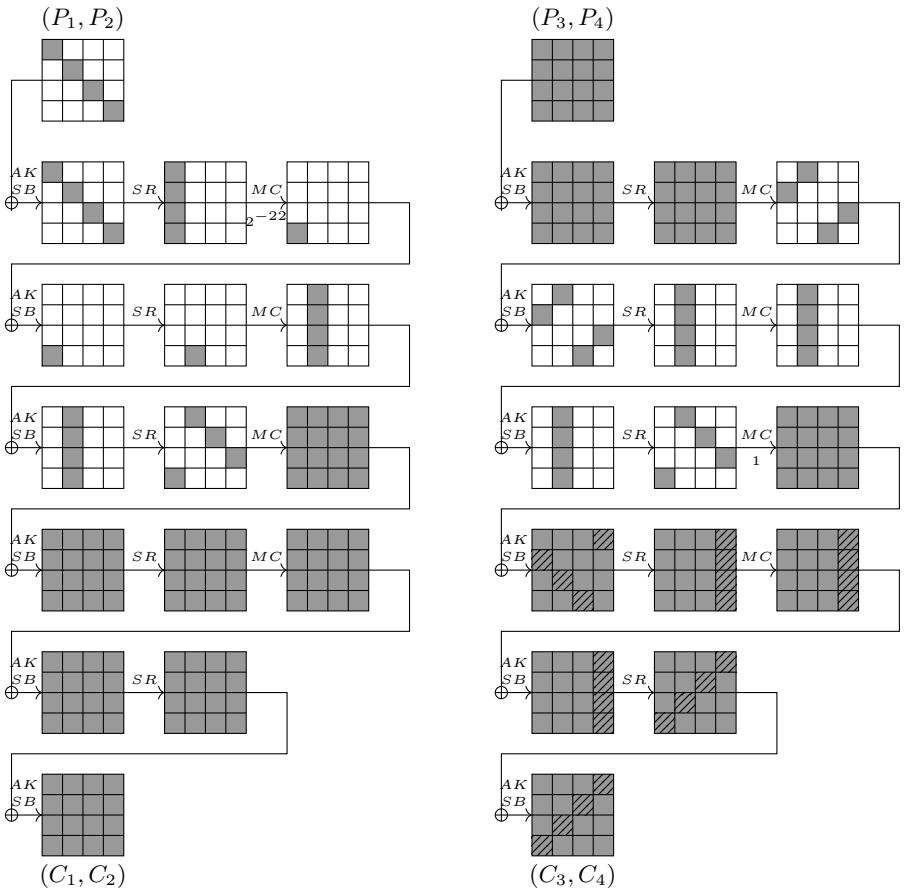

Fig. 3. Fully active exchanged boomerang trail

that follows the fully active exchanged boomerang trail, all friend pairs where the 0th diagonal is the same as (P_1, P_2) and the other diagonals use different constants compared to (P_1, P_2) are also right pairs that follow the fully active exchanged boomerang trail. Therefore, for any plaintext pair, the probability that the pair and all its friend pairs also satisfy the exchanged boomerang trail is still 2^{-22}. However, if we use 2^6 friend pairs, then the probability that all returned pairs of the pair and its 2^6 friend pairs are randomly either fully active or inactive in each diagonal is

$$((((1-2^{-8})^4+2^{-32})^4)^4)^{2^6} \approx 2^{-23.13} < 2^{-22}.$$

Therefore, since the fully active exchanged boomerang probability is bigger than the random probability, a distinguisher can be constructed.

We need 2^{22} plaintext pairs to obtain one right pair. Using a plaintext structure of size $2^{11.5}$, where only the 0th diagonal can take values and the remaining

bytes are any constants, we can obtain 2^{22} plaintext pairs. For all 2^{22} plaintext pairs, 2^6 friend pairs are generated for each. A right pair and all of its friend pairs follow the fully active exchanged boomerang trail with a probability of 1. On the other hand, all returned pairs of a wrong pair and its friend pairs are randomly either fully active or inactive in each diagonal with a probability of $2^{-23.13}$. Therefore, for all returned pairs of a pair and its friend pairs that are either fully active or inactive in each diagonal, on average,

$$1 + 2^{22} \cdot 2^{-23.13} = 1 + 2^{-1.13} \approx 1.46 > 1$$

such pairs exist for 5-round AES, while for a random permutation, on average,

$$2^{22} \cdot 2^{-23.13} = 2^{-1.13} \approx 0.46 < 1$$

such pairs exist. Therefore, if there exists a plaintext pair and its friend pair such that all generated returned plaintext pairs are either fully active or inactive in each diagonal, we output 5-round AES; otherwise, we output a random permutation. This allows us to distinguish 5-round AES from a random permutation. The fully active exchanged boomerang distinguisher for 5-round AES is as follows, and the pseudocode is given in Algorithm 1.

1. Choose a plaintext structure of size $2^{11.5}$ in which the four bytes in the 0th diagonal can take values and the remaining bytes are any constants.
2. For each plaintext pair (P_1, P_2), generate friend pairs (P_1', P_2') where the 0th diagonal is the same, but the constants are different and ask for the corresponding ciphertexts.
3. For each $j \in \{0, 1, 2, 3\}$, exchange the j-th active inverse diagonal of ciphertext pair (C_1, C_2) to obtain (C_3, C_4) and ask for the decryption of (C_3, C_4) to obtain (P_3, P_4).
4. If there exists one pair (P_1, P_2) such that all returned pair (P_3', P_4') of a pair and its friend pairs that are either inactive or have all bytes of the diagonal active for all diagonals, the distinguishing result is 5-round AES, otherwise it is a random permutation.

Complexity

In step 1, we need $2^{11.5}$ chosen plaintexts. In step 2, we generate $2^{22} \cdot 2^6 = 2^{28}$ plaintext pairs, so $2^{28} \cdot 2 = 2^{29}$ chosen plaintexts are required. In step 3, we generate $2^{28} \cdot 4 = 2^{30}$ ciphertext pairs, so $2^{30} \cdot 2 = 2^{31}$ adaptive chosen ciphertexts are required. Therefore, the data complexity of a distinguishing process is 2^{31} ACC, and the time complexity is 2^{31}.

Success Probability

The probability of the distinguisher succeeding is given by the average of the probability that the distinguisher outputs 5-round AES when the black box is

Algorithm 1 Fully active exchanged boomerang distinguisher for 5-round AES

1: Ask for the encryption of a plaintext structure of size $2^{11.5}$ in which the four bytes in the 0th diagonal can take values and the remaining bytes are any constants
2: **for** each plaintext pair **do**
3: Ask for the encryption of the pair and its 2^6 friend pairs, where the 0th diagonal is the same, and the other diagonals have different constants
4: **for** each ciphertext pair **do**
5: Exchange the j-th active inverse diagonal of (C_1, C_2) to obtain four pairs (C_3, C_4) for $j \in \{0, 1, 2, 3\}$
6: Ask for the decryption of four pairs (C_3, C_4) to obtain four pairs (P_3, P_4)
7: **end for**
8: **if** all returned pair are either inactive or have all bytes of the diagonal active for all diagonals **then**
9: **return** 5-round AES
10: **end if**
11: **end for**
12: **return** random permutation

a 5-round AES and the probability that the distinguisher outputs a random permutation when the black box is a random permutation. Each probability can be calculated using the Poisson distribution. When the black box is 5-round AES, it follows a Poisson distribution with $\lambda = 1.46$, and when the black box is a random permutation, it follows a Poisson distribution with $\lambda = 0.46$. The probability of having 1 or more occurrences in a Poisson distribution with $\lambda = 1.46$ is approximately

$$\Pr[X \geq 1] \approx 0.77$$

and for a Poisson distribution with $\lambda = 0.46$, the probability of 0 occurrences is approximately

$$\Pr[X = 0] \approx 0.63.$$

Therefore, the distinguisher succeeds with a probability of

$$\frac{0.77 + 0.63}{2} = 0.7$$

on average.

Experimental Verification

To verify the fully active exchanged boomerang distinguisher, we first count the number of pairs (P_1, P_2) such that all returned pairs (P_3', P_4') of the pair and its friend pairs are either inactive or have all bytes of the diagonal active for all diagonals. We conducted 100 experiments for each case and verified that, for 5-round AES, there is an average of 1.63 pairs, while for the random permutation (10-round AES), there is an average of 0.46 pairs, which is close to the theoretical expectation. The experimental results for this are shown in Table 2.

Table 2. Experimental results of the number of detected pairs in the fully active exchanged boomerang distinguisher for 5-round AES

Number of experiments	Blackbox Primitive	Experimental number of pairs	Theoretical number of pairs
100	5-round AES	1.63	1.46
100	Rand. Perm.	0.46	0.46

Additionally, to experimentally verify the success probability of the distinguisher, we counted the number of cases where the distinguisher outputs 5-round AES when the black box is 5-round AES, and the number of cases where the distinguisher outputs a random permutation when the black box is a random permutation. As in the previous experiment, we conducted 100 times each for 5-round AES and the random permutation (10-round AES). The results showed that when the black box was 5-round AES, the distinguisher outputted 5-round AES 74 times, and when the black box was a random permutation, the distinguisher outputted a random permutation 58 times. Therefore, the experimental success probability is $(0.74 + 0.58)/2 = 0.66$, which is similar to the theoretical probability. The experimental results for this are shown in Table 3.

Table 3. Experimental results of a success probability of the fully active exchanged boomerang distinguisher for 5-round AES

Number of experiments	Blackbox Primitive	Returned as 5-round AES	Returned as Rand. Perm.	Experimental Success Probability
100	5-round AES	74	26	$\frac{0.74+0.58}{2} = 0.66$
100	Rand. Perm.	42	58	

Key Recovery Attack

The fully active exchanged boomerang distinguisher can be directly used in the key recovery attacks for 5-round AES with the complexity of the distinguisher itself, which is higher than that of the retracing boomerang attack. The right pairs following the fully active exchanged boomerang trail have three inactive bytes in the column after first round of MC, allowing the filtering of the 0th round key. Since the returned pairs can also be used to filter the 0th round key, the 0th round key can be recovered by a single use of the distinguisher. Key guessing can be performed with negligible complexity compared to the complexity of the fully active exchanged boomerang distinguisher, using the meet-in-the-middle (MITM) technique [3] with a complexity of 2^{17}. Therefore, it requires a

complexity of 2^{31}, which is less efficient compared to the retracing boomerang attack using friendly exchanged boomerang trails for key recovery. The key recovery process is as follows.

1. Execute the distinguishing attack and obtain quartets (P_1, P_2, P_3^j, P_4^j) which follow the fully active exchanged boomerang, where (P_1, P_2) is active in the 0th diagonal and (P_3^j, P_4^j) is either fully active or inactive in each diagonal.
2. Guess and filter 0th round key according to the fact that the difference of (P_3^j, P_4^j) after first round MC are active at most one byte in each column. Since we have $4 \cdot 2^6 = 2^8$ pairs of (P_3^j, P_4^j), we can sufficiently filter the diagonal of the 0th round key by a factor of $2^{32} \cdot (2^{-22})^{2^8}$. Therefore, we can obtain the 0th round key.

4 Multiple exchanged boomerang distinguisher

In this section, we propose the multiple exchanged boomerang distinguisher by using multiple exchanged boomerang trails which have the same input truncated differences. The multiple exchanged boomerang distinguisher for 5-round AES has a complexity of $2^{27.08}$. This is, to the best of our knowledge, the best-known distinguisher for 5-round AES. We first present the multiple exchanged boomerang distinguisher algorithm, followed by an analysis of the distinguisher's complexity and success probability. Then, we provide experimentally verified data and consider key recovery attack.

The idea of the multiple exchanged boomerang distinguisher is to utilize multiple exchanged boomerangs that use the same input truncated differences, $\mathcal{D}_{\text{in}}$ and $\mathcal{D}'_{\text{in}}$. We have found four exchanged boomerang trails in total: three trails with probabilities better than the random probability and one trail with a probability equal to the random probability. We combine the four exchanged boomerang trails to significantly increase the boomerang probability.

We introduce the multiple exchanged boomerang trail. The multiple exchanged boomerang uses four exchanged boomerang trails which have the same D_{in} and D'_{in}. The input truncated difference $\mathcal{D}_{\text{in}}$ is active only in the 0th diagonal, same as in the fully active exchanged boomerang trail, and the truncated difference for returned plaintext pairs $\mathcal{D}'_{\text{in}}$ is inactive in one diagonal. We define the truncated differences D'_{in} for the four exchanged boomerang trails as $\mathcal{D}^1_{\text{out}}$, $\mathcal{D}^2_{\text{out}}$, $\mathcal{D}^3_{\text{out}}$, and $\mathcal{D}^4_{\text{out}}$.

The truncated difference $\mathcal{D}^1_{\text{out}}$ for the upper part E_0 of the first exchanged boomerang trail is active only in a one inverse diagonal. The probability of $\mathcal{D}_{\text{in}} \xrightarrow{E_0} \mathcal{D}^1_{\text{out}}$ is

$$\Pr[\mathcal{D}_{\text{in}} \xrightarrow{E_0} \mathcal{D}^1_{\text{out}}] = \overrightarrow{p} = 4 \cdot 2^{-24} = 2^{-22}$$

and the probability of $\mathcal{D}^1_{\text{out}} \xrightarrow{E_0^{-1}} \mathcal{D}_{\text{in}}$ is

$$\Pr[\mathcal{D}^1_{\text{out}} \xrightarrow{E_0^{-1}} \mathcal{D}_{\text{in}}] = \overleftarrow{p} = 2^{-8} \cdot 4 = 2^{-6}.$$

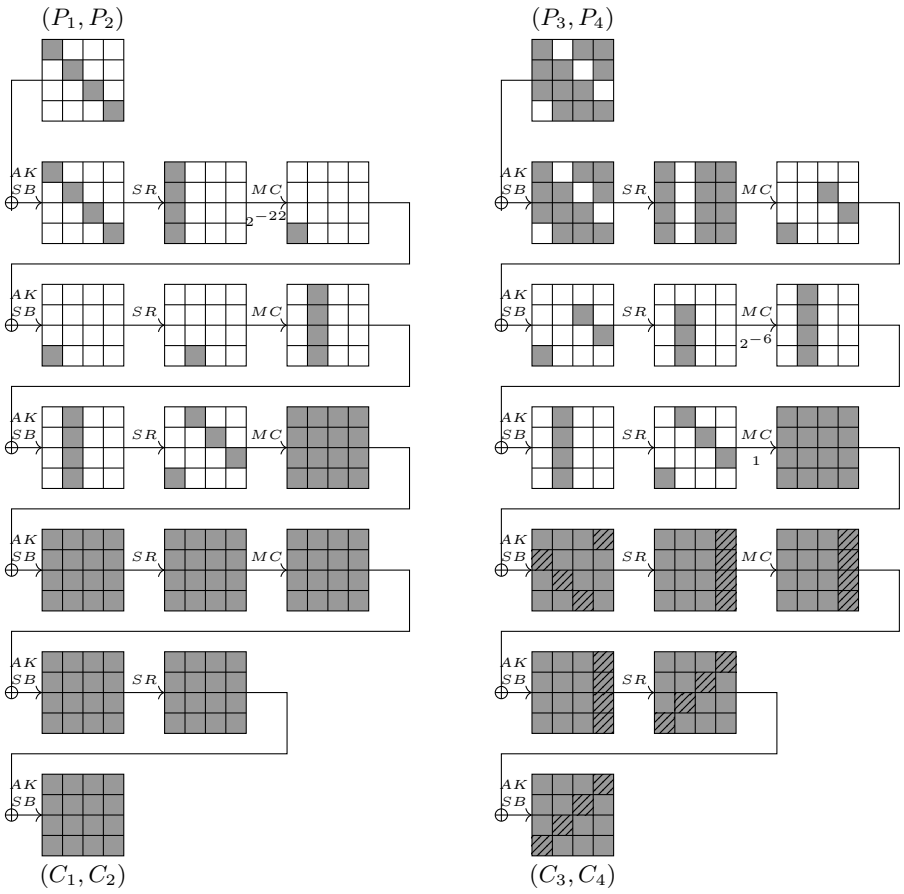

Fig. 4. First exchanged boomerang trail

Therefore, the probability of the first exchanged boomerang trail is

$$\overrightarrow{p} \cdot \overleftarrow{p} = 2^{-22} \cdot 2^{-6} = 2^{-28}.$$

The first trail can be seen in Figure 4.

The truncated difference $\mathcal{D}^2_{\text{out}}$ for the upper part E_0 of the second exchanged boomerang trail is active in two inverse diagonals. The probability of $\mathcal{D}_{\text{in}} \xrightarrow{E_0} \mathcal{D}^2_{\text{out}}$ is

$$\Pr[\mathcal{D}_{\text{in}} \xrightarrow{E_0} \mathcal{D}^2_{\text{out}}] = \overrightarrow{p} = 6 \cdot 2^{-16} = 2^{-13.4}$$

and the probability of $\mathcal{D}^2_{\text{out}} \xrightarrow{E_0^{-1}} \mathcal{D}_{\text{in}}$ is

$$\Pr[\mathcal{D}^2_{\text{out}} \xrightarrow{E_0^{-1}} \mathcal{D}_{\text{in}}] = \overleftarrow{p} = 4 \cdot 2^{-16} = 2^{-14}.$$

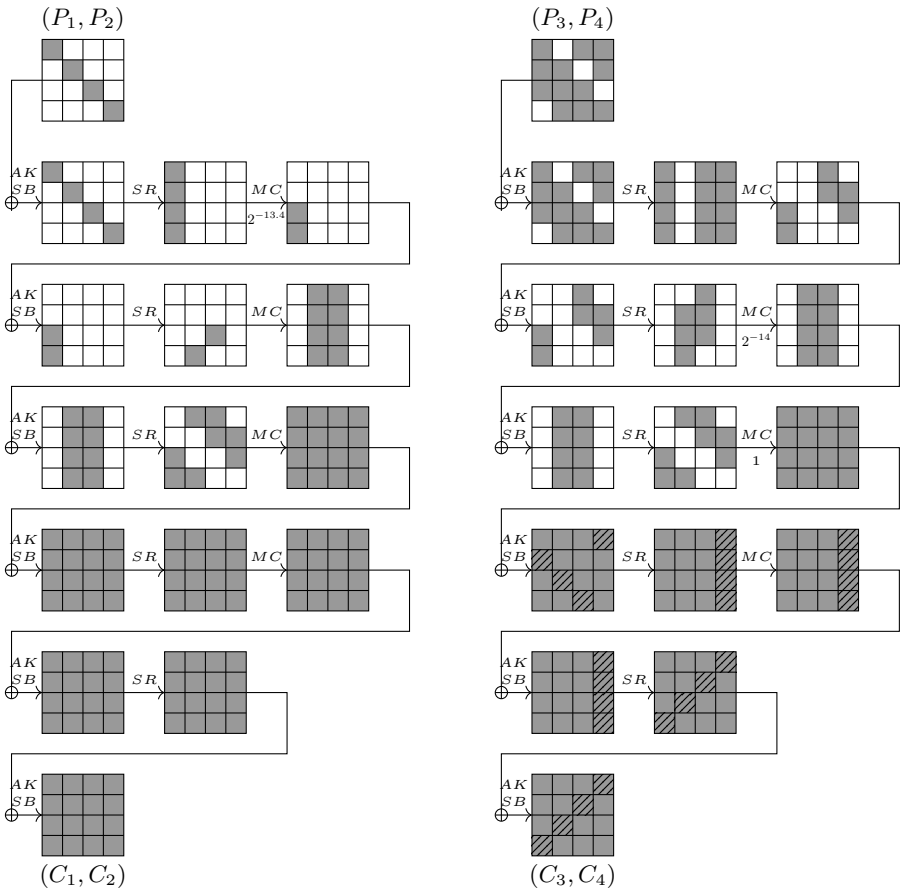

Fig. 5. Second exchanged boomerang trail

Therefore, the probability of the second exchanged boomerang trail is

$$\overrightarrow{p} \cdot \overleftarrow{p} = 2^{-13.4} \cdot 2^{-14} = 2^{-27.4}.$$

The second trail can be seen in Figure 5.

The truncated difference $\mathcal{D}^3_{\text{out}}$ for the upper part E_0 of the third exchanged boomerang trail is active in three inverse diagonals. The probability of $\mathcal{D}_{\text{in}} \xrightarrow{E_0} \mathcal{D}^3_{\text{out}}$ is

$$\Pr[\mathcal{D}_{\text{in}} \xrightarrow{E_0} \mathcal{D}^3_{\text{out}}] = \overrightarrow{p} = 4 \cdot 2^{-8} = 2^{-6}$$

and the probability of $\mathcal{D}^3_{\text{out}} \xrightarrow{E_0^{-1}} \mathcal{D}_{\text{in}}$ is

$$\Pr[\mathcal{D}^3_{\text{out}} \xrightarrow{E_0^{-1}} \mathcal{D}_{\text{in}}] = \overleftarrow{p} = 4 \cdot 2^{-24} = 2^{-22}.$$

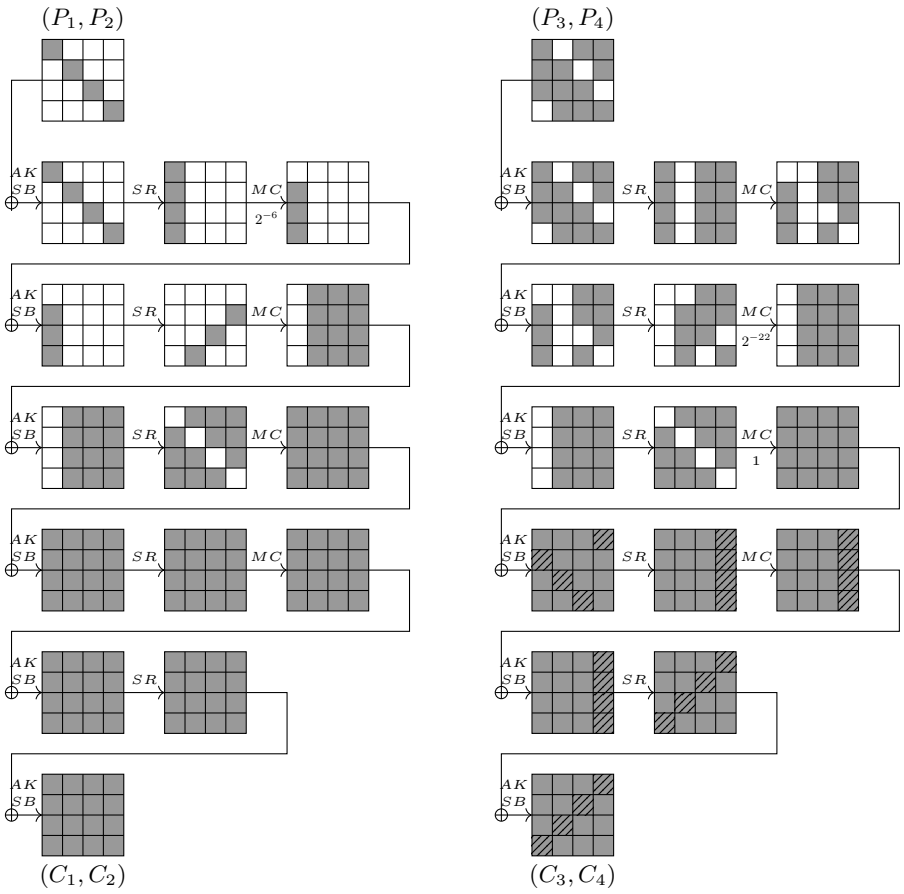

Fig. 6. Third exchanged boomerang trail

Therefore, the probability of the third exchanged boomerang trail is

$$\overrightarrow{p} \cdot \overleftarrow{p} = 2^{-6} \cdot 2^{-22} = 2^{-28}.$$

The third trail can be seen in Figure 6.

The truncated difference $\mathcal{D}^4_{\text{out}}$ for the upper part E_0 of the fourth exchanged boomerang trail is active in four inverse diagonals. The probability of $\mathcal{D}_{\text{in}} \xrightarrow{E_0} \mathcal{D}^4_{\text{out}}$ is

$$\Pr[\mathcal{D}_{\text{in}} \xrightarrow{E_0} \mathcal{D}^4_{\text{out}}] = \overrightarrow{p} = 1$$

and the probability of $\mathcal{D}^4_{\text{out}} \xrightarrow{E_0^{-1}} \mathcal{D}_{\text{in}}$ is

$$\Pr[\mathcal{D}^4_{\text{out}} \xrightarrow{E_0^{-1}} \mathcal{D}_{\text{in}}] = \overleftarrow{p} = 4 \cdot 2^{-32} = 2^{-30}.$$

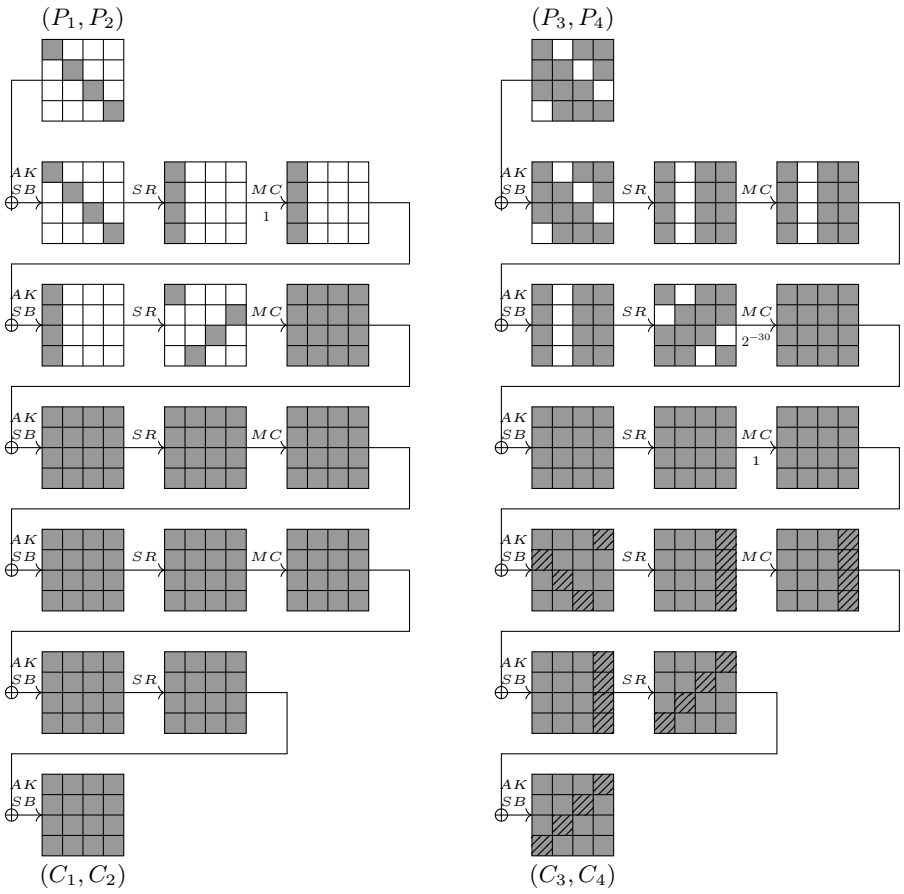

Fig. 7. Fourth exchanged boomerang trail

Therefore, the probability of the third exchanged boomerang trail is

$$\overrightarrow{p} \cdot \overleftarrow{p} = 1 \cdot 2^{-30} = 2^{-30}.$$

The fourth trail can be seen in Figure 7.

By combining four exchanged boomerang trails with the same D_{in} and D'_{in}, the probability of the multiple exchanged boomerang is

$$2^{-28} + 2^{-27.4} + 2^{-28} + 2^{-30} = 2^{-26.08}.$$

The probability that the returned plaintext pair is randomly inactive in one diagonal is $4 \cdot 2^{-32} = 2^{-30}$. Therefore, since the multiple exchanged boomerang probability is better than the random probability, a distinguisher can be constructed.

We need $2^{26.08}$ pairs to obtain one right pair. Since we can generate four additional ciphertext pairs by exchanging the active inverse diagonal in the ciphertext pairs, $2^{24.08}$ plaintext pairs are required. Using a plaintext structure of size $2^{12.58}$, where only the 0th diagonal can take values and the remaining bytes are any constants, we can obtain $2^{24.08}$ plaintext pairs. A right pair satisfy the multiple exchanged boomerang with a probability of 1. On the other hand, a wrong returned pair is randomly inactive in one diagonal with a probability of 2^{-30}. Therefore, for returned pair that is inactive in one diagonal, on average,

$$1 + 2^{-26.08} \cdot 2^{30} = 1 + 2^{-3.92} \approx 1.066 > 1$$

such pairs exist for 5-round AES, while for a random permutation, on average,

$$2^{-26.08} \cdot 2^{30} = 2^{-3.92} \approx 0.066 < 1$$

such pairs exist. Therefore, if there exists a plaintext pair such that returned plaintext pair is inactive in one diagonal, we output 5-round AES; otherwise, we output a random permutation. This allows us to distinguish 5-round AES from a random permutation. The multiple exchanged boomerang distinguisher for 5-round AES is as follows, and the pseudocode is given in Algorithm 2.

1. Choose a plaintext structure of size $2^{12.58}$ in which the four bytes in the 0th diagonal can take values and the remaining bytes are any constants, and ask for the corresponding ciphertexts.
2. For each $j \in \{0, 1, 2, 3\}$, exchange the j-th active inverse diagonal of ciphertext pair (C_1, C_2) to obtain (C_3, C_4) and ask for the decryption of (C_3, C_4) to obtain (P_3, P_4).
3. If there exist a pair (P_3, P_4) that is inactive in one diagoal, the distinguishing result is 5-round AES, otherwise it is a random permutation.

Algorithm 2 Multiple exchanged boomerang distinguisher for 5-round AES

Ask for the encryption of a plaintext structure of size $2^{12.58}$ in which the four bytes in the 0th diagonal can take values and the remaining bytes are any constants
for each ciphertext pair **do**
    Exchange the $j - th$ active inverse diagonal of (C_1, C_2) to obtain four pairs (C_3, C_4) for $j \in \{0, 1, 2, 3\}$
    Ask for the decryption of four pairs (C_3, C_4) to obtain four pairs (P_3, P_4)
    if returned pair is inactive in one diagonal **then**
        return 5-round AES
    end if
end for
return random permutation

Complexity

In step 1, we need $2^{12.58}$ chosen plaintexts. In step 2, we generate $2^{24.08} \cdot 4 = 2^{26.08}$ ciphertext pairs, so $2^{26.08} \cdot 2 = 2^{27.08}$ adaptive chosen ciphertexts are required. Therefore, the data complexity of a distinguishing process is $2^{27.08}$ ACC, and the time complexity is $2^{27.08}$.

Success Probability

The probability of the distinguisher succeeding is given by the average of the probability that the distinguisher outputs 5-round AES when the black box is a 5-round AES and the probability that the distinguisher outputs a random permutation when the black box is a random permutation. Each probability can be calculated using the Poisson distribution. When the black box is 5-round AES, it follows a Poisson distribution with $\lambda = 1.066$, and when the black box is a random permutation, it follows a Poisson distribution with $\lambda = 0.066$. The probability of having 1 or more occurrences in a Poisson distribution with $\lambda = 1.066$ is approximately

$$\Pr[X \geq 1] \approx 0.713$$

and for a Poisson distribution with $\lambda = 0.066$, the probability of 0 occurrences is approximately

$$\Pr[X = 0] \approx 0.936.$$

Therefore, the distinguisher succeeds with a probability of

$$\frac{0.713 + 0.936}{2} = 0.8245$$

on average.

Experimental Verification

To verify the multiple exchanged boomerang distinguisher, we first count the number of returned pairs (P_3, P_4) that are inactive in one diagonal. We conducted 100 experiments for each case and verified that, for 5-round AES, there is an average of 1.12 pairs, while for the random permutation (10-round AES), there is an average of 0.08 pairs, which is close to the theoretical expectation. The experimental results for this are shown in Table 4.

Additionally, to experimentally verify the success probability of the distinguisher, we counted the number of cases where the distinguisher outputs 5-round AES when the black box is 5-round AES, and the number of cases where the distinguisher outputs a random permutation when the black box is a random permutation. As in the previous experiment, we conducted 100 times each for 5-round AES and the random permutation (10-round AES). The results showed that when the black box was 5-round AES, the distinguisher outputted 5-round AES 57 times, and when the black box was a random permutation, the distinguisher outputted a random permutation 91 times. Therefore, the experimental success probability is $(0.57 + 0.91)/2 = 0.74$, which is similar to the theoretical probability. The experimental results for this are shown in Table 5.

Table 4. Experimental results of the number of detected pairs in the multiple exchanged boomerang distinguisher for 5-round AES

Number of experiments	Blackbox Primitive	Experimental number of pairs	Theoretical number of pairs
100	5-round AES	1.12	1.066
100	Rand. Perm.	0.08	0.066

Table 5. Experimental results of a success probability of the multiple exchanged boomerang distinguisher for 5-round AES

Number of experiments	Blackbox Primitive	Returned as 5-round AES	Returned as Rand. Perm.	Experimental Success Probability
100	5-round AES	57	43	$\frac{0.57+0.91}{2} = 0.74$
100	Rand. Perm.	9	91	

Key Recovery Attack

Similar to the fully active exchanged boomerang distinguisher, the multiple exchanged boomerang distinguisher can be directly used in key recovery attacks for 5-round AES with the complexity of the distinguisher itself, which is higher than that of the retracing boomerang attack. Among the four exchanged boomerang trails used in the multiple exchanged boomerang distinguisher, the three trails with the highest probabilities have inactive bytes after the first round MC. Therefore, by leveraging the fact that the right pair has at least one inactive byte with high probability after the first round MC, the 0th round key can be filtered. The returned pairs of a right pair all have the same zero difference pattern as the right pair after the first round MC. Therefore, using a total of five pairs, we can filter one diagonal from the input plaintext pair and three diagonals from the four returned plaintext pairs by a factor of 2^{-6}. Therefore, by performing the distinguisher twice to obtain two right pairs, the 0th round key can be sufficiently filtered. Key guessing also can be performed with negligible complexity compared to the complexity of the multiple exchanged boomerang distinguisher, using the meet-in-the-middle (MITM) technique [3] with a complexity of 2^{17}. Therefore, it requires a complexity of $2 \cdot 2^{27.08} = 2^{28.08}$, which is less efficient compared to the retracing boomerang attack using friendly exchanged boomerang trails for key recovery. The key recovery process is as follows.

1. Execute the distinguishing attack and obtain quartets (P_1, P_2, P_3^j, P_4^j) which follow the fully active exchanged boomerang, where (P_1, P_2) is active in the 0th diagonal and (P_3^j, P_4^j) is inactive in one diagonal.
2. Guess and filter 0th round key according to the fact that the differences of (P_1, P_2) and (P_3^j, P_4^j) after first round MC are inactive at least one byte in

each column. In a single execution of the distinguisher, the key is filtered by a factor of $(2^{-6})^{1+3\cdot 4} = 2^{-78}$.
3. Repeat the above two steps once more to sufficiently filter the 0th round key.
4. We can sufficiently filter the 0th round key by a factor of $2^{128} \cdot (2^{-78})^2$. Therefore, we can obtain the 0th round key.

5 Conclusion

In this paper, we proposed the fully active exchanged boomerang and multiple exchanged boomerang distinguishers for 5-round AES by utilizing the friend pairs technique and multiple trails. The fully active exchanged boomerang distinguisher for 5-round AES has the data and time complexities 2^{31} and success probability 70%. The multiple exchanged boomerang distinguisher for 5-round AES has the data and time complexities $2^{27.08}$ and success probability 82%. To the best of our knowledge, this is the best-known distinguisher for 5-round AES. The fully active exchanged boomerang and multiple exchanged boomerang distinguishers can also be applied to other AES-like block ciphers. In the fully active exchanged boomerang distinguisher, distinguishing by checking whether the diagonal is inactive or if all bytes of the diagonal are active could be considered for future research, potentially combined with other cryptanalysis techniques.

References

1. Banik, S. et al.: Midori: A Block Cipher for Low Energy. In: Iwata, T., Cheon, J. (eds) Advances in Cryptology – ASIACRYPT 2015. ASIACRYPT 2015. Lecture Notes in Computer Science(), vol 9453. Springer, Berlin, Heidelberg. (2015). https://doi.org/10.1007/978-3-662-48800-3_17
2. Bao, Z., Guo, C., Guo, J., Song, L.: TNT: How to tweak a block cipher. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology– EUROCRYPT 2020, Part II. Lecture Notes in Computer Science, vol. 12106, pp. 641–673. Springer, Heidelberg, Germany, Zagreb, Croatia (May 10–14, 2020). https://doi.org/10.1007/978-3-030-45724-2_22
3. Bar-On, A., Dunkelman, O., Keller, N., Ronen, E., Shamir, A.: Improved key recovery attacks on reduced-round AES with practical data and memory complexities. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology– CRYPTO 2018, Part II. Lecture Notes in Computer Science, vol. 10992, pp. 185–212. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 19–23, 2018). https://doi.org/10.1007/978-3-319-96881-0_7
4. Bardeh, N.G., Rønjom, S.: The exchange attack: How to distinguish six rounds of AES with 288.2 chosen plaintexts. In: Galbraith, S.D., Moriai, S. (eds.) Advances in Cryptology– ASIACRYPT 2019, Part III. Lecture Notes in Computer Science, vol. 11923, pp. 347–370. Springer, Heidelberg, Germany, Kobe, Japan (Dec 8–12, 2019). https://doi.org/10.1007/978-3-030-34618-8_12
5. Bariant, A., Leurent, G.: Truncated boomerang attacks and application to AES based ciphers. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology– EUROCRYPT 2023, Part IV. Lecture Notes in Computer Science, vol. 14007, pp. 3–35. Springer, Heidelberg, Germany, Lyon, France (Apr 23–27, 2023). https://doi.org/10.1007/978-3-031-30634-1_1

6. Beierle, C. et al.: The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS . In: Robshaw, M., Katz, J. (eds) Advances in Cryptology – CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science(), vol 9815. Springer, Berlin, Heidelberg. (2016). https://doi.org/10.1007/978-3-662-53008-5_5
7. Beierle, C., Leander, G., Todo, Y.: Improved differential-linear attacks with applications to ARX ciphers. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology– CRYPTO 2020, Part III. Lecture Notes in Computer Science, vol. 12172, pp. 329–358. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 17–21, 2020). https://doi.org/10.1007/978-3-030-56877-1_12
8. Biham, E., Dunkelman, O., Keller, N.: The Rectangle Attack — Rectangling the Serpent. In: Pfitzmann, B. (eds) Advances in Cryptology — EUROCRYPT 2001. EUROCRYPT 2001. Lecture Notes in Computer Science, vol 2045. Springer, Berlin, Heidelberg. (2001). https://doi.org/10.1007/3-540-44987-6_21
9. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. In: Menezes, A.J., Vanstone, S.A. (eds.) Advances in Cryptology– CRYPTO'90. Lecture Notes in Computer Science, vol. 537, pp. 2–21. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 11–15, 1991). https://doi.org/10.1007/3540-38424-3_1
10. Cho, J., Choi, K.Y., Dinur, I., Dunkelman, O., Keller, N., Moon, D., Veidberg, A.: WEM: A new family of white-box block ciphers based on the Even-Mansour construction. In: Handschuh, H. (ed.) Topics in Cryptology– CT-RSA 2017. Lecture Notes in Computer Science, vol. 10159, pp. 293–308. Springer, Heidelberg, Germany, San Francisco, CA, USA (Feb 14–17, 2017). https://doi.org/10.1007/978-3319-52153-4_17
11. Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: Boomerang connectivity table: A new cryptanalysis tool. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology– EUROCRYPT 2018, Part II. Lecture Notes in Computer Science, vol. 10821, pp. 683–714. Springer, Heidelberg, Germany, Tel Aviv, Israel (Apr 29 May 3, 2018). https://doi.org/10.1007/978-3-319-78375-8_22
12. Daemen, J., Rijmen, V.: The Design of Rijndael: AES- The Advanced Encryption Standard. Information Security and Cryptography, Springer, Heidelberg, Germany (2002). https://doi.org/10.1007/978-3-662-04722-4
13. Delaune, S., Derbez, P., Vavrille, M.: Catching the fastest boomerangs application to SKINNY. IACR Transactions on Symmetric Cryptology 2020(4), 104–129 (2020). https://doi.org/10.46586/tosc.v2020.i4.104-129
14. Derbez, P., Fouque, P.A., Jean, J.: Improved key recovery attacks on reduced-round AES in the single-key setting. In: Johansson, T., Nguyen, P.Q. (eds.) Advances in Cryptology– EUROCRYPT 2013. Lecture Notes in Computer Science, vol. 7881, pp. 371–387. Springer, Heidelberg, Germany, Athens, Greece (May 26–30, 2013). https://doi.org/10.1007/978-3-642-38348-9_23
15. Dunkelman, O., Keller, N., Shamir, A.: A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. Journal of Cryptology 27(4), 824–849 (Oct 2014). https://doi.org/10.1007/s00145-013-9154-9
16. Dunkelman, O., Keller, N., Ronen, E., Shamir, A.: The retracing boomerang attack. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology– EUROCRYPT 2020, Part I. Lecture Notes in Computer Science, vol. 12105, pp. 280–309. Springer, Heidelberg, Germany, Zagreb, Croatia (May 10–14, 2020). https://doi.org/10.1007/978-3-030-45721-1_11

17. Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D., Whiting, D.: Improved cryptanalysis of Rijndael. In: Schneier, B. (ed.) Fast Software Encryption– FSE 2000. Lecture Notes in Computer Science, vol. 1978, pp. 213–230. Springer, Heidelberg, Germany, New York, NY, USA (Apr 10–12, 2001). https://doi.org/10.1007/3-540-44706-7_15
18. Fouque, P.A., Karpman, P., Kirchner, P., Minaud, B.: Efficient and provable white box primitives. In: Cheon, J.H., Takagi, T. (eds.) Advances in Cryptology– ASIACRYPT2016, PartI.Lecture Notes in Computer Science, vol. 10031, pp. 159–188. Springer, Heidelberg, Germany, Hanoi, Vietnam (Dec 4–8, 2016). https://doi.org/10.1007/978-3-662-53887-6_6
19. Grassi, L.: Mixture differential cryptanalysis: a new approach to distinguishers and attacks on round-reduced AES. IACR Transactions on Symmetric Cryptology 2018(2), 133–160 (2018). https://doi.org/10.13154/tosc.v2018.i2.133-160
20. Grassi, L., Rechberger, C., Rønjom, S.: A new structural-differential property of 5-round AES. In: Coron, J.S., Nielsen, J.B. (eds.) Advances in Cryptology– EUROCRYPT2017, Part II. Lecture Notes in Computer Science, vol. 10211, pp. 289–317. Springer, Heidelberg, Germany, Paris, France (Apr 30– May 4, 2017). https://doi.org/10.1007/978-3-319-56614-6_10
21. Grassi, L., Rechberger, C., Rønjom, S.: Subspace trail cryptanalysis and its applications to AES. IACR Transactions on Symmetric Cryptology 2016(2), 192 225 (2016). https://doi.org/10.13154/tosc.v2016.i2.192-225
22. Hu, K., Cui, T., Gao, C., Wang, M.: Towards key-dependent integral and impos sible differential distinguishers on 5-round AES. In: Cid, C., Jacobson Jr:, M.J. (eds.) SAC 2018: 25th Annual International Workshop on Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 11349, pp. 139–162. Springer, Heidelberg, Germany, Calgary, AB, Canada (Aug 15–17, 2019). https://doi.org/10.1007/978-3-030-10970-7_7
23. Jean, J., Nikolić, I., Peyrin, T.: KIASU v1. Submitted to the CAESAR competition (2014). http://competitions.cr.yp.to/round1/kiasuv1.pdf
24. Jean, J., Nikolić, I., Peyrin, T. et al. The Deoxys AEAD Family. J Cryptol 34, 31 (2021). https://doi.org/10.1007/s00145-021-09397-w
25. Kelsey, J., Kohno, T., Schneier, B.: Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent. In: Goos, G., Hartmanis, J., van Leeuwen, J., Schneier, B. (eds) Fast Software Encryption. FSE 2000. Lecture Notes in Computer Science, vol 1978. Springer, Berlin, Heidelberg. (2001). https://doi.org/10.1007/3-540-44706-7_6
26. Knudsen, L.: Deal-a 128-bit block cipher. complexity 258(2), 216 (1998)
27. Knudsen, L.R.: Truncated and higher order differentials. In: Preneel, B. (ed.) Fast Software Encryption– FSE'94. Lecture Notes in Computer Science, vol. 1008, pp. 196–211. Springer, Heidelberg, Germany, Leuven, Belgium (Dec 14–16, 1995). https://doi.org/10.1007/3-540-60590-816
28. Langford, S.K., Hellman, M.E.: Differential-linear cryptanalysis. In: Advances in Cryptology—CRYPTO'94: 14th Annual International Cryptology Conference Santa Barbara, California, USA August 21–25, 1994 Proceedings 14, pp. 17–25 (1994). Springer. https://doi.org/10.1007/3-540-48658-5_3
29. Leurent, G., Pernot, C.: New representations of the AES key schedule. In: Can teaut, A., Standaert, F.X. (eds.) Advances in Cryptology– EUROCRYPT 2021, Part I. Lecture Notes in Computer Science, vol. 12696, pp. 54–84. Springer, Heidelberg, Germany, Zagreb, Croatia (Oct 17–21, 2021). https://doi.org/10.1007/9783-030-77870-5_3

30. Matsui, M.: Linear cryptanalysis method for des cipher. In: Workshop on the Theory and Application of of Cryptographic Techniques, pp. 386–397 (1993). Springer. https://doi.org/10.1007/3-540-48285-7_33
31. Mondal, S.K., Rahman, M., Sarkar, S., Adhikari, A.: Revisiting yoyo tricks on AES. IACR Transactions on Symmetric Cryptology 2023(4), 28–57 (2023). https://doi.org/10.46586/tosc.v2023.i4.28-57
32. Murphy, S.: The return of the cryptographic boomerang. IEEE Transactions on Information Theory 57(4), 2517–2521 (2011). https://doi.org/10.1109/TIT.2011.2111091
33. Rønjom, S., Bardeh, N.G., Helleseth, T.: Yoyo tricks with AES. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology– ASIACRYPT 2017, Part I. Lec ture Notes in Computer Science, vol. 10624, pp. 217–243. Springer, Heidelberg, Germany, Hong Kong, China (Dec 3–7, 2017). https://doi.org/10.1007/978-3-31970694-8_8
34. Shin, H. et al.: Revisiting The Multiple-of Property for SKINNY: The Exact Computation of the number of right pairs. IEEE Access (2024). https://doi.org/10.1109/ACCESS.2024.3371712
35. Song, L., Qin, X., Hu, L.: Boomerang connectivity table revisited. IACR Transactions on Symmetric Cryptology 2019(1), 118–141 (2019). https://doi.org/10.13154/tosc.v2019.i1.118-141
36. Sun, B., Liu, M., Guo, J., Qu, L., Rijmen, V.: New insights on AES-like SPN ciphers. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology– CRYPTO 2016, Part I. Lecture Notes in Computer Science, vol. 9814, pp. 605–624. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 14–18, 2016). https://doi.org/10.1007/978-3-662-53018-4_22
37. Wagner, D.: The boomerang attack. In: Knudsen, L.R. (ed.) Fast Software Encryption– FSE'99. Lecture Notes in Computer Science, vol. 1636, pp. 156–170. Springer, Heidelberg, Germany, Rome, Italy (Mar 24–26, 1999). https://doi.org/10.1007/3-540-48519-8_12
38. Wang, H., Peyrin, T.: Boomerang switch in multiple rounds. IACR Transactions on Symmetric Cryptology 2019(1), 142–169 (2019). https://doi.org/10.13154/tosc.v2019.i1.142-169
39. Yan, X., Tan, L., Xu, H., Qi, W.: The Boomerang Chain Distinguishers: New Record for 6-Round AES. In: Chung, KM., Sasaki, Y. (eds) Advances in Cryptology – ASIACRYPT 2024. ASIACRYPT 2024. Lecture Notes in Computer Science, vol 15490. Springer, Singapore (2025). https://doi.org/10.1007/978-981-96-0941-3_10
40. Yang, Q., Song, L., Sun, S., Shi, D., Hu, L.: New properties of the double boomerang connectivity table. IACR Transactions on Symmetric Cryptology 2022(4), 208–242 (2022). https://doi.org/10.46586/tosc.v2022.i4.208-242