New Exchanged Boomerang Distinguishers for 5-Round AES

Hanbeom Shin[1], Seonkyu Kim[1], Byoungjin Seok[2], Deukjo Hong[3], Jaechul Sung[4], Seokhie Hong[5], and Dongjae Lee[6(✉)]

[1] School of Cybersecurity, Korea University, Seoul, Republic of Korea
newonetiger@korea.ac.kr
[2] Department of Convergence Security, Hansung University, Seoul, Republic of Korea
[3] Department of Information and Engineering, Jeonbuk National University, Jeonju, Republic of Korea
[4] Department of Mathematics, University of Seoul, Seoul, Republic of Korea
[5] SmartM2M, Seoul, Republic of Korea
[6] Department of Convergence Security, Kangwon National University, Chuncheon, Republic of Korea
dongjae.lee@kangwon.ac.kr

Abstract. In block cipher design, it should be infeasible for an attacker to distinguish a block cipher from a random permutation; hence the existence of a distinguisher is of fundamental importance. Cryptanalysis of reduced-round variants of block ciphers also plays a crucial role in assessing their security. AES is the most widely used block cipher, and secret-key distinguishers for its 5-round variant have been studied since the introduction of the multiple-of-8 property. In this paper, we propose the massive exchanged boomerang and multiple exchanged boomerang distinguishers for 5-round AES. The massive exchanged boomerang distinguisher exploits the property that, for the returned plaintext pairs, the truncated difference in each diagonal is either fully active or fully inactive. While this event occurs with high probability in a random permutation, we significantly reduce its probability using the friend pairs technique, without affecting the boomerang probability. This enables us to effectively distinguish 5-round AES from a random permutation. The massive exchanged boomerang distinguisher achieves data and time complexity 2^{31} with a success probability of approximately 69.8%. Furthermore, the multiple exchanged boomerang distinguisher is constructed by clustering four trails with identical input and output truncated differences, enabling a lower complexity and higher success probability. It achieves data and time complexity $2^{27.1}$ with a success probability of 79.6%. All proposed distinguishers are experimentally verified.

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

1 Introduction

A block cipher is a cryptographic algorithm that encrypts data in fixed-size blocks using a secret key. It is typically constructed by repeating a round func-

tion multiple times. While increasing the number of rounds generally enhances security, it also reduces efficiency. Therefore, in order to design a block cipher that is both secure and efficient, it is crucial to analyze reduced-round variants against various attacks to estimate the minimum secure number of rounds. The designer then determines the final number of rounds by adding a security margin.

The security of a block cipher is generally evaluated by demonstrating its resistance against various known attacks, which are typically divided into two categories: distinguishing attacks and key-recovery attacks. A distinguishing attack seeks to determine whether a block cipher can be distinguished from a random permutation, and is referred to as a distinguisher. In particular, a secret-key distinguisher evaluates the randomness of the cipher under any fixed secret key.

Well-known attacks on block ciphers include differential cryptanalysis (DC) [12] and linear cryptanalysis (LC) [32]. These methods were initially introduced for the Data Encryption Standard (DES) and have since led to various extensions and improvements. As these 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 [30], impossible differential cryptanalysis [29], high-order differentials [30], boomerang attacks [39], differential-linear attacks [31], integral attacks [20], meet-in-the-middle attacks [17] and others. More recently, variants of DC have been proposed, such as subspace trail cryptanalysis [23], the yoyo trick [35,33], the multiple-of-8 property [24], mixture-differential cryptanalysis [22,4], the exchange attacks [6], and the fixed property [36].

In particular, we focus on the boomerang attack [39] first 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 in the boomerang trail under the adaptively chosen ciphertext 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, such as the amplified boomerang [28] and rectangle attack [11], were presented shortly after. To further study the dependence and connectivity between the upper and lower differentials in the boomerang attack, Dunkelman et al. proposed the sandwich attack [19]. Murphy showed that some boomerang characteristics were in fact impossible [34]. Cid et al. used the boomerang connectivity table (BCT) [14] to analyze the case where the middle round is a single s-box layer. In [16,38,40], researchers studied the case where the middle round is composed of several rounds. Yang et al. introduced the double boomerang connectivity table (DBCT) [43] and showed that the relation between neighboring rounds cannot be ignored. The truncated boomerang attack, which utilizes truncated differentials with boomerang, was presented at EUROCRYPT 2023 [8]. The exchanged boomerang attack is an attack that utilizes the mixing technique

(exchange property [6]) from the retracing boomerang attack [18,7], and it has also been utilized in the re-boomerang and boomerang chain distinguishers [42].

The Advanced Encryption Standard (AES) [15] is the most widely used block cipher and has proven its security over the past 25 years. AES was designed by Daemen and Rijmen in 1997 and standardized by NIST in 2001. Due to its security, several block ciphers with structures similar to AES have been proposed, such as SKINNY [9] and MIDORI [1]. Additionally, many tweakable block ciphers, such as KIASU-BC [26] and DEOXYS-BC [27], reuse the round function of AES in their designs. Moreover, some block ciphers incorporate reduced-round AES as a core component, such as Hound [21] and WEM [13], which use 5-round AES, and TNT-AES [2], 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 introduced by Grassi et al. at EUROCRYPT 2017 [24]. In [35], Rønjom et al. presented the 5-round and 6-round yoyo distinguishers in the adaptively chosen plaintext and ciphertext setting at ASIACRYPT 2017. However, Mondal et al. [33] later pointed out that the complexity calculation in [35] was flawed because it neglected the false positive probability of a random permutation. They subsequently corrected this error using a rigorous hypothesis testing framework based on binomial distributions, which raises the corrected complexity to $2^{29.95}$ (55% success) and $2^{30.65}$ (81% success). We adopt the same framework throughout this paper. In ASIACRYPT 2019, Bardeh et al. proposed 5-round and 6-round distinguishers, known as exchange attacks [6]. More recently, Yan et al. [41] used related differentials to improve the 5-round distinguishers and to present the first 7-round secret-key distinguisher. A key-independent secret-key distinguisher for 7-round AES was also proposed in [37]. The current secret-key distinguishers for 5-, 6-, and 7-round AES are summarized 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 introduces the fully-active-pairs approach by exploiting the property that, for all returned plaintext pairs, each diagonal is fully (all four bytes) active or fully inactive. The second, and our main result, 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, which uses plaintext pairs with one active diagonal and checks whether, in all returned plaintext pairs, each diagonal is either fully active (all four bytes) or fully inactive. The right pairs following the massive exchanged boomerang trail have at most one active byte after the first round MC, which guarantees

this property. While the probability of such an event is very high for a random permutation, we significantly reduce it by applying the friend pairs technique [10] and the exchange active inverse diagonal technique, without changing the boomerang probability. The massive exchanged boomerang distinguisher on 5-round AES requires 2^{31} data and time complexities, with a success probability of 69.8%. Although it does not outperform existing distinguishers, its significance lies in introducing a new approach for constructing boomerang distinguishers based on fully active pairs.
- We propose the multiple exchanged boomerang distinguisher, which uses plaintext pairs with one active diagonal and checks whether the returned plaintext pair is inactive in one diagonal. This distinguisher is constructed by clustering four boomerang trails that share the same input and output truncated differences, thereby enabling it to distinguish a block cipher from a random permutation with lower complexity and higher success probability. For 5-round AES, the multiple exchanged boomerang distinguisher achieves $2^{27.1}$ data and time complexities with a success probability of 79.6%.
- We provide a rigorous complexity analysis based on the hypothesis testing framework established in [33], and compare our distinguishers with the corrected complexities of the yoyo distinguisher under the same framework.

Although related-differential distinguishers achieve lower complexity than ours (Table 1), our work uses the exchanged boomerang as a secret-key distinguisher for 5-round AES. Distinguishing is a security goal in its own right, since key recovery implies distinguishability but not the converse, and a distinguisher breaks the cipher's pseudorandomness without recovering any key. Reduced-round distinguishers also quantify the security margin, since the largest number of distinguishable rounds bounds the structural security of the full cipher.

Despite the existence of a 6-round distinguisher for AES, our work focuses on the 5-round case. A similar pattern is seen in key-recovery, where attacks on 7-round AES have long been known [17], yet attacks on 5- and 6-round AES have continued to be improved in 2020 [18] and 2024 [7]. Therefore, the study of 5-round distinguishers remains important and relevant, even though a 6-round distinguisher is already known.

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 as the basis for our distinguishers and review previously proposed examples. Section 4 presents the massive exchanged boomerang distinguisher for 5-round AES. In Section 5, we detail the multiple exchanged boomerang distinguisher for 5-round AES. Finally, Section 6 concludes the paper. The source code for our experiments is publicly available at https://github.com/shb115/exchanged-boomerang-aes5.

Table 1. Summary of secret-key distinguishers for 5-, 6-, and 7-round AES. Data complexity is measured in chosen plaintexts (CP), adaptively chosen plaintexts (ACP), adaptively chosen ciphertexts (ACC), or adaptively chosen plaintexts and ciphertexts (ACPC). Time complexity is measured in the number of equivalent round-reduced 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%	[24]
Exchange	5	2^{30} CP	2^{30} E	63%	[6]
Yoyo	5	$2^{29.95}$ ACPC	$2^{29.95}$ M	55%†	[33]
Yoyo	5	$2^{30.65}$ ACPC	$2^{29.95}$ M	81%†	[33]
RD & ZD	5	$2^{27.2}$ CP	$2^{28.05}$ E	63%	[41]
RD & ZD	5	$2^{24.07}$ ACP	$2^{24.29}$ E	81%	[41]
RD & ZD	5	$2^{23.32}$ ACP	$2^{23.54}$ E	63%	[41]
Massive ex. boom.	5	2^{31} ACC	2^{31} M	69.8%†	Sect. 4
Multiple ex. boom.	5	$2^{27.1}$ ACC	$2^{27.1}$ M	79.6%†	Sect. 5
Truncated Differential	6	$2^{89.4}$ CP	$2^{96.5}$ M	95%	[3]
Exchange Attack	6	$2^{88.2}$ CP	$2^{88.2}$ E	73%	[6]
Truncated Boomerang	6	2^{87} ACC	2^{87} E	84%	[8]
Exchange Attack	6	2^{84} ACC	2^{83} E	63%	[5]
Re-boomerang	6	$2^{82.33}$ ACPC	$2^{82.33}$ E	64%	[42]
Triple Boomerangs	6	$2^{77.82}$ ACPC	$2^{77.82}$ E	66%	[42]
Boomerang Chain	6	$2^{76.57}$ ACPC	$2^{76.57}$ E	60%	[42]
RD & Exchange	7	$2^{125.6}$ CP	$2^{127.18}$ E	63%	[41]
Joint Zero-Difference	7	$2^{126.2}$ CP	$2^{126.2}$ E	77.8%†	[37]

† Success probability computed as $(\Pr[\text{AES} \to \text{AES}] + \Pr[\text{Rand} \to \text{Rand}])/2$, i.e., averaging correct identification of AES and of a random permutation; all other entries report only $\Pr[\text{AES} \to \text{AES}]$. The massive and multiple exchanged boomerang distinguishers achieve one-sided $\Pr[\text{AES} \to \text{AES}]$ of 76.9% and 65.6%, respectively.

2 Preliminaries

2.1 Description of the AES

AES [15], designed by Daemen and Rijmen in 1997, 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, respectively, for these key sizes. The internal state of AES is represented as a 4×4 array of bytes, indexed column-wise. The round function of AES consists of four operations, performed in the following order, as illustrated in Figure 1.

- *SubBytes* (SB): Applies the non-linear S-box substitution to each byte of the internal state.
- *ShiftRows* (SR): Rotates the second, third, and fourth rows to the left by 1, 2, and 3 bytes, respectively.
- *MixColumns* (MC): Multiplies each column by a fixed 4×4 Maximum Distance Separable (MDS) matrix over $\mathbb{F}_{2^8}$.
- *AddRoundKey* (AK): XORs the state with the 128-bit round key.

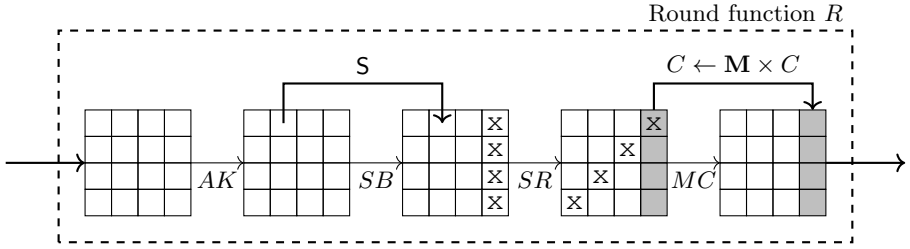


Fig. 1. Round function of AES [25]

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

The bytes of each AES state are numbered $0, 1, ..., 15$. For $0 \leq i, j \leq 3$, the j-th byte in the i-th row is numbered as $i + 4j$. We define the notions of column, diagonal, and inverse diagonal with respect to the state of AES.

- Each column consists of the sets of bytes $\{0, 1, 2, 3\}$, $\{4, 5, 6, 7\}$, $\{8, 9, 10, 11\}$, and $\{12, 13, 14, 15\}$, respectively.
- Each diagonal consists of the sets of bytes $\{0, 5, 10, 15\}$, $\{1, 6, 11, 12\}$, $\{2, 7, 8, 13\}$, and $\{3, 4, 9, 14\}$, respectively.
- Each inverse diagonal consists of 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) [12] is a statistical technique that studies how input differences propagate to output differences. A differential is defined by an input difference $\Delta_{\text{in}} \in \{0,1\}^n$ and an 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 [30] is defined by a set of input differences $\mathcal{D}_{\text{in}}$ and a set of output differences $\mathcal{D}_{\text{out}}$. We denote the existence of a truncated differential by $\mathcal{D}_{\text{in}} \xrightarrow{E} \mathcal{D}_{\text{out}}$ 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, the forward and reverse truncated differential probabilities are not equal, but they are 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 and Truncated Boomerang Attacks

In 1999, Wagner introduced the boomerang attack [39], which combines two differential trails to construct a boomerang trail, thereby covering more rounds under the adaptive chosen-ciphertext setting. In this 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. 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 exploiting 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 denote $C_i = E(P_i)$, and define $E_0(P_i) = X_i = E_1^{-1}(C_i)$ for $i \in \{1,2,3,4\}$. The boomerang procedure can then be described as follows.

1. Choose a plaintext pair (P_1, P_2) such that $P_1 \oplus P_2 = \Delta_{\text{in}}$, and obtain the corresponding ciphertexts (C_1, C_2).

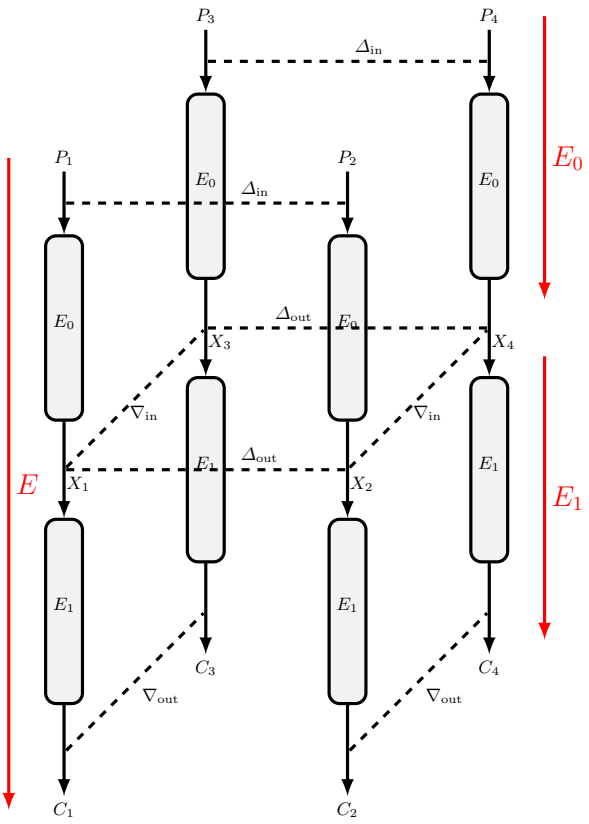


Fig. 2. Boomerang Distinguisher [25]

2. Generate $C_3 = C_1 \oplus \nabla_{\text{out}}$ and $C_4 = C_2 \oplus \nabla_{\text{out}}$, and obtain the corresponding plaintexts (P_3, P_4).
3. Check whether $P_3 \oplus P_4 = \Delta_{\text{in}}$.

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) satisfies $P_3 \oplus P_4 = \Delta_{\text{in}}$ — is given by p^2q^2. This serves as a distinguisher when p^2q^2 is significantly larger than 2^{-n}, the probability for a random permutation. The boomerang probability is $p_b = \Pr[P_3 \oplus P_4 = \Delta_{\text{in}}] \geq p^2q^2$.

In EUROCRYPT 2023, Bariant et al. extended the boomerang framework by replacing all differential trails with truncated differential trails, thereby introducing the truncated boomerang attack [8]. The truncated boomerang attacks use structures on both plaintext and ciphertext sides, which leads to a significant reduction in complexity.

For the upper part E_0, there exist truncated differential trails $\mathcal{D}^0_{\text{in}} \xrightarrow{E_0} \mathcal{D}^0_{\text{out}}$ with probability $\overrightarrow{p}$ and $\mathcal{D}^0_{\text{out}} \xrightarrow{E_0^{-1}} \mathcal{D}^0_{\text{in}}$ 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 follows the same quartet procedure as the boomerang attack, with each single difference replaced by a truncated difference set.

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) satisfies $P_3 \oplus P_4 \in \mathcal{D}_{\text{in}}^0$ is given by

$$p_b = \overrightarrow{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r,$$

where

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

This serves as a distinguisher when $\overrightarrow{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r$ is significantly greater than 2^{-n}, the corresponding probability for a random permutation.

3 Exchanged Boomerang Attack on 5-round AES

3.1 Overview of Exchanged Boomerang Attack on 5-round AES

The works in [35,18,42] applied the exchange technique to design a new boomerang attack on reduced-round AES, which we refer to as the exchanged boomerang attack. This attack can be regarded as a single execution of the yoyo game introduced in [35], and is also equivalent to the mixing retracing boomerang described in [18]. In particular, Dunkelman et al. demonstrated a key-recovery attack on 5-round AES using the mixing retracing boomerang [18], while Yan et al. proposed a distinguisher for 6-round AES based on the boomerang chain derived from the exchanged boomerang [42].

The exchanged boomerang attack employs truncated differential trails in the forward characteristic, and differential trails in the backward characteristic. Consequently, it can exploit structures on the plaintext side, but not on the ciphertext side. The main idea of the exchanged boomerang on AES is to define a swap operation on some active inverse diagonals. We obtain the new ciphertext pair (C_3, C_4) by swapping the values of C_1 and C_2 only at the positions corresponding to some of the active inverse diagonals. That is, for these certain positions, C_3 takes the value of C_2 and C_4 takes the value of C_1, whereas for all other positions, C_3 retains the value of C_1 and C_4 retains the value of C_2.

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

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

corresponds to the upper 2.5 rounds, up to MC operation in the third round, and

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

corresponds to the final 2 rounds.

Let (P_1, P_2) denote 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). Furthermore, 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. This property can be exploited 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 evaluate to 1. Hence, for 5-round AES, if a plaintext structure is constructed with a single active diagonal and the returned ciphertext pair is generated by swapping the values of C_1 and C_2 on a certain active inverse diagonal, the resulting boomerang probability simplifies to

$$\overrightarrow{p} \cdot \overleftarrow{p}.$$

3.2 Example of Exchanged Boomerang Attack on 5-round AES

As an example, we introduce a key-recovery attack on 5-round AES, which is based on a single execution of the yoyo game described in [35]. It is worth noting the terminological distinction between our approach and the yoyo attack. The yoyo attack typically involves an adaptive game with multiple rounds of encryption and decryption (a ping-pong behavior). In contrast, the exchanged boomerang attack operates within a standard boomerang framework involving a single encryption-decryption sequence. Therefore, to emphasize this structural difference, we use the term exchanged boomerang.

In this attack, a plaintext structure with one active diagonal is used, and a certain inverse diagonal is selected on the ciphertext side for the swap operation. The attack exploits 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 the new ciphertext pair (C_3, C_4) generated by swapping the values of C_1 and C_2 only at the position corresponding to the certain active inverse diagonal, is inactive in the l-th diagonal after the first round MC with probability 1. By exploiting this property with multiple plaintext pairs, all keys for which the l-th diagonal is

not inactive after the first round MC can be discarded, leaving only the correct key. 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 obtain the corresponding (C_1, C_2).
2. Generate four pairs (C_3^j, C_4^j) by exchanging each of the four inverse diagonals, and obtain 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, defined as a pair with one inactive byte after the first round MC, occurs 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 4 in Appendix A. Each right forward pair yields exactly one correct key, whereas a wrong pair produces on average $2^{32-40} = 2^{-8}$ key candidates. Hence, the correct key can be recovered.

The previously introduced example of the exchanged boomerang has been applied for key-recovery attacks, whereas our objective is to construct a distinguisher by analyzing the pattern of the returned plaintext pairs. Since the exchanged boomerang enables the construction of one of the most efficient key-recovery attacks on 5-round AES [18], we argue that it can also serve as the basis for a low-complexity distinguisher for 5-round AES. Furthermore, because the exchanged boomerang satisfies $\overleftarrow{q} = 1$ and $r = 1$, we focus on the boomerang probability $p_b = \overrightarrow{p} \cdot \overleftarrow{p}$, and propose two distinguishers based on this property.

4 Massive Exchanged Boomerang Distinguisher

In this section, we propose the massive exchanged boomerang distinguisher, which distinguishes 5-round AES from a random permutation by exploiting the structural properties of returned plaintext pairs in the boomerang framework. The key idea is that, after the boomerang process, every diagonal of all returned plaintext pairs is either fully active or fully inactive. A diagonal is fully active if all four bytes have non-zero differences, and fully inactive if all four bytes have zero differences.

Even when a massive number of friend pairs are used, the boomerang probability for 5-round AES remains unchanged. In contrast, for a random permutation, the probability that all returned pairs are fully active or fully inactive in every diagonal decreases rapidly as the number of pairs increases. Consequently, once the number of friend pairs exceeds a certain threshold, the probability in 5-round AES becomes significantly higher than that in a random permutation, thereby enabling us to distinguish 5-round AES from a random permutation.

The intuition comes from the MDS property of the MC operation and its inverse (MC^{-1}). If, after the first round MC, a column of a returned pair has at most one active byte, then the column necessarily becomes either fully active

or fully inactive. A single active byte is expanded into four by MC^{-1}, whereas entirely inactive columns remain inactive. Hence, each column is either fully active or fully inactive, which forms the basis of the distinguisher.

Formally, in the upper trail E_0, the input truncated difference $\mathcal{D}_{\text{in}}$ activates only the 0th diagonal. After the first round MC, (P_1, P_2) has only one active byte in a column, while the other three bytes remain inactive. In this case, the corresponding inverse diagonal of $\mathcal{D}_{\text{out}}$ becomes active. For the returned plaintexts, $\mathcal{D}'_{\text{in}}$ ensures that every diagonal is either fully active or fully inactive. The forward probability of this transition is

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

whereas the backward trail holds with probability 1:

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

Hence the overall boomerang probability is determined by the forward transition.

In the lower trail E_1, one inverse diagonal of a ciphertext pair (C_1, C_2) is exchanged to generate (C_3^j, C_4^j) for $j \in \{0, 1, 2, 3\}$. Let X denote the intermediate state, defined as $X = E_0(P) = E_1^{-1}(C)$. Since the swap operation is performed only on the active inverse diagonal, it follows that

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

and therefore the exchanged boomerang trail preserves the same probability 2^{-22}. Figure 5 in Appendix B illustrates this structure, where white, gray, and hatched boxes denote inactive, truncated, and exchanged bytes, respectively, while red, orange, green, and blue boxes indicate diagonals that are either fully active or fully inactive.

We now analyze the probability for a random permutation, denoted p_{rand}. For a random permutation, a diagonal is fully active with probability $(1-2^{-8})^4$ and fully inactive with probability 2^{-32}. Thus the probability that a diagonal is either fully active or fully inactive is $(1-2^{-8})^4 + 2^{-32}$, and for all four diagonals this is approximately $2^{-0.09}$. This is much higher than the target threshold 2^{-22}. To reduce it, we first note that four returned plaintext pairs can be generated by exchanging each inverse diagonal in the ciphertext pairs. All four must simultaneously be either fully active or fully inactive, which reduces the probability to about $2^{-0.36}$. Although smaller, this is still insufficient. In contrast, for 5-round AES, since all returned pairs of a right pair following the massive exchanged boomerang trail are fully active or fully inactive with probability 1, the overall boomerang probability remains 2^{-22}.

A second reduction is achieved by employing friend pairs [10]. By definition, friend pairs (P_1, P_2) and (P'_1, P'_2) share the same values in the active diagonal but differ in the constants on the inactive diagonals. If (P_1, P_2) is a right pair, then its friend pair also has only one active byte after the first round MC, and therefore it is always a right pair as well. Consequently, all their returned pairs

are either fully active or fully inactive with the same boomerang probability 2^{-22}, whereas the random probability decreases exponentially. With 2^6 friend pairs, the probability that all returned pairs are either fully active or fully inactive becomes approximately $2^{-23.1}$, which is finally below 2^{-22}. This gap between the probability for 5-round AES and the random probability forms the basis of the distinguisher.

On average, 2^{22} plaintext pairs are required to obtain one right pair. Using a plaintext structure of size $2^{11.5}$, where only the 0th diagonal varies while the remaining bytes are fixed constants, we can generate 2^{22} plaintext pairs. For each of the 2^{22} plaintext pairs, 2^6 friend pairs are constructed. Since a right pair and all of its friend pairs follow the massive exchanged boomerang trail, all returned pairs for each pair are either fully active or fully inactive in each diagonal. In contrast, all returned pairs of a wrong pair and its friend pairs are randomly either fully active or fully inactive in each diagonal with a probability of $2^{-23.1}$. Therefore, the expected number of pairs such that the pair and all of its friend pairs are either fully active or fully inactive in every diagonal is

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

for 5-round AES, while for a random permutation it is

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

Therefore, if there exists a plaintext pair together with its friend pairs such that all generated returned plaintext pairs are either fully active or fully inactive in every diagonal, we output 5-round AES; otherwise, we output a random permutation. This criterion allows us to distinguish 5-round AES from a random permutation. The massive exchanged boomerang distinguisher for 5-round AES is described below, and the corresponding pseudocode is provided in Algorithm 1.

1. Choose a plaintext structure of size $2^{11.5}$ where the four bytes in the 0th diagonal vary freely, while the other bytes are fixed constants.
2. For each plaintext pair (P_1, P_2), generate friend pairs (P_1', P_2') that share the same 0th diagonal but differ in constants of the inactive diagonals, and obtain the corresponding ciphertexts.
3. For each $j \in \{0, 1, 2, 3\}$, exchange the j-th inverse diagonal of ciphertext pair (C_1, C_2) to obtain (C_3^j, C_4^j) and then decrypt (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), together with those of its friend pairs, are either fully active or fully inactive in every diagonal, then we output 5-round AES; otherwise, we output a random permutation.

Complexity

In step 1, $2^{11.5}$ chosen plaintexts are required. In step 2, we generate $2^{22} \cdot 2^6 = 2^{28}$ plaintext pairs, which correspond to $2^{28} \cdot 2 = 2^{29}$ chosen plaintexts. In step 3,

Algorithm 1 Massive exchanged boomerang distinguisher for 5-round AES

1: Encrypt a plaintext structure of size $2^{11.5}$, where the four bytes in the 0th diagonal are active and the other bytes are fixed constants
2: **for** each plaintext pair **do**
3: Encrypt the pair together with its 2^6 friend pairs, which share the same 0th diagonal but differ in the constants of the other diagonals
4: **for** each ciphertext pair **do**
5: Exchange the j-th inverse diagonal of (C_1, C_2) to obtain four ciphertext pairs (C_3, C_4) for $j \in \{0, 1, 2, 3\}$
6: Decrypt the four pairs (C_3, C_4) to obtain four pairs (P_3, P_4)
7: **end for**
8: **if** all returned pairs are either fully inactive or fully active in every diagonal **then**
9: **return** 5-round AES
10: **end if**
11: **end for**
12: **return** random permutation

we generate $2^{28} \cdot 4 = 2^{30}$ ciphertext pairs, which correspond to $2^{30} \cdot 2 = 2^{31}$ adaptive chosen ciphertexts. Therefore, the data complexity of the distinguishing process is 2^{31} adaptive chosen ciphertexts, and the time complexity is 2^{31} memory accesses.

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

Success Probability

The success probability of the massive exchanged boomerang distinguisher is defined as the average of the probability that the distinguisher outputs 5-round AES when the black box is indeed 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 analyzed using the binomial distribution. For $n = 2^{22}$ independent trials, let $K \sim \text{Binomial}(n, p)$ denote the number of pairs whose returned pairs are fully active or fully inactive in every diagonal when the black box is a 5-round AES with success probability $p = 2^{-22} + 2^{-23.1}$. Similarly, let $K' \sim \text{Binomial}(n, q)$ with $q = 2^{-23.1}$ denote the corresponding number for a random permutation. The distinguisher outputs 5-round AES if $K \geq 1$, and outputs random otherwise. Therefore, the overall success probability is

$$P_{\text{succ}} = \tfrac{1}{2}\big[\Pr(K \geq 1) + \Pr(K' = 0)\big] = \tfrac{1}{2}\Big[1 - (1-p)^n + (1-q)^n\Big] \approx 0.698.$$

The decision rule $K \geq 1$ is the discrete form of the midpoint-threshold criterion $t = (p+q)/2$, whose count threshold $nt \approx 0.967$ rounds to 1 for $n = 2^{22}$.

Experimental Verification

Throughout our experiments, we use the full 10-round AES as the random permutation, since no secret-key distinguisher for AES is known beyond 7 rounds. To verify the massive exchanged boomerang distinguisher, we first count the number of plaintext 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 fully inactive in every diagonal. We conducted 1000 experiments for each case and observed that, for 5-round AES, the average number of such pairs is 1.464, while for the random permutation (10-round AES), the average is 0.433, which is close to the theoretical expectation.

Additionally, to experimentally verify the success probability of the distinguisher, we counted the number of cases in which the distinguisher outputs 5-round AES when the black box is 5-round AES, and the number of cases in which it outputs a random permutation when the black box is a random permutation. As in the previous experiment, we conducted 1000 independent trials for both 5-round AES and the random permutation (10-round AES). The results showed that, when the black box was 5-round AES, the distinguisher output 5-round AES 780 times, and when the black box was a random permutation, it output a random permutation 652 times. Therefore, the experimental success probability is

$$(0.780 + 0.652)/2 = 0.716,$$

which is close to the theoretical probability. Both experiments are summarized in Table 2.

Table 2. Experimental verification of the massive exchanged boomerang distinguisher for 5-round AES (1000 trials each)

Primitive	Detected pairs (exp./theo.)	Output (5R / Rand.)	Succ.
5-round AES	1.464 / 1.46	780 / 220	0.716
Rand. Perm.	0.433 / 0.46	348 / 652	

5 Multiple Exchanged Boomerang Distinguisher

In this section, we propose the multiple exchanged boomerang distinguisher, which leverages multiple exchanged boomerang trails sharing the same input truncated differences. It distinguishes the block cipher from a random permutation by verifying whether the returned plaintext pair is inactive in a diagonal. To increase the overall boomerang probability, we cluster four exchanged boomerang trails.

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

exchanged boomerang distinguisher algorithm, followed by an analysis of its complexity and success probability. Finally, we provide experimentally verified data.

The idea of the multiple exchanged boomerang distinguisher is to exploit multiple exchanged boomerang trails that share the same input truncated differences, $\mathcal{D}_{\text{in}}$ and $\mathcal{D}'_{\text{in}}$. We found four such trails, which we cluster to raise the overall boomerang probability above the random probability.

We introduce the multiple exchanged boomerang trails. The multiple exchanged boomerang distinguisher employs four exchanged boomerang trails that share 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, as in the massive exchanged boomerang trail, while the truncated difference for returned plaintext pairs $\mathcal{D}'_{\text{in}}$ is inactive in a diagonal. We denote 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 $\mathcal{D}^4_{\text{out}}$.

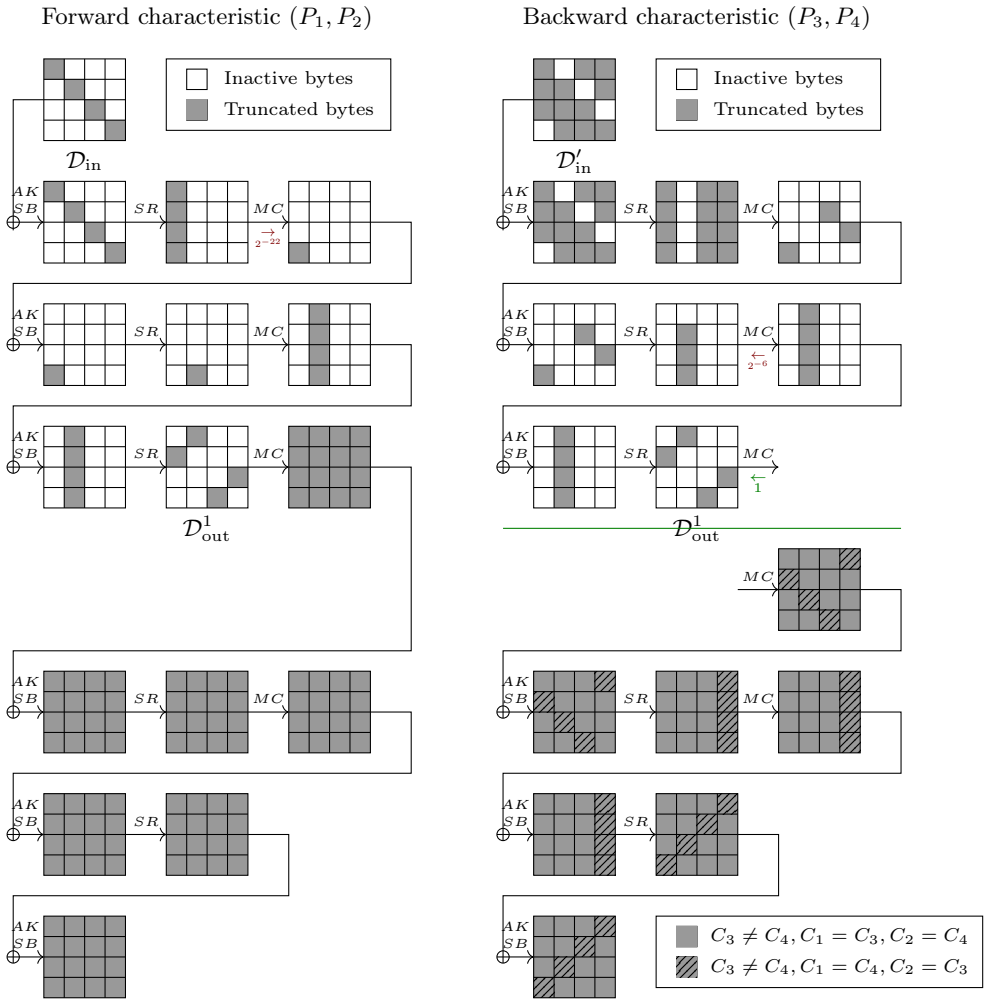
The four trails share the same $\mathcal{D}_{\text{in}}$ and $\mathcal{D}'_{\text{in}}$, differing only in $\mathcal{D}^i_{\text{out}}$, which is active in i inverse diagonals for $i \in \{1, 2, 3, 4\}$. The forward transition $\mathcal{D}_{\text{in}} \xrightarrow{E_0} \mathcal{D}^i_{\text{out}}$ corresponds to the probability that exactly $4-i$ bytes are inactive after the first-round MC, and the backward transition $\mathcal{D}^i_{\text{out}} \xrightarrow{E_0^{-1}} \mathcal{D}'_{\text{in}}$ to the probability that one inverse diagonal becomes inactive before the second-round MC, which requires i bytes to be inactive. Explicitly, $\overrightarrow{p}(i) = \binom{4}{4-i}2^{-8(4-i)}$ and $\overleftarrow{p}(i) = \binom{4}{1}2^{-8i} = 4 \cdot 2^{-8i}$, where the factor $\binom{4}{1} = 4$ counts the choice of which of the four diagonals of the returned pair becomes inactive, the same factor as in the random probability $4 \cdot 2^{-32}$. For example, trail 2 gives $\overrightarrow{p}(2) = \binom{4}{2}2^{-16} = 2^{-13.4}$ and $\overleftarrow{p}(2) = 4 \cdot 2^{-16} = 2^{-14}$. The resulting forward, backward, and trail probabilities are listed in Table 3. Trail 1 is illustrated in Figure 3, and trails 2–4 in Appendix C.

Table 3. Approximate forward, backward, and overall probabilities of the four exchanged boomerang trails

Trail i	$\overrightarrow{p}$	$\overleftarrow{p}$	$\overrightarrow{p} \cdot \overleftarrow{p}$
1	2^{-22}	2^{-6}	2^{-28}
2	$2^{-13.4}$	2^{-14}	$2^{-27.4}$
3	2^{-6}	2^{-22}	2^{-28}
4	1	2^{-30}	2^{-30}

By clustering four exchanged boomerang trails that share the same $\mathcal{D}_{\text{in}}$ and $\mathcal{D}'_{\text{in}}$, the overall probability of the multiple exchanged boomerang becomes

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



Parameters for the boomerang trail: $\overrightarrow{p} = 2^{-22}$, $\overleftarrow{p} \approx 2^{-6}$, $\overleftarrow{q} = 1$, $p_b \approx 2^{-28}$, $p_{\text{rand}} = 2^{-30}$

Fig. 3. First exchanged boomerang trail

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

We need $2^{26.1}$ pairs to obtain one right pair on average. Since four additional ciphertext pairs can be generated by exchanging the active inverse diagonal in the ciphertext pairs, only $2^{24.1}$ plaintext pairs are required. Using a plaintext structure of size $2^{12.55}$, in which the four bytes in the 0th diagonal can take arbitrary values while the remaining bytes are fixed to 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. In contrast, 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 whose returned plaintext pair is inactive in one diagonal, we output 5-round AES; otherwise, we output a random permutation. This criterion allows us to distinguish 5-round AES from a random permutation. The multiple exchanged boomerang distinguisher for 5-round AES is described below, and the corresponding 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 arbitrary values while the other bytes are fixed constants, and obtain the corresponding ciphertexts.
2. For each $j \in \{0, 1, 2, 3\}$, exchange the j-th active inverse diagonal of the ciphertext pair (C_1, C_2) to obtain (C_3, C_4) and decrypt (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 diagonal, the distinguisher outputs 5-round AES; otherwise, it outputs a random permutation.

Complexity

In step 1, $2^{12.55}$ chosen plaintexts are required. In step 2, we generate $2^{24.1} \cdot 4 = 2^{26.1}$ ciphertext pairs, which corresponds to $2^{26.1} \cdot 2 = 2^{27.1}$ adaptive chosen ciphertexts. Therefore, the data complexity of the 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: $2^{27.1}$ memory accesses

Algorithm 2 Multiple exchanged boomerang distinguisher for 5-round AES

1: Encrypt a plaintext structure of size $2^{12.55}$ in which the four bytes in the 0th diagonal can take arbitrary values while the other bytes are fixed constants, and obtain the corresponding ciphertexts
2: **for** each ciphertext pair (C_1, C_2) **do**
3: Exchange the j-th active inverse diagonal of (C_1, C_2) to obtain four pairs (C_3, C_4) for $j \in \{0, 1, 2, 3\}$
4: Decrypt four pairs (C_3, C_4) to obtain four pairs (P_3, P_4)
5: **if** there exists a returned pair (P_3, P_4) that is inactive in one diagonal **then**
6: **return** 5-round AES
7: **end if**
8: **end for**
9: **return** random permutation

Success Probability

The success probability can be analyzed within the same binomial framework as the massive exchanged boomerang distinguisher. For $n = 2^{26.1}$ trials, let $K \sim \text{Binomial}(n, p)$ with $p = 2^{-26.1} + 2^{-30}$ under 5-round AES, and let $K' \sim \text{Binomial}(n, q)$ with $q = 2^{-30}$ under a random permutation. Applying the midpoint rule with threshold $t = (p+q)/2$ yields a cutoff $nt \approx 0.567$, so the effective integer threshold is 1. The resulting success probability is

$$P_{\text{succ}} = \tfrac{1}{2}\big[1 - (1-p)^n + (1-q)^n\big] \approx 0.796.$$

Increasing n makes the success probability approach 1.

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 observed that, for 5-round AES, the average number of such pairs is 1.017, while for a random permutation (10-round AES), it is 0.058, which is consistent with the theoretical expectation.

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 it outputs a random permutation when the black box is a random permutation. As in the previous experiment, we conducted 1000 trials 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 output 5-round AES 637 times, and when the black box was a random permutation, it output a random permutation 932 times. Therefore, the experimental success probability is $(0.637 + 0.932)/2 = 0.7845$, which is close to the theoretical probability. Both experiments are summarized in Table 4.

Table 4. Experimental verification of the multiple exchanged boomerang distinguisher for 5-round AES (1000 trials each)

Primitive	Detected pairs (exp./theo.)	Output (5R / Rand.)	Succ.
5-round AES	1.017 / 1.066	637 / 363	0.7845
Rand. Perm.	0.058 / 0.066	68 / 932	

6 Conclusion

In this paper, we proposed the massive exchanged boomerang and multiple exchanged boomerang distinguishers for 5-round AES, utilizing the friend pairs technique and multiple trails, respectively. The massive exchanged boomerang distinguisher for 5-round AES has data and time complexities of 2^{31} and a success probability of 69.8%. The multiple exchanged boomerang distinguisher for 5-round AES has data and time complexities of $2^{27.1}$ and a success probability of 79.6%.

We analyzed our distinguishers under the rigorous hypothesis-testing framework of [33] and verified them experimentally. Because our techniques rely on the MDS MixColumns of AES, they transfer to ciphers that reuse the AES round function, such as Deoxys-BC [27] and KIASU-BC [26]; we leave their concrete instantiation as future work.

The two distinguishers we proposed 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 [18] is more effective. For 6-round key-recovery attacks, the exchanged boomerang trails from [7] are more suitable. Furthermore, when considering 6-round distinguishers, the exchanged boomerang trail employed in the boomerang chain distinguisher from [42] is also more effective. Nevertheless, our focus was on secret-key distinguishers for 5-round AES. Moreover, since several ciphers are designed on the basis of 5-round AES, 5-round distinguishers remain important even in the presence of 6- and 7-round distinguishers.

Acknowledgments. This work was supported in part by the Institute of Information Communications Technology Planning and Evaluation (IITP) Grant funded by the Korea Government (MSIT) under Grant RS-2023-00229028.

References

1. Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., Regazzoni, F.: Midori: A block cipher for low energy. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 411–436. Springer (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: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 641–673. Springer (2020). https://doi.org/10.1007/978-3-030-45724-2_22
3. Bao, Z., Guo, J., List, E.: Extended truncated-differential distinguishers on round-reduced aes. Cryptology ePrint Archive (2019), https://eprint.iacr.org/2019/622
4. 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. Journal of Cryptology **33**(3), 1003–1043 (2020). https://doi.org/10.1007/s00145-019-09336-w
5. Bardeh, N.G.: A key-independent distinguisher for 6-round aes in an adaptive setting. Cryptology ePrint Archive (2019), https://eprint.iacr.org/2019/945
6. Bardeh, N.G., Rønjom, S.: The exchange attack: How to distinguish six rounds of aes with chosen plaintexts. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 347–370. Springer (2019). https://doi.org/10.1007/978-3-030-34618-8_12
7. Bariant, A., Dunkelman, O., Keller, N., Leurent, G., Mollimard, V.: Improved boomerang attacks on 6-round aes. Cryptology ePrint Archive (2024), https://eprint.iacr.org/2024/977
8. Bariant, A., Leurent, G.: Truncated boomerang attacks and application to aes-based ciphers. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 3–35. Springer (2023). https://doi.org/10.1007/978-3-031-30634-1_1
9. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The skinny family of block ciphers and its low-latency variant mantis. In: Annual international cryptology conference. pp. 123–153. Springer (2016). https://doi.org/10.1007/978-3-662-53008-5_5
10. Beierle, C., Leander, G., Todo, Y.: Improved differential-linear attacks with applications to arx ciphers. In: Annual International Cryptology Conference. pp. 329–358. Springer (2020). https://doi.org/10.1007/978-3-030-56877-1_12
11. Biham, E., Dunkelman, O., Keller, N.: The rectangle attack—rectangling the serpent. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 340–357. Springer (2001). https://doi.org/10.1007/3-540-44706-7_6
12. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. Journal of CRYPTOLOGY **4**(1), 3–72 (1991). https://doi.org/10.1007/BF00630563
13. 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: Cryptographers' Track at the RSA Conference. pp. 293–308. Springer (2017). https://doi.org/10.1007/978-3-319-52153-4_17
14. Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: Boomerang connectivity table: A new cryptanalysis tool. In: Annual international conference on the theory and applications of cryptographic techniques. pp. 683–714. Springer (2018). https://doi.org/10.1007/978-3-319-78375-8_22
15. Daemen, J., Rijmen, V.: The design of Rijndael, vol. 2. Springer, New York (2002). https://doi.org/10.1007/978-3-662-60769-5
16. Delaune, S., Derbez, P., Vavrille, M.: Catching the fastest boomerangs: Application to skinny. IACR Transactions on Symmetric Cryptology pp. 104–129 (2020). https://doi.org/10.46586/tosc.v2020.i4.104-129

17. Derbez, P., Fouque, P.A., Jean, J.: Improved key recovery attacks on reduced-round aes in the single-key setting. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 371–387. Springer (2013). https://doi.org/10.1007/978-3-642-38348-9_23
18. Dunkelman, O., Keller, N., Ronen, E., Shamir, A.: The retracing boomerang attack. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 280–309. Springer (2020). https://doi.org/10.1007/978-3-030-45721-1_11
19. Dunkelman, O., Keller, N., Shamir, A.: A practical-time related-key attack on the kasumi cryptosystem used in gsm and 3g telephony. In: Annual cryptology conference. pp. 393–410. Springer (2010). https://doi.org/10.1007/978-3-642-14623-7_21
20. Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D., Whiting, D.: Improved cryptanalysis of rijndael. In: International Workshop on Fast Software Encryption. pp. 213–230. Springer (2000). https://doi.org/10.1007/3-540-44706-7_15
21. Fouque, P.A., Karpman, P., Kirchner, P., Minaud, B.: Efficient and provable white-box primitives. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 159–188. Springer (2016). https://doi.org/10.1007/978-3-662-53887-6_6
22. Grassi, L.: Mixture differential cryptanalysis: a new approach to distinguishers and attacks on round-reduced aes. IACR Transactions on Symmetric Cryptology pp. 133–160 (2018). https://doi.org/10.13154/tosc.v2018.i2.133-160
23. Grassi, L., Rechberger, C., Rønjom, S.: Subspace trail cryptanalysis and its applications to aes. Cryptology ePrint Archive (2016), https://eprint.iacr.org/2016/592
24. Grassi, L., Rechberger, C., Rønjom, S.: A new structural-differential property of 5-round aes. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 289–317. Springer (2017). https://doi.org/10.1007/978-3-319-56614-6_10
25. Jean, J.: Tikz for cryptographers (2016)
26. Jean, J., Nikolic, I., Peyrin, T.: Kiasu v1. Submitted to the CAESAR competition pp. 43–45 (2014)
27. Jean, J., Nikolić, I., Peyrin, T., Seurin, Y.: The deoxys aead family. Journal of Cryptology **34**(3), 31 (2021). https://doi.org/10.1007/s00145-021-09397-w
28. Kelsey, J., Kohno, T., Schneier, B.: Amplified boomerang attacks against reduced-round mars and serpent. In: International Workshop on Fast Software Encryption. pp. 75–93. Springer (2000). https://doi.org/10.1007/3-540-44706-7_6
29. Knudsen, L.: Deal-a 128-bit block cipher. complexity **258**(2), 216 (1998)
30. Knudsen, L.R.: Truncated and higher order differentials. In: International Workshop on Fast Software Encryption. pp. 196–211. Springer (1994). https://doi.org/10.1007/3-540-60590-8_16
31. Langford, S.K., Hellman, M.E.: Differential-linear cryptanalysis. In: Annual International Cryptology Conference. pp. 17–25. Springer (1994). https://doi.org/10.1007/3-540-48658-5_3
32. Matsui, M.: Linear cryptanalysis method for des cipher. In: Workshop on the Theory and Application of of Cryptographic Techniques. pp. 386–397. Springer (1993). https://doi.org/10.1007/3-540-48285-7_33
33. 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

34. 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
35. Rønjom, S., Bardeh, N.G., Helleseth, T.: Yoyo tricks with aes. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 217–243. Springer (2017). https://doi.org/10.1007/978-3-319-70694-8_8
36. Shin, H., Kim, I., Kim, S., Kim, S., Hong, D., Sung, J., Hong, S.: Revisiting the multiple-of property for skinny: The exact computation of the number of right pairs. IEEE Access **12**, 35502–35511 (2024). https://doi.org/10.1109/ACCESS.2024.3371712
37. Shin, H., Kim, S., Seok, B., Hong, D., Sung, J., Hong, S., Lee, S., Lee, D.: Key-independent secret-key distinguisher for 7-round AES based on the joint generalized zero-difference property. Cryptology ePrint Archive, Paper 2026/980 (2026), https://eprint.iacr.org/2026/980
38. Song, L., Qin, X., Hu, L.: Boomerang connectivity table revisited. application to skinny and aes. IACR Transactions on Symmetric Cryptology pp. 118–141 (2019). https://doi.org/10.13154/tosc.v2019.i1.118-141
39. Wagner, D.: The boomerang attack. In: International Workshop on Fast Software Encryption. pp. 156–170. Springer (1999). https://doi.org/10.1007/3-540-48519-8_12
40. Wang, H., Peyrin, T.: Boomerang switch in multiple rounds. application to aes variants and deoxys. IACR Transactions on Symmetric Cryptology pp. 142–169 (2019). https://doi.org/10.13154/tosc.v2019.i1.142-169
41. Yan, X., Tan, L., Qi, W.: Related-differential distinguishers on up to 7 rounds of AES. Cryptology ePrint Archive, Paper 2026/1039 (2026), https://eprint.iacr.org/2026/1039
42. Yan, X., Tan, L., Xu, H., Qi, W.: The boomerang chain distinguishers: New record for 6-round aes. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 301–329. Springer (2024). https://doi.org/10.1007/978-981-96-0941-3_10
43. Yang, Q., Song, L., Sun, S., Shi, D., Hu, L.: New properties of the double boomerang connectivity table. IACR Transactions on Symmetric Cryptology pp. 208–242 (2022). https://doi.org/10.46586/tosc.v2022.i4.208-242

A Trail for the Exchanged Boomerang Example

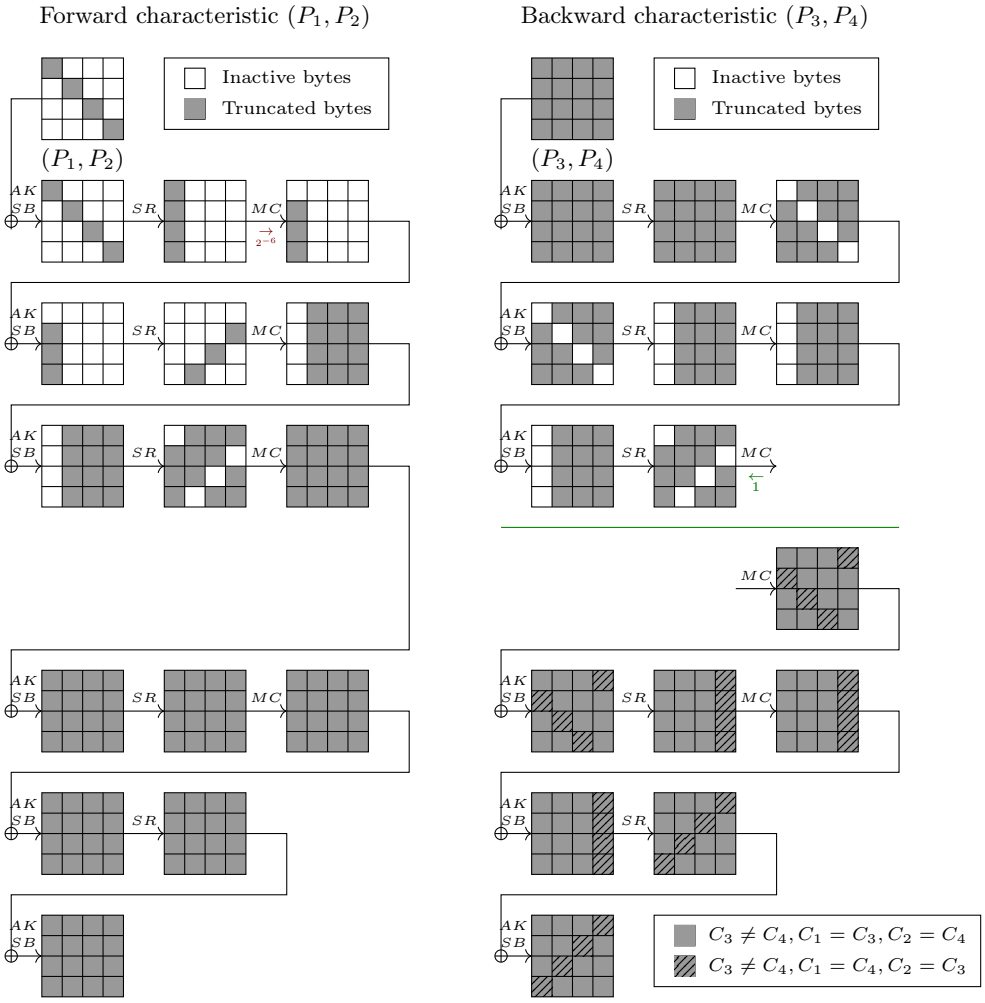
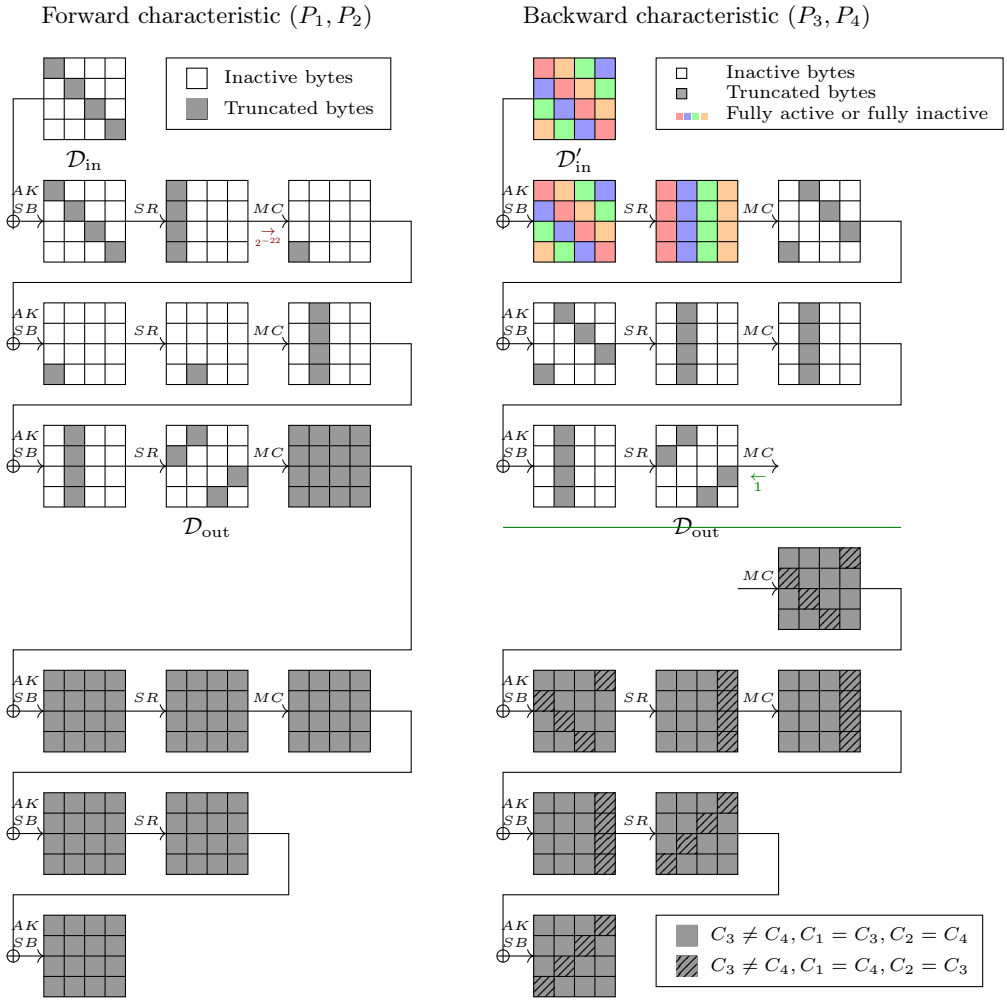


Fig. 4. Example of Exchanged Boomerang Trail

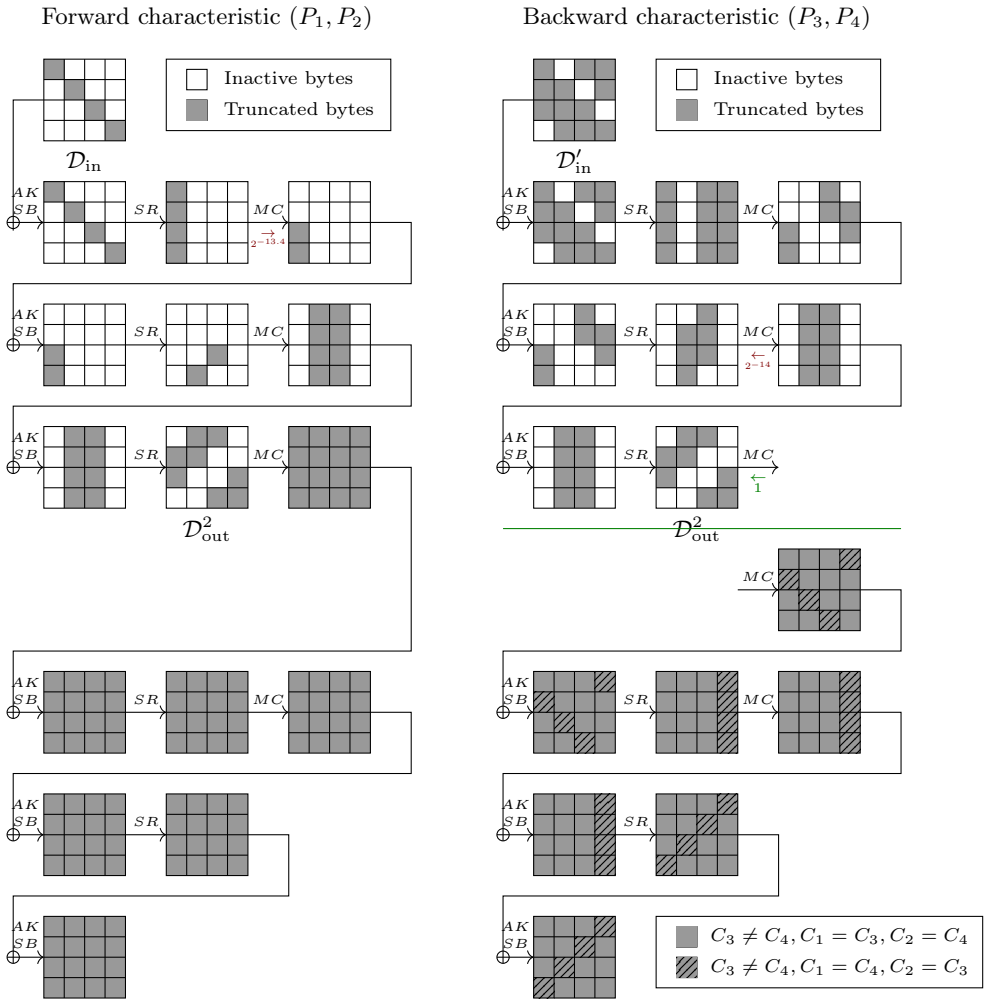
B Massive Exchanged Boomerang Trail



Parameters for the boomerang trail: $\overrightarrow{p} = 2^{-22}$, $\overleftarrow{p} = 1$, $\overleftarrow{q} = 1$, $p_b = 2^{-22}$, $p_{\text{rand}} \approx 2^{-0.09}$

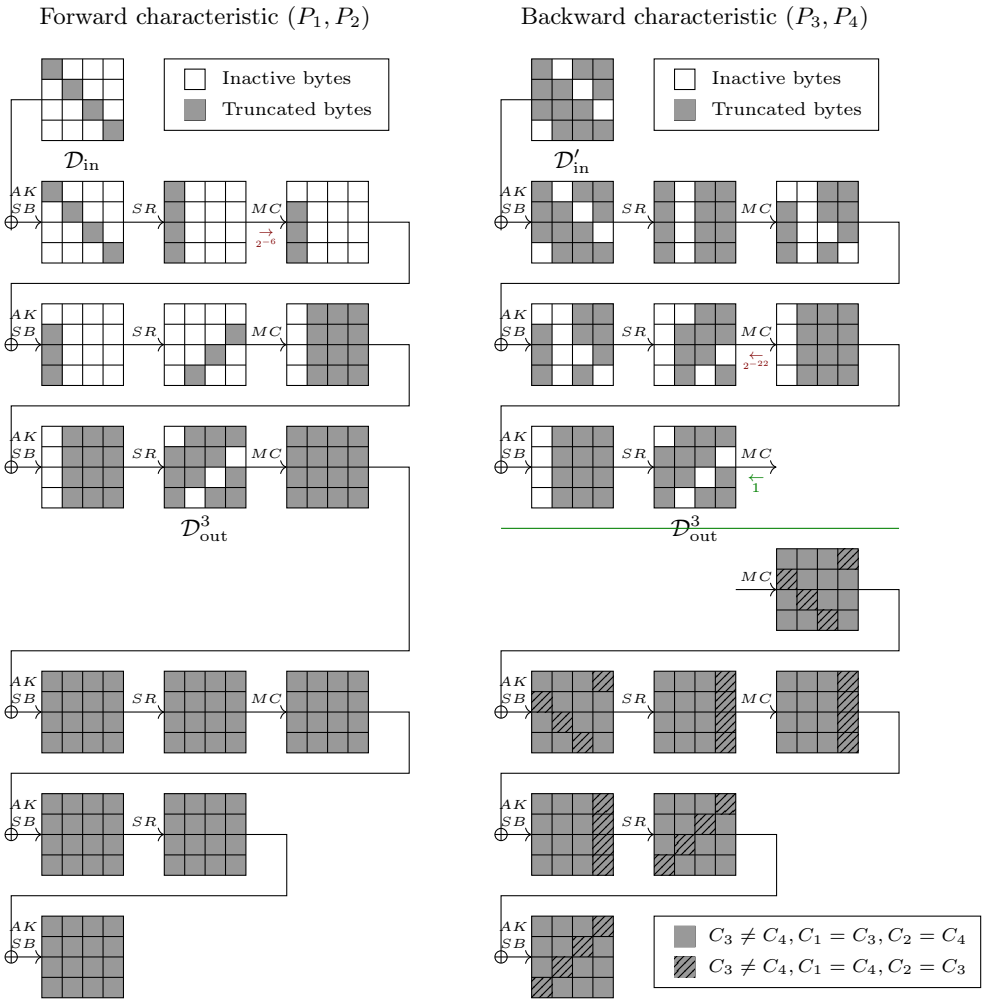
Fig. 5. Massive exchanged boomerang trail

C Additional Trails of the Multiple Exchanged Boomerang



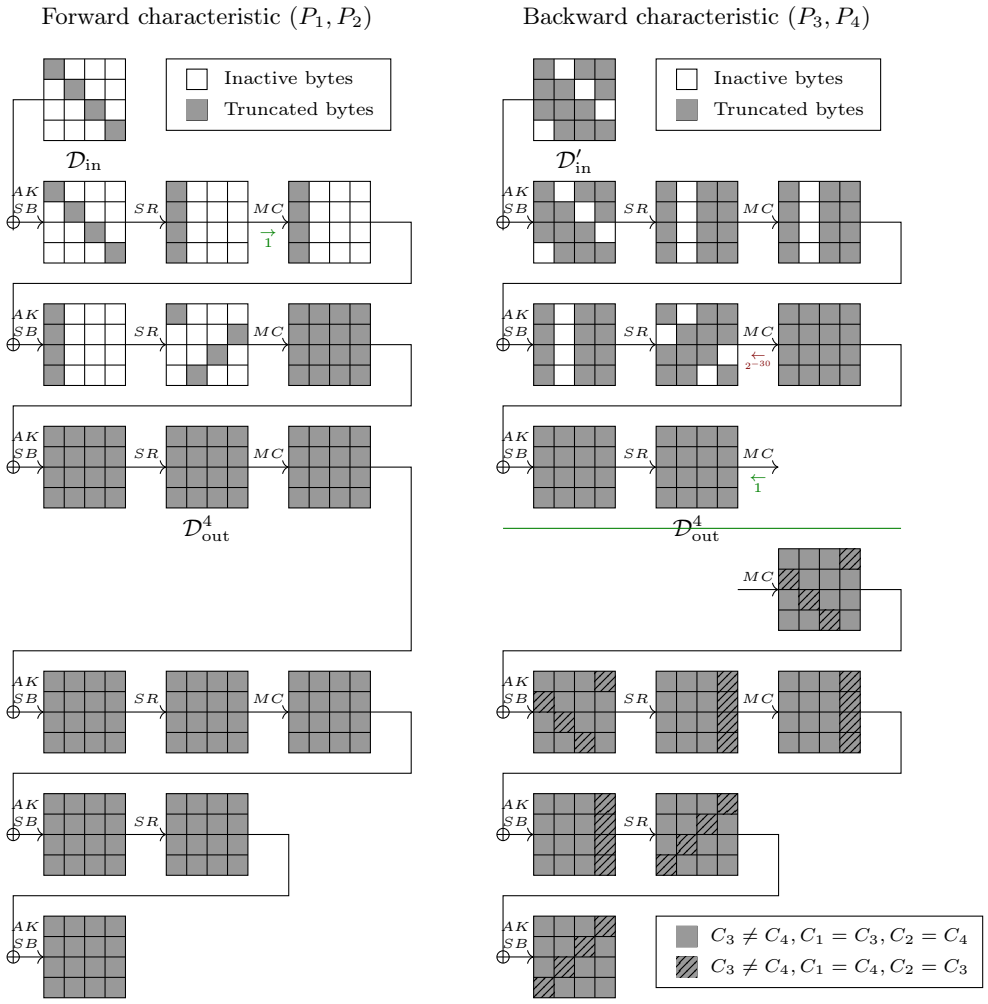
Parameters for the boomerang trail: $\overrightarrow{p} \approx 2^{-13.4}$, $\overleftarrow{p} \approx 2^{-14}$, $\overleftarrow{q} = 1$, $p_b \approx 2^{-27.4}$, $p_{\text{rand}} = 2^{-30}$

Fig. 6. Second exchanged boomerang trail



Parameters for the boomerang trail: $\overrightarrow{p} \approx 2^{-6}$, $\overleftarrow{p} = 2^{-22}$, $\overleftarrow{q} = 1$, $p_b \approx 2^{-28}$, $p_{\text{rand}} = 2^{-30}$

Fig. 7. Third exchanged boomerang trail



Parameters for the boomerang trail: $\overrightarrow{p} \approx 1$, $\overleftarrow{p} \approx 2^{-30}$, $\overleftarrow{q} = 1$, $p_b \approx 2^{-30}$, $p_{\text{rand}} = 2^{-30}$

Fig. 8. Fourth exchanged boomerang trail