New Exchanged Boomerang Distinguishers for 5-Round AES

Hanbeom Shin[1], Seonkyu Kim[1], Byoungjin Seok[2], Dongjae Lee[3], Deukjo Hong[4], Jaechul Sung[5] and Seokhie Hong[1]

[1] Korea University, Seoul, South Korea, {newonetiger,kimsg125,shhong}@korea.ac.kr
[2] Hansung University, Seoul, South Korea, bjseok@hansung.kr
[3] Kangwon National University, Chuncheon, South Korea, dongjae.lee@kangwon.ac.kr
[4] Jeonbuk National University, Jeonju, South Korea, deukjo.hong@jbnu.ac.kr
[5] University of Seoul, 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; therefore the existence of a distinguisher is 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 massive exchanged boomerang and multiple exchanged boomerang distinguishers for 5-round AES. The massive exchanged boomerang distinguisher utilizes the probability that the truncated difference for the returned plaintext pairs is such that, in each of its diagonals, the 4 bytes are either all active, or all inactive. Although this probability is very high for a random permutation, we significantly reduce it using the friend pairs technique, while keeping the boomerang probability unchanged. This enables us to distinguish a block cipher from a random permutation. The massive exchanged boomerang distinguisher for 5-round AES has a data and time complexity of 2^{31} with a success probability of 70%. The multiple exchanged boomerang distinguisher is constructed by clustering four trails that have the same input and output truncated differences, enabling it to distinguish a block cipher from a random permutation with lower complexity and higher success probability. The multiple exchanged boomerang distinguisher for 5-round AES has a data and time complexity of $2^{27.1}$ and a success probability of 79.6%, which represents a new best-known result for the secret-key distinguisher on 5-round AES.

Keywords: AES · Distinguisher · Boomerang · Exchanged Boomerang · Yoyo

1 Introduction

A block cipher is a cryptographic algorithm that encrypts data in fixed-size units using a secret key. A block cipher 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. Then designer determines the appropriate number of rounds by adding margin rounds.

The security of a block cipher 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) [BS91] and linear cryptanalysis (LC) [Mat94]. 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 [Knu95], impossible differential cryptanalysis [Knu98], high-order differentials [Knu95], boomerang attacks [Wag99], differential-linear attacks [LH94], integral [FKL+01], meet-in-the-middle [DFJ13] and others. Most recently, variations of DC have been proposed, such as the subspace trail [GRR16], the yoyo trick [RBH17, MRSA23], the multiple-of-8 property [GRR17], mixture-differential cryptanalysis [Gra18, BDK+18], the exchange attacks [BR19], and the fixed property [SKK+23].

In particular, we focus on the boomerang attack [Wag99] 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 [KKS01] and the rectangle attacks [BDK01], 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 [DKS10]. Murphy showed that some boomerang characteristics were in fact impossible [Mur11]. Cid et al. used the boomerang connectivity table (BCT) [CHP+18] to analyze the case where the middle round is a single s-box layer. In [DDV20, SQH19, WP19], researchers studied the case where the middle round is composed of several rounds. Yang et al. introduced the double boomerang connectivity table (DBCT) [YSS+22] and showed that the relation between neighboring rounds cannot be ignored. The truncated boomerang attack which utilizes truncated differentials with boomerang is presented in EUROCRYPT 2023 [BL23]. The exchanged boomerang attack is an attack that utilizes the mixing technique (exchange property [BR19]) from the retracing boomerang attack [DKRS20, BDK+24], and it has also been utilized in the re-boomerang and boomerang chain distinguishers [YTXQ24].

The Advanced Encryption Standard (AES) [AES01] is the most widely used block cipher and has demonstrated its security over the past 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 [BJK+16] and MIDORI [BBI+15]. Additionally, many tweakable block ciphers, like KIASU-BC [JNP14] and DEOXYS-BC [JNPS21], reuse the round function of AES in their designs and some block cipher use reduced-round AES as a core component, such as Hound [FKKM16] and WEM [CCD+17], which use 5-round AES, and TNT-AES [BGGS20], which uses 6-round AES. Therefore, analyzing reduced-round variants of AES is particularly important.

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 [GRR17]. In [RBH17], 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 [RBH17], and it was recomputed in [MRSA23]. In ASIACRYPT 2019, Bardeh et al. presented 5-round and 6-round distinguishers, known as exchange attacks [BR19]. The current secret-key distinguishers for 5- and 6-round AES are shown in Table 1.

Our Contributions

In this work, we propose two new distinguishers for 5-round AES based on the exchanged boomerang technique. The first is the massive exchanged boomerang distinguisher, which uses the probability that the truncated difference of the returned plaintext pair is such that, in each of its diagonals, the four bytes are either all active, or all inactive. The second is the multiple exchanged boomerang distinguisher, which clusters four boomerang trails that share the same input and output truncated differences. Both distinguishers are experimentally verified. The main results are summarized in Table 1.

- We propose the massive exchanged boomerang distinguisher. It uses plaintext pairs with one active diagonal and checks whether the truncated difference of the returned plaintext pair is such that, in each of its diagonals, the four bytes are either all active, or all inactive. The right pairs following the massive exchanged boomerang trail have at most one active byte per column after the first round MC, which ensures that the truncated difference of the returned pair is such that, in each of its diagonals, the four bytes are either all active, or all inactive. Although this probability is very high for a random permutation, we significantly reduce it using the friend pairs technique [BLT20] and exchange active inverse diagonal technique, while keeping the boomerang probability unchanged. The massive 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 distinguishers, it is significant because it introduces a new approach for constructing boomerang distinguishers based on fully active pairs.
- 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. It is constructed by clustering four trails that have the same input and output truncated differences, enabling it to distinguish a block cipher from a random permutation with lower complexity and higher success probability. The multiple exchanged boomerang distinguisher for 5-round AES has the data and time complexities of $2^{27.1}$ with a success probability of 79.6%. The multiple exchanged boomerang distinguisher is, to the best of our knowledge, the best distinguisher for 5-round AES.

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 exchanged boomerang attack, which serves as the basis for the distinguishers we propose, and presents previously proposed examples. Section 4 introduces the massive exchanged boomerang distinguisher for 5-round AES. In Section 5, we introduce the massive exchanged boomerang distinguisher for 5-round AES. Finally, Section 6 concludes the paper. The source code for the experiments in this paper is available online.[1]

2 Preliminaries

2.1 Description of the AES

AES [AES01] 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,

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

Table 1: Summary of secret-key distinguishers for 5- and 6-round AES. Data complexity is measured in chosen plaintexts (CP), adaptively chosen ciphertexts (ACC), or adaptively chosen plaintexts and ciphertexts (ACPC). Time complexity is measured in the number of equivalent 5-round AES encryptions (E) or memory accesses (M).

Property	Rounds	Data	Time	Succ.	Ref.
Multiple-of-8	5	2^{32} CP	$2^{35.6}$ M	99%	[GRR17]
Exchange	5	2^{30} CP	2^{30} E	63%	[BR19]
Yoyo	5	$2^{29.95}$ ACPC	$2^{29.95}$ M	55%	[MRSA23]
Yoyo	5	$2^{30.65}$ ACPC	$2^{29.95}$ M	81%	[MRSA23]
Massive ex. boom.	5	2^{31} ACC	2^{31} M	70%	Sect. 4
Multiple ex. boom.	5	$2^{27.1}$ ACC	$2^{27.1}$ M	80%	Sect. 5
Truncated Differential	6	$2^{89.4}$ CP	$2^{96.5}$ M	95%	[BGL20]
Exchange Attack	6	$2^{88.2}$ CP	$2^{88.2}$ E	73%	[BR19]
Truncated Boomerang	6	2^{87} ACC	2^{87} E	84%	[BL23]
Exchange Attack	6	2^{84} ACC	2^{83} E	63%	[Bar19]
Re-boomerang	6	$2^{82.33}$ ACPC	$2^{82.33}$ E	64%	[YTXQ24]
Triple Boomerangs	6	$2^{77.82}$ ACPC	$2^{77.82}$ E	66%	[YTXQ24]
Boomerang Chain	6	$2^{76.57}$ ACPC	$2^{76.57}$ E	60%	[YTXQ24]

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.

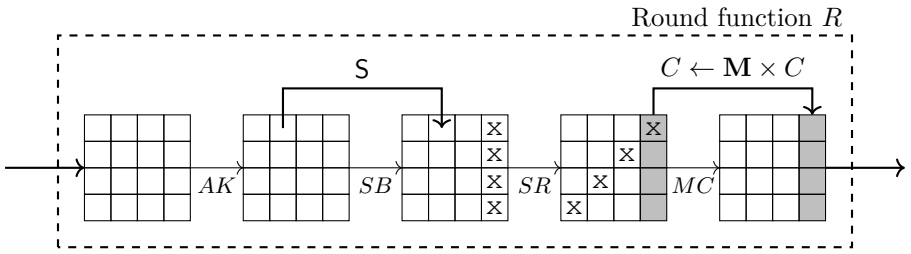

Figure 1: Round function of AES [Jea16]

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.

The bytes of each state of AES are numbered $0, 1, ..., 15$, where for $0 \leq i, j \leq 3$, the j-th byte in the i-th row is numbered $i + 4j$. We define the notions of column, diagonal, and inverse diagonal with respect to the state of AES. We define each column as the set of bytes $\{0, 1, 2, 3\}$, $\{4, 5, 6, 7\}$, $\{8, 9, 10, 11\}$, and $\{12, 13, 14, 15\}$, respectively. Each diagonal is defined as the set of bytes $\{0, 5, 10, 15\}$, $\{1, 6, 11, 12\}$, $\{2, 7, 8, 13\}$, and $\{3, 4, 9, 14\}$, respectively. Each inverse diagonal is defined as the set of bytes $\{3, 6, 9, 12\}$, $\{2, 5, 8, 15\}$, $\{1, 4, 11, 14\}$, and $\{0, 7, 10, 13\}$, respectively.

2.2 Differential and Truncated Differential Cryptanalysis

Differential cryptanalysis (DC) [BS91] is a well-known and powerful cryptanalysis technique for block ciphers. DC is a statistical attack on block ciphers that studies the propagation 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 [Knu95] 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, and related as follows:

$$\frac{\Pr(\mathcal{D}_{\text{in}} \xrightarrow{E} \mathcal{D}_{\text{out}})}{|\mathcal{D}_{\text{out}}|} = \frac{\Pr(\mathcal{D}_{\text{out}} \xrightarrow{E^{-1}} \mathcal{D}_{\text{in}})}{|\mathcal{D}_{\text{in}}|}.$$

2.3 Boomerang Attacks

In 1999, Wagner introduced the boomerang attack [Wag99], 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 p, and for the lower part E_1, there exists a differential trail $\nabla_{\text{in}} \xrightarrow{E_1} \nabla_{\text{out}}$ with probability q. Wagner proposed to use these two differentials by constructing a quartet (P_1, P_2, P_3, P_4) of the following form:

$$(P_1, P_1 \oplus \Delta_{\text{in}}, E^{-1}(E(P_1) \oplus \nabla_{\text{out}}), E^{-1}(E(P_1 \oplus \Delta_{\text{in}}) \oplus \nabla_{\text{out}})).$$

To simplify the explanation and the corresponding Figure 2, we write $C_i = E(P_i)$, and $E_0(P_i) = X_i = E_1^{-1}(C_i)$ for $i \in \{1, 2, 3, 4\}$. The boomerang process is as follows.

1. Choose plaintext pairs (P_1, P_2) such that $P_1 \oplus P_2 = \Delta_{\text{in}}$, 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 $P_3 \oplus P_4 = \Delta_{\text{in}}$.

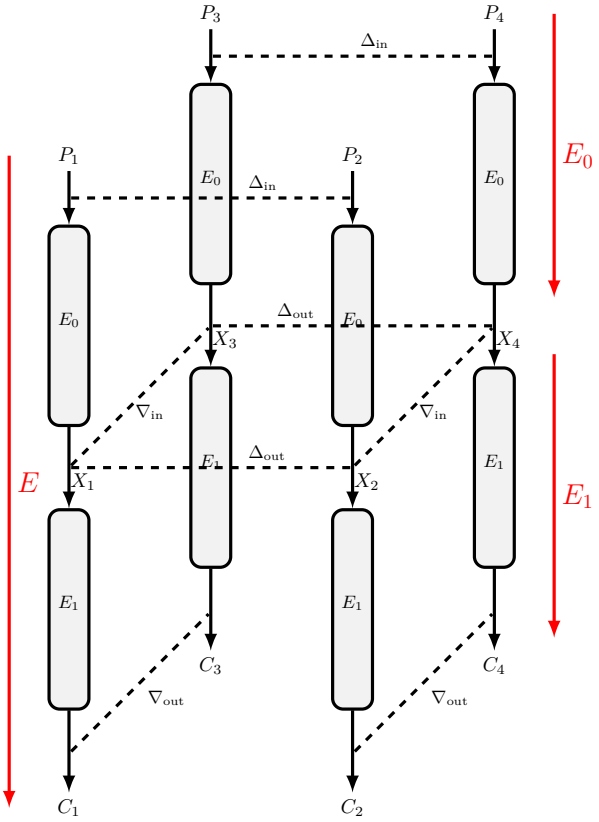

Figure 2: The Boomerang Distinguisher [Jea16]

Wagner remarked that, under the assumption that E_0 and E_1 are independent, the boomerang probability p_b that a quartet (P_1, P_2, P_3, P_4) holds $P_3 \oplus P_4 = \Delta_{\text{in}}$ is p^2q^2. It can be used as a distinguisher when p^2q^2 is significantly greater than 2^{-n}, which is the expected probability that a randomly constructed quartet (P_1, P_2, P_3, P_4) holds the boomerang property for a random permutation. Given $P_1 \oplus P_2 = \Delta_{\text{in}}$ and $C_1 \oplus C_3 = C_2 \oplus C_4 = \nabla_{\text{out}}$, the probability p_b is calculated as follows:

$$
\begin{aligned}
p_b &= \Pr[P_3 \oplus P_4 = \Delta_{\text{in}}] \\
&\geq \Pr[P_3 \oplus P_4 = \Delta_{\text{in}} \mid X_3 \oplus X_4 = \Delta_{\text{out}}] \cdot \Pr[X_3 \oplus X_4 = \Delta_{\text{out}}] \\
&\geq p \cdot \Pr[X_3 \oplus X_4 = \Delta_{\text{out}} \mid X_1 \oplus X_2 = \Delta_{\text{out}}] \cdot \Pr[X_1 \oplus X_2 = \Delta_{\text{out}}] \\
&\geq p \cdot \Pr[X_1 \oplus X_2 = X_3 \oplus X_4] \cdot p \\
&\geq p^2 \cdot \Pr[X_1 \oplus X_3 = X_2 \oplus X_4] \\
&\geq p^2 \cdot \Pr[X_1 \oplus X_3 = \nabla_{\text{in}}] \cdot \Pr[X_2 \oplus X_4 = \nabla_{\text{in}}] \\
&\geq p^2 q^2.
\end{aligned}
$$

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 [BL23]. The truncated boomerang attacks use structures on both plaintext and ciphertext sides, which can reduce the complexity effectively. For the upper part E_0, there exist truncated differential trails $\mathcal{D}_{\text{in}}^0 \xrightarrow{E_0} \mathcal{D}_{\text{out}}^0$ with probability $\overrightarrow{p}$ and $\mathcal{D}_{\text{out}}^0 \xrightarrow{E_0^{-1}} \mathcal{D}_{\text{in}}^0$ with probability $\overleftarrow{p}$. Similarly, for the lower part E_1, there are truncated differential trails $\mathcal{D}_{\text{in}}^1 \xrightarrow{E_1} \mathcal{D}_{\text{out}}^1$ with probability $\overrightarrow{q}$ and $\mathcal{D}_{\text{out}}^1 \xrightarrow{E_1^{-1}} \mathcal{D}_{\text{in}}^1$ with probability $\overleftarrow{q}$. The truncated boomerang attack proceeds as follows:

1. Choose a plaintext pair (P_1, P_2) such that $P_1 \oplus P_2 \in \mathcal{D}_{\text{in}}^0$, and ask for the corresponding ciphertext pairs (C_1, C_2).
2. Generate (C_3, C_4) such that $C_1 \oplus C_3 \in \mathcal{D}_{\text{out}}^1$ and $C_2 \oplus C_4 \in \mathcal{D}_{\text{out}}^1$, and ask for the corresponding plaintext pairs (P_3, P_4).
3. Check if $P_3 \oplus P_4 \in \mathcal{D}_{\text{in}}^0$.

Bariant et al. remarked that, under the assumption that E_0 and E_1 are independent, the boomerang probability p_b that a quartet (P_1, P_2, P_3, P_4) holds $P_3 \oplus P_4 \in \mathcal{D}_{\text{in}}^0$ is $\overrightarrow{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r$, where

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

It can be used as a distinguisher when $\overrightarrow{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r$ is significantly greater than 2^{-n}, which is the expected probability that a randomly constructed quartet (P_1, P_2, P_3, P_4) holds the boomerang property for a random permutation. Given $P_1 \oplus P_2 \in \mathcal{D}_{\text{in}}^0$ and $C_1 \oplus C_3, C_2 \oplus C_4 \in \mathcal{D}_{\text{out}}^1$, the boomerang probability p_b can be computed as follows, similarly to the case of using differential trails:

$$\begin{aligned}
p_b =& \Pr[P_3 \oplus P_4 \in \mathcal{D}_{\text{in}}^0] \\
\geq& \Pr[P_3 \oplus P_4 \in \mathcal{D}_{\text{in}}^0 \mid X_3 \oplus X_4 \in \mathcal{D}_{\text{out}}^0] \cdot \Pr[X_3 \oplus X_4 \in \mathcal{D}_{\text{out}}^0] \\
\geq& \overleftarrow{p} \cdot \Pr[X_3 \oplus X_4 \in \mathcal{D}_{\text{out}}^0 \mid (X_1 \oplus X_2 \in \mathcal{D}_{\text{out}}^0) \ \wedge (X_1 \oplus X_3 \in \mathcal{D}_{\text{in}}^1) \ \wedge (X_2 \oplus X_4 \in \mathcal{D}_{\text{in}}^1)] \\
& \cdot \Pr[(X_1 \oplus X_2 \in \mathcal{D}_{\text{out}}^0) \ \wedge (X_1 \oplus X_3 \in \mathcal{D}_{\text{in}}^1) \ \wedge (X_2 \oplus X_4 \in \mathcal{D}_{\text{in}}^1)] \\
\geq& \overleftarrow{p} \cdot r \cdot \Pr[X_1 \oplus X_2 \in \mathcal{D}_{\text{out}}^0] \cdot \Pr[X_1 \oplus X_3 \in \mathcal{D}_{\text{in}}^1] \cdot \Pr[X_2 \oplus X_4 \in \mathcal{D}_{\text{in}}^1] \\
\geq& \overrightarrow{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r.
\end{aligned}$$

3 Exchanged Boomerang Attack on 5-round AES

3.1 Overview of Exchanged Boomerang Attack on 5-round AES

The authors of [RBH17, DKRS20, YTXQ24] utilized the exchange technique to construct a new boomerang attack on reduced-round AES. We call it the exchanged boomerang attack. The exchanged boomerang is equivalent to performing the yoyo game from [RBH17] once, and is also similar to the mixing retracing boomerang described in [DKRS20]. The authors of [DKRS20] presented a key-recovery attack on 5-round AES using the mixing retracing boomerang, while the authors of [YTXQ24] proposed a distinguisher for 6-round AES based on the boomerang chain constructed from the exchange boomerang.

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. The main idea of the exchanged boomerang on AES is to define ∇_{out} active on diagonals, such that the pairs $(C_1, C_1 \oplus \nabla_{\text{out}})$ and $(C_2, C_2 \oplus \nabla_{\text{out}})$ have the same pair of values on the active inverse diagonal: i.e. either $C_1 = C_2$ or $C_1 = C_2 \oplus \nabla_{\text{out}}$ on the active inverse diagonal. The exchanged boomerang chooses ∇_{out} active on an inverse diagonal, such that $\nabla_{\text{out}} = C_1 \oplus C_2$ on that inverse diagonal. This leads to $C_1 = C_4$ and $C_2 = C_3$ on the inverse diagonal.

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). 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). Futhermore, as $E_{1,0} = AK \circ MC$, (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.

This implies that in the boomerang probability $p_b = \overrightarrow{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r$, both $\overleftarrow{q}$ and r are equal to 1. Therefore, for 5-round AES, when a plaintext structure is constructed with activity only in a single diagonal and the exchanged boomerang uses a difference $\nabla_{\text{out}} = C_1 \oplus C_2$ on a specific inverse diagonal, the resulting boomerang probability is $\overrightarrow{p} \cdot \overleftarrow{p}$.

3.2 Example of Exchanged Boomerang Attack on 5-round AES

We introduce, as an example, a key-recovery attack on 5-round AES that is based on performing the yoyo game once, as described in [RBH17]. They used a plaintext structure with one active diagonal and chose a difference ∇_{out} such that $\nabla_{\text{out}} = C_1 \oplus C_2$ on a specific inverse diagonal.

They also utilized the fact that if P_1 and P_2 are inactive in the l-th byte after the first round MC, then the returned pair (P_3, P_4), obtained by decrypting $(C_3, C_4) = (C_1 \oplus \nabla_{\text{out}}, C_2 \oplus \nabla_{\text{out}})$, is inactive in the l-th diagonal after the first round MC with probability 1. By exploiting this property with multiple plaintext pairs, keys for which the l-th diagonal is not inactive after the first round MC are discarded, and only the correct key remains. The key-recovery attack on 5-round AES using the exchanged boomerang proceeds as follows:

1. Choose a plaintext pair (P_1, P_2) from a plaintext structure where only the 0th diagonal is active and ask for the corresponding (C_1, C_2).

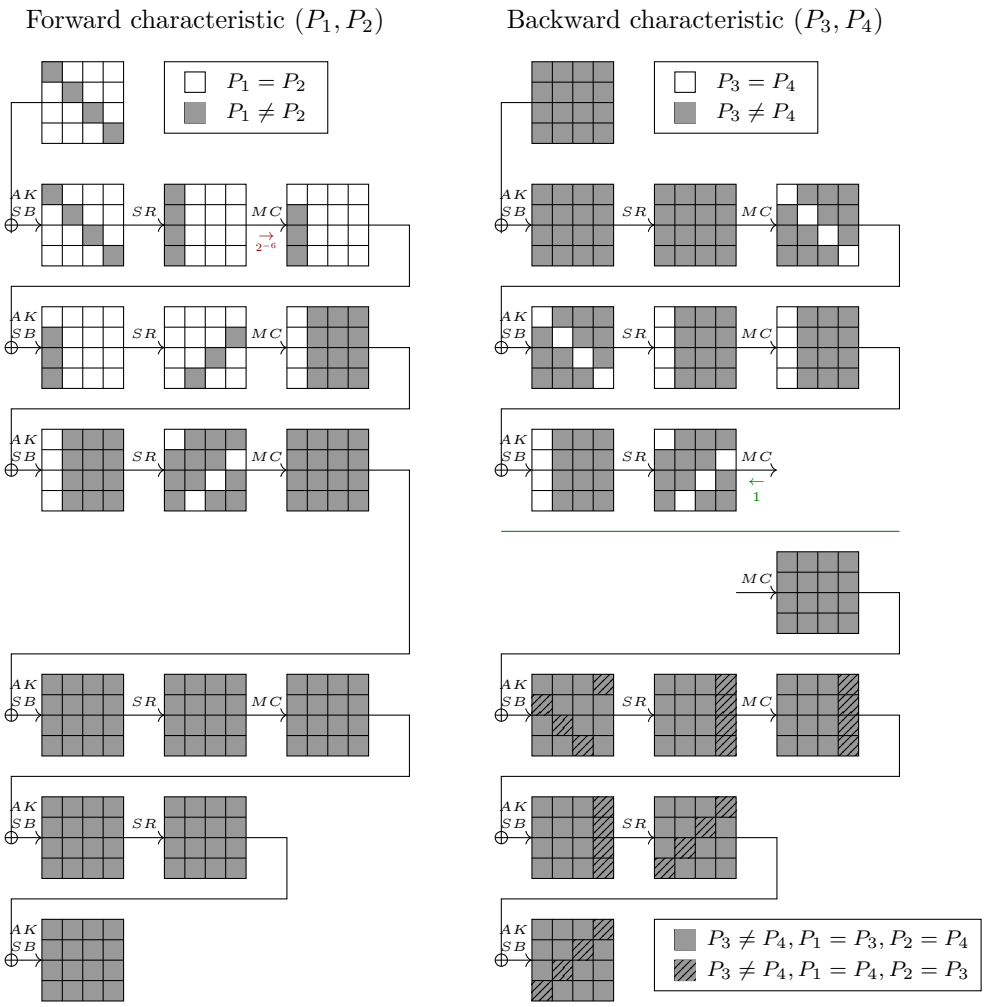

Figure 3: Example of Exchanged Boomerang Trail

2. Generate four pairs (C_3^j, C_4^j) by exchanging each of the four inverse diagonals, and ask for the corresponding plaintext pairs (P_3^j, P_4^j) for $j \in \{0, 1, 2, 3\}$.

3. Recover the key that makes the l-th byte inactive after the first round MC for (P_1, P_2), and the l-th diagonal inactive after the first round MC for (P_3^j, P_4^j), for each $l \in \{0, 1, 2, 3\}$.

A right forward pair, which has one inactive byte after the first round MC, exists with probability 2^{-6}. In 5-round AES, since $\overleftarrow{q} = 1$,$r = 1$, $\overrightarrow{p} = 2^{-6}$ and $\overleftarrow{p} = 1$, the exchanged boomerang trail in this example has a probability of 2^{-6}, as illustrated in Figure 3. Each right forward pair yields exactly one correct key, while a wrong pair produces on average $2^{32-40} = 2^{-8}$ key candidates. Therefore, the correct key can be recovered.

The previously introduced example of the exchange boomerang has been used for key-recovery attacks, but our goal is to construct a distinguisher by analyzing the pattern of the returned plaintext pairs. Since the exchange boomerang enables the construction of the best-known key-recovery attack on 5-round AES, we believe that it can also be used to construct the best-known distinguisher for 5-round AES. Furthermore, as the exchange boomerang has $\overleftarrow{q} = 1$ and $r = 1$, we focus on the boomerang probability $p_b = \overrightarrow{p} \cdot \overleftarrow{p}$, and propose two distinguishers based on this observation.

4 Massive Exchanged Boomerang Distinguisher

In this section, we propose the massive exchanged boomerang distinguisher, which distinguishes by checking whether the returned plaintext pair through the boomerang is fully active or inactive in each diagonal. To be fully active means that all four bytes in the column have non-zero differences. Although the probability that each diagonal is randomly either fully active or inactive is very high, we significantly reduce this random probability by using the friend pairs technique and by exploiting the fact that multiple inverse diagonals can be exchanged in the ciphertext. If the random probability becomes significantly lower than the boomerang probability, it can be used as a distinguisher. The massive exchanged boomerang distinguisher is named as such because it utilizes the friend pairs technique to throw a large (massive) number of pairs through the boomerang.

The massive exchanged boomerang distinguisher for 5-round AES has a complexity of 2^{31} with a success probability of 70%. We first present the massive exchanged boomerang distinguisher algorithm, followed by an analysis of the distinguisher's complexity and success probability. Then, we provide experimentally verified data.

The idea of the massive exchanged boomerang distinguisher is that if each column of returned pair has at most one active byte after the first round MC, then the plaintext pair must be either fully active or inactive because the MC and MC^{-1} use an MDS matrix. Constructing a distinguisher using fully active pairs has been previously used in [BFL+23]. When using the exchanged boomerang on 5-round AES, if (P_1, P_2) is inactive in three bytes after the first round MC, then the returned plaintext pair (P_3^j, P_4^j) will be inactive in the corresponding three diagonals after the first round MC. Since the three diagonals of (P_3^j, P_4^j) are inactive after the first round MC, each column contains either three inactive bytes or all four bytes inactive. If each column of the returned plaintext pair (P_3^j, P_4^j) has three inactive bytes after the first round MC, the corresponding column of (P_3^j, P_4^j) after the first round SR will be fully active due to the MDS property of MC^{-1}. If all four bytes are inactive after the first round MC, the corresponding column of (P_3^j, P_4^j) after the first round SR will remain inactive. Therefore, each column of the returned plaintext pair (P_3^j, P_4^j) is either fully active or inactive. The fully active boomerang trail requires that (P_1, P_2) be inactive in three bytes after the first round MC, resulting in a boomerang probability of $4 \cdot 2^{-24} = 2^{-22}$.

The probability that a returned plaintext pair is either fully active or inactive on each diagonal 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 each inverse diagonal in the ciphertext pair of a right pair also become 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 massive 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 such that, in each of its diagonals, the 4 bytes are either all active, or all inactive. 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

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

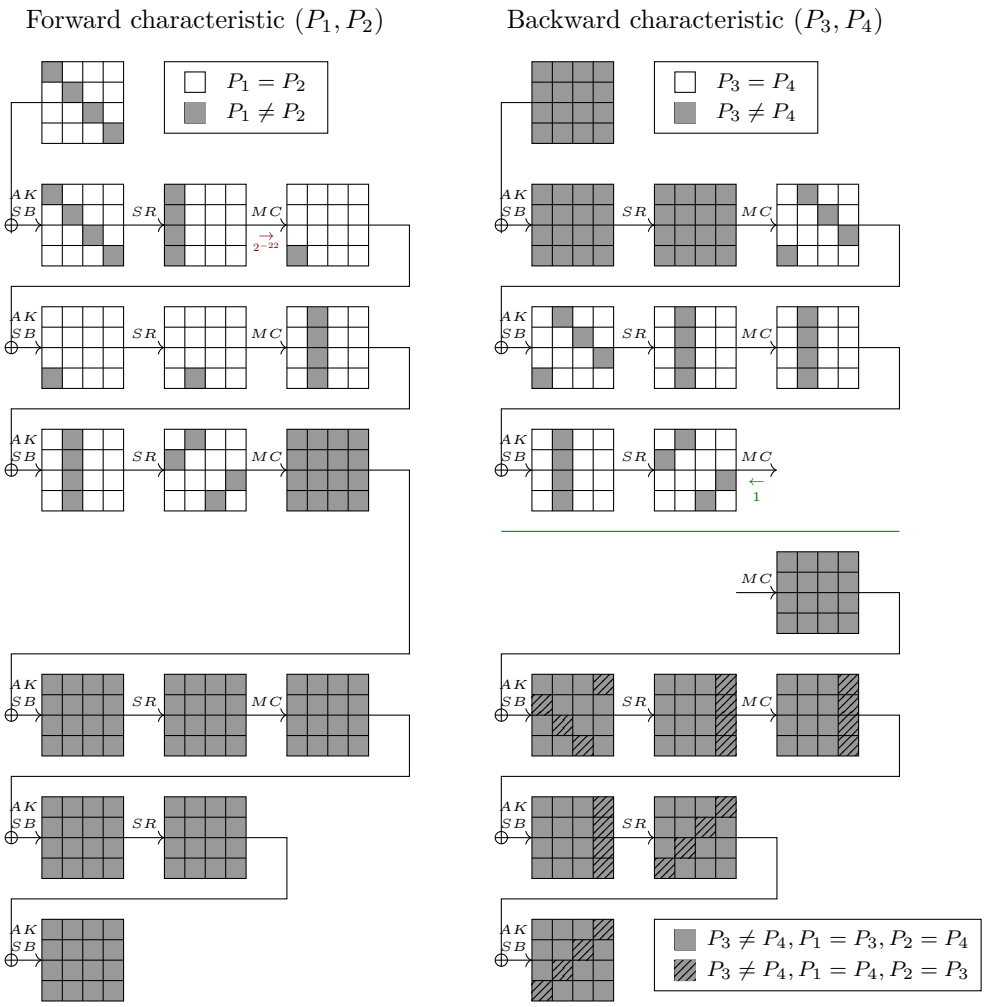

Figure 4: Massive exchanged boomerang trail

In the backward characteristic, not all bytes in the corresponding column may be active before the second round MC. Any byte that is inactive before the second round MC will result in the entire column being inactive after the first round MC. Consequently, each inactive byte before the second round MC corresponds to an inactive diagonal in the returned plaintext pair (P_3, P_4). Therefore, 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 $j \in \{0, 1, 2, 3\}$. (C_3^j, C_4^j) is generated as $(C_1 \oplus \nabla_{\text{out}}, C_2 \oplus \nabla_{\text{out}})$, where $\nabla_{\text{out}} = C_1 \oplus C_2$ on the j-th inverse diagonal and zero on all other diagonals. Given that $\nabla_{\text{out}} = C_1 \oplus C_2$ on the j-th inverse diagonal and zero on all other diagonals, 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 massive exchanged boomerang trail is 2^{-22}. The massive exchanged boomerang trail can be seen in Figure 4. 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

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

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

We aim to make this random probability lower than the boomerang probability of 2^{-22}, allowing us to distinguish the block cipher from a random permutation. We first focus on the fact that, starting from (C_1, C_2), we can generate four ciphertext pairs (C_3^j, C_4^j) by exchanging each of the four inverse diagonals. If (P_1, P_2) is a right forward pair, meaning that it is inactive in three bytes after the first round MC, then each returned plaintext pair (P_3^j, P_4^j), corresponding to the four exchanged ciphertext pairs (C_3^j, C_4^j), will be inactive in the same three diagonals after the first round MC. As a result, all returned pairs (P_3^j, P_4^j) are either fully active or inactive in each diagonal simultaneously. Therefore, while the boomerang probability remains the same at 2^{-22}, the probability that all four returned plaintext pairs are randomly either fully active or inactive in each diagonal is

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

which reduces the random probability from $2^{-0.09}$ to $2^{-0.36}$. However, this probability is still too high to distinguish the block cipher from a random permutation.

Second, we further reduce this random probability by applying the previously proposed friend pairs technique [BLT20]. Friend pairs are pairs (P_1, P_2) and (P_1', P_2') that have the same values in the active diagonal and different constant values in the inactive diagonals. If (P_1, P_2) is a right pair, meaning that three bytes are inactive after the first round MC, then the friend pair (P_1', P_2') also has the same values in the active diagonal and therefore has three inactive bytes after the first round MC. As a result, (P_1', P_2') is always a right pair with probability 1. For a right pair, all of its friend pairs also produce returned plaintext pairs that are either fully active or inactive in each diagonal, with the same boomerang probability of 2^{-22}. However, the probability that all of these returned pairs are randomly either fully active or inactive in each diagonal decreases exponentially. If 2^6 friend pairs are used, then the probability that all returned pairs are simultaneously either fully active or inactive in each diagonal becomes

$$((((1-2^{-8})^4+2^{-32})^4)^4)^{2^6} \approx 2^{-23.1} < 2^{-22}.$$

Therefore, since the massive 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 on average. 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 each of the 2^{22} plaintext pairs, we generate 2^6 friend pairs. Since a right pair and all of its friend pairs follow the massive exchanged boomerang trail, all of their returned pairs are either fully active or inactive in each diagonal. 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 $2^{-23.1}$. Therefore, for all returned pairs of a pair and its friend pairs that are either fully active or inactive in each diagonal, on average,

$$1+2^{22}\cdot 2^{-23.1} = 1+2^{-1.1} \approx 1.46 > 1$$

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

$$2^{22}\cdot 2^{-23.1} = 2^{-1.1} \approx 0.46 < 1$$

such pairs exist.

Therefore, if there exists a plaintext pair and its friend pairs 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 massive 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^j, C_4^j) and ask for the decryption of (C_3^j, C_4^j) to obtain (P_3^j, P_4^j).

4. If there exists at least one pair (P_1, P_2) such that all returned pair (P_3^j, P_4^j) of a pair and its friend pairs that are either fully active or inactive in each diagonal, the distinguishing result is 5-round AES, otherwise it is a random permutation.

Algorithm 1 Massive exchanged boomerang distinguisher for 5-round AES

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
for each plaintext pair **do**
    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
    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)
    end for
    if all returned pair are either inactive or have all bytes of the diagonal active for all diagonals **then**
        return 5-round AES
    end if
end for
return 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} memory accesses.

- Data Complexity: 2^{31} adaptive chosen ciphertexts
- Time Complexity: 2^{31} memory accesses

Table 2: Experimental results of the number of detected pairs in the massive exchanged boomerang distinguisher for 5-round AES

Number of experiments	Blackbox Primitive	Experimental number of pairs	Theoretical number of pairs
1000	5-round AES	1.464	1.46
1000	Rand. Perm.	0.433	0.46

Success Probability

The success probability of the massive exchanged boomerang distinguisher 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 $\lambda = 1.46$, 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.

If more pairs are used, the number of returned plaintext pairs in which each diagonal is either fully active or inactive increases rapidly for 5-round AES, while it increases more slowly for a random permutation. As a result, the corresponding Poisson distributions change for each case, and the success probability is determined by how many such pairs exist and where the distinguishing threshold is set. However, since the number of such pairs eventually increases in both 5-round AES and a random permutation, if we aim for a success probability close to 1, it is more efficient to simply run the proposed the massive exchanged boomerang distinguisher twice, rather than increasing the complexity further.

Experimental Verification

To verify the massive exchanged boomerang distinguisher, we first count the number of pairs (P_1, P_2) such that all returned pairs (P_3^j, P_4^j) of the pair and its friend pairs are either fully active or inactive in each diagonal. We conducted 1000 experiments for each case and verified that, for 5-round AES, there is an average of 1.464 pairs, while for the random permutation (10-round AES), there is an average of 0.433 pairs, which is close to the theoretical expectation. The experimental results for this are shown in Table 2.

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 1000 times each for 5-round AES and the random permutation

Table 3: Experimental results of a success probability of the massive exchanged boomerang distinguisher for 5-round AES

Number of experiments	Blackbox Primitive	Returned as 5-round AES	Returned as Rand. Perm.	Experimental Success Probability
1000	5-round AES	780	220	$\frac{0.780+0.652}{2} = 0.716$
1000	Rand. Perm.	348	652	

(10-round AES). The results showed that when the black box was 5-round AES, the distinguisher outputted 5-round AES 780 times, and when the black box was a random permutation, the distinguisher outputted a random permutation 652 times. Therefore, the experimental success probability is $(0.780 + 0.652)/2 = 0.716$, which is similar to the theoretical probability. The experimental results for this are shown in Table 3.

5 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. It distinguishes the block cipher from a random permutation by checking whether the returned plaintext pair is inactive in one diagonal. We cluster four exchanged boomerang trails to increase the overall boomerang probability.

The multiple exchanged boomerang distinguisher for 5-round AES has a complexity of $2^{27.1}$ with a success probability 79.6%. 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.

The idea of the multiple exchanged boomerang distinguisher is to utilize multiple exchanged boomerang trails that use the same input truncated differences, $\mathcal{D}_{\text{in}}$ and $\mathcal{D}'_{\text{in}}$. We have found four exchanged boomerang trails with probabilities 2^{-28}, $2^{-27.4}$, 2^{-28}, and 2^{-30}, respectively. By clustering these trails, the boomerang probability can be significantly increased to

$$2^{-28} + 2^{-27.4} + 2^{-28} + 2^{-30} = 2^{-26.1}.$$

Since the probability that a returned plaintext pair is randomly inactive in one diagonal is $4 \cdot 2^{-32} = 2^{-30} < 2^{-26.1}$, that is, the boomerang probability is higher than the random probability, we can construct a multiple exchanged boomerang distinguisher.

We introduce the multiple exchanged boomerang trails. The multiple exchanged boomerang distinguisher uses four exchanged boomerang trails which have the same $\mathcal{D}_{\text{in}}$ and $\mathcal{D}'_{\text{in}}$. The input truncated difference $\mathcal{D}_{\text{in}}$ is active only in the 0th diagonal, same as in the massive 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 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

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

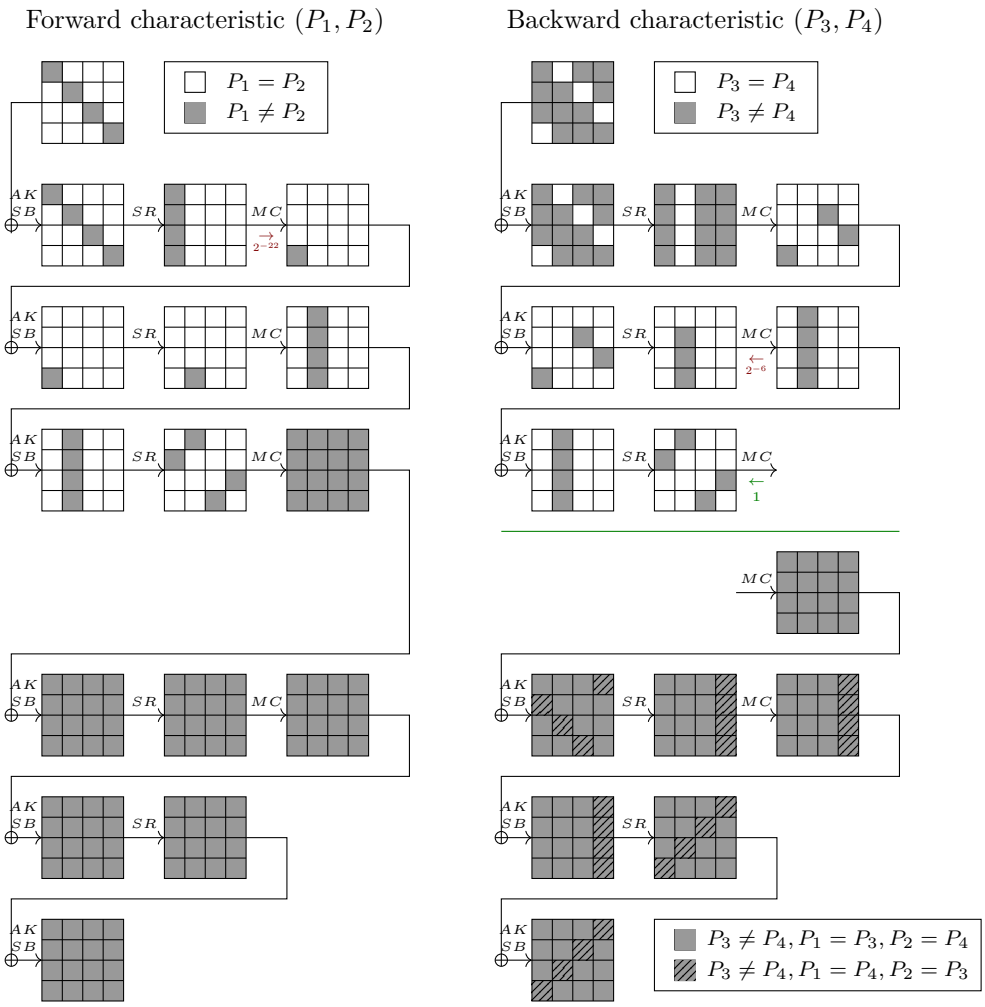

Figure 5: First exchanged boomerang trail

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 5.

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

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

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 6.

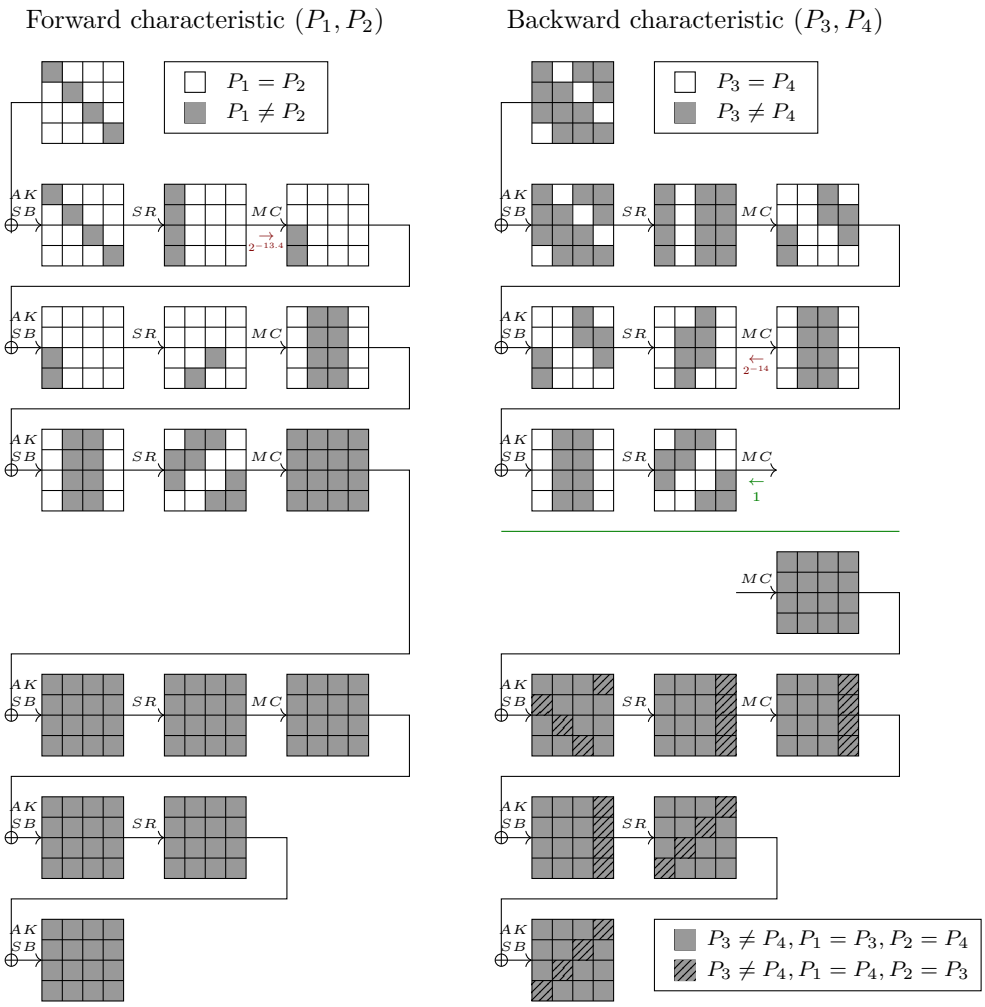

Figure 6: Second exchanged boomerang trail

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

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

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 7.

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

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

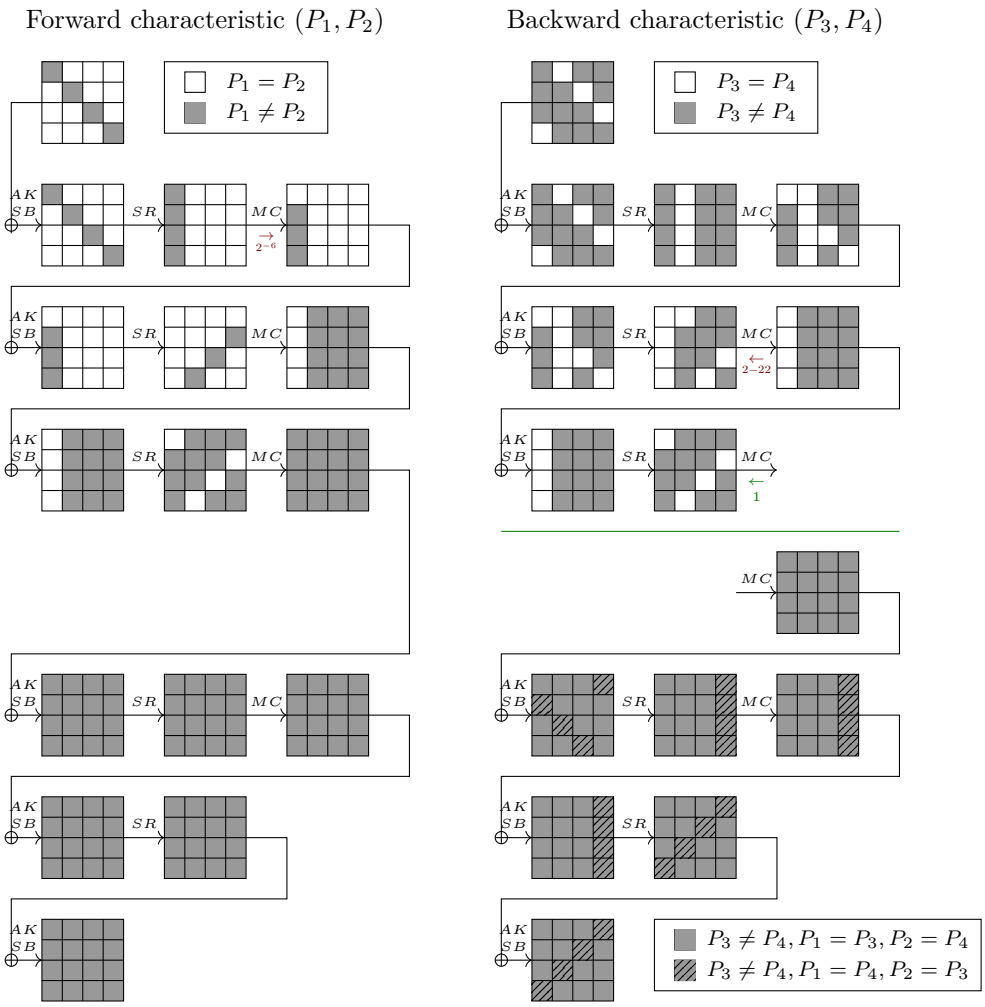

Figure 7: Third exchanged boomerang trail

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

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

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 8.

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

$$2^{-28} + 2^{-27.4} + 2^{-28} + 2^{-30} = 2^{-26.1}.$$

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 $2^{26.1}$ pairs to obtain one right pair on average. Since we can generate four additional ciphertext pairs by exchanging the active inverse diagonal in the ciphertext

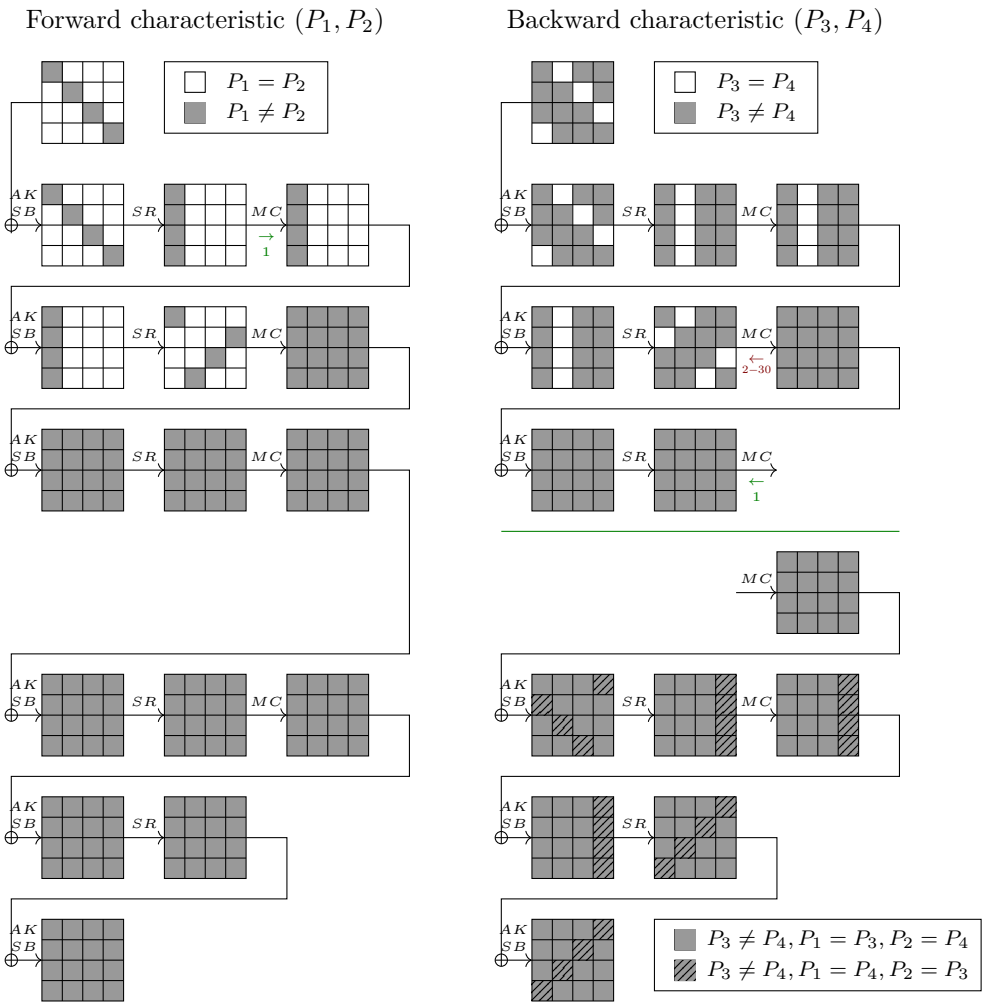

Figure 8: Fourth exchanged boomerang trail

pairs, $2^{24.1}$ plaintext pairs are required. Using a plaintext structure of size $2^{12.55}$, where only the 0th diagonal can take values and the remaining bytes are any constants, we can obtain $2^{24.1}$ plaintext pairs.

Since a right pair follows the multiple exchanged boomerang with probability 1, the returned plaintext pair of a right pair is inactive in one diagonal. On the other hand, the returned plaintext pair of a wrong 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,

$$1 + 2^{-26.1} \cdot 2^{30} = 1 + 2^{-3.9} \approx 1.066 > 1$$

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

$$2^{-26.1} \cdot 2^{30} = 2^{-3.9} \approx 0.066 < 1$$

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 $2^{12.55}$ 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 exists 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 (C1, C2) to obtain four pairs (C3, C4) for j ∈ {0, 1, 2, 3}
    Ask for the decryption of four pairs (C3, C4) to obtain four pairs (P3, P4)
    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 $2^{12.55}$ chosen plaintexts. In step 2, we generate $2^{24.1} \cdot 4 = 2^{26.1}$ ciphertext pairs, so $2^{26.1} \cdot 2 = 2^{27.1}$ adaptive chosen ciphertexts are required. Therefore, the data complexity of a distinguishing process is $2^{27.1}$ ACC, and the time complexity is $2^{27.1}$ memory accesses.

- Data Complexity: $2^{27.1}$ adaptive chosen ciphertexts
- Time Complexity: 2^{31} memory accesses

Success Probability

The success probability of the multiple exchanged boomerang distinguisher 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

$$\Pr[X \geq 1] \approx 0.656$$

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

$$\frac{0.656 + 0.936}{2} = 0.796$$

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
1000	5-round AES	1.017	1.066
1000	Rand. Perm.	0.058	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
1000	5-round AES	637	363	$\frac{0.613+0.932}{2} = 0.7725$
1000	Rand. Perm.	68	932	

on average.

In the multiple exchanged boomerang distinguisher, as with the massive exchanged boomerang distinguisher, using more pairs leads to a rapid increase in the number of returned plaintext pairs with one inactive diagonal for 5-round AES, while the increase is slower for a random permutation. As a result, the corresponding Poisson distributions change for each case, and the success probability depends on how many such pairs exist and where the distinguishing threshold is set. However, since the number of such returned pairs increases in both 5-round AES and a random permutation, if a distinguishing success probability close to 1 is desired, it is more efficient to simply run the proposed multiple exchanged boomerang distinguisher twice at the given complexity.

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 1000 experiments for each case and verified that, for 5-round AES, there is an average of 1.017 pairs, while for the random permutation (10-round AES), there is an average of 0.058 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 1000 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 637 times, and when the black box was a random permutation, the distinguisher outputted a random permutation 932 times. Therefore, the experimental success probability is $(0.637 + 0.932)/2 = 0.7845$, which is similar to the theoretical probability. The experimental results for this are shown in Table 5.

6 Conclusion

In this paper, we proposed the massive exchanged boomerang and multiple exchanged boomerang distinguishers for 5-round AES by utilizing the friend pairs technique and multiple trails, respectively. The massive 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 $2^{27.1}$ and success probability 80%. To the best of our knowledge, the multiple exchanged boomerang distinguisher is the best-known distinguisher for 5-round AES. We experimentally verified both distinguishers. The massive exchanged boomerang and multiple exchanged boomerang distinguishers can also be applied to other AES-like block ciphers.

The two distinguishers we propose have good complexity in terms of distinguishing, but they have limitations when applied to key-recovery attacks. For 5-round key-recovery attacks, using the exchanged boomerang trail from the retracing boomerang attack in [DKRS20] is more effective. For 6-round key-recovery attacks as well, the exchanged boomerang trails from [BDK+24] are more suitable. Moreover, when considering 6-round distinguishers, the exchanged boomerang trail used in the boomerang chain distinguisher from [YTXQ24] is also more effective. However, our focus was on constructing the best distinguisher for 5-round AES, and by considering these two distinguishers, we were able to achieve that goal.

References

[AES01] Advanced Encryption Standard (AES). National Institute of Standards and Technology, NIST FIPS PUB 197, U.S. Department of Commerce, November 2001.

[Bar19] Navid Ghaedi Bardeh. A key-independent distinguisher for 6-round AES in an adaptive setting. Cryptology ePrint Archive, Report 2019/945, 2019.

[BBI+15] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 411–436. Springer, Berlin, Heidelberg, November / December 2015.

[BDK01] Eli Biham, Orr Dunkelman, and Nathan Keller. The rectangle attack - rectangling the Serpent. In Birgit Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 340–357. Springer, Berlin, Heidelberg, May 2001.

[BDK+18] Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. Improved key recovery attacks on reduced-round AES with practical data and memory complexities. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part II*, volume 10992 of *LNCS*, pages 185–212. Springer, Cham, August 2018.

[BDK+24] Augustin Bariant, Orr Dunkelman, Nathan Keller, Gaëtan Leurent, and Victor Mollimard. Improved boomerang attacks on 6-round AES. Cryptology ePrint Archive, Report 2024/977, 2024.

[BFL+23] Jules Baudrin, Patrick Felke, Gregor Leander, Patrick Neumann, Léo Perrin, and Lukas Stennes. Commutative cryptanalysis made practical. *IACR Trans. Symm. Cryptol.*, 2023(4):299–329, 2023.

[BGGS20] Zhenzhen Bao, Chun Guo, Jian Guo, and Ling Song. TNT: How to tweak a block cipher. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 641–673. Springer, Cham, May 2020.

[BGL20] Zhenzhen Bao, Jian Guo, and Eik List. Extended truncated-differential distinguishers on round-reduced AES. *IACR Trans. Symm. Cryptol.*, 2020(3):197–261, 2020.

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 123–153. Springer, Berlin, Heidelberg, August 2016.

[BL23] Augustin Bariant and Gaëtan Leurent. Truncated boomerang attacks and application to AES-based ciphers. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part IV*, volume 14007 of *LNCS*, pages 3–35. Springer, Cham, April 2023.

[BLT20] Christof Beierle, Gregor Leander, and Yosuke Todo. Improved differential-linear attacks with applications to ARX ciphers. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part III*, volume 12172 of *LNCS*, pages 329–358. Springer, Cham, August 2020.

[BR19] Navid Ghaedi Bardeh and Sondre Rønjom. The exchange attack: How to distinguish six rounds of AES with $2^{88.2}$ chosen plaintexts. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 347–370. Springer, Cham, December 2019.

[BS91] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. In Alfred J. Menezes and Scott A. Vanstone, editors, *CRYPTO'90*, volume 537 of *LNCS*, pages 2–21. Springer, Berlin, Heidelberg, August 1991.

[CCD+17] Jihoon Cho, Kyu Young Choi, Itai Dinur, Orr Dunkelman, Nathan Keller, Dukjae Moon, and Aviya Veidberg. WEM: A new family of white-box block ciphers based on the Even-Mansour construction. In Helena Handschuh, editor, *CT-RSA 2017*, volume 10159 of *LNCS*, pages 293–308. Springer, Cham, February 2017.

[CHP+18] Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. Boomerang connectivity table: A new cryptanalysis tool. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part II*, volume 10821 of *LNCS*, pages 683–714. Springer, Cham, April / May 2018.

[DDV20] Stéphanie Delaune, Patrick Derbez, and Mathieu Vavrille. Catching the fastest boomerangs application to SKINNY. *IACR Trans. Symm. Cryptol.*, 2020(4):104–129, 2020.

[DFJ13] Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean. Improved key recovery attacks on reduced-round AES in the single-key setting. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 371–387. Springer, Berlin, Heidelberg, May 2013.

[DKRS20] Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. The retracing boomerang attack. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part I*, volume 12105 of *LNCS*, pages 280–309. Springer, Cham, May 2020.

[DKS10] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 393–410. Springer, Berlin, Heidelberg, August 2010.

[FKKM16] Pierre-Alain Fouque, Pierre Karpman, Paul Kirchner, and Brice Minaud. Efficient and provable white-box primitives. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 159–188. Springer, Berlin, Heidelberg, December 2016.

[FKL+01] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 213–230. Springer, Berlin, Heidelberg, April 2001.

[Gra18] Lorenzo Grassi. Mixture differential cryptanalysis: a new approach to distinguishers and attacks on round-reduced AES. *IACR Trans. Symm. Cryptol.*, 2018(2):133–160, 2018.

[GRR16] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. Subspace trail cryptanalysis and its applications to AES. *IACR Trans. Symm. Cryptol.*, 2016(2):192–225, 2016.

[GRR17] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. A new structural-differential property of 5-round AES. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part II*, volume 10211 of *LNCS*, pages 289–317. Springer, Cham, April / May 2017.

[Jea16] Jérémy Jean. Tikz for cryptographers, 2016.

[JNP14] Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Kiasu v1. *Submitted to the CAESAR competition*, pages 43–45, 2014.

[JNPS21] Jérémy Jean, Ivica Nikolic, Thomas Peyrin, and Yannick Seurin. The deoxys AEAD family. *Journal of Cryptology*, 34(3):31, July 2021.

[KKS01] John Kelsey, Tadayoshi Kohno, and Bruce Schneier. Amplified boomerang attacks against reduced-round MARS and Serpent. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 75–93. Springer, Berlin, Heidelberg, April 2001.

[Knu95] Lars R. Knudsen. Truncated and higher order differentials. In Bart Preneel, editor, *FSE'94*, volume 1008 of *LNCS*, pages 196–211. Springer, Berlin, Heidelberg, December 1995.

[Knu98] Lars Knudsen. Deal-a 128-bit block cipher. *complexity*, 258(2):216, 1998.

[LH94] Susan K. Langford and Martin E. Hellman. Differential-linear cryptanalysis. In Yvo Desmedt, editor, *CRYPTO'94*, volume 839 of *LNCS*, pages 17–25. Springer, Berlin, Heidelberg, August 1994.

[Mat94] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 386–397. Springer, Berlin, Heidelberg, May 1994.

[MRSA23] Sandip Kumar Mondal, Mostafizar Rahman, Santanu Sarkar, and Avishek Adhikari. Revisiting yoyo tricks on aes. *IACR Transactions on Symmetric Cryptology*, 2023(4):28–57, 2023.

[Mur11] Sean Murphy. The return of the cryptographic boomerang. *IEEE Transactions on Information Theory*, 57(4):2517–2521, 2011.

[RBH17] Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth. Yoyo tricks with AES. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 217–243. Springer, Cham, December 2017.

[SKK+23] Hanbeom Shin, Insung Kim, Sunyeop Kim, Seonggyeom Kim, Deukjo Hong, Jaechul Sung, and Seokhie Hong. Revisiting the multiple of property for SKINNY the exact computation of the number of right pairs. Cryptology ePrint Archive, Report 2023/1944, 2023.

[SQH19] Ling Song, Xianrui Qin, and Lei Hu. Boomerang connectivity table revisited. *IACR Trans. Symm. Cryptol.*, 2019(1):118–141, 2019.

[Wag99] David Wagner. The boomerang attack. In Lars R. Knudsen, editor, *FSE'99*, volume 1636 of *LNCS*, pages 156–170. Springer, Berlin, Heidelberg, March 1999.

[WP19] Haoyang Wang and Thomas Peyrin. Boomerang switch in multiple rounds. *IACR Trans. Symm. Cryptol.*, 2019(1):142–169, 2019.

[YSS+22] Qianqian Yang, Ling Song, Siwei Sun, Danping Shi, and Lei Hu. New properties of the double boomerang connectivity table. *IACR Trans. Symm. Cryptol.*, 2022(4):208–242, 2022.

[YTXQ24] Xueping Yan, Lin Tan, Hong Xu, and Wen-Feng Qi. The boomerang chain distinguishers: New record for 6-round AES. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part VII*, volume 15490 of *LNCS*, pages 301–329. Springer, Singapore, December 2024.