IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2019, No. 1, pp. 142–169. DOI:10.13154/tosc.v2019.i1.142-169

Boomerang Switch in Multiple Rounds

Application to AES Variants and Deoxys

Haoyang Wang and Thomas Peyrin

School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, Singapore
wang1153@e.ntu.edu.sg, thomas.peyrin@ntu.edu.sg

Abstract. The boomerang attack is a cryptanalysis technique that allows an attacker to concatenate two short differential characteristics. Several research results (ladder switch, S-box switch, sandwich attack, Boomerang Connectivity Table (BCT), ...) showed that the dependency between these two characteristics at the switching round can have a significant impact on the complexity of the attack, or even potentially invalidate it. In this paper, we revisit the issue of boomerang switching effect, and exploit it in the case where multiple rounds are involved. To support our analysis, we propose a tool called Boomerang Difference Table (BDT), which can be seen as an improvement of the BCT and allows a systematic evaluation of the boomerang switch through multiple rounds. In order to illustrate the power of this technique, we propose a new related-key attack on 10-round `AES`-256 which requires only 2 simple related-keys and 2^{75} computations. This is a much more realistic scenario than the state-of-the-art 10-round `AES`-256 attacks, where subkey oracles, or several related-keys and high computational power is needed. Furthermore, we also provide improved attacks against full `AES`-192 and reduced-round `Deoxys`.

Keywords: Boomerang attack · Switching effect · BCT · Boomerang Difference Table · AES · Deoxys

1 Introduction

Differential cryptanalysis [BS91] is one of the most significant technique applicable to symmetric-key block ciphers, which exploits the high probability of a differential. The *boomerang attack* [Wag99] is an extension of the traditional differential attack, where two differentials are combined in an elegant way to provide a distinguishing property of the cipher. More precisely, it regards the targeted cipher E as a cascade of two sub-ciphers, *i.e.*, $E = E_1 \circ E_0$ as depicted in Figure 1. Assume that there is a differential $\alpha \to \beta$ with probability p for E_0 and a differential $\gamma \to \delta$ with probability q for E_1, the boomerang attack exploits the probability of the following differential:

$$Pr[E^{-1}(E(x) \oplus \delta) \oplus E^{-1}(E(x \oplus \alpha) \oplus \delta) = \alpha] = p^2 q^2. \quad (1)$$

The basic boomerang attack requires an adaptive chosen-plaintext/ciphertext scenario as the attacker needs to ensure the α difference on the encryption queries and the δ difference on the decryption queries. Later, the *amplified boomerang attack* [KKS01] was proposed, which only requires a chosen-plaintext scenario and where a right quartet is obtained with probability $p^2 q^2 2^{-n}$. Furthermore, it was pointed out in [BDK01, BDK02] that any value of β and γ is allowed as long as $\beta \neq \gamma$. As a result, the probability of the right quartet is increased to $2^{-n}\hat{p}^2\hat{q}^2$, where $\hat{p} = \sqrt{\Sigma_i \mathrm{Pr}^2(\alpha \to \beta_i)}$ and $\hat{q} = \sqrt{\Sigma_j \mathrm{Pr}^2(\gamma_j \to \delta)}$, which is known as the *rectangle attack*.

Received: 2018-11-23, Accepted: 2019-01-23, Published: 2019-03-08

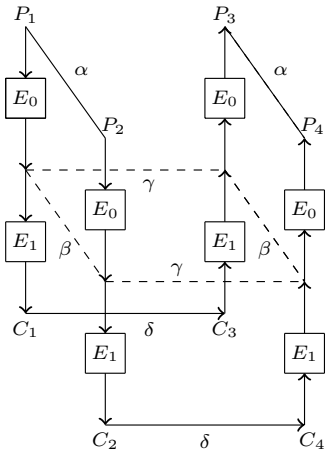


Figure 1: The boomerang attack

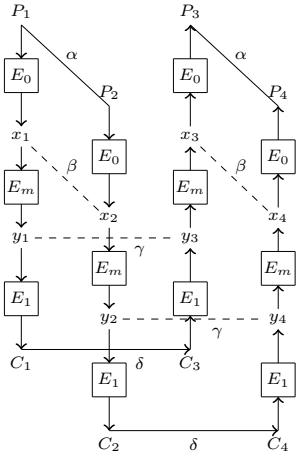


Figure 2: The sandwich attack

In boomerang-style attacks, the probability of obtaining a right quartet is computed based on the assumption that the two sub-ciphers E_0 and E_1 are independent. However, Murphy [Mur11] pointed out that the independence assumption is not always legitimate. He provided some counterexamples where two independently chosen differential characteristics may be *incompatible*, which causes a zero probability of the boomerang distinguisher. Interestingly, he also showed that some other cases lead in contrary to a much higher probability. Besides, many improvements taking advantages of the dependency between the two differential characteristics have been proposed, such as the *middle round S-box trick* [BDD03], *ladder switch*, *S-box switch* and *Feistel switch* [BK09].

Those observations can be captured in the framework of *sandwich attack* [DKS10, DKS14], which decomposes the cipher as $E = E_1 \circ E_m \circ E_0$, with the middle part E_m consisting of relatively short transformations (as depicted in Figure 2). The differential characteristics of E_0 and E_1 specify the input difference β and output difference γ to E_m separately. Then, a small boomerang distinguisher is applied on E_m with probability r computed by:

$$r = Pr[E_m^{-1}(E_m(x) \oplus \gamma) \oplus E_m^{-1}(E_m(x \oplus \beta) \oplus \gamma) = \beta] \tag{2}$$

The entire boomerang distinguisher succeeds only if a right quartet of E_m is generated, thus the overall success probability becomes p^2q^2r. Then, the boomerang switching effects can be unified as the dependency between the two characteristics lie now in E_m. We call the interaction between the two characteristics *boomerang switch*, just as the name chosen in [BK09].

At Eurocrypt 2018, Cid *et al.* [CHP+18] proposed an efficient and systematic method to evaluate r. It narrows the switching effect of a state to a single S-box with a newly created table, called *Boomerang Connectivity Table (BCT)*. The entries in the BCT record the probability of generating a right quartet for each input/output difference at the S-box level, such that the boomerang incompatibility, ladder switch and S-box switch can easily be detected. Moreover, the BCT provides a potentially stronger switching effect than those in the previous observations. Later, a follow-up work on the uniformity of the BCT was produced in [BC18].

Note that all the switching effects and the BCT tool are derived under the scenario where E_m is a simple operation, such as one S-box layer. However, practical experiments from [CHP+17] show that additional improvements might be obtained when E_m contains two rounds, and the analysis of `SKINNY` cipher [BJK+16] in [CHP+18] also highlights that

boomerang switching effect in 2-round E_m is possible. Then, from the research results summarized above, the following questions naturally arise:

- What is the maximum number of rounds that can compose E_m, such that the boomerang switching effect still exists?
- Can we directly apply the current switching techniques to E_m when it is composed of multiple rounds? If not, are there other switching techniques that can provide a systematic evaluation?

Our contributions. In this paper, we provide a systematic analysis of the boomerang switching effect in multiple rounds for S-box based ciphers. First, we exploit the principle behind the ladder switch and show that the boomerang switch is applicable in multiple rounds, *e.g.*, a 4-round boomerang distinguisher of `SKINNY` can be constructed with probability 1. Then, the applicability of the BCT in multiple rounds is shown to be defective with an incompatibility example on two rounds of `AES`. In order to capture the switching effect in multiple rounds, we propose a new tool, so-called *Boomerang Difference Table (BDT)*. The BDT is created at the S-box level and is a combination of the BCT and the DDT (Difference Distribution Table). It represents the differential propagation and the boomerang switch in a unified manner. With the help of the BDT, we present a general evaluation of the 2-round boomerang switch for the first time.

To illustrate the power of the boomerang switch in multiple rounds, we exhibit a full key recovery related-key attack on 10-round `AES`-256 with only 2^{75} computations and 2 related-keys. Previously, the best attack [BDK+10] on this reduced-round variant of `AES`-256 required 2^{44} computations, but only recovered 35 subkey bits (the rest of the key having to be brute-forced). Moreover, it has to be conducted under a much less realistic related-subkey scenario, where the attacker is allowed to choose differences on different subkeys. Known attacks [BDK05, KHP07] on 10-round `AES`-256 in the classical related-key scenario require much more related keys (64 or 256) and computations effort (2^{172}).

Besides, we further showcase the practical usage of the BDT by extending from one round to two rounds the boomerang switch in the attacks against full `AES`-192 [BK09, BN10] (the attack from [BN10] remained the best publicly known attack on full round `AES`-192).

Finally, we describe how to improve the boomerang attack [CHP+17] against 10-round `Deoxys`-BC [JNPS16] by accurately detecting from which parts of the attack the differential probabilities are coming from.

Organization. In Section 2, we provide a brief description of boomerang attacks and the current switching techniques, followed by the notations adopted throughout the paper. In Section 3, we discuss the boomerang switch in the case of multiple rounds, and introduce the boomerang difference table as a method to evaluate the switching effect and its applications on 2-round boomerang switch. In Section 4, the boomerang attack on 10-round `AES`-256 is proposed by applying the 2-round boomerang switch. The applications on `AES`-192 and `Deoxys`-BC with the 2-round boomerang switch is presented in Section 5 and 6. Section 7 summarizes this paper.

2 Preliminaries

2.1 Related-Key Boomerang Attacks

Boomerang attacks under the related-key setting were formulated in [BDK05]. Let ΔK and ∇K be the key differences for subciphers E_0 and E_1, respectively. The attacker needs to access four related-key oracles with $K_1 \in \mathbb{K}$, where $\mathbb{K}$ denotes the key space:

$K_2 = K_1 \oplus \Delta K$, $K_3 = K_1 \oplus \nabla K$ and $K_4 = K_1 \oplus \Delta K \oplus \nabla K$. The attack is then performed with the following process:

1. Choose a plaintext P_1 at random, compute another plaintext $P_2 = P_1 \oplus \alpha$.
2. Ask for the encryption of P_1 and P_2 with secret key K_1 and K_2 separately, denote the ciphertexts C_1 and C_2 respectively.
3. Compute $C_3 = C_1 \oplus \delta$ and $C_4 = C_2 \oplus \delta$.
4. Ask for the decryption of C_3 and C_4 with K_3 and K_4 separately, denote the new plaintexts P_3 and P_4 respectively.
5. Check whether $P_3 \oplus P_4 = \alpha$.

2.2 Boomerang Switch and Boomerang Connectivity Table.

The boomerang switch, proposed in [BK09], was used to obtain free rounds in the middle of the cipher in the attacks against full AES-192 and AES-256. The idea was to optimize the transition between the sub-paths of E_0 and E_1 in order to minimize the overall complexity of the distinguisher. In [BK09], two S-box based switches were introduced: the ladder switch, and the S-box switch. The idea of the ladder switch is to realize that instead of necessarily decomposing the cipher into rounds, one can decompose it into smaller parallel transformations and this may lead to better distinguishers. The idea of the S-box switch is that when a same S-box is activated in both E_0 and E_1, and when the output difference in E_0 is identical to the input difference in E_1, then the differential transition through the S-box is free in one of the two directions.

These switches were further generalized with the *boomerang connectivity table* [CHP+18] and we provide here the definition.

Definition 1 ([CHP+18])**.** Let S be an invertible function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, and Δ_0, $\nabla_0 \in \mathbb{F}_2^n$. The boomerang connectivity table (BCT) of S is defined by a $2^n \times 2^n$ table, in which the entry for (Δ_0, ∇_0) is computed by:

$$BCT(\Delta_0, \nabla_0) = \#\{x \in \{0,1\}^n | S^{-1}(S(x) \oplus \nabla_0) \oplus S^{-1}(S(x \oplus \Delta_0) \oplus \nabla_0) = \Delta_0\}.$$

The generation of the BCT can be visualized in Figure 3. The ladder switch is captured by the BCT in the case where at least one of the index equals to zero. The S-box switch is captured by the BCT in the case where ∇_0 equals Δ_1. Moreover, the incompatibility pointed out by Murphy [Mur11] simply corresponds to zero entries in the BCT.

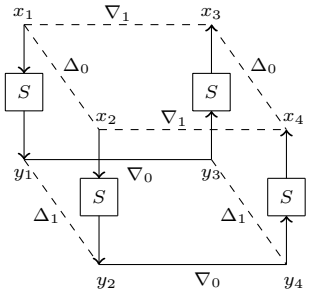


Figure 3: Generation of a right quartet at the S-box level

2.3 Notations

The subkey of round i is denoted by K^i, i starting from 0, K^0 being the master key. We use (i, j) to point the position located at the i-th row and j-th column of the state array. We denote by $x^r_{i,j}$ the cell at position (i, j) before the S-box layer at round r, and by $y^r_{i,j}$ the cell after the S-box layer. Besides, by Δ we denote the difference in the upper trail, and by ∇ the same for the lower trail.

In this paper, we mainly focus on the iterative ciphers with substitution-permutation network (SPN), which consists of predefined S-box and linear layer.

3 Boomerang Switch

In this section, we analyze the boomerang switching effect in E_m. The notations in Figure 2 and 3 are adopted. Note that the linear layers at the head and the tail of the round operations in E_m are not considered, because linear layers make no difference on the switching effect.

3.1 Determining The Number of Rounds in E_m

At FSE 2018 [CHP+17], Cid *et al.* proposed a MILP-based method to exploit the switching effect in two rounds of `Deoxys`-BC [JNPS16]. Their method adopts the idea of ladder switch that the round function can be divided into two independent parts. Suppose one part is only active in E_0 and the other part is only active in E_1, then by assigning the former as a part of E_1 and the latter as a part of E_0, the differential probability of all the S-boxes becomes 1. Since the round function of `Deoxys`-BC can operate on two independent parts for two rounds, Cid *et al.* set the length of E_m to 2 rounds in their search tool.

Recalling the procedure of boomerang attack, the differential characteristic of E_0 is used in the forward direction for the pair (P_1, P_2) and the backward direction for the pair (P_3, P_4), and the differential characteristic of E_1 is used in the backward direction for both pairs (C_1, C_3) and (C_2, C_4). The principle behind the ladder switch in E_m is that the backward diffusion of the active cells in γ has no interaction with the forward diffusion of the active cells in β, thus the difference between y_3 and y_4 can backtrack to β with probability 1. We formalize it into the following lemma:

Lemma 1. *In E_m, if the forward diffusion of the active cells in β has no interaction with the backward diffusion of the active cells in γ, a right quartet of E_m can be generated with probability* 1*.*

The effect of Lemma 1 is not exactly the same as the ladder switch and we use the following example to highlight the difference.

Example 1. Let `SKINNY` [BJK+16] be the block cipher considered (its round function is given in Appendix A). By applying Lemma 1, we find that a right quartet of E_m can be generated with probability 1 up to four rounds with nonzero β and γ. One example is depicted in Figure 4, which is composed of two truncated differential characteristics. With any instantiated values of β and γ, the boomerang can always return to β with probability 1, *i.e.*, $r = 1$. However, by the original definition of ladder switch the round function of `SKINNY` cannot be divided into two independent parts for more than two rounds.

Thus, using Lemma 1, the maximal number of rounds for E_m can be easily determined for a specific cipher. Briefly, start from a 1-round E_m, iterate the truncated difference of β and γ to meet the condition in Lemma 1, if it is satisfied, increase the number of rounds in E_m by 1 and repeat the previous process until the condition cannot be met, then the maximal number of rounds for E_m is the one of the last E_m that meets the condition.

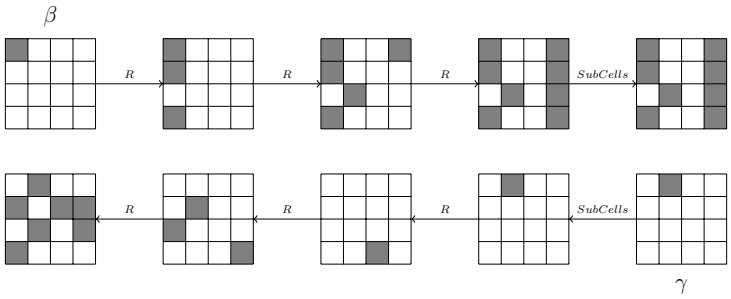


Figure 4: An example of 4-round E_m for SKINNY, the two differential characteristics are given in truncated notation (gray denotes an active nibble, white denotes an inactive nibble), the above one is used for encryption and the below one is used for decryption.

In particular, E_m can contain more rounds for the ciphers with a sparser diffusion layer. Besides, we note that the above E_m is actually a 4-round distinguisher of SKINNY with probability 1, which is an interesting observation.

3.2 Incompatibility in Multiple Rounds

As stated in [CHP+18], the BCT provides a unified representation of the existing observations on the boomerang switch. Nevertheless, it was proposed to evaluate E_m when composed of a single S-box layer, the applicability of the BCT to the boomerang switch in multiple rounds remaining unknown so far.

We give an example in Figure 5 and show that the BCT is actually incapable of detecting incompatibilities when E_m consists of two rounds.

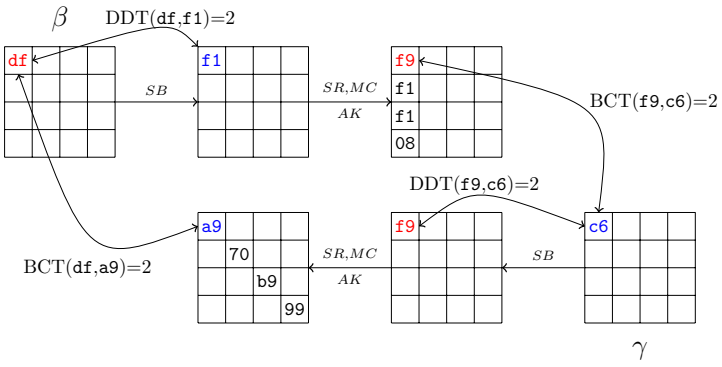


Figure 5: A 2-round E_m example for AES, with the actual β and γ values, which will never generate a right quartet. The differences are represented in hexadecimal.

In Figure 5, both differential characteristics are established with probability 2^{-7}. In the first S-box layer, the upper differential characteristic fixes the Δ_0 of the active S-box to 0xdf and the lower differential characteristic fixes $\nabla_0 =$ 0xa9, with which the BCT entry is 2. At the second S-box layer, for the targeted S-box, the BCT entry is 2 for $\Delta_0 =$ 0xf9 and $\nabla_0 =$ 0xc6. All the other S-boxes in the two rounds will be bypassed with probability 1 (entries of the BCT are 2^8). Thus, according to the BCT, the difference pairs (Δ_0, ∇_0) of all S-boxes in the two S-box layers are compatible, which implies that the two differential characteristics of E_m are compatible in a boomerang distinguisher. Let us focus on the Sbox at position $(0, 0)$ in the first S-box layer, a right quartet requires that the DDT entry for (0xdf, 0xf1) and the BCT entry for (0xdf, 0xa9) are nonzero simultaneously. However,

a brute-force search of $\mathbb{F}_2^n$ shows that there is no value satisfying this condition. Hence, a right quartet will never be generated for the E_m, which contradicts the conclusion derived by the BCT.

3.3 Generalized Switching Effect in Multiple Rounds

The above incompatible example implies that the BCT has limitation on the evaluation of boomerang switch in multiple rounds. In the definition of the BCT, it takes into account Δ_0 and ∇_0 to evaluate the switching probability of a single S-box. Δ_0 and ∇_0 correspond to β and γ respectively when E_m only consists in one S-box layer, and only β and γ matter in computing the switching probability (as shown in formula 2). Thus, the BCT measures the switching effect nicely for one S-box layer. However, when it comes to multiple S-box layers, this correspondence no longer exists. Consecutive multiple S-box layers are highly related. Such as the S-box with input difference $\Delta_0 =$ `0xdf` in the first round in Figure 5, the first round switch requires $\nabla_0 =$ `0xa9`, while the second round switch requires the output difference Δ_1 to be `0xf1`, which causes an incompatibility. This fact reveals that several independent compatible boomerang switches could lead to incompatibilities when they are combined together. Therefore, it is necessary to find a way to consider consecutive rounds in a unified manner.

The above example shows a contradiction of the 3-tuple $(\Delta_0, \Delta_1, \nabla_0)$ for a S-box. Hence, it is crucial to analyze the relation among them. In the following, we provide two lemmas which are applicable to any S-box.

Lemma 2. *For any fixed Δ_0 and Δ_1, for which the DDT entry is $2l$, l being a nonzero integer, the maximum number of nontrivial values of ∇_0, for which a right quartet could be generated, is $2\binom{l}{2}+1$.*

Proof. The straightforward case is when ∇_0 can always take the value of Δ_1. Apart from that case, when $l > 1$, there are l paired values satisfying the differential propagation, then each two paired values can construct a quartet. In total, $\binom{l}{2}$ distinct quartets can be built. For each quartet, we denote the two paired values of S-box outputs by $\{(y_1, y_2), (y_3, y_4)\}$. There are two new ways to define ∇_0 such that a boomerang quartet could be generated: $y_1 \oplus y_3$ and $y_1 \oplus y_4$. Hence, there are $2\binom{l}{2}+1$ nontrivial choices of ∇_0. □

Lemma 3. *For any fixed Δ_0 and ∇_0, for which the BCT entry is $2l$ and the DDT entry is $2l'$, l and l' being nonzero integers, the maximum number of choices of Δ_1, for which a right quartet could be generated, is $1 + (2l - 2l')/4$.*

We omit the proof here, as it follows the same idea as the lemma above.

In order to capture all these observations and to easily analyze the switching effect, we propose a new tool: the *Boomerang Difference Table (BDT)*.

Definition 2 (Boomerang Difference Table (BDT))**.** Let S be an invertible function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, and $(\Delta_0, \Delta_1, \nabla_0) \in \mathbb{F}_2^n$. The boomerang difference table (BDT) of S is a three-dimensional table, in which the entry for $(\Delta_0, \Delta_1, \nabla_0)$ is computed by:

$$\begin{aligned} BDT(\Delta_0, \Delta_1, \nabla_0) = &\#\{x \in \{0,1\}^n | S^{-1}(S(x) \oplus \nabla_0) \oplus S^{-1}(S(x \oplus \Delta_0) \oplus \nabla_0) = \Delta_0, \\ &S(x) \oplus S(x \oplus \Delta_0) = \Delta_1\}. \end{aligned}$$

The BDT reveals the probability of generating a boomerang quartet with a certain differential trail at the S-box level. Inspired by the efficient construction of the BCT proposed by Orr Dunkelman [Dun18], we show that the time complexity for generating the BDT for an n-bit S-box is $O(2^{2n})$, the algorithm is depicted in Algorithm 1.

Algorithm 1: The algorithm for constructing the BDT

```
for all values of ∇0 do
    Initialize an empty table T of 2^n lists
    for all values of x do
        Compute y = x ⊕ S^{-1}(S(x) ⊕ ∇0)
        Concatenate x to T[y]
    end
    Initialize a two-dimensional array Slice of 2^n × 2^n entries
    for all entries in T do
        if the entry is not empty then
            for all pairs of values (x_i, x_j) in the entry do
                Increment Slice[x_i ⊕ x_j, S(x_i) ⊕ S(x_j)] by 1
            end
        end
    end
    The entries of Slice corresponds to the entries of the BDT with the fixed ∇0
end
```

It is easy to see that the BDT is a combination of the BCT and the DDT. Their relations and a property of the BDT are listed below:

$$DDT(\Delta_0, \Delta_1) = BDT(\Delta_0, \Delta_1, 0) = BDT(\Delta_0, \Delta_1, \Delta_1) \tag{3}$$

$$BCT(\Delta_0, \nabla_0) = \sum_{\Delta_1=0}^{2^n} BDT(\Delta_0, \Delta_1, \nabla_0) \tag{4}$$

$$BDT(0, 0, \nabla_0) = 2^n \tag{5}$$

As we can see from Equation (4), the BDT undermines the switching effect offered by the BCT with the additional requirement of Δ_1. To illustrate this point, we provide the following example.

Example 2. The S-box of `AES` is used as illustration here. Suppose that the DDT entry is 4 for a fixed difference pair (Δ_0, Δ_1), then a right quartet can be generated by two new choices of ∇_0 according to Lemma 1. Take ∇_0' as one of them for example, the BCT entry for (Δ_0, ∇_0') would be 6 (for any fixed Δ_0 in `AES`, the value of two positions in the BCT, for which the DDT value is 2, will increase by 4). However, among the three paired values, only two pairs lead to output difference of the S-box to Δ_1, and the other pair leads to ∇_0'. Thus, the BDT entry for $(\Delta_0, \Delta_1, \nabla_0')$ is 4, and the entry for $(\Delta_0, \nabla_0', \nabla_0')$ is 2, both are lower than the BCT entry for (Δ_0, ∇_0'). If the output difference is required to be either Δ_1 or ∇_0', the switching probability from Δ_0 to ∇_0' for the S-box is lower than the probability $6/2^8$ evaluated by the BCT.

The above observation can be incorporated into the following lemma. Note that we define the *uniformity* of the BDT as the maximal value in the table, except the values where Δ_0 and Δ_1 are zero.

Lemma 4. *For any S-box, the uniformity of the BDT equals to the uniformity of the DDT.*

Proof. Firstly, the BDT entry for $(\Delta_0, \Delta_1, \nabla_0)$ is no greater than $\mathrm{DDT}(\Delta_0, \Delta_1)$ and $\mathrm{BCT}(\Delta_0, \nabla_0)$. Secondly, for any choices of (Δ_0, Δ_1), the entry in the DDT is smaller than or equal to the one in the BCT[1]. Thirdly, Equation (3) always holds. The lemma is accordingly proved by the three observations. □

[1] Lemma 1 in [CHP+18].

Incompatibility. A 3-tuple $(\Delta_0, \Delta_1, \nabla)$ is incompatible if the corresponding entry of the BDT is 0. The incompatible difference pair (Δ_0, ∇) detected by the BCT can also be detected by the BDT through Equation (4). Moreover, the BDT is able to detect new incompatibilities even if the corresponding values of the BCT and the DDT are nonzero.

With the help of the BDT, the incompatibility exhibited in Section 3.2 can be easily detected: the BDT entry for $(\texttt{0xdf}, \texttt{0xf1}, \texttt{0xa9})$ is 0.

Variants of BDT. When the boomerang returns back in the decryption direction, the ∇_1 of the S-box in the last S-box layer of E_m determines the differential characteristic in the backward rounds. Thus, naturally a variant BDT′ that takes into account $(\nabla_0, \nabla_1, \Delta_0)$ can be proposed to evaluate the last S-box layer:

$$BDT'(\nabla_0, \nabla_1, \Delta_0) = \#\{x \in \{0,1\}^n | S(S^{-1}(x) \oplus \Delta_0) \oplus S(S^{-1}(x \oplus \nabla_0) \oplus \Delta_0) = \nabla_0, \\ S^{-1}(x) \oplus S^{-1}(x \oplus \nabla_0) = \nabla_1\}.$$

From the symmetry of the boomerang, all the previous analysis of the BDT also applies to the BDT′. Furthermore, another variant of the BDT to capture all the four factors $(\Delta_0, \nabla_0, \Delta_1, \nabla_1)$ is needed when analyzing the middle S-box layers in the case where E_m consists of more than two rounds. The analysis is also similar, but as it is not used in this paper, we ignore it to prevent redundancy.

3.4 Boomerang Switch in Two Rounds

In this section, we discuss the application of the BDT (BDT′) to the boomerang switch in two rounds. E_m consists of two S-box layers and one linear layer in between — as depicted in Figure 6, the S-box layer being denoted by SL and the linear layer by R. The switching probability of the first S-box layer is denoted by p_1, and the switching probability of the second S-box layer is denoted by p_2, the whole probability of E_m is then computed by $r = p_1 p_2$.

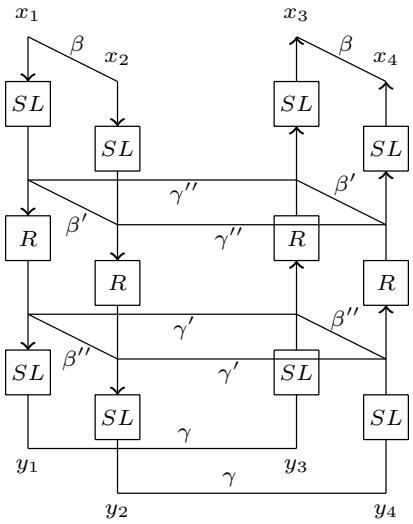


Figure 6: A 2-round E_m which consists of two S-box layers and one linear layer.

In the analysis of the boomerang switch, the BDT is applied at the first S-box layer, and the BDT′ is applied at the second S-box layer. In general, the probability p_1 and p_2 are the product of the switching probability of each S-box in the internal state, and are

computed by:

$$p_1 = \prod_{(\Delta_0,\Delta_1,\nabla_0)\in L_1} BDT(\Delta_0,\Delta_1,\nabla_0)/2^n, \tag{6}$$

$$p_2 = \prod_{(\nabla_0,\nabla_1,\Delta_0)\in L_2} BDT'(\nabla_0,\nabla_1,\Delta_0)/2^n, \tag{7}$$

where L_1 contains the 3-tuple difference of the S-box in $(\beta, \beta', \gamma'')$, and L_2 contains the same in $(\gamma, \gamma', \beta'')$.

Notice that given E_m with the fixed β and γ, there might exist several differential characteristics satisfying this differential, which could contribute to increase the probability.

In practice, the 2-round boomerang switch can be classified into three cases:

(a) The two differential characteristics have no same active S-box in both S-box layers.

(b) The two differential characteristics activate the same S-boxes only in one of the two S-box layers.

(c) The two differential characteristics activate the same S-boxes in both S-box layers.

Examples of the three cases are presented in Figure 7. In the following, we explain the three cases and provide simplified analysis for the first two cases.

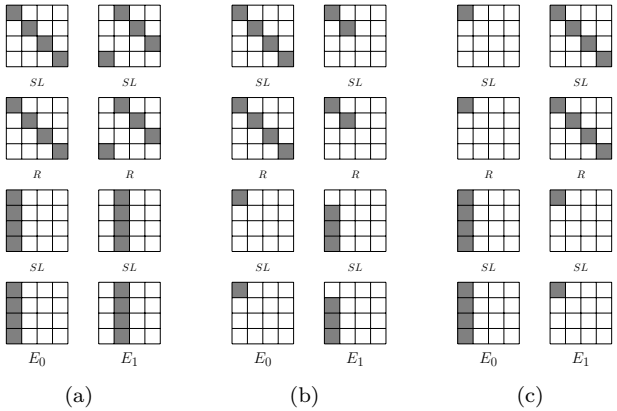


Figure 7: Examples of three cases for the boomerang switch in two rounds

Analysis of The Three Cases

Due to the relation among the BDT, the BCT and the DDT, in the BDT-based analysis, we are able to switch the BDT to the BCT when there is no requirement for Δ_1 (Equation (4)), and to switch the BDT to the DDT when ∇_0 equals to zero (Equation (3)). And the BDT$'$ can be handled similarly.

Case (a). If each S-box layer is evaluated independently, no S-box differential probability has to be paid due to the ladder switch. However, the result is different when they are combined together.

Recalling that the BDT entry is 2^n when both Δ_0 and Δ_1 equal to zero, the S-box with zero input/output difference can be switched with probability 1. Then, regarding the first S-box layer, the switching probability only comes from the active S-boxes corresponding to β (β'). Since the difference ∇_0 equals to zero for those S-boxes, we can utilize the

DDT to evaluate their switching probabilities instead of the BDT. Thus, p_1 equals to the probability of the differential propagation from β to β', *i.e.*, $p_1 = pr(\beta \xrightarrow{SL} \beta')$. In particular, the probability is 1 if no specific value of β' is required.

The analysis is similar for the second S-box layer with the help of the BDT′, and $p_2 = pr(\gamma \xrightarrow{SL^{-1}} \gamma')$. Also, p_2 equals to 1 if there is no requirement for the value of γ'.

Case (b). If the same active S-boxes are present in the first S-box layer, the analysis for the second S-box layer is similar to Case (a), *i.e.*, $p_2 = pr(\gamma \xrightarrow{SL^{-1}} \gamma')$.

As for the first S-box layer, the switching probability p_2 can be directly computed from the analysis of the BCT if there is no requirement for β'. Otherwise, the 3-tuple $(\Delta_0, \Delta_1, \nabla_0)$ has to be evaluated in the BDT, and the switching probability should be computed by Equation 6.

Finally, the case where the same active S-boxes are located in the second S-box layer can be analyzed similarly because of the symmetry of the boomerang attack.

Case (c). The BDT has to be applied to both S-box layers. Since specific values of all the intermediate states (β', β'', γ' and γ'') are required, there is a high chance of incompatibility.

4 Attack on 10-Round AES-256

In this section, we propose a related-key attack on 10-round AES-256 by applying the 2-round boomerang switch. The best previously published attack on this variant required 2^{45} time to partially obtain 35 subkey bits [BDK+10] (the rest of the key having to be brute-forced for full recovery), and it used a strong type of related-subkey oracles. The related-subkey setting requires a complex key access scheme [BK03] when compared to the related-key setting, and it could be too contrived for academic interest according to [**?**]. Our boomerang attack is mounted under a much realistic scenario: a simple related-key setting with only two related keys, instead of four (or more) for most related-key boomerang attacks. We are able to recover the full 256-bit key with 2^{75} computations. This also compares favourably to previously known attacks in the same setting [BDK05, KHP07], which require more related-keys and much more computations. We summarize the current attacks in Table 1.

Table 1: Summary of attacks on 10-round AES-256.

Scenario	# keys	Time	Data	Result	Reference
Key Diff.	64/256	2^{172}	2^{114}	Full key	[KHP07]/ [BDK05]
Subkey Diff.	2	2^{45}	2^{44}	35 subkey bits	[BDK+10]
Key Diff.	2	2^{75}	2^{75}	Full key	this paper

4.1 A Short Description of AES

The Advanced Encryption Standard (AES) [DR02] is an iterated block cipher which encrypts 128-bit plaintexts with a secret key of size 128, 192, or 256 bits. Its internal state can be represented as a 4×4 matrix whose elements are byte values, seen as elements of the finite field $GF(2^8)$. The round function consists of four basic transformations in the following order:

- `SubBytes` (SB) is a nonlinear substitution that applies the same S-box to each byte of the internal state.
- `ShiftRows` (SR) is a cyclic rotation of the byte positions, where the i-th row of the internal state is rotated by i positions to the left, for $i = 0, 1, 2, 3$.
- `MixColumns` (MC) is a multiplication of each column of the internal state with a Maximum Distance Separable (MDS) matrix over $GF(2^8)$.
- `AddRoundKey` (AK) is an exclusive-or of the incoming round key to the internal state.

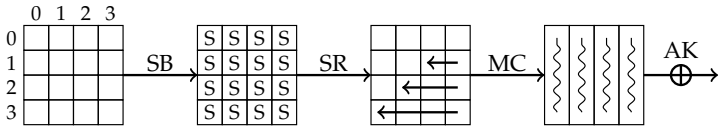


Figure 8: `AES` round function

At the very beginning of the encryption, an additional whitening key addition is performed, and the last round does not contain `MixColumns`. `AES`-128, `AES`-192, and `AES`-256 share the same round function with different number of rounds: 10, 12, and 14, respectively.

The key schedule of `AES` transforms the master key into subkeys which are used in each of the rounds. Here, we describe the key schedule of `AES`-256. The 256-bit master key is divided into 8 32-bit words $(W[0], W[1], ..., W[7])$, then $W[i]$ for $i \geqslant 8$ is computed as

$$W[i] = \begin{cases} W[i-8] \oplus \texttt{SB}(\texttt{RotByte}(W[i-1])) \oplus Rcon[i/8] & i \equiv 0 \bmod 8, \\ W[i-8] \oplus \texttt{SB}(W[i-1]) & i \equiv 4 \bmod 8, \\ W[i-8] \oplus W[i-1] & \text{otherwise} \end{cases}$$

The i-th round key is the concatenation of 4 words $W[i] \parallel W[i+1] \parallel W[i+2] \parallel W[i+3]$. `RotByte` is a cyclic shift by one byte to the left, and $Rcon$ are the round byte constants. We denote the 256-bit i-th subkey by K^i, and K^0 is the master key. The key schedule of `AES`-128 and `AES`-192 is slightly different due to the different key sizes, we refer to [DR02] for full details.

4.2 The Boomerang Distinguisher

The boomerang distinguisher[2] is given in Figure 14. The trail used in E_0 is a 9-round related-key differential characteristic which is produced with the local collision strategy introduced in [BKN09]. There are five active S-boxes in rounds 1-7, and we require all of them use the optimal S-box differential transition `0x02` $\rightarrow$ `0x14`. The key relation $\Delta K = K_A \oplus K_B$ is chosen as shown in Figure 14. The trail used in E_1 is a single-key differential characteristic that covers rounds 8-10, while round 10 is used for key recovery. The switching state is located at rounds 8 and 9.

Let us now compute the probability of this 9-round boomerang distinguisher. There are five active S-boxes in rounds 1-7, each of them is passed with differential probability 2^{-6}. Thus the overall differential probability for the first seven rounds is 2^{-30}.

Since rounds 8 and 9 are for boomerang switch and round 10 is for key recovery, the 9-round distinguisher is actually composed of E_0 and E_m, without E_1. The 2-round boomerang switch is depicted in Figure 9, and the actual values are specified in Table 3.

[2] As we use colors in the diagrams of the trails, we advise the reader to refer to the color scheme defined in Appendix B.

The value of $\Delta y^8_{0,0}$ is fixed to `0x14` so that the three S-boxes in round 9 are inactive. In order to generate a right quartet, $\nabla y^8_{0,0}$ can take three values according to Lemma 2, and the values are `0x14`, `0x8c` and `0x98`. Hence, we can obtain three trails for the boomerang switch. Since the active S-boxes marked with ■ are not concerned, the switching probability in round 8 only comes from the first S-box, and the BDT entries for $(\texttt{0x02}, \texttt{0x14}, \texttt{0x14})$, $(\texttt{0x02}, \texttt{0x14}, \texttt{0x8c})$ and $(\texttt{0x02}, \texttt{0x14}, \texttt{0x98})$ are all 4 so that the switching probability is 2^{-6} for all the three trails. Regarding the boomerang switch in round 9, only the first S-box is concerned, and the BDT entries for the three trails are 2, 2 and 4 respectively. Finally the switching probability in the two rounds are $2^{-6} \cdot 2^{-7} + 2^{-6} \cdot 2^{-7} + 2^{-6} \cdot 2^{-6} = 2^{-11}$. In the end, the probability of the 9-round boomerang distinguisher is $2^{-30-30-11} = 2^{-71}$.

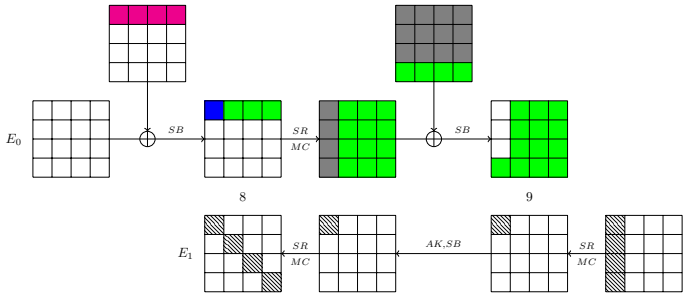


Figure 9: 2-round boomerang switch for the 9-round distinguisher against `AES-256`

Experimental Verification. In order to verify the switching probability in round 8 and 9, we mounted an experiment following the algorithm in Section 2.1. The amount of data used in each test is 2^{20}, and the test is iterated for 1000 randomly chosen key quartets satisfying the required key difference. In the end, the average number of right quartets obtained was 510, so the switching probability is $510/2^{20} = 2^{-11}$, which matches our evaluation.

4.3 Key Recovery

In the key recovery attack, round 10 is added at the end of the distinguisher. The attack works in the reverse direction of the normal boomerang attack, *i.e.*, we first choose the ciphertexts then choose the plaintexts. The algorithm is as follows.

1. Prepare a structure F of 2^{32} ciphertexts, by exhausting all possible values of the dark bytes  while keeping the other bytes fixed.
2. Ask for decryption of F with K_A, and denote by G the set of plaintexts obtained.
3. For each plaintext $P \in G$, compute $P' = P \oplus \alpha$, and denote by H the new set of values P' .
4. Ask for encryption of H with K_B and insert the obtained ciphertexts into a hash table according to the 12 bytes which are inactive in  .
5. In case of a collision of ciphertexts (C_3, C_4) in the hash table: we search the corresponding ciphertext pair (C_1, C_2) in F. Then, save all the candidates of the 32-bit K^{10}_A and K^{10}_B for which $D_{bK_A}(C_1) \oplus D_{bK_A}(C_2) = D_{bK_B}(C_3) \oplus D_{bK_B}(C_4) = \delta$. By D_b we denote the last decryption round.

6. Repeat steps 1-5 $2^{41.5}$ times.

From each structure we can compose 2^{63} unordered pairs, $2^{63-32} = 2^{31}$ of them pass the last round. Thus, we expect $2^{31-71} = 2^{-40}$ right quartet per structure, and 3 right quartets out of $2^{41.5}$ structures.

Let us now compute the number of candidate quartets. The ciphertext has a 96-bit filter, so we are left with $2^{63+41.5-96} = 2^{8.5}$ candidate quartets. On average, each remaining quartet suggests 2^4 guesses for the 32-bit of K_A^{10} and K_B^{10}, respectively, or 2^8 in total. Thus, the $2^{8.5}$ candidate quartets would propose $2^{8+8.5} = 2^{16.5}$ key guesses for the 64 subkey bits, while 3 right quartets would all vote for the correct 64-bit subkey. No wrong key guesses survive and we can get the 32-bit subkeys $k_{0,0}^{10}$, $k_{3,1}^{10}$, $k_{2,2}^{10}$, $k_{1,3}^{10}$ of K_A and K_B as a result.

Notice that the trail in E_1 can follow two other truncated differential characteristics, see Figure 10. For either of the two, we can produce the actual differences similarly to the previous one, and the final probability of the two new distinguishers will remain unchanged. When we run the above algorithm, a right quartet is captured as long as it belongs to one of the three distinguishers. On average, we expect one right quartet per 2^{40} structures for each distinguisher, then 2^{40} structures are enough in order to have 3 right quartets.

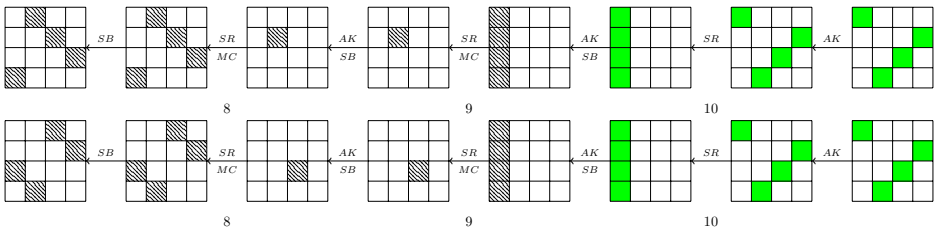


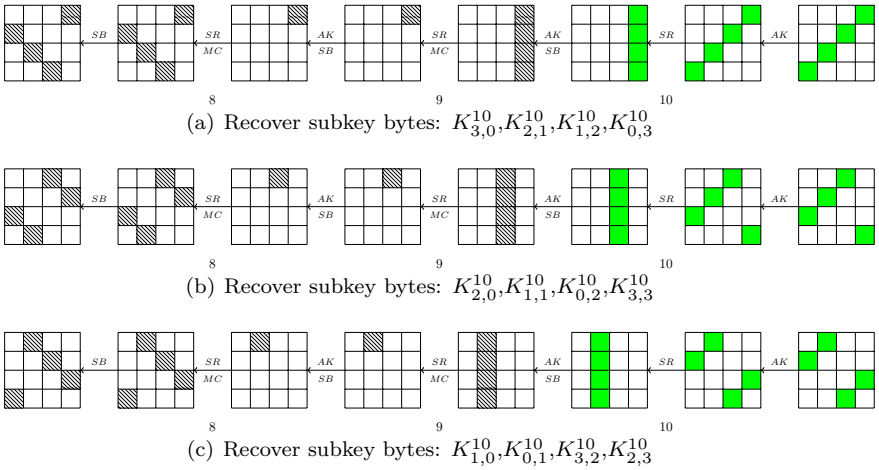
Figure 10: 2 other truncated differential characteristics for E_1 on AES

Recovering other key bytes We can change the trail in E_1 to derive other subkey bytes of K^{10}. We can construct three differential characteristics (see Figure 11) to recover the left 12 bytes of K^{10}. The algorithm and complexity analysis are similar to the previous case and this allows to derive the full K^{10} subkey. Eventually, from the knowledge of this subkey, we can now reduce the cipher to 9 round and recover the full key with various approaches with lower costs (for example, one can use the attack from [BDK+10] that requires only 2^{39} computations to recover the key on 9 round of AES-256).

Complexity Analysis. The memory complexity is dominated by the hash table whose size is 2^{32}. As for the time and data complexity, step 2 and 4 need 2^{33} encryption/decryption oracle accesses for each structure, step 3 and 5 are negligible, thus we need $2^{33+40+2} = 2^{75}$ time and data to complete the attack.

5 Applications to AES-192

In [BK09] Biryukov and Khovratovich proposed the first related-subkey amplified boomerang attack against full AES-192. Later, improvements were made [BN10] by slightly modifying the trail of E_0, and this attack remains the best one as of today. In this section, by exploiting the boomerang switch in two rounds, we show an improvement of the attack in [BN10] and that the actual probability in [BK09] is much higher. Table 2 summarizes the attacks and the improvements. Note that both attacks use the optimal S-box differential: 0x01 → 0x1f in the boomerang trail.



(a) Recover subkey bytes: $K^{10}_{3,0}, K^{10}_{2,1}, K^{10}_{1,2}, K^{10}_{0,3}$

(b) Recover subkey bytes: $K^{10}_{2,0}, K^{10}_{1,1}, K^{10}_{0,2}, K^{10}_{3,3}$

(c) Recover subkey bytes: $K^{10}_{1,0}, K^{10}_{0,1}, K^{10}_{3,2}, K^{10}_{2,3}$

Figure 11: Recovery of other subkey bytes in the boomerang attack against 10-round AES-256

Table 2: Summary of existing attacks against full-round AES-192 and the corresponding improvements with the help of 2-round boomerang switch.

Reference	Time	Data	Improvement
[BN10]	2^{169}	2^{116}	$2^{1.3}$
[BK09]	2^{176}	2^{123}	$2^{4.8}$

5.1 Improvement of The Attack from [BN10]

The attack in [BN10] uses 6-round differential characteristics for both E_0 and E_1, and the first and last round is used for key extraction. The ladder switch is applied to round 6. Since the boomerang switching effect could exist in two rounds for AES, we tried to analyze their distinguisher with the method we developed. However, we found that it is hard to apply the 2-round boomerang switch in their attack, due to the smaller dependency between the two differential characteristics. Hence, we are supposed to create a higher dependency in order to gain additional advantages from the 2-round boomerang switch. Finally, we managed to produce a new differential characteristic for E_0, while keeping the same differential characteristic for E_1 as in [BN10]. The distinguisher is shown in Figure 15 of the Appendix.

We switch the boomerang at rounds 6 and 7, and the switching states are depicted in Figure 12. For the boomerang switch in round 6, we do not pay the S-boxes in the first three rows, and since the values of ■ are not concerned, the three S-boxes in the last row are free due to the analysis from the BDT. Thus only the S-box at position $(3, 1)$ should be counted. For the boomerang switch in round 7, only the S-box at position $(0, 2)$ has to be counted due to analysis of the BDT′. The choices of input/output differences of these two S-boxes might lead to different cases of 2-round boomerang switch described in Section 3.4.

After we iterated all possible input/output differences, four trails were found and they are given in Table 4. Take the first trail for example, it belongs to case (a). Although there is no overlapped S-box in the two rounds, a cost has to be paid. At the first S-box layer, the value of $\Delta y^6_{3,1}$ is fixed to 0x1f, then the 3-tuple $(\Delta_0, \Delta_1, \nabla_0)$ of the S-box at $(3, 1)$ equals to $(\texttt{0x01}, \texttt{0x1f}, \texttt{0x00})$, for which the BDT entry is 4. At the second S-box layer, the value of $\nabla x^7_{0,2}$ is fixed to 0x01, then the 3-tuple $(\nabla_0, \nabla_1, \Delta_0)$ equals to $(\texttt{0x1f}, \texttt{0x01}, \texttt{0x00})$,

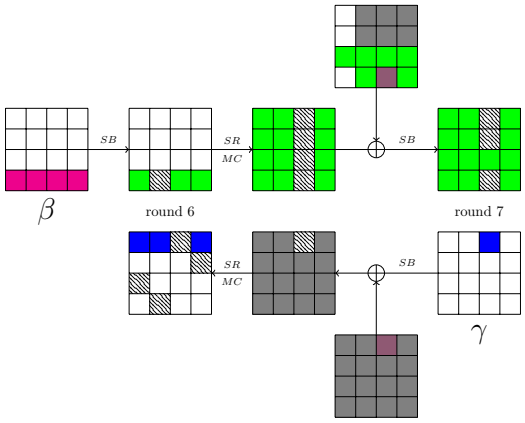


Figure 12: The middle two rounds of the boomerang attack against full AES-192 in Section 5.1. The differences of the bytes marked with slash are not fixed.

for which the BDT′ entry is 4. Thus the 2-round boomerang switch has probability $4/2^8 \cdot 4/2^8 = 2^{-12}$ for the first trail. As for the other three trails, whose differential probabilities can be computed by a similar analysis of the BDT (BDT′), they have the same probability 2^{-13}. To sum up, the switching probability for rounds 6 and 7, for the given β and γ, is $2^{12} + 3 \cdot 2^{-13} = 2^{-10.7}$. Compared to the cost of the two rounds in [BN10], which is 2^{-12}, we get a speed-up of $2^{1.3}$, and the other parts of the attack remain the same: the new boomerang attack requires $2^{114.7}$ data and $2^{167.7}$ time.

Experimental Verification. Following the algorithm in Section 2.1, we mounted an experiment to search for right quartets for the 2-round E_m in Figure 12. In the experiment, we set the data amount to 2^{20} and iterated the test for 1000 randomly chosen key quartets satisfying the required key difference. Finally the average number of right quartets obtained was 640. Hence, the success probability is $640/2^{20} = 2^{-10.7}$, which matches our analysis.

5.2 Evaluation and Improvement on The Attack from [BK09]

The attack in [BK09] is the first published attack against the full AES-192. Here, we evaluate the boomerang distinguisher from their attack, and point out some mistakes in their evaluation. It turns out that their attack can actually be even more powerful. The boomerang trail is depicted in Figure 15 of the Appendix.

Their attack uses 6-round differential characteristics for both E_0 and E_1, and applies the ladder switch in round 7. In their evaluation, they fix the value of $\Delta y^6_{0,2}$ to `0x1f` with probability 2^{-6} in the upper trail so that they can get a ladder switch in round 7. They claim that the output difference of the other two active S-boxes ($\Delta y^6_{0,1}$, $\Delta y^6_{0,3}$) can be any value such that it is the same as in the second related-key pair. Thus, in their analysis round 7 is free, and round 6 requires probability $2^{(-6-2\cdot 3.5)\cdot 2} = 2^{-26}$ for the both sides of the boomerang.

However, when considering the switching effect in round 6 and 7, we found out that the values of $\Delta y^6_{0,1}$ and $\Delta y^6_{0,3}$ should be fixed as shown in Figure 13. For the two S-boxes in round 6, the value of Δ_1 has no effect on the boomerang switch in the round 7, which means that Δ_1 could be any value. However, Δ_0 and ∇_0 are fixed to `0x01` and `0x1f`, so the number of choices of Δ_1 is only 1 according to Lemma 3: since the entries of the DDT and the BCT for (`0x01`, `0x1f`) are both 4, Δ_1 can only take the value `0x1f`. The corresponding BDT entry is 4, hence the switching probability of the two S-boxes is $2^{-6-6} = 2^{-12}$. Now, we are only left with two S-boxes: the one at $(0, 2)$ in round 6 and the other one at $(0, 2)$

in round 7. In order to get non-zero entries of the BDT (BDT′) on the two S-boxes at the same time, we iterated all the values of $\Delta y^6_{0,2}$ and obtained several valid trails which are recorded in Table 5. The probability of each trail can be computed from the analysis of the BDT (BDT′). To sum up, the probability of the 2-round boomerang switch is $2^{-22.4}$. Compared to the previous evaluation, we get a speed-up of $2^{3.6}$.

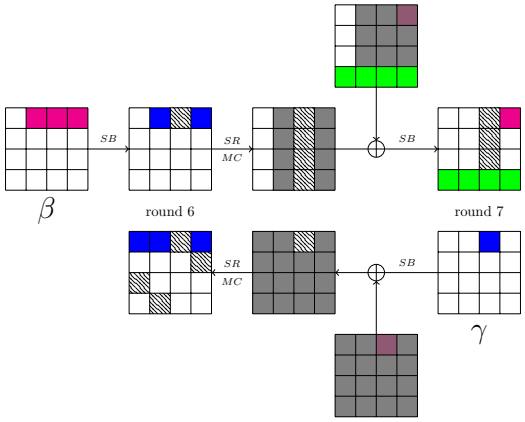


Figure 13: The middle two rounds of the boomerang attack against full AES-192 in Section 5.2. The differences of the bytes marked with slash are not fixed.

Experimental Verification. Following the algorithm in Section 2.1, we mounted a test on this reduced 2-round boomerang distinguisher using 2^{28} data, and iterated it for 100 randomly chosen key quartets. The result shows that the average success probability is $2^{-22.45}$, which demonstrates the validity of our analysis.

Further Improvement and Summary. Recall that the maximum switching probability for AES S-box is $6/2^8 = 2^{-5.4}$. Moreover, note that we can directly apply the BCT to the two S-boxes at $(0, 1)$ and $(0, 3)$ in round 6, because the output difference Δ_1 is not required to be a specific value. Hence, we can choose $\nabla_0 =$ 0x06 with which the entry of the BCT is 6 so that the switching probability for each of the two S-boxes is $2^{-5.4}$, instead of 2^{-6}. We can simply replace the difference of the truncated characteristic for E_1 by using the optimal S-box differential transition: 0xbc $\rightarrow$ 0x06 instead. The probability of other parts remains the same, so the attack can be further improved by a factor of $2^{1.2}$.

Although the improvement fails to beat the result in Section 5.1, our point is that it indicates that the boomerang switch in multiple rounds do exist in a boomerang attack. The previous boomerang attacks that ignore the switching effect are thus unlikely to be evaluated properly.

6 Applications to Deoxys-BC

In this section, we apply our method to improve the boomerang switch in the related-tweakey boomerang attacks against Deoxys-BC [CHP+17].

6.1 A Short Description of Deoxys-BC

Deoxys [JNPS16] is an authenticated encryption scheme and was selected as one of the CAESAR finalist. Its internal primitive Deoxys-BC is a 128-bit AES-based tweakable block cipher following the TWEAKEY framework [JNP14]. It has a linear tweakey

schedule and the same round function as AES[3]. Deoxys-BC has two versions: Deoxys-BC-256 and Deoxys-BC-384. Both versions take three inputs: a plaintext, a key and a tweak. The concatenation of key and tweak is named as *tweakey*, whose size is 256-bit for Deoxys-BC-256 and 384-bit for Deoxys-BC-384. In this paper, we focus on the attack of Deoxys-BC-256.

6.2 Improved 10-Round Boomerang Attack

At FSE 2018, Cid *et al.* [CHP+17] proposed a boomerang attack against 10-round Deoxys-BC-256 including a 9-round boomerang distinguisher with probability 2^{-122}, as shown in Table 6. The distinguisher is produced by taking into account the ladder switch in two rounds, which are rounds 5 and 6. However, they did not provide a concrete analysis of the two rounds. Here, our goal is to provide a specific BDT-based analysis, then search for new differential characteristics with higher probability.

As we can see in Table 6, both differential characteristics for E_0 and E_1 have an active S-box at position $(1,1)$ in round 6, and the S-box is regarded as a part of E_1 by the ladder switch. The characteristic for E_1 specifies the input and output difference (from 0x32 to 0x2f), which has differential probability 2^{-7}, and the differential characteristics for E_0 and E_1 have no same active S-box in round 5, so the probability for rounds 5 and 6 is 2^{-14} in the boomerang distinguisher. In their analysis, the differential for the S-box at position $(1,1)$ in round 6 of E_0 is denoted with **, which means its value is not crucial to the distinguisher. However, we show that the differential in E_0 is crucial by the analysis on the BDT′. For the targeted S-box, the characteristic for E_1 fixes the ∇_0 and ∇_1 to 0x2f and 0x32, respectively. We confirmed that there exists only one choice of Δ_0 such that the BDT′ entry for $(\texttt{0x2f}, \texttt{0x32}, \Delta_0)$ is nonzero. The value is 0x32 (0x00 is excluded due to the characteristics for E_0), and the BDT entry is 2. Then, we can uniquely obtain the value $\Delta y^5_{1,2} = \texttt{0x19}$ in the characteristic for E_0 through the inverse MixColumns. For the S-box at position $(1,2)$ in round 5, the differential characteristic for E_0 fixes the $\Delta_0 = \texttt{0x80}$ and $\Delta_1 = \texttt{0x19}$, and the characteristic for E_1 fixes $\nabla_1 = 0$. The BDT entry for $(\texttt{0x80}, \texttt{0x19}, \texttt{0x00})$ is 2. Therefore, the probability 2^{-14} of the two rounds comes from the two bytes in round 5 and round 6, respectively.

Since the switching probability is determined, the possible direction to improve the attack becomes clear. Recall that the optimal switching probability is $2^{-5.4}$ for the AES S-box, thus a potential direction is to try to improve the switching probability in round 5 or round 6 or both. Due to the careful optimization done in [CHP+17], we will use the same truncated differential characteristics and only replace the difference. We borrowed the strategy of using an automated search tool from [CHP+17], and obtained a new differential characteristic for E_1, as shown in Table 7. At position $(1,2)$ in round 5, the BDT entry for $(\texttt{0x80}, \texttt{0xae}, \texttt{0x00})$ is 4 which gives probability 2^{-6}, and the switching probability at position $(1,1)$ in round 6 is 2^{-7} because the BDT′ entry is 2 for $(\texttt{0xe1}, \texttt{0x47}, \texttt{0x47})$. Moreover, there exists another differential characteristic with the same differential and has probability 2^{-14}, as shown in Table 8. In the end, the switching probability in rounds 5 and 6 is $2^{-13} + 2^{-14} = 2^{-12.4}$. We get a speed-up of $2^{1.6}$ and the probability of the new boomerang distinguisher is $2^{-120.4}$.

Experimental Verification. In the experiment, we used 2^{20} data, and iterated it for 1000 randomly chosen key quartets. The result shows that the average success probability is $2^{-12.4}$, which confirms our improvement evaluation.

[3]We omit the specification of Deoxys-BC here, the reader can refer to Section 4.1

7 Conclusions

In this paper, we performed an extensive analysis of the switching effect between the two differential characteristics of a boomerang distinguisher. Specifically, we exploited the principle behind the ladder switch, and showed that the sparser the diffusion layer is, the more rounds the switching effect exists. Moreover, we introduced the BDT as a generalized method to easily evaluate the boomerang switching probability in multiple rounds. The extended switching effect was demonstrated by several applications, which includes the currently best related-key attack on 10-round `AES`-256, two improved attacks on full `AES`-192 and an improved attack on `Deoxys`-BC.

Finally, we would like to emphasize that the boomerang switching effect can exist in multiple rounds, regardless of the attacker creating it deliberately or not. This phenomenon was so far widely ignored by the cryptanalysis community.

Acknowledgments

The authors would like to thank the anonymous referees for their helpful comments. The authors are supported by Temasek Labs (DSOCL16194).

References

[BC18] Christina Boura and Anne Canteaut. On the boomerang uniformity of cryptographic sboxes. *IACR Transactions on Symmetric Cryptology*, 2018(3):290–310, 2018.

[BDD03] Alex Biryukov, Christophe De Cannière, and Gustaf Dellkrantz. Cryptanalysis of SAFER++. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 195–211, Santa Barbara, CA, USA, August 17–21, 2003. Springer, Heidelberg, Germany.

[BDK01] Eli Biham, Orr Dunkelman, and Nathan Keller. The rectangle attack - rectangling the Serpent. In Birgit Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 340–357, Innsbruck, Austria, May 6–10, 2001. Springer, Heidelberg, Germany.

[BDK02] Eli Biham, Orr Dunkelman, and Nathan Keller. New results on boomerang and rectangle attacks. In Joan Daemen and Vincent Rijmen, editors, *Fast Software Encryption – FSE 2002*, volume 2365 of *Lecture Notes in Computer Science*, pages 1–16, Leuven, Belgium, February 4–6, 2002. Springer, Heidelberg, Germany.

[BDK05] Eli Biham, Orr Dunkelman, and Nathan Keller. Related-key boomerang and rectangle attacks. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 507–525, Aarhus, Denmark, May 22–26, 2005. Springer, Heidelberg, Germany.

[BDK+10] Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir. Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 299–319, French Riviera, May 30 – June 3, 2010. Springer, Heidelberg, Germany.

[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, *Advances in Cryptology – CRYPTO 2016, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153, Santa Barbara, CA, USA, August 14–18, 2016. Springer, Heidelberg, Germany.

[BK03] Mihir Bellare and Tadayoshi Kohno. A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 491–506, Warsaw, Poland, May 4–8, 2003. Springer, Heidelberg, Germany.

[BK09] Alex Biryukov and Dmitry Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 1–18, Tokyo, Japan, December 6–10, 2009. Springer, Heidelberg, Germany.

[BKN09] Alex Biryukov, Dmitry Khovratovich, and Ivica Nikolic. Distinguisher and related-key attack on the full AES-256. In Shai Halevi, editor, *Advances in Cryptology – CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 231–249, Santa Barbara, CA, USA, August 16–20, 2009. Springer, Heidelberg, Germany.

[BN10] Alex Biryukov and Ivica Nikolic. Automatic search for related-key differential characteristics in byte-oriented block ciphers: Application to AES, Camellia, Khazad and others. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 322–344, French Riviera, May 30 – June 3, 2010. Springer, Heidelberg, Germany.

[BS91] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. In Alfred J. Menezes and Scott A. Vanstone, editors, *Advances in Cryptology – CRYPTO'90*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21, Santa Barbara, CA, USA, August 11–15, 1991. Springer, Heidelberg, Germany.

[CHP+17] Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. A security analysis of Deoxys and its internal tweakable block ciphers. *IACR Transactions on Symmetric Cryptology*, 2017(3):73–107, 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, *Advances in Cryptology – EUROCRYPT 2018, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 683–714, Tel Aviv, Israel, April 29 – May 3, 2018. Springer, Heidelberg, Germany.

[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, *Advances in Cryptology – CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 393–410, Santa Barbara, CA, USA, August 15–19, 2010. Springer, Heidelberg, Germany.

[DKS14] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. *Journal of Cryptology*, 27(4):824–849, October 2014.

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

[Dun18] Orr Dunkelman. Efficient construction of the boomerang connection table. *IACR Cryptology ePrint Archive*, 2018:631, 2018.

[JNP14] Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Tweaks and keys for block ciphers: The TWEAKEY framework. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014, Part II*, volume 8874 of *Lecture Notes in Computer Science*, pages 274–288, Kaoshiung, Taiwan, R.O.C., December 7–11, 2014. Springer, Heidelberg, Germany.

[JNPS16] Jérémy Jean, Ivica Nikolic, Thomas Peyrin, and Yannick Seurin. Deoxys v1. 41. *Submitted to CAESAR*, 2016.

[KHP07] Jongsung Kim, Seokhie Hong, and Bart Preneel. Related-key rectangle attacks on reduced AES-192 and AES-256. In Alex Biryukov, editor, *Fast Software Encryption – FSE 2007*, volume 4593 of *Lecture Notes in Computer Science*, pages 225–241, Luxembourg, Luxembourg, March 26–28, 2007. Springer, Heidelberg, Germany.

[KKS01] John Kelsey, Tadayoshi Kohno, and Bruce Schneier. Amplified boomerang attacks against reduced-round MARS and Serpent. In Bruce Schneier, editor, *Fast Software Encryption – FSE 2000*, volume 1978 of *Lecture Notes in Computer Science*, pages 75–93, New York, NY, USA, April 10–12, 2001. Springer, Heidelberg, Germany.

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

[Wag99] David Wagner. The boomerang attack. In Lars R. Knudsen, editor, *Fast Software Encryption – FSE'99*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170, Rome, Italy, March 24–26, 1999. Springer, Heidelberg, Germany.

A The Round Function of SKINNY

The internal state of SKINNY [BJK+16] is represented as a 4×4 array, the round function consisting of five operations:

1. *Subcells* - The S-box is applied to all cells (4-bit S-box for SKINNY-64, 8-bit S-box for SKINNY-128).
2. *AddRoundConstants* - Three round constants are added to the first column of the internal state.
3. *AddRoundTweakey* - The round tweakey is XORed to the first two rows of the internal state.
4. *ShiftRows* - A cyclic shift of the i-th row by i positions is applied to the right, for $i = 0, 1, 2, 3$.
5. *MixColumns* - Each array column is multiplied by a binary matrix M. The matrix M^{-1} of the inverse *MixColumns* is also shown below.

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \qquad M^{-1} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

B Differential Paths and Boomerang Distinguishers

In this section, we give all the details of the differential characteristics that are used in this paper. By ΔA we denote the upper trail difference in the internal state, and by ∇A the same for the lower trail. The differences are represented in hexadecimal and differences that are not crucial to the distinguishers are denoted with "$**$". The S-boxes that are crucial for the boomerang switch are highlighted in red.

Color Scheme. We extensively use colors in our figures in order to provide better understanding. Here is the color scheme utilized.

- Fixed S-box input difference.
- Fixed S-box output difference.
- Arbitrary difference.
- Unfixed difference, depending on different characteristics.
- `MixColumns` expansion of .

Table 3: Internal state difference for rounds 8 and 9 in the 9-round distinguisher of `AES`-256. The trails denoted with † have the same ΔA as trail 1.

trail		round 8		round 9		prob.
		before SB	after SB	before SB	after SB	
1	ΔA	02 02 02 02 00 00 00 00 00 00 00 00 00 00 00 00	14 ** ** ** 00 00 00 00 00 00 00 00 00 00 00 00	00 ** ** ** 00 ** ** ** 00 ** ** ** ** ** ** **	00 ** ** ** 00 ** ** ** 00 ** ** ** ** ** ** **	$2^{-6} \cdot 2^{-7}$
	∇A	** 00 00 00 00 ** 00 00 00 00 ** 00 00 00 00 **	14 00 00 00 00 1e 00 00 00 00 a9 00 00 00 00 c8	6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
2†	∇A	** 00 00 00 00 ** 00 00 00 00 ** 00 00 00 00 **	8c 00 00 00 00 ca 00 00 00 00 a2 00 00 00 00 fe	1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	$2^{-6} \cdot 2^{-7}$
3†	∇A	** 00 00 00 00 ** 00 00 00 00 ** 00 00 00 00 **	98 00 00 00 00 d4 00 00 00 00 0b 00 00 00 00 36	71 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	$2^{-6} \cdot 2^{-6}$

Table 4: Differential characteristic of the middle two rounds that is used in the boomerang attack against AES-192 in Section 5.1.

trail		round 6		round 7		prob.
		before SB	after SB	before SB	after SB	
1	ΔA	00 00 00 00 00 00 00 00 00 00 00 00 01 01 01 01	00 00 00 00 00 00 00 00 00 00 00 00 ** 1f ** **	** ** 00 ** ** ** 00 ** ** ** ** ** ** ** 01 **	** ** 00 ** ** ** 00 ** ** ** ** ** ** ** ** **	$2^{-6} \cdot 2^{-6}$
	∇A	** ** ** ** 00 00 00 00 00 00 00 00 00 00 00 00	1f 1f 1f 1f 00 00 00 00 00 00 00 00 00 00 00 00	00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 1f 00 00 00 00 00 00 00 00 00 00 00 00 00	
2	ΔA	00 00 00 00 00 00 00 00 00 00 00 00 01 01 01 01	00 00 00 00 00 00 00 00 00 00 00 00 ** 1f ** **	** ** 00 ** ** ** 00 ** ** ** ** ** ** ** 01 **	** ** 00 ** ** ** 00 ** ** ** ** ** ** ** ** **	$2^{-6} \cdot 2^{-7}$
	∇A	** ** ** ** 00 00 00 ** ** 00 00 00 00 01 00 00	1f 1f ce 1f 00 00 00 34 62 00 00 00 00 1f 00 00	00 00 99 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 1f 00 00 00 00 00 00 00 00 00 00 00 00 00	
3	ΔA	00 00 00 00 00 00 00 00 00 00 00 00 01 01 01 01	00 00 00 00 00 00 00 00 00 00 00 00 ** $a3$ ** **	** ** bc ** ** ** bc ** ** ** ** ** ** ** 62 **	** ** 06 ** ** ** ** ** ** ** ** ** ** ** ** **	$2^{-7} \cdot 2^{-6}$
	∇A	** ** ** ** 00 00 00 00 00 00 00 00 00 00 00 00	1f 1f 1f 1f 00 00 00 00 00 00 00 00 00 00 00 00	00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 1f 00 00 00 00 00 00 00 00 00 00 00 00 00	
4	ΔA	00 00 00 00 00 00 00 00 00 00 00 00 01 01 01 01	00 00 00 00 00 00 00 00 00 00 00 00 ** 1e ** **	** ** 01 ** ** ** 01 ** ** ** ** ** ** ** 03 **	** ** 1f ** ** ** ** ** ** ** ** ** ** ** ** **	$2^{-7} \cdot 2^{-6}$
	∇A	** ** ** ** 00 00 00 00 00 00 00 00 00 00 00 00	1f 1f 1f 1f 00 00 00 00 00 00 00 00 00 00 00 00	00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 1f 00 00 00 00 00 00 00 00 00 00 00 00 00	

Table 5: Differential characteristic of the middle two rounds that is used in the boomerang attack against AES-192 in Section 5.2. The trails denoted with † have the same ΔA as trail 1.

trail		round 6		round 7		prob.
		before SB	after SB	before SB	after SB	
1	ΔA	00 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00	00 1f 1f 1f 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 ** 00 00 00 00 00 00 00 00 ** ** ** **	00 00 00 ** 00 00 00 00 00 00 00 00 ** ** ** **	$2^{-18} \cdot 2^{-6}$
	∇A	** 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00	1f 1f 1f 1f 00 00 00 00 00 00 00 00 00 00 00 00	00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 1f 00 00 00 00 00 00 00 00 00 00 00 00 00	
2†	∇A	** 01 00 01 00 00 00 ** ** 00 00 00 00 ** 00 00	1f 1f 00 1f 00 00 00 9d 45 00 00 00 00 f1 00 00	00 00 37 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 1f 00 00 00 00 00 00 00 00 00 00 00 00 00	$2^{-18} \cdot 2^{-7}$
3†	∇A	** 01 bc 01 00 00 00 ** ** 00 00 00 00 ** 00 00	1f 1f 06 1f 00 00 00 98 fb 00 00 00 00 2c 00 00	00 00 5f 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 1f 00 00 00 00 00 00 00 00 00 00 00 00 00	$2^{-18} \cdot 2^{-7}$
4†	∇A	** 01 bd 01 00 00 00 ** ** 00 00 00 00 ** 00 00	1f 1f 19 1f 00 00 00 05 be 00 00 00 00 d5 00 00	00 00 69 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 1f 00 00 00 00 00 00 00 00 00 00 00 00 00	$2^{-18} \cdot 2^{-7}$
5	ΔA	00 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00	00 1f 89 1f 00 00 00 00 00 00 00 00 00 00 00 00	00 00 37 ** 00 00 96 00 00 00 96 00 ** ** ** **	00 00 1f ** 00 00 ** 00 00 00 ** 00 ** ** ** **	$2^{-19} \cdot 2^{-7}$
	∇A	** 01 00 01 00 00 00 ** ** 00 00 00 00 ** 00 00	1f 1f 00 1f 00 00 00 9d 45 00 00 00 00 f1 00 00	00 00 37 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 1f 00 00 00 00 00 00 00 00 00 00 00 00 00	
6	ΔA	00 01 01 01 00 00 00 00 00 00 00 00 00 00 00 00	00 1f b2 1f 00 00 00 00 00 00 00 00 00 00 00 00	00 00 41 ** 00 00 ad 00 00 00 ad 00 ** ** ** **	00 00 1f ** 00 00 ** 00 00 00 ** 00 ** ** ** **	$2^{-19} \cdot 2^{-7}$
	∇A	** 01 01 01 00 00 00 ** ** 00 00 00 00 ** 00 00	** 01 b2 01 00 00 00 76 6d 00 00 00 00 f6 00 00	00 00 41 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 1f 00 00 00 00 00 00 00 00 00 00 00 00 00	

Table 6: The 9-round distinguisher of Deoxys-BC-256 from [CHP+17]

round	initial Δ	tweakey Δ	before SB	after SR	prob.
1	00 00 7*b* 00 *b*0 *c*0 00 00 00 00 *af* 00 00 00 00 *c*2	00 00 7*b* 00 *b*0 *c*0 00 00 00 00 *af* 00 00 00 00 *c*2	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	1
2	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	*e*0 80 00 00 00 4*d* 00 00 00 00 00 00 00 00 00 *ea*	*e*0 80 00 00 00 4*d* 00 00 00 00 00 00 00 00 00 *ea*	*b*4 *c*9 00 00 21 00 00 00 00 00 00 00 73 00 00 00	2^{-28}
3	63 89 00 00 85 *c*9 00 00 00 *c*9 00 00 00 40 00 00	00 89 00 00 85 00 00 00 00 *c*9 00 00 00 40 00 00	63 00 00 00 00 *c*9 00 00 00 00 00 00 00 00 00 00	8*d* 00 00 00 8*c* 00 00 00 00 00 00 00 00 00 00 00	2^{-14}
4	8*e* 00 00 00 8*e* 00 00 00 01 00 00 00 00 00 00 00	8*e* 00 00 00 8*e* 00 00 00 01 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	1
5	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 80 03 13 00 00 00 00 98 00 00	00 00 00 00 00 00 80 03 13 00 00 00 00 98 00 00	00 00 00 00 00 ** ** 00 00 00 ** 00 00 00 ** 00	1
6	00 ** ** 00 00 ** ** 00 00 ** ** 00 00 ** ** 00	00 00 81 07 00 00 00 35 00 00 00 *b*4 00 1*d* 00 00	00 ** ** 07 00 ** ** 35 00 ** ** *b*4 00 ** ** 00	00 ** ** ** ** ** ** 00 ** ** 00 ** 00 00 ** **	1
5	** ** 00 ** ** ** 00 55 00 ** ** ** ** 00 ** **	00 00 00 00 00 00 00 55 00 00 00 00 00 00 00 84	** ** 00 ** ** ** 00 00 00 ** ** ** ** 00 ** **	** *e*4 00 ** ** 00 00 ** ** 8*f* 00 ** ** 5*c* 00 **	1
6	** 00 00 49 00 32 00 00 00 05 00 00 00 00 00 **	00 00 00 49 00 00 00 00 00 05 00 00 00 00 00 00	** 00 00 00 00 32 00 00 00 00 00 00 00 00 00 **	*ee* 00 00 00 2*f* 00 00 00 00 00 00 00 *b*6 00 00 00	2^{-7}
7	00 00 00 00 06 00 00 00 00 00 00 00 71 00 00 00	00 00 00 00 06 00 00 00 00 00 00 00 71 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	1
8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	1
9	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 *e*3 00 00 00 00 00 00 00 0*c* 00 00	00 00 00 00 00 *e*3 00 00 00 00 00 00 00 0*c* 00 00	00 00 00 00 72 00 00 00 00 00 00 00 00 00 9*d* 00	2^{-12}

Table 7: Improved 9-round distinguisher for Deoxys-BC-256. The probabilities marked with † are only counted once due to the 2-round boomerang switch.

round	initial Δ	tweakey Δ	before SB	after SR	prob.
5	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 80 03 13 00 00 00 00 98 00 00	00 00 00 00 00 00 80 03 13 00 00 00 00 98 00 00	00 00 00 00 00 ae ** 00 00 00 ** 00 00 00 ** 00	2^{-6} †
6	00 $e9$ ** 00 00 47 ** 00 00 ae ** 00 00 ae ** 00	00 00 81 07 00 00 00 35 00 00 00 $b4$ 00 1d 00 00	00 $e9$ ** 07 00 47 ** 35 00 ae ** $b4$ 00 $b3$ ** 00	00 ** ** ** ** ** ** 00 ** ** 00 ** 00 00 ** **	1
5	** ** 00 ** ** ** 00 2a 00 ** ** ** ** 00 ** **	00 00 00 00 00 00 00 2a 00 00 00 00 00 00 00 11	** ** 00 ** ** ** 00 00 00 ** ** ** ** 00 ** **	** ab 00 ** ** 00 00 ** ** dd 00 ** ** 90 00 **	1
6	** 00 00 24 00 47 00 00 00 $a1$ 00 00 00 00 00 **	00 00 00 24 00 00 00 00 00 $a1$ 00 00 00 00 00 00	** 00 00 00 00 47 00 00 00 00 00 00 00 00 00 **	$e9$ 00 00 00 $e1$ 00 00 00 00 00 00 00 $f1$ 00 00 00	2^{-7} †
7	00 00 00 00 $c1$ 00 00 00 00 00 00 00 38 00 00 00	00 00 00 00 $c1$ 00 00 00 00 00 00 00 38 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	1
8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	1
9	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 71 00 00 00 00 00 00 00 83 00 00	00 00 00 00 00 71 00 00 00 00 00 00 00 83 00 00	00 00 00 00 $c0$ 00 00 00 00 00 00 00 00 00 8f 00	2^{-12}
Master tweakey difference ∇K 00 00 00 00 00 $d0$ 00 $7e$ 00 00 00 00 00 00 00 00 00 00 00 00 00 df 00 66 00 00 00 00 00 00 00 00					

Table 8: Another 2-round differential characteristic of the boomerang distinguisher in Table 7. The probabilities marked with † are only counted once due to the 2-round boomerang switch.

round	initial Δ	tweakey Δ	before SB	after SR	prob.
5	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 80 03 13 00 00 00 00 98 00 00	00 00 00 00 00 00 80 03 13 00 00 00 00 98 00 00	00 00 00 00 00 96 ** 00 00 00 ** 00 00 00 ** 00	2^{-7} †
6	00 $a1$ ** 00 00 37 ** 00 00 96 ** 00 00 96 ** 00	00 00 81 07 00 00 00 35 00 00 00 $b4$ 00 1d 00 00	00 $a1$ ** 07 00 37 ** 35 00 96 ** $b4$ 00 $8b$ ** 00	00 ** ** ** ** ** ** 00 ** ** 00 ** 00 00 ** **	1
5	** ** 00 ** ** ** 00 2a 00 ** ** ** ** 00 ** **	00 00 00 00 00 00 00 2a 00 00 00 00 00 00 00 11	** ** 00 ** ** ** ** 00 00 ** ** 00 ** 00 ** **	** 96 00 ** ** 96 00 ** ** 00 00 ** ** 96 00 **	1
6	** 00 00 24 00 37 00 00 00 $a1$ 00 00 00 00 00 **	00 00 00 24 00 00 00 00 00 $a1$ 00 00 00 00 00 00	** 00 00 00 00 37 00 00 00 00 00 00 00 00 00 **	$e9$ 00 00 00 $e1$ 00 00 00 00 00 00 00 $f1$ 00 00 00	2^{-7} †

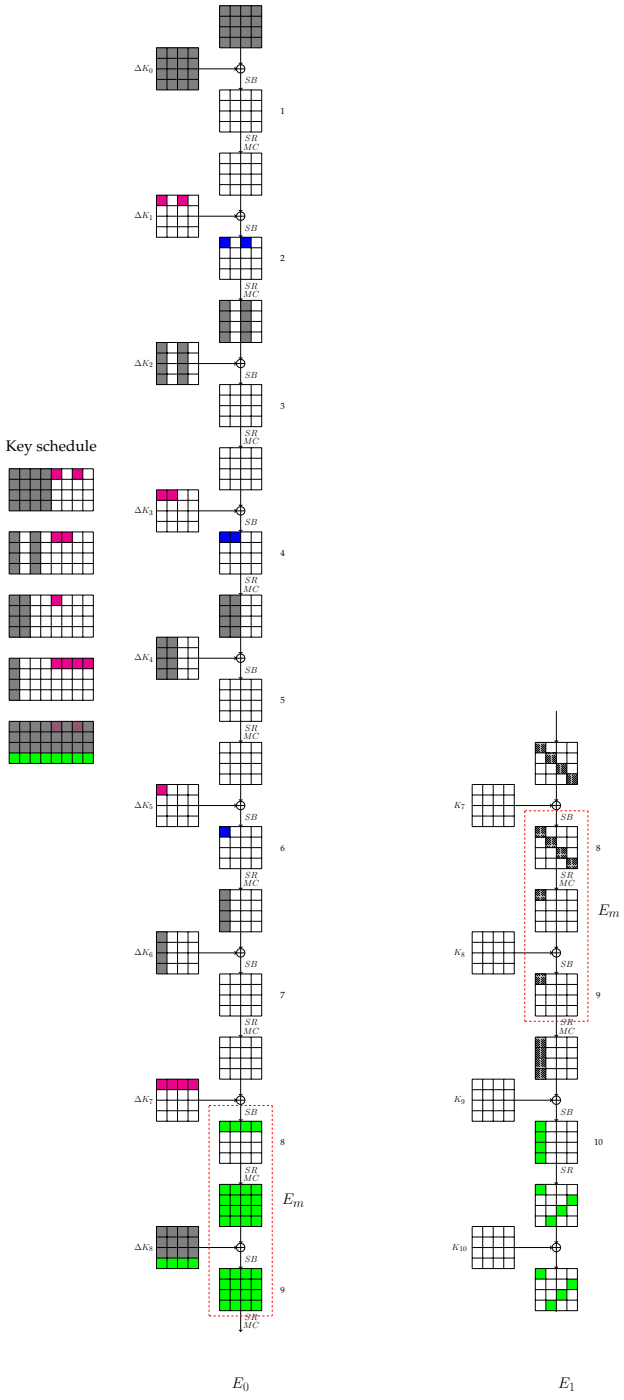


Figure 14: Boomerang attack on 10-round AES-256. The red rectangles depict the locations of 2-round boomerang switch.

Figure 15: Two boomerang attacks on full-round AES-192. For E_0, the left trail is the one used in [BK09] and is evaluated in Section 5.2, the middle trail is the one used in Section 5.1. Both attacks use the same trail for E_1 as shown on the right-hand side. The red rectangles depict the locations of 2-round boomerang switch.