Des. Codes Cryptogr. (2011) 60:123–143
DOI 10.1007/s10623-010-9421-9

The (related-key) impossible boomerang attack and its application to the AES block cipher

Jiqiang Lu

Received: 6 July 2009 / Revised: 5 July 2010 / Accepted: 22 July 2010 /
Published online: 10 August 2010

Abstract The Advanced Encryption Standard (AES) is a 128-bit block cipher with a user key of 128, 192 or 256 bits, released by NIST in 2001 as the next-generation data encryption standard for use in the USA. It was adopted as an ISO international standard in 2005. Impossible differential cryptanalysis and the boomerang attack are powerful variants of differential cryptanalysis for analysing the security of a block cipher. In this paper, building on the notions of impossible differential cryptanalysis and the boomerang attack, we propose a new cryptanalytic technique, which we call the impossible boomerang attack, and then describe an extension of this attack which applies in a related-key attack scenario. Finally, we apply the impossible boomerang attack to break 6-round AES with 128 key bits and 7-round AES with 192/256 key bits, and using two related keys we apply the related-key impossible boomerang attack to break 8-round AES with 192 key bits and 9-round AES with 256 key bits. In the two-key related-key attack scenario, our results, which were the first to achieve this amount of attacked rounds, match the best currently known results for AES with 192/256 key bits in terms of the numbers of attacked rounds. The (related-key) impossible boomerang attack is a general cryptanalytic technique, and can potentially be used to cryptanalyse other block ciphers.

Keywords Cryptology · Block cipher · AES · Differential cryptanalysis · Boomerang attack · Related-key attack

Mathematics Subject Classification (2000) 94A60

Communicated by Vincent van Rijmen.

An earlier version appeared in 2008 in the PhD thesis [35] of the author.

J. Lu (✉)
Department of Mathematics and Computer Science, Eindhoven University of Technology,
5600 MB Eindhoven, The Netherlands
e-mail: lvjiqiang@hotmail.com

1 Introduction

Differential cryptanalysis, proposed by Biham and Shamir [11] in 1990, is well known as a powerful technique for analysing the security of a block cipher. Typically, to break a block cipher, differential cryptanalysis uses a relatively long differential (i.e. that operating on as many rounds of the cipher as possible) with a probability larger than that for a random permutation that operates on data blocks of the same length. In 1998 and 1999, Knudsen [33] and Biham et al. [3] independently proposed a variant of differential cryptanalysis, known as impossible differential cryptanalysis; it uses a (relatively long) differential with a zero probability, called an impossible differential. In 1999, Wagner [46] proposed the boomerang attack—another variant of differential cryptanalysis, which, unlike differential cryptanalysis, involves something called a boomerang distinguisher that treats a block cipher as two parts and uses two short differentials with relatively large probabilities on the two parts of the cipher, instead of a long differential with a small probability on the entire cipher. Subsequently, several variants of the boomerang attack have been proposed, including the amplified boomerang attack [27], the rectangle attack [5], the differential-(bi)linear boomerang attack [7] and the related-key boomerang and rectangle attacks [8,24,30].

The Advanced Encryption Standard (AES) [43] is a 128-bit block cipher with a user key of 128, 192 or 256 bits. It was released by NIST [44] in 2001 as the new-generation data encryption standard for use in the USA, and was adopted as an ISO [25] international standard in 2005. We denote by AES-128/192/256 the versions of AES that respectively use 128, 192 and 256 key bits. Due to its increasingly wide use in many real-life cryptographic applications, AES has always been being analysed against different cryptanalytic techniques, and a variety of cryptanalytic results have been published [1,8, 10,12–16,18,19,21–24,26,29,36,40,45,48–51]. In summary, in terms of the numbers of attacked rounds, the most significant results are Biryukov and Khovratovich's related-key (amplified) boomerang attacks on the full-round AES-192/256 [14], and each attack uses four related keys. (We note that Murphy [42] commented recently that the claims made in [14] by Biryukov and Khovratovich for a related key boomerang analysis of AES must be regarded as unsubstantiated). A related-key attack [2,28,31] assumes that the attacker knows or can choose the differences between two or more unknown keys; the more keys are involved, the more difficult and impractical the attack is to conduct. We assume that exhaustive key search (i.e. brute force search) is the best generic attack in the related-key attack scenarios as well as in the one key attack scenario, and an attack is regarded as effective if it is faster (i.e. it has lower time complexity) than exhaustive key search. The two-key related-key attack scenario is the simplest among the related-key attack scenarios. Thus, it is still of great significance to continue investigating the security of AES in the single-key attack scenario and the two-key related-key attack scenario. In the single-key attack scenario, attacks on 7-round AES-128, 8-round AES-192 and 8-round AES-256 [1,21,23,36,50] are the best currently known results for AES-128/192/256; and in the two-key related-key attack scenario, attacks on 8-round AES-192 and 9-round AES-256 [13,26,29,48,51] are the best currently known results for AES-192/256.[1]

[1] When we initially submitted this paper, the related-key impossible differential attack on 8-round AES-256 given in [49] was the best cryptanalytic result for AES-256 in the two-key related-key attack scenario. Recently, Biryukov et al. [13] gave a related-key differential attack on 9-round AES-256 in the two-key related-key attack scenario; and they also described a few cryptanalytic results in a related-subkey attack scenario—a more difficult attack scenario than a related-key attack scenario. In this revised version, we incorporate Biryukov et al.'s 9-round AES-256 attack in the two-key related-key attack scenario, and do not consider the related-subkey attack scenario.

Since the standardization of AES in 2001, few new techniques have been reported, despite the efforts of many cryptanalysts. Like AES, most modern block ciphers are designed to be secure against differential cryptanalysis and linear cryptanalysis [41]. Thus, proposing new cryptanalytic techniques is always desirable in the sense that it provides a better evaluation of the security of a block cipher and also enables more secure ciphers to be designed. Impossible differential cryptanalysis and the boomerang-type attacks (including the boomerang, amplified boomerang and rectangle attacks as well as their variants in a related-key attack scenario) have been used to yield the best currently published cryptanalytic results for a number of state-of-the-art block ciphers [9,14,20,36]. These techniques are thus clearly of importance.

In this paper, inspired by the notions that impossible differential cryptanalysis and the boomerang attack use, we propose a new cryptanalytic technique, which we call the impossible boomerang attack. Such an attack is based on the use of a so-called impossible-boomerang distinguisher, which, like a boomerang distinguisher, treats a block cipher $\mathbf{E}$ as two sub-ciphers $\mathbf{E}^0 \circ \mathbf{E}^1$. Typically, it uses two (or more) differentials with probability 1 for $\mathbf{E}^0$ and two (or more) differentials with probability 1 for $\mathbf{E}^1$, where the XOR of the intermediate differences of these differentials is not equal to zero (this point makes it different in nature from the boomerang distinguisher). We then describe an extension of this attack that applies in a related-key attack scenario, giving rise to what we call a related-key impossible boomerang attack. Finally, we apply the impossible boomerang attack to break 6-round AES-128 and 7-round AES-192/256 (in the single-key attack scenario), and apply the related-key impossible boomerang attack to break 8-round AES-192 and 9-round AES-256 in the two-key related-key attack scenario. In terms of the numbers of attacked rounds, the impossible boomerang attacks on AES-128/192/256 are one round less than the best currently known cryptanalytic results in the single-key attack scenario, and the related-key impossible boomerang attacks on 8-round AES-192 and 9-round AES-256 match the best currently known results for AES-192/256 in the two-key related-key attack scenario. Table 1 summarises our new and the currently known main cryptanalytic results on AES in the single-key attack scenario and the two-key related-key attack scenario, where CP and RK-CP respectively refer to the required numbers of chosen plaintexts and related-key chosen plaintexts, Enc. refers to the required number of encryption operations of the relevant reduced-round version of AES-128/192/256, and MA refers to the number of memory accesses.

The reminder of the paper is organised as follows. In the next section we briefly describe the notation and the AES block cipher. In Sect. 3 we propose the (related-key) impossible boomerang attack. In Sects. 4 and 5 we present our new cryptanalytic results on AES. Sect. 6 concludes this paper.

2 Preliminaries

2.1 Notation

The 16 bytes of a 4×4 byte array are numbered from left to right from top to bottom, starting with 0, as shown in Fig. 1. We use the following notation throughout this paper.

$\oplus$ bitwise logical exclusive OR (XOR) of two bit strings of the same length

$\circ$ functional composition. When composing functions X and Y, $X \circ Y$ denotes the function obtained by first applying X and then applying Y

$\star$ an arbitrary 8-bit value, where two values represented by the $\star$ symbol may be different

Table 1 Summary of our new and the currently known main cryptanalytic results on AES in the single-key attack scenario and the two-key related-key attack scenario

Cipher	Keys	Attack technique	Rounds	Data	Time	Source
AES-128	1	Square	7	2^{119}–2^{128}CP	2^{120}Enc.	[21]
		Collision	7	2^{32}CP	2^{128}Enc.	[23]
		Impossible differential	7	$2^{112.2}$CP	$2^{117.2}$MA	[36]
		Impossible boomerang	6	$2^{112.2}$CP	$2^{112.3}$Enc.	Sect. 4.2
AES-192	1	Square	8	2^{119}–2^{128}CP	2^{188}Enc.	[21]
		Impossible boomerang	7	$2^{112.5}$CP	$2^{186.3}$Enc.	Sect. 4.2
	2	Related-key impossible differential	8	2^{88}RK-CP	2^{183}Enc.	[26]
			8	2^{112}RK-CP	2^{136}Enc.	[48]
		Related-key rectangle	8	2^{94}RK-CP	2^{120}Enc.	[29]
		Related-key differential-linear	8	2^{118}RK-CP	2^{165}Enc.	[51]
		Related-key impossible boomerang	8	$2^{122.4}$RK-CP	$2^{167.7}$Enc.	Sect. 5.1
AES-256	1	Square	8	2^{119}–2^{128}CP	2^{204}Enc.	[21]
		Meet-in-the-middle	8	2^{32}CP	2^{200}Enc.	[19]
		Impossible differential	8	$2^{89.1}$CP	$2^{229.7}$MA	[36]
		Impossible boomerang	7	$2^{112.8}$CP	$2^{186.9}$Enc.	Sect. 4.2
	2	Related-key impossible differential	8	2^{112}RK-CP	2^{143}Enc.	[49]
		Related-key differential	9	2^{38}RK-CP	2^{39}Enc.	[13]
		Related-key impossible boomerang	9	2^{123}RK-CP	$2^{239.9}$Enc.	Sect. 5.2

Fig. 1 The 16 byte positions of a 4 × 4 byte array

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

$\lfloor x \rfloor$ the largest integer that is less than or equal to x
$\mathbf{E}_K$ a block cipher $\mathbf{E}$ when used with a user key K

2.2 The AES block cipher

AES [43] takes as input a 128-bit plaintext block P, represented as a 4 × 4 byte array, and has a total of N_r rounds, where N_r is 10 for AES-128, 12 for AES-192, and 14 for AES-256. AES uses the following four elementary operations to construct the round function:

– The AddRoundKey operation (denoted below by ARK) XORs a 4 × 4 byte array with a 16-byte subkey.
– The SubBytes operation (denoted below by SB) applies the same 8 × 8-bit bijective S-box 16 times in parallel to a 4 × 4 byte array.
– The ShiftRows operation (denoted below by SR) cyclically shifts the jth row of a 4 × 4 byte array to the left by j bytes, $(0 \leq j \leq 3)$.
– The MixColumns operation (denoted below by MC) pre-multiplies a 4 × 4 byte array by a fixed 4 × 4 byte matrix.

The encryption procedure is, where K_0, K_i and K_{N_r} are 16-byte subkeys, and x is a 16-byte variable.

```
1. $x = \mathrm{ARK}(P, K_0)$.
2. For $i = 1$ to $N_r - 1$:
       $x = \mathrm{SB}(x)$,
       $x = \mathrm{SR}(x)$,
       $x = \mathrm{MC}(x)$,
       $x = \mathrm{ARK}(x, K_i)$.
3. $x = \mathrm{SB}(x), x = \mathrm{SR}(x)$.
4. Ciphertext $= \mathrm{ARK}(x, K_{N_r})$.
```

An equivalent description of the algorithm can be derived by reversing the order of the third and fourth operations of Step 2 of the above description, i.e. the operations involving MC and ARK. These two steps then become:

$x = \mathrm{ARK}(x, \widehat{K}_i)$,
$x = \mathrm{MC}(x)$,

where $\widehat{K}_i = \mathrm{MC}^{-1}(K_i)$. We use this alternative representation in certain of the attacks described later.

The ith iteration of Step 2 in the above description is referred to below as Round i, and the transformations in Steps 3 and 4 are referred to below as the final round (i.e. Round N_r). We write $K_{i,j}$ (respectively, $\widehat{K}_{i,j}$) for the jth byte of K_i (respectively, $\widehat{K}_i$), ($0 \leq j \leq 15$).

3 The (related-key) impossible boomerang attack

Typically, when formulating a differential cryptanalysis attack, it is desirable to use a relatively long differential. Of course, the longer the differential is, the smaller its probability is likely to be. The boomerang attack is based on a somewhat different idea, namely of using two differentials with large probabilities on two different parts of the cipher, instead of using a single differential with a small probability on the entire cipher. Impossible differential cryptanalysis involves using a differential that will never occur. The attack we propose in this paper, i.e. what we call the impossible boomerang attack, combines the boomerang attack with impossible differential cryptanalysis. Possible combinations of cryptanalytic techniques have been proposed in the past, and have proved effective [6–8,24,30,34]; a good example is provided by differential-linear cryptanalysis [6,34].

3.1 The basic impossible boomerang attack

As mentioned earlier, an impossible boomerang attack is constructed on an impossible-boomerang distinguisher.

3.1.1 Impossible-boomerang distinguisher using two tuples

An impossible-boomerang distinguisher is defined as follows.

Definition 1 Suppose $\mathbf{E} : \{0, 1\}^n \times \{0, 1\}^k \rightarrow \{0, 1\}^n$ is a block cipher and $K \in \{0, 1\}^k$ is a key for $\mathbf{E}$. If $\alpha, \alpha', \delta, \delta'$ are n-bit blocks, and any pair of plaintexts (X, X') cannot simultaneously meet $\mathbf{E}_K(X) \oplus \mathbf{E}_K(X') = \delta$ and $\mathbf{E}_K(X \oplus \alpha) \oplus \mathbf{E}_K(X' \oplus \alpha') = \delta'$, then the combination of $\alpha, \alpha', \delta, \delta'$ is called an impossible-boomerang distinguisher for $\mathbf{E}_K$, written $(\Delta\alpha, \Delta\alpha') \nrightarrow (\Delta\delta, \Delta\delta')$.

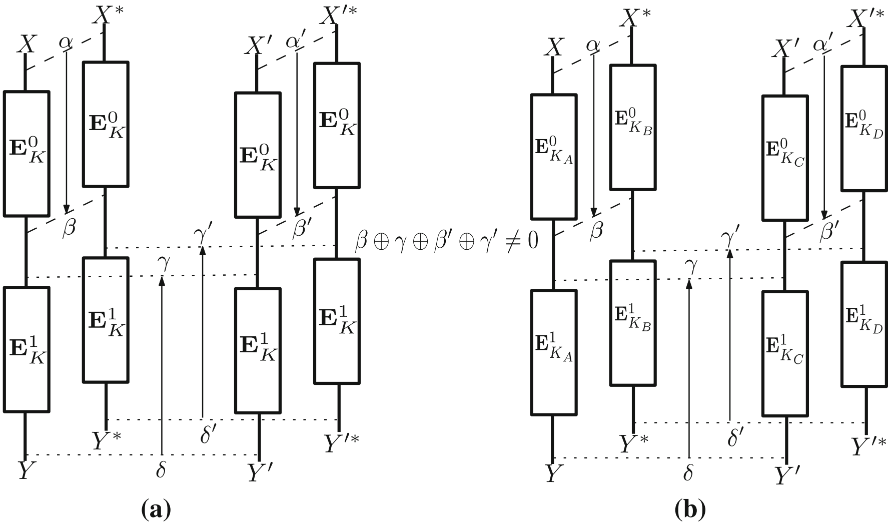

Fig. 2 Basic impossible-boomerang and related-key impossible-boomerang distinguishers

Subsequently, we formulate an impossible-boomerang distinguisher. An impossible-boomerang distinguisher treats a block cipher $\mathbf{E} : \{0, 1\}^n \times \{0, 1\}^k \rightarrow \{0, 1\}^n$ as two sub-ciphers $\mathbf{E}^0$ and $\mathbf{E}^1$, where $\mathbf{E} = \mathbf{E}^0 \circ \mathbf{E}^1$. Such a distinguisher is made up of four related differentials (or truncated differentials [32]), two for $\mathbf{E}^0$ and two for $(\mathbf{E}^1)^{-1}$, all of which must have probability 1. That is, an impossible-boomerang distinguisher consists of:

- a differential $\Delta\alpha \rightarrow \Delta\beta$ with probability 1 for $\mathbf{E}^0$;
- a differential $\Delta\alpha' \rightarrow \Delta\beta'$ with probability 1 for $\mathbf{E}^0$;
- a differential $\Delta\delta \rightarrow \Delta\gamma$ with probability 1 for $(\mathbf{E}^1)^{-1}$;
- a differential $\Delta\delta' \rightarrow \Delta\gamma'$ with probability 1 for $(\mathbf{E}^1)^{-1}$,

where α, α', β, β', γ, γ', δ and δ' are all n-bit blocks, and β, β', γ and γ' meet the condition $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$. This condition makes it different in nature from the boomerang distinguisher (where the XOR of the intermediate differences of the differentials used to construct a boomerang distinguisher is equal to zero). An impossible-boomerang distinguisher is shown pictorially in Fig. 2a.

The following theorem provides the theoretical basis for the impossible-boomerang distinguisher.

Theorem 1 *Suppose that X and X' are n-bit blocks and K is a key for an n-bit block cipher $\mathbf{E}$, where $\mathbf{E} = \mathbf{E}^0 \circ \mathbf{E}^1$ for some $\mathbf{E}^0$ and $\mathbf{E}^1$. Suppose that $\Delta\alpha \rightarrow \Delta\beta$ and $\Delta\alpha' \rightarrow \Delta\beta'$ are differentials with probability 1 for $\mathbf{E}_K^0$, and $\Delta\delta \rightarrow \Delta\gamma$ and $\Delta\delta' \rightarrow \Delta\gamma'$ are differentials with probability 1 for $(\mathbf{E}_K^1)^{-1}$, where $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$. Then the following pair of equations cannot both hold:*

$$\mathbf{E}_K(X) \oplus \mathbf{E}_K(X') = \delta, \tag{1}$$

$$\mathbf{E}_K(X \oplus \alpha) \oplus \mathbf{E}_K(X' \oplus \alpha') = \delta'. \tag{2}$$

Proof Suppose that Eqs. 1 and 2 both hold for some X, X' and K. Since both the differentials $\Delta\alpha \to \Delta\beta$ and $\Delta\alpha' \to \Delta\beta'$ for $\mathbf{E}_K^0$ hold with probability 1, we have

$$\mathbf{E}_K^0(X) \oplus \mathbf{E}_K^0(X \oplus \alpha) = \beta,$$
$$\mathbf{E}_K^0(X') \oplus \mathbf{E}_K^0(X' \oplus \alpha') = \beta'.$$

As both the differentials $\Delta\delta' \to \Delta\gamma'$ and $\Delta\delta \to \Delta\gamma$ for $(\mathbf{E}_K^1)^{-1}$ hold with probability 1, we can get the following equation with probability 1:

$$\begin{aligned}
&\mathbf{E}_K^0(X') \oplus \mathbf{E}_K^0(X' \oplus \alpha')\\
&\quad = (\mathbf{E}_K^0(X') \oplus \mathbf{E}_K^0(X)) \oplus (\mathbf{E}_K^0(X) \oplus \mathbf{E}_K^0(X \oplus \alpha)) \oplus (\mathbf{E}_K^0(X \oplus \alpha)\\
&\qquad \oplus \mathbf{E}_K^0(X' \oplus \alpha'))\\
&\quad = ((\mathbf{E}_K^1)^{-1}(\mathbf{E}_K(X')) \oplus (\mathbf{E}_K^1)^{-1}(\mathbf{E}_K(X))) \oplus (\mathbf{E}_K^0(X) \oplus \mathbf{E}_K^0(X \oplus \alpha))\\
&\qquad \oplus ((\mathbf{E}_K^1)^{-1}(\mathbf{E}_K(X \oplus \alpha)) \oplus (\mathbf{E}_K^1)^{-1}(\mathbf{E}_K(X' \oplus \alpha')))\\
&\quad = \gamma \oplus \beta \oplus \gamma'.
\end{aligned}$$

Hence, from the above discussion we have $\mathbf{E}_K^0(X') \oplus \mathbf{E}_K^0(X' \oplus \alpha') = \beta' = \gamma \oplus \beta \oplus \gamma'$. However, this contradicts with the condition that $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$. Therefore, the result follows. □

From Theorem 1 we know that a distinguisher of the form shown in Fig. 2a is an impossible-boomerang distinguisher, i.e., $(\Delta\alpha, \Delta\alpha') \nrightarrow (\Delta\delta, \Delta\delta')$.

Note that the two differentials for $\mathbf{E}^0$ or for $(\mathbf{E}^1)^{-1}$ may be identical, as long as the condition $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$ holds.

3.1.2 A key recovery attack

Typically, an impossible boomerang attack involves treating a block cipher $\mathbf{E} : \{0, 1\}^n \times \{0, 1\}^k \to \{0, 1\}^n$ as a cascade of four sub-ciphers $\mathbf{E} = \mathbf{E}^a \circ \mathbf{E}^0 \circ \mathbf{E}^1 \circ \mathbf{E}^b$, where $\mathbf{E}^0 \circ \mathbf{E}^1$ denotes the rounds for which the impossible-boomerang distinguisher $(\Delta\alpha, \Delta\alpha') \nrightarrow (\Delta\delta, \Delta\delta')$ holds, $\mathbf{E}^a$ denotes a number of rounds before $\mathbf{E}^0$, and $\mathbf{E}^b$ denotes a number of rounds after $\mathbf{E}^1$.

In a chosen plaintext attack scenario, given a guess for the subkeys used in $\mathbf{E}^a$ and $\mathbf{E}^b$, the impossible boomerang attack involves checking whether a candidate quartet consisting of two pairs of plaintext blocks meets the differential conditions required by the impossible-boomerang distinguisher. Specifically, suppose K_a is the guess for the subkey used in $\mathbf{E}^a$, and K_b is the guess for the subkey used in $\mathbf{E}^b$, then the attacker checks whether a candidate quartet of known plaintext-ciphertext pairs $(((P, C), (P^*, C^*)), ((P', C'), (P'^*, C'^*)))$ satisfies the following four conditions:

$$\mathbf{E}_{K_a}^a(P) \oplus \mathbf{E}_{K_a}^a(P^*) = \alpha, \tag{3}$$
$$\mathbf{E}_{K_a}^a(P') \oplus \mathbf{E}_{K_a}^a(P'^*) = \alpha', \tag{4}$$
$$(\mathbf{E}_{K_b}^b)^{-1}(C) \oplus (\mathbf{E}_{K_b}^b)^{-1}(C') = \delta, \tag{5}$$
$$(\mathbf{E}_{K_b}^b)^{-1}(C^*) \oplus (\mathbf{E}_{K_b}^b)^{-1}(C'^*) = \delta'. \tag{6}$$

If there exists a candidate quartet satisfying Eqs. 3–6, then the subkey guess (K_a, K_b) must be incorrect, and can be discarded. Thus, given a sufficient number of chosen plaintext pairs, the attacker can find the correct subkeys used in $\mathbf{E}^a$ and $\mathbf{E}^b$ by discarding all the wrong guesses.

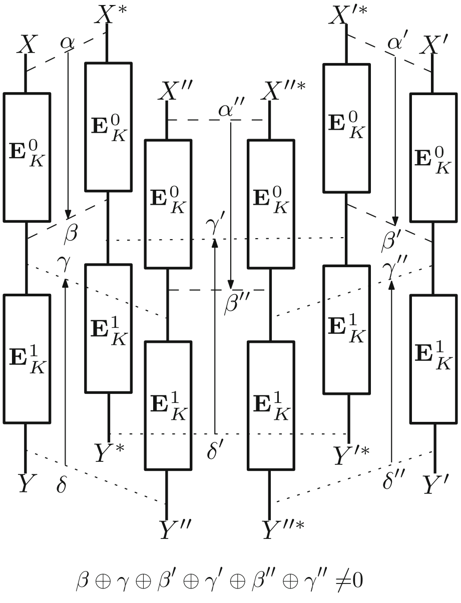

Fig. 3 A 6-fold impossible-boomerang distinguisher

Depending on the design of **E**, the attacker can use the early abort techniques described in [37–39] to improve the efficiency of the attack; see Chap. 4 of [35] for a summarized description of the early abort techniques.

3.2 The impossible boomerang attack using more tuples

The impossible-boomerang distinguisher described above uses two tuples, i.e. $(X, X^* = X \oplus \alpha)$ and $(X', X'^* = X' \oplus \alpha')$. In fact, we can construct an impossible-boomerang distinguisher using more tuples.

For example, suppose we have a third tuple $(X'', X''^* = X'' \oplus \alpha'')$, and we have two additional differentials $\Delta\alpha'' \to \Delta\beta''$ and $\Delta\delta'' \to \Delta\gamma''$ for $\mathbf{E}^0$ and $(\mathbf{E}^1)^{-1}$, respectively, both with probability 1. Suppose also that $\beta \oplus \beta' \oplus \beta'' \oplus \gamma \oplus \gamma' \oplus \gamma'' \neq 0$. Then we can construct a 6-fold impossible-boomerang distinguisher, as shown pictorially in Fig. 3, which can be used to construct an attack, given a sufficient number of plaintext pairs.

3.3 The related-key impossible boomerang attack

A related-key attack scenario [2,28,31] assumes that the attacker knows or can choose the specific differences between one or more pairs of unknown keys. As shown in [28], some of the current real-world applications allow for practical such attacks, say key-exchange protocols.

A related-key impossible-boomerang distinguisher involving four related keys is defined as follows.

Definition 2 Suppose $\mathbf{E} : \{0, 1\}^n \times \{0, 1\}^k \to \{0, 1\}^n$ is a block cipher and $K_A, K_B, K_C, K_D \in \{0, 1\}^k$ are related user keys for **E**. If $\alpha, \alpha', \delta, \delta'$ are n-bit blocks, and any pair of plaintexts (X, X') cannot simultaneously meet $\mathbf{E}_{K_A}(X) \oplus \mathbf{E}_{K_C}(X') = \delta$ and $\mathbf{E}_{K_B}(X \oplus \alpha) \oplus \mathbf{E}_{K_D}(X' \oplus \alpha') = \delta'$, then the combination of $\alpha, \alpha', \delta, \delta'$ is called a related-key impossible-boomerang distinguisher for $\mathbf{E}$ with respect to (K_A, K_B, K_C, K_D), written $(\Delta\alpha, \Delta\alpha') \overset{K_A,K_B,K_C,K_D}{\nrightarrow} (\Delta\delta, \Delta\delta')$.

Such a related-key impossible-boomerang distinguisher is depicted in Fig. 2b, where $\beta, \beta', \gamma, \gamma'$ are n-bit blocks. Under the requirement that all the four related-key differentials $\Delta\alpha \rightarrow \Delta\beta$, $\Delta\alpha' \rightarrow \Delta\beta'$, $\Delta\delta \rightarrow \Delta\gamma$ and $\Delta\delta' \rightarrow \Delta\gamma'$ hold with probability 1 and $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$, we can similarly learn that the distinguisher is a related-key impossible-boomerang distinguisher, i.e., $(\Delta\alpha, \Delta\alpha') \overset{K_A,K_B,K_C,K_D}{\nrightarrow} (\Delta\delta, \Delta\delta')$. Similarly to the impossible boomerang attack described in Sect. 3.1.2, we can use a related-key impossible-boomerang distinguisher as the basis for an attack in the related-key attack scenario. Following the descriptions in Sect. 3.2 we can similarly construct a related-key impossible-boomerang distinguisher involving more related keys.

It is worthy to note that with slight modifications the (related-key) impossible boomerang attack can also work in an adaptively chosen plaintext and ciphertext attack scenario, in a similar way to the boomerang attack [46].

3.4 A comparison

Below we compare the (related-key) impossible boomerang attack with (related-key) impossible differential cryptanalysis and the boomerang-type attacks.

Proposition 1 *From an impossible-boomerang distinguisher, an impossible differential for the same number of rounds can be obtained. A block cipher resistant to related-key impossible differential cryptanalysis will not necessarily resist a related-key impossible boomerang attack.*

Consider an impossible-boomerang distinguisher using two tuples. From the condition $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$ we have $\beta \oplus \gamma \neq \beta' \oplus \gamma'$, which implies that the values $\beta \oplus \gamma$ and $\beta' \oplus \gamma'$ cannot both be equal to zero. Since the four differentials required by the impossible-boomerang distinguisher have a probability of one and they work under the same key K, we always have an impossible differential $\alpha \nrightarrow \delta$ or $\alpha' \nrightarrow \delta'$, and thus the above result applies when using two tuples. A similar result holds when using more tuples. This makes a limitation to the impossible boomerang attack; however, this limitation does not necessarily hold for their variants in a related-key attack scenario, for the related-key differentials work under the four keys K_A, K_B, K_C and K_D and we cannot concatenate two related-key differentials when they work under a different set of keys. When formulating a related-key impossible differential, choosing the subkey difference for $\mathbf{E}^0$ usually incurs a fixed subkey difference for $\mathbf{E}^1$, and vice versa; but when formulating a related-key impossible-boomerang distinguisher we have more flexibility in choosing the subkey differences for $\mathbf{E}^0$ and $\mathbf{E}^1$: we can use a subkey difference for $\mathbf{E}^0$ and use an independent subkey difference for $\mathbf{E}^1$, and even more flexibly, we can use two different subkey differences for $\mathbf{E}^0$ or $\mathbf{E}^1$. These degrees of freedom in choosing the key differences may potentially enable us to break more rounds of the cipher using a related-key impossible boomerang attack, as exhibited by our attacks on reduced-round AES-192 and AES-256 in Sect. 5. Given only the two differentials (with probability 1) used to build an impossible differential, one may suppose that they can be used to build an impossible-boomerang distinguisher involving an odd number of tuples, with one used for $\mathbf{E}^0$ and the other used for $\mathbf{E}^1$. However, after a simple analysis we learn this is not correct.

The (related-key) boomerang attack works in an adaptively chosen plaintext and ciphertext attack scenario, and the (related-key) amplified boomerang and rectangle attacks work in a chosen plaintext (or ciphertext) attack scenario. The (related-key) impossible boomerang attack can work in a chosen plaintext (or ciphertext) attack scenario, or in an adaptively chosen plaintext and ciphertext attack scenario. One advantage of the (related-key) impossible boomerang attack over the boomerang-type attacks is analogous to that of (related-key) impossible differential cryptanalysis over (related-key) differential cryptanalysis.

Proposition 2 *A block cipher resistant to the boomerang-type attacks will not necessarily resist a (related-key) impossible boomerang attack. A (related-key) impossible-boomerang distinguisher is more reasonable than the boomerang-type distinguishers.*

A (related-key) impossible-boomerang distinguisher is more reasonable than the boomerang-type distinguishers, in that the latter use (related-key) differentials usually under the following independence assumptions: (1) The output of one intermediate round of the cipher is uniformly distributed and is independent from that of previous rounds, (or a different assumption with an equivalent meaning); and (2) The two groups of (related-key) differentials used for either sub-cipher are treated as independent. These assumptions are often observed to give probability values that are highly inaccurate [42,47]. However, a (related-key) impossible-boomerang distinguisher does not require the assumptions, and it has an accurate probability value (i.e. 0).

4 Impossible boomerang attacks on 6-round AES-128, 7-round AES-192 and 7-round AES-256

In the single-key attack scenario, the square attack [17], the collision attack, the meet-in-the-middle attack [4], the impossible differential attack and the boomerang attack are the currently known cryptanalytic techniques that have been used to break 6 or more rounds of AES-128/192/256. In this section we show that the impossible boomerang attack can also break 6 or more rounds of AES-128/192/256. We first describe certain 4-round impossible-boomerang distinguishers (using two tuples) of AES. These then allow us to construct an impossible boomerang attack on 6-round AES-128, 7-round AES-192 and 7-round AES-256.

4.1 4-Round impossible-boomerang distinguishers

Let $\mathbf{E}^0$ denote Rounds 2 and 3 including the ARK operation of Round 1, and $\mathbf{E}^1$ denote Rounds 4 and 5 excluding the MC operation for Round 5. Fig. 4 shows the set of four differentials making up the 4-round impossible-boomerang distinguishers for $\mathbf{E}^0 \circ \mathbf{E}^1$. In this figure, a (small) square corresponds to a byte, a blank indicates a zero 8-bit difference, and a square labeled a value $a, b, \cdots$ indicates an (arbitrary[2]) nonzero 8-bit difference. The symbols given in the figure for individual byte differences are used to simplify our description below.

The first differential $\Delta\alpha \rightarrow \Delta\beta$ for $\mathbf{E}^0$ is $((a, 0, 0, 0)$, (0,0,0,0), (0,0,0,0), $(0,0,0,0)) \rightarrow ((e_0, e_1, e_2, e_3), (e_4, e_5, e_6, e_7), (e_8, e_9, e_{10}, e_{11}), (e_{12}, e_{13}, e_{14}, e_{15}))$, as shown in Fig. 4a.

The second differential $\Delta\alpha' \rightarrow \Delta\beta'$ for $\mathbf{E}^0$ has the same format with $\Delta\alpha \rightarrow \Delta\beta$; we denote it by $((a', 0, 0, 0)$, (0,0,0,0), (0,0,0,0), $(0,0,0,0)) \rightarrow ((e'_0, e'_1, e'_2, e'_3), (e'_4, e'_5, e'_6, e'_7), (e'_8, e'_9, e'_{10}, e'_{11}), (e'_{12}, e'_{13}, e'_{14}, e'_{15}))$.

The first differential $\Delta\delta \rightarrow \Delta\gamma$ for $(\mathbf{E}^1)^{-1}$ is $((f_0, 0, 0, 0), (f_4,0,0,0), (f_8,0,0,0), (0,0,0,0)) \rightarrow ((i_0, i_1, i_2, 0), (0, i_5, i_6, i_7), (i_8, 0, i_{10}, i_{11}), (i_{12}, i_{13}, 0, i_{15}))$, as shown in Fig. 4b.

[2] By “arbitrary” we mean that these differentials hold with probability 1.

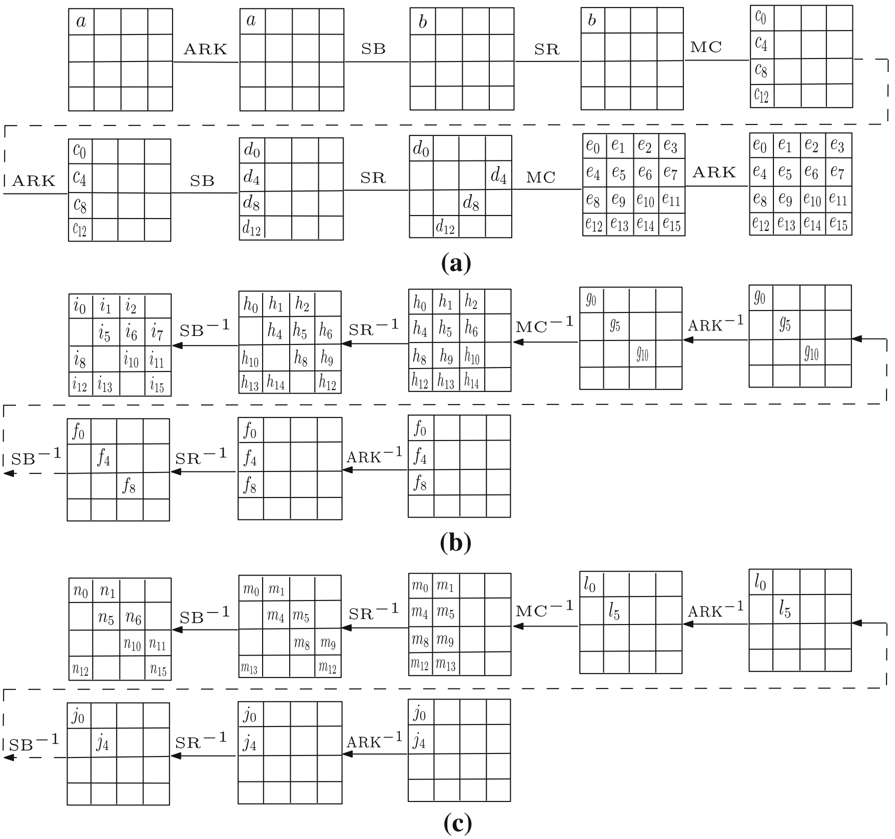

Fig. 4 The differentials making up the 4-round impossible-boomerang distinguisher

The second differential $\Delta\delta' \to \Delta\gamma'$ for $(\mathbf{E}^1)^{-1}$ is ((j_0,0,0,0), (j_4,0,0,0), (0,0,0,0), (0,0,0,0)) $\to$ ((n_0, n_1, 0, 0), (0, n_5, n_6, 0), (0, 0, n_{10}, n_{11}), (n_{12}, 0, 0, n_{15})), as shown in Fig. 4c.

We can now give the following result.

Property 1 *The four differentials described above constitute an impossible-boomerang distinguisher for* $\mathbf{E}^0 \circ \mathbf{E}^1$*:* $(((a, 0, 0, 0), (0, 0, 0, 0), (0, 0, 0, 0), (0, 0, 0, 0)), ((a', 0, 0, 0), (0,0,0, 0), (0, 0, 0, 0), (0, 0, 0, 0))) \nrightarrow (((f_0, 0, 0, 0), (f_4, 0,0, 0), (f_8, 0, 0, 0), (0,0,0,0)), ((j_0, 0, 0, 0), (j_4, 0, 0, 0), (0, 0, 0, 0), (0, 0, 0, 0)))$, *where* $a, a', f_0, f_4, f_8, j_0, j_4$ *are arbitrary but nonzero* 8*-bit values.*

Proof For the differential $\Delta\alpha \to \Delta\beta$, we have (by definition of MC):

$$e_4 = d_0, \tag{7}$$

$$e_8 = d_0. \tag{8}$$

Similarly, for the differential $\Delta\alpha' \to \Delta\beta'$, we have:

$$e'_4 = d'_0, \tag{9}$$

$$e'_8 = d'_0. \tag{10}$$

From [18] we know that MC has a branch number of 5; hence $h_{10} \neq 0$. Consequently, $i_8 \neq 0$.

Note that the 4th and 8th bytes of $\Delta\gamma$ are 0 and i_8, respectively; and the 4th and 8th bytes of $\Delta\gamma'$ are both 0. Thus, from Eqs. 7 and 9, the 4th byte of $\beta \oplus \beta' \oplus \gamma \oplus \gamma'$ is $e_4 \oplus e'_4 = d_0 \oplus d'_0$, and by Eqs. 8 and 10 the 8th byte of $\beta \oplus \beta' \oplus \gamma \oplus \gamma'$ is $e_8 \oplus e'_8 \oplus i_8 = d_0 \oplus d'_0 \oplus i_8$.

Since $i_8 \neq 0$, then $d_0 \oplus d'_0$ and $d_0 \oplus d'_0 \oplus i_8$ cannot both be zero, and hence $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$ holds for the four differentials. The result follows. □

Before proceeding observe that there are many other similar 4-round impossible-boomerang distinguishers for AES; for example, the differences a and a' in the above 4-round distinguisher can locate in any one or two positions of the first column.

4.2 Attacking 6-round AES-128, 7-round AES-192 and 7-round AES-256

We can use the 4-round impossible-boomerang distinguishers to mount impossible boomerang attacks on 6-round AES-128, 7-round AES-192 and 7-round AES-256. The 6-round AES-128 attack is based on encrypting $2^{112.2}$ chosen plaintexts and has a time complexity of $2^{112.3}$ encryptions; the 7-round AES-192 attack is based on encrypting $2^{112.5}$ chosen plaintexts and has a time complexity of $2^{186.3}$ encryptions; and the 7-round AES-256 attack is based on encrypting $2^{112.8}$ chosen plaintexts and has a time complexity of $2^{186.9}$ encryptions. As these attacks are similar to those attacks in Sect. 5, we omit the full details here and refer the interested reader to [35]. We note certain of these attacks rely on the following property:

Property 2 *Let Ω be the set of $4 \times 255 \approx 2^{10}$ differences in bytes (0, 5, 10, 15) just after the SB operation, each of which is transformed by the SR $\circ$ MC operation to a difference with only one nonzero byte in the first column. Then, the differences in Ω have distinct values in the pair of byte positions (0, 5).*

Proof Suppose there exist two differences x and y from Ω that have the same value in bytes $(0, 5)$, that is to say, $x \oplus y$ is equal to zero in the first two bytes. Since x and y are transformed by the $\mathrm{MC}^{-1} \circ \mathrm{SR}^{-1}$ operation from two differences with only one non-zero byte in the first column, say $\widetilde{x}$ and $\widetilde{y}$, it follows that at least two out of the four bytes of $\widetilde{x} \oplus \widetilde{y}$ should be zero; however, this is impossible, because the MC operation has a branch number of 5 [18]. □

5 Related-key impossible boomerang attacks on 8-round AES-192 and 9-round AES-256 in the two-key related-key attack scenario

In this section we describe 6-round related-key impossible-boomerang distinguishers (using two tuples) of AES-192/256, and use them as the basis of a related-key impossible boomerang attack on 8-round AES-192 and 9-round AES-256 in the two-key related-key attack scenario. We use a related-key impossible-boomerang distinguisher such that $K_A = K_C$ and $K_B = K_D$, that is, it involves two keys.

Let $\mathbf{E}^0$ denote Rounds 2–5 (of AES-192/256) including the ARK operation of Round 1, and $\mathbf{E}^1$ denote Rounds 6–7 excluding the MC operation of Round 7. We choose non-zero key differences for differentials of $\mathbf{E}^0$ and a zero key difference for differentials of $\mathbf{E}^1$.

5.1 Attacking 8-round AES-192 in the two-key related-key attack scenario

5.1.1 6-Round related-key impossible-boomerang distinguishers

The two related-key differentials $\Delta\alpha \to \Delta\beta$ and $\Delta\alpha' \to \Delta\beta'$ for $\mathbf{E}^0$ are both $((0, 0, a, a), (0, 0, 0, 0), (0, 0, 0, 0), (0, 0, 0, 0)) \rightarrow ((\star, \star, \star, \star), (\star, \star, \star, \star), (\star, \star, \star, \star), (\star, \star, \star, \star))$,

Table 2 The subkey differences for the 8-round AES-192 attack

i	ΔK_{5i}	ΔK_{5i+1}	ΔK_{5i+2}	ΔK_{5i+3}	ΔK_{5i+4}
0	$\begin{pmatrix} a & 0 & a & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & a & a \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & a & a \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$
1	$\begin{pmatrix} a & a & a & a \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} a & 0 & a & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ b & b & b & b \end{pmatrix}$	$\begin{pmatrix} a & 0 & a & a \\ 0 & 0 & 0 & 0 \\ 0 & 0 & c & c \\ b & b & b & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & a & a \\ 0 & 0 & 0 & 0 \\ c & c & c & c \\ b & 0 & b & 0 \end{pmatrix}$	/

where the key difference is $K_A \oplus K_B (= K_C \oplus K_D) = ((a, 0, a, 0, 0, 0), (0{,}0{,}0{,}0{,}0{,}0), (0{,}0, 0{,}0{,}0{,}0), (0, 0, 0, 0, 0, 0))$, with a being a specific nonzero 8-bit value. The differentials for $(\mathbf{E}^1)^{-1}$ are the same as those in Fig. 4b and c. Table 2 gives the subkey differences for the first eight rounds of AES-192 given the user key difference $((a, 0, a, 0, 0, 0), (0, 0, 0, 0, 0, 0), (0, 0, 0, 0, 0, 0), (0, 0, 0, 0, 0, 0))$, where b and c are indeterminate 8-bit nonzero values.

Similar to that described in Sect. 4.1, we can learn that there exist the following 6-round related-key impossible-boomerang distinguishers for $\mathbf{E}^0 \circ \mathbf{E}^1$: $(((0{,}0, a, a), (0{,}0{,}0{,}0), (0{,}0{,}0{,}0), (0{,}0{,}0{,}0)), ((0, 0, a, a), (0{,}0{,}0{,}0), (0{,}0{,}0{,}0), (0{,}0{,}0{,}0))) \overset{K_A, K_B, K_A, K_B}{\nrightarrow} (((\star, 0, 0, 0), (\star, 0, 0, 0), (\star, 0, 0, 0), (0, 0, 0, 0)), ((\star, 0, 0, 0), (\star, 0, 0, 0), (0, 0, 0, 0), (0, 0, 0, 0)))$.

5.1.2 Attack procedure

We now describe a related-key impossible boomerang attack on 8-round AES-192 based on a 6-round related-key impossible-boomerang distinguisher.

The attacked 8 rounds are the first 8 rounds (i.e. Rounds 1–8). We reverse the order of the operations MC and ARK for Round 7. From Table 2 we know that both $\Delta K_{8,0}$ and $\Delta K_{8,7}$ are zero. The attack procedure is as follows.

1. Choose $2^{57.4}$ structures S_i, $(i = 1, 2, \ldots, 2^{57.4})$, where a structure S_i is defined to be a set of 2^{64} plaintexts $P_{i,j}$ with bytes (2, 3, 4, 7, 8, 9, 13, 14) of the 2^{64} plaintexts taking all the possible values and the other 8 bytes being fixed, $(j = 1, 2, \ldots, 2^{64})$. In a chosen-plaintext attack scenario, obtain all the $2^{121.4}$ ciphertexts for the 2^{64} plaintexts in each of the $2^{57.4}$ structures encrypted with K_A; we denote by $C_{i,j}$ the ciphertext for plaintext $P_{i,j}$.
2. Choose $2^{57.4}$ structures $\widetilde{S}_i$, $(i = 1, 2, \ldots, 2^{57.4})$, where a structure $\widetilde{S}_i$ is defined to be a set of 2^{64} plaintexts $\widetilde{P}_{i,j}$ with $\widetilde{P}_{i,j} = P_{i,j} \oplus ((a, 0, 0, 0), (0{,}0{,}0{,}0), (0{,}0{,}0{,}0), (0{,}0{,}0{,}0))$, $(j = 1, 2, \ldots, 2^{64})$. In a chosen-plaintext attack scenario, obtain all the $2^{121.4}$ ciphertexts for the 2^{64} plaintexts in each of the $2^{57.4}$ structures encrypted with K_B; let $\widetilde{C}_{i,j}$ be the ciphertext for plaintext $\widetilde{P}_{i,j}$.
3. Identify the ciphertext quartets $((C_{i_1,j_1}, \widetilde{C}_{i_1,j_2}), (C_{i_2,j_3}, \widetilde{C}_{i_2,j_4}))$ with the property $C_{i_1,j_1} \oplus C_{i_2,j_3} = ((\star, 0, 0, 0), (0, 0, 0, \star), (0, 0, 0, 0), (0, 0, 0, 0))$ and $\widetilde{C}_{i_1,j_2} \oplus \widetilde{C}_{i_2,j_4} = ((\star, 0, 0, 0), (0, 0, 0, \star), (0, 0, \star, 0), (0, 0, 0, 0))$ in the following way, where $1 \leq i_1, i_2 \leq 2^{57.4}$, $1 \leq j_1 \neq j_2, j_3 \neq j_4 \leq 2^{64}$.

   (a) Store the $2^{121.4}$ ciphertexts $C_{i,j}$ in a hash table indexed by bytes $(1, 2, \ldots, 6, 8, 9, \ldots, 15)$ of the ciphertexts $C_{i,j}$, and obtain the ciphertext pairs $(C_{i_1,j_1}, C_{i_2,j_3})$ that meet $C_{i_1,j_1} \oplus C_{i_2,j_3} = ((\star, 0, 0, 0), (0, 0, 0, \star), (0, 0, 0, 0), (0, 0, 0, 0))$.

(b) Store the $2^{121.4}$ ciphertexts $\widetilde{C}_{i,j}$ in a hash table indexed by bytes $(1, 2, \ldots, 6, 8, 9, 11, \ldots, 15)$ of the ciphertexts $\widetilde{C}_{i,j}$, and obtain the ciphertext pairs $(\widetilde{C}_{l_1,t_1}, \widetilde{C}_{l_2,t_2})$ that meet $\widetilde{C}_{l_1,t_1} \oplus \widetilde{C}_{l_2,t_2} = ((\star, 0, 0, 0), (0, 0, 0, \star), (0, 0, \star, 0), (0, 0, 0, 0))$, where $1 \leq l_1, l_2 \leq 2^{57.4}$, $1 \leq t_1, t_2 \leq 2^{57.4}$. Store the ciphertext pairs $(\widetilde{C}_{l_1,t_1}, \widetilde{C}_{l_2,t_2})$ in a hash table $\mathcal{T}$ indexed by (l_1, l_2).

(c) For each ciphertext pair $(C_{i_1,j_1}, C_{i_2,j_3})$ obtained in Step 3(a), go to entry (i_1, i_2) of the hash table $\mathcal{T}$, and record all the possible quartets $((C_{i_1,j_1}, \widetilde{C}_{i_1,j_2}), (C_{i_2,j_3}, \widetilde{C}_{i_2,j_4}))$.

4. Guess a value for the subkey bytes $(K_{8,0}, K_{8,7})$, and perform the following two sub-steps for every remaining quartet $((C_{i_1,j_1}, \widetilde{C}_{i_1,j_2}), (C_{i_2,j_3}, \widetilde{C}_{i_2,j_4}))$.

(a) Partially decrypt C_{i_1,j_1} and C_{i_2,j_3} with $(K_{8,0}, K_{8,7})$ to get the corresponding values for bytes (0,4) just after the MC operation of Round 7, and check whether they produce a difference that has a zero in only one of bytes (0, 4, 8, 12) just after the ARK operation of Round 7. Keep only the ciphertext quartets that meet this condition.

(b) Guess a value for the subkey byte $K^B_{8,10}$ under K_B. Partially decrypt $\widetilde{C}_{i_1,j_2}$ and $\widetilde{C}_{i_2,j_4}$ with $(K_{8,0}, K_{8,7}, K^B_{8,10})$ to get the corresponding values for bytes (0, 4, 8) just after the MC operation of Round 7, and check whether they produce a difference that has a zero in only two of bytes (0, 4, 8, 12) just after the ARK operation of Round 7, where the two byte positions include the one byte position with a zero difference in Step 4(a). Keep only the ciphertext quartets that meet this condition.

5. For every plaintext quartet $((P_{i_1,j_1}, \widetilde{P}_{i_1,j_2}), (P_{i_2,j_3}, \widetilde{P}_{i_2,j_4}))$ corresponding to a remaining ciphertext quartet $((C_{i_1,j_1}, \widetilde{C}_{i_1,j_2}), (C_{i_2,j_3}, \widetilde{C}_{i_2,j_4}))$, do as follows.

(a) Guess a value for the subkey byte $K_{0,2}$. Partially encrypt P_{i_1,j_1} and $\widetilde{P}_{i_1,j_2}$ with $K_{0,2}$ and $K_{0,2} \oplus a$ respectively to get the corresponding values for byte (2) just after the SR operation of Round 1, and check whether they have a difference equal to byte (0) of $\mathrm{MC}^{-1}(a, 0, 0, 0)$; and partially encrypt P_{i_2,j_3} and $\widetilde{P}_{i_2,j_4}$ with $K_{0,2}$ and $K_{0,2} \oplus a$ respectively to get the corresponding values for byte (2) just after the SR operation of Round 1, and check whether they have a difference equal to byte (0) of $\mathrm{MC}^{-1}(a, 0, 0, 0)$. Keep only the plaintext quartets that meet both the conditions.

(b) Perform the following two sub-steps for $m = 7, 8, 13$:
- Guess a value for the subkey byte $K_{0,m}$.
- Partially encrypt P_{i_1,j_1} and $\widetilde{P}_{i_1,j_2}$ with $K_{0,m}$ to get the corresponding values for byte $((m - 5\lfloor\frac{m}{4}\rfloor) \bmod 4 + 4\lfloor\frac{m}{4}\rfloor)$ just after the SR operation of Round 1, and check whether they have a difference equal to byte $(\lfloor\frac{m}{4}\rfloor)$ of $\mathrm{MC}^{-1}(a, 0, 0, 0)$; and partially encrypt P_{i_2,j_3} and $\widetilde{P}_{i_2,j_4}$ with $K_{0,m}$ to get the corresponding values for byte $((m-5\lfloor\frac{m}{4}\rfloor) \bmod 4+4\lfloor\frac{m}{4}\rfloor)$ just after the SR operation of Round 1, and check whether they have a difference equal to byte $(\lfloor\frac{m}{4}\rfloor)$ of $\mathrm{MC}^{-1}(a, 0, 0, 0)$. Keep only the plaintext quartets that meet both the conditions.

6. For every remaining plaintext quartet $((P_{i_1,j_1}, \widetilde{P}_{i_1,j_2}), (P_{i_2,j_3}, \widetilde{P}_{i_2,j_4}))$, do as follows.

(a) Perform the following two sub-steps for $m = 3, 4, 9$:
- Guess a value for the subkey byte $K_{0,m}$.
- Partially encrypt P_{i_1,j_1} and $\widetilde{P}_{i_1,j_2}$ with $K_{0,m}$ to get the corresponding values for byte $((m - 5\lfloor\frac{m}{4}\rfloor) \bmod 4 + 4\lfloor\frac{m}{4}\rfloor)$ just after the SR operation of Round 1, and check whether they have a difference equal to byte $(\lfloor\frac{m}{4}\rfloor)$ of $\mathrm{MC}^{-1}(a, 0, 0, 0)$;

and partially encrypt P_{i_2,j_3} and $\widetilde{P}_{i_2,j_4}$ with $K_{0,m}$ to get the corresponding values for byte $((m-5\lfloor\frac{m}{4}\rfloor) \bmod 4+4\lfloor\frac{m}{4}\rfloor)$ just after the SR operation of Round 1, and check whether they have a difference equal to byte $(\lfloor\frac{m}{4}\rfloor)$ of $\mathrm{MC}^{-1}(a,0,0,0)$. Keep only the plaintext quartets that meet both the conditions.

(b) Guess a value for the subkey byte $K_{0,14}$. Partially encrypt P_{i_1,j_1} and $\widetilde{P}_{i_1,j_2}$ with $K_{0,14}$ to get the corresponding values for byte (15) just after the SR operation of Round 1, and check whether they have a difference equal to byte (3) of $\mathrm{MC}^{-1}(a,0,0,0)$; and partially encrypt P_{i_2,j_3} and $\widetilde{P}_{i_2,j_4}$ with $K_{0,14}$ to get the corresponding values for byte (15) just after the SR operation of Round 1, and check whether they have a difference equal to byte (3) of $\mathrm{MC}^{-1}(a,0,0,0)$. If there exists a plaintext quartet meeting both the conditions, discard the guessed value for $(K_{8,0}, K_{8,7}, K^B_{8,10}, K_{0,2}, K_{0,3}, K_{0,4}, K_{0,7}, K_{0,8}, K_{0,9}, K_{0,13}, K_{0,14})$, and repeat Steps 4–6 with another guess; otherwise, execute Step 7.

7. For every remaining value of $(K_{0,2}, K_{0,3}, K_{0,4}, K_{0,7}, K_{0,8}, K_{0,9}, K_{0,13}, K_{0,14})$ after Step 6, determine the correct user key by exhaustively searching the remaining 128 key bits.

The attack requires $2^{122.4}$ chosen plaintexts. There are $2^{121.4} \times 2^{121.4} \times 2^{-14\times 8} = 2^{130.8}$ qualified ciphertext pairs $(C_{i_1,j_1}, C_{i_2,j_3})$ in Step 3(a), and $2^{121.4} \times 2^{121.4} \times 2^{-13\times 8} = 2^{138.8}$ qualified ciphertext pairs $(\widetilde{C}_{l_1,t_1}, \widetilde{C}_{l_2,t_2})$ in Step 3(b). For each of the $2^{57.4} \times 2^{57.4} = 2^{114.8}$ possible pairs of structure indexes (i_1, i_2), on average there are $\frac{2^{138.8}}{2^{114.8}} = 2^{24}$ ciphertext pairs $(\widetilde{C}_{i_1,t_1}, \widetilde{C}_{i_2,t_2})$. As a result, in Step 3(c), for each of the $2^{130.8}$ ciphertext pairs $(C_{i_1,j_1}, C_{i_2,j_3})$ there are $2^{24} \times \frac{1}{2} = 2^{23}$ ciphertext pairs $(\widetilde{C}_{i_1,j_2}, \widetilde{C}_{i_2,j_4})$ that can form a useful quartet. It is expected that $2^{130.8} \times 2^{23} = 2^{153.8}$ candidate ciphertext quartets are recorded in Step 3. In Step 4(a), a ciphertext quartet meets the condition with probability $\binom{4}{1} \times 2^{-8} = 2^{-6}$, so it is expected that after Step 4(a) there remain $2^{153.8} \times 2^{-6} = 2^{147.8}$ ciphertext quartets for every subkey guess. In Step 4(b), a ciphertext quartet meets the condition with probability $\binom{3}{1} \times 2^{-16} = 2^{-14.42}$, and thus $2^{147.8} \times 2^{-14.42} \approx 2^{133.38}$ ciphertext quartets are expected to pass Step 4(b) for every subkey guess. In Step 5(a) and each iteration of Step 5(b), a plaintext quartet meets both the conditions with probability $(2^{-8})^2 = 2^{-16}$, and thus after Step 5 there remain $2^{133.38} \times 2^{-16\times 4} = 2^{69.38}$ plaintext quartets for every subkey guess. In each iteration of Step 6(a), a plaintext quartet meets both the conditions with probability $(2^{-8})^2 = 2^{-16}$; thus it is expected that $2^{69.38} \times 2^{-16\times 3} = 2^{21.38}$ plaintext quartets pass Step 6(a) for every subkey guess. In Step 6(b), the probability that there exists a plaintext quartet meeting both the conditions is $2^{-8\times 2} = 2^{-16}$; thus after analysing the remaining $2^{21.38}$ plaintext quartets we get that there remain only $2^{88} \times (1-2^{-16})^{2^{21.38}} \approx 2^{28.04}$ guessed values for $(K_{8,0}, K_{8,7}, K^B_{8,10}, K_{0,2}, K_{0,3}, K_{0,4}, K_{0,7}, K_{0,8}, K_{0,9}, K_{0,13}, K_{0,14})$. Therefore, it is expected that we can find the correct key using $2^{28.04} \times 2^{128} = 2^{156.04}$ trial encryptions in Step 7.

Steps 1 and 2 have a time complexity of $2^{122.4}$ 8-round AES-192 encryptions. In Step 3(a), a simple implementation takes $2^{121.4}$ memory accesses to obtain the $2^{130.8}$ qualified ciphertext pairs $(C_{i_1,j_1}, C_{i_2,j_3})$; and in Step 3(b), a simple implementation takes $2^{121.4}$ memory accesses to obtain the $2^{138.8}$ qualified ciphertext pairs $(\widetilde{C}_{l_1,t_1}, \widetilde{C}_{l_2,t_2})$. Step 3(c) takes $2^{130.8} \times 2^{23} = 2^{153.8}$ memory accesses to obtain the useful ciphertext quartets. Step 4(a) has a time complexity of $2 \times 2^{153.8} \times 2^{16} \times \frac{2}{16} \times \frac{1}{8} = 2^{164.8}$ 8-round AES-192 encryptions. Step 4(b) has a time complexity of $2 \times 2^{147.8} \times 2^{24} \times \frac{3}{16} \times \frac{1}{8} \approx 2^{167.38}$ 8-round AES-192 encryptions. Step 5(a) has a time complexity of $4 \times 2^{133.48} \times 2^{32} \times \frac{1}{16} \times \frac{1}{8} = 2^{160.48}$ 8-round AES-192

Table 3 The subkey differences for the 9-round AES-256 attack

i	ΔK_{5i}	ΔK_{5i+1}	ΔK_{5i+2}	ΔK_{5i+3}	ΔK_{5i+4}
0	$\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$	$\begin{pmatrix}0&a&a&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$	$\begin{pmatrix}0&a&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$
1	$\begin{pmatrix}0&a&a&a\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\b&b&b&b\end{pmatrix}$	$\begin{pmatrix}0&a&0&a\\0&0&0&0\\0&0&0&0\\c&c&c&c\end{pmatrix}$	$\begin{pmatrix}0&0&0&0\\0&0&0&0\\d&d&d&d\\b\oplus e&e&b\oplus e&e\end{pmatrix}$	$\begin{pmatrix}0&a&a&0\\0&0&0&0\\f&f&f&f\\g\oplus c&g&g\oplus c&g\end{pmatrix}$

encryptions. Step 5(b) has a time complexity of $\sum_{l=0}^{2}(4 \times 2^{117.48-16\times l} \times 2^{32+(l+1)\times 8} \times \frac{1}{16} \times \frac{1}{8}) \approx 2^{152.48}$ 8-round AES-192 encryptions. Step 6(a) has a time complexity of $\sum_{l=0}^{2}(4 \times 2^{69.48-16\times l} \times 2^{56+(l+1)\times 8} \times \frac{1}{16} \times \frac{1}{8}) \approx 2^{128.48}$ 8-round AES-192 encryptions. Step 6(b) has a time complexity of $4 \times 2^{88} \times [1+(1-2^{-16})+\cdots+(1-2^{-16})^{2^{21.48}}] \times \frac{1}{16} \times \frac{1}{8} \approx 2^{99}$ 8-round AES-192 encryptions. Therefore, the attack has a total time complexity of approximately $2^{167.7}$ 8-round AES-192 encryptions.

5.2 Attacking 9-round AES-256 in the two-key related-key attack scenario

5.2.1 6-Round related-key impossible-boomerang distinguishers

The two related-key differentials $\Delta\alpha \to \Delta\beta$ and $\Delta\alpha' \to \Delta\beta'$ for $\mathbf{E}^0$ are both $((0, a, a, 0), (0, 0, 0, 0), (0, 0, 0, 0), (0, 0, 0, 0)) \to ((\star, \star, \star, \star), (\star, \star, \star, \star), (\star, \star, \star, \star), (\star, \star, \star, \star))$, where the key difference is $K_A \oplus K_B (= K_C \oplus K_D) = ((0, 0, 0, 0, 0, a, a, 0), (0, 0, 0, 0, 0, 0, 0, 0), (0, 0, 0, 0, 0, 0, 0, 0), (0, 0, 0, 0, 0, 0, 0, 0))$, with a being a specific nonzero 8-bit value. The same differentials as those in Fig. 4b and c are used for $(\mathbf{E}^1)^{-1}$. Table 3 gives the subkey differences for the first nine rounds of AES-256 given the user key difference $((0, 0, 0, 0, 0, a, a, 0), (0, 0, 0, 0, 0, 0, 0, 0), (0, 0, 0, 0, 0, 0, 0, 0), (0, 0, 0, 0, 0, 0, 0, 0))$, where b, c, d, e, f, g are indeterminate 8-bit nonzero values.

We can similarly learn that there exist the following 6-round related-key impossible-boomerang distinguishers for $\mathbf{E}^0 \circ \mathbf{E}^1$: $(((0, a, a, 0), (0, 0, 0, 0), (0, 0, 0, 0), (0, 0, 0, 0)), ((0, a, a, 0), (0, 0, 0, 0), (0, 0, 0, 0), (0, 0, 0, 0))) \overset{K_A,K_B,K_A,K_B}{\not\rightarrow} (((\star, 0, 0, 0), (\star, 0, 0, 0), (\star, 0, 0, 0), (0, 0, 0, 0)), ((\star, 0, 0, 0), (\star, 0, 0, 0), (0, 0, 0, 0), (0, 0, 0, 0)))$.

5.2.2 Attack procedure

Using a 6-round related-key impossible-boomerang distinguisher, we can conduct a related-key impossible boomerang attack on AES-256 reduced to the first 9 rounds (i.e. Rounds 1 to 9).

We reverse the order of the operations MC and ARK for Rounds 7 and 8. From the key difference $K_A \oplus K_B$ we have: (i) $\Delta K_{9,0}$, $\Delta K_{9,3}$, $\Delta K_{9,6}$ and $\Delta K_{9,7}$ are all zero; (ii) $\Delta K_{9,9}$ and $\Delta K_{9,10}$ are identical and indeterminate nonzero values; (iii) $\Delta K_{9,12}$ and $\Delta K_{9,13}$ are different and indeterminate nonzero values, with neither of them equal to $\Delta K_{9,9}$ (or $\Delta K_{9,10}$); and (iv) $\Delta \widehat{K}_{8,0}$ and $\Delta \widehat{K}_{8,7}$ are indeterminate.

1. Choose 2^{58} structures S_i, $(i = 1, 2, \ldots, 2^{58})$, where a structure S_i is defined to be a set of 2^{64} plaintexts $P_{i,j}$ with bytes $(1, 2, 6, 7, 8, 11, 12, 13)$ of the 2^{64} plaintexts

taking all the possible values and the other 8 bytes being fixed, ($j = 1, 2, \ldots, 2^{64}$). In a chosen-plaintext attack scenario, obtain all the 2^{122} ciphertexts for the 2^{64} plaintexts in each of the 2^{58} structures encrypted with K_A and K_B; let $C_{i,j}$ be the ciphertext for plaintext $P_{i,j}$ encrypted with K_A.

2. Guess a value for the subkey bytes $(K_{0,1}, K_{0,2}, K_{0,6}, K_{0,7}, K_{0,8}, K_{0,11}, K_{0,12}, K_{0,13})$. Partially encrypt every plaintext $P_{i,j}$ in S_i with $(K_{0,1}, K_{0,2}, K_{0,6}, K_{0,7}, K_{0,8}, K_{0,11}, K_{0,12}, K_{0,13})$ to get the corresponding value for bytes (1, 2, 5, 6, 9, 10, 13, 14) just after the MC operation of Round 1; we denote it by $\varepsilon_{i,j}$. Then, partially decrypt $\varepsilon_{i,j} \oplus ((0, a, a, 0), (0, 0, 0, 0), (0, 0, 0, 0), (0, 0, 0, 0))$ with $(K_{0,1}, K_{0,2}, K_{0,6}, K_{0,7}, K_{0,8}, K_{0,11}, K_{0,12}, K_{0,13})$ through $\mathrm{MC}^{-1} \circ \mathrm{SR}^{-1} \circ \mathrm{SB}^{-1} \circ \mathrm{ARK}^{-1}$ to get its corresponding plaintext in S_i; we denote it by $\widetilde{P}_{i,j}$. Let $\widetilde{C}_{i,j}$ be the ciphertext for plaintext $\widetilde{P}_{i,j}$ encrypted with K_B. Finally, identify the ciphertext quartets $((C_{i_1,j_1}, \widetilde{C}_{i_1,j_1}), (C_{i_2,j_2}, \widetilde{C}_{i_2,j_2}))$ such that $C_{i_1,j_1} \oplus C_{i_2,j_2} = ((\star, 0, 0, \star), (0, 0, \star, \star), (0, \star, \star, 0), (\star, \star, 0, 0))$ and $\widetilde{C}_{i_1,j_1} \oplus \widetilde{C}_{i_2,j_2} = ((\star, 0, \star, \star), (0, \star, \star, \star), (\star, \star, \star, 0), (\star, \star, 0, \star))$, where $1 \leq i_1, i_2 \leq 2^{58}$, $1 \leq j_1, j_2 \leq 2^{64}$.

3. Guess a value for the subkey bytes $(K_{9,0}, K_{9,7}, K_{9,10}, K_{9,13})$, and do as follows.

   (a) For every remaining ciphertext quartet $((C_{i_1,j_1}, \widetilde{C}_{i_1,j_1}), (C_{i_2,j_2}, \widetilde{C}_{i_2,j_2}))$, partially decrypt C_{i_1,j_1} and C_{i_2,j_2} with $(K_{9,0}, K_{9,7}, K_{9,10}, K_{9,13})$ to get the corresponding values for bytes (0, 4, 8, 12) just after the ARK operation of Round 8, and check whether they have a nonzero byte difference only in byte (0). Keep only the ciphertext quartets that meet the condition.

   (b) Guess a value for the subkey difference $(\Delta K_{9,10}, \Delta K_{9,13})$. For every remaining ciphertext quartet $((C_{i_1,j_1}, \widetilde{C}_{i_1,j_1}), (C_{i_2,j_2}, \widetilde{C}_{i_2,j_2}))$, partially decrypt $\widetilde{C}_{i_1,j_1}$ and $\widetilde{C}_{i_2,j_2}$ with $(K_{9,0}, K_{9,7}, K_{9,10} \oplus \Delta K_{9,10}, K_{9,13} \oplus \Delta K_{9,13})$ to get the corresponding values for bytes (0, 4, 8, 12) just after the ARK operation of Round 8, and check whether they have a nonzero byte difference only in byte (0). Keep only the ciphertext quartets that meet the condition.

4. Guess a value for the subkey bytes $(K_{9,3}, K_{9,6}, K_{9,9}, K_{9,12})$, and do as follows.

   (a) For every remaining ciphertext quartet $((C_{i_1,j_1}, \widetilde{C}_{i_1,j_1}), (C_{i_2,j_2}, \widetilde{C}_{i_2,j_2}))$, partially decrypt C_{i_1,j_1} and C_{i_2,j_2} with $(K_{9,3}, K_{9,6}, K_{9,9}, K_{9,12})$ to get the corresponding values for bytes (3, 7, 11, 15) just after the ARK operation of Round 8, and check whether they have a nonzero byte difference only in byte (7). Keep only the ciphertext quartets that meet the condition.

   (b) Guess a value for the subkey difference $\Delta K_{9,12}$. For every remaining ciphertext quartet $((C_{i_1,j_1}, \widetilde{C}_{i_1,j_1}), (C_{i_2,j_2}, \widetilde{C}_{i_2,j_2}))$, partially decrypt $\widetilde{C}_{i_1,j_1}$ and $\widetilde{C}_{i_2,j_2}$ with $(K_{9,3}, K_{9,6}, K_{9,9} \oplus \Delta K_{9,10}, K_{9,12} \oplus \Delta K_{9,12})$ to get the corresponding values for bytes (3, 7, 11, 15) just after the ARK operation of Round 8, and check whether they have a nonzero byte difference only in byte (7). Keep only the ciphertext quartets that meet the condition.

5. Guess a value for the subkey difference $(K^B_{9,2}, K^B_{9,5}, K^B_{9,8}, K^B_{9,15})$ under K_B. For every remaining ciphertext quartet $((C_{i_1,j_1}, \widetilde{C}_{i_1,j_1}), (C_{i_2,j_2}, \widetilde{C}_{i_2,j_2}))$, partially decrypt $\widetilde{C}_{i_1,j_1}$ and $\widetilde{C}_{i_2,j_2}$ with $(K^B_{9,2}, K^B_{9,5}, K^B_{9,8}, K^B_{9,15})$ to get the corresponding values for bytes (2, 6, 10, 14) just after the ARK operation of Round 8, and check whether they have a nonzero byte difference only in byte (10). Keep only the ciphertext quartets that meet the condition.

6. Perform the following two sub-steps for every remaining quartet $((C_{i_1,j_1}, \widetilde{C}_{i_1,j_1}), (C_{i_2,j_2}, \widetilde{C}_{i_2,j_2}))$.

(a) Guess a value for the subkey bytes $(\widehat{K}^A_{8,0}, \widehat{K}^A_{8,7})$ under K_A. For C_{i_1,j_1} and C_{i_2,j_2}, partially decrypt the corresponding values for bytes (0, 7) just after the ARK operation of Round 8 with $(\widehat{K}^A_{8,0}, \widehat{K}^A_{8,7})$ to get the corresponding values for bytes (0,4) just after the MC operation of Round 7, and check whether they produce a difference that has a zero in only one of bytes (0, 4, 8, 12) just after the ARK operation of Round 7. Keep only the ciphertext quartets that meet this condition.

(b) Guess a value for the subkey bytes $(\widehat{K}^B_{8,0}, \widehat{K}^B_{8,7}, \widehat{K}^B_{8,10})$ under K_B. For $\widetilde{C}_{i_1,j_1}$ and $\widetilde{C}_{i_2,j_2}$, partially decrypt the corresponding values for bytes (0, 7, 10) just after the ARK operation of Round 8 with $(\widehat{K}^B_{8,0}, \widehat{K}^B_{8,7}, \widehat{K}^B_{8,10})$ to get the corresponding values for bytes (0, 4, 8) just after the MC operation of Round 7, and check whether they produce a difference that has a zero in only two of bytes (0, 4, 8, 12) just after the ARK operation of Round 7, where the two byte positions include the one byte position with a zero difference in Step 6(a). If there exists a ciphertext quartet meeting both the conditions, discard the guessed value for $(\widehat{K}^A_{8,0}, \widehat{K}^A_{8,7}, \widehat{K}^B_{8,0}, \widehat{K}^B_{8,7}, \widehat{K}^B_{8,10}, K_{0,1}, K_{0,2}, K_{0,6}, K_{0,7}, K_{0,8}, K_{0,11}, K_{0,12}, K_{0,13}, K_{9,0}, K_{9,3}, K_{9,6}, K_{9,7}, K_{9,9}, K_{9,10}, K_{9,12}, K_{9,13}, K^B_{9,2}, K^B_{9,5}, K^B_{9,8}, K^B_{9,15}, \Delta K_{9,10}, \Delta K_{9,12}, \Delta K_{9,13})$, and repeat Steps 2–5 with another guess; otherwise, execute Step 6.

7. For every remaining value for $(\widehat{K}^B_{8,0}, \widehat{K}^B_{8,7}, \widehat{K}^B_{8,10}, K_{9,0}, K^B_{9,2}, K_{9,3}, K^B_{9,5}, K_{9,6}, K_{9,7}, K^B_{9,8}, K_{9,9}, K_{9,10}, K_{9,12}, K_{9,13}, K^B_{9,15}, \Delta K_{9,10}, \Delta K_{9,12}, \Delta K_{9,13})$, determine the correct user key by exhaustively searching the remaining 136 bits of K_B.

The attack requires 2^{123} chosen plaintexts. In Step 2, a structure S_i yields 2^{64} plaintext pairs $((P_{i,j}, \widetilde{P}_{i,j})$ that produce difference ((0, a, a, 0), (0, 0, 0, 0), (0,0,0,0), (0,0,0,0)) just after the MC operation of Round 1 under the subkey guess, and thus the 2^{58} structures yield a total of $\binom{2^{58+64}}{2} \approx 2^{243}$ candidate ciphertext quartets $((C_{i_1,j_1}, \widetilde{C}_{i_1,j_1}), (C_{i_2,j_2}, \widetilde{C}_{i_2,j_2}))$; however, it is expected that there remain $2^{243} \times 2^{-8\times 8} \times 2^{-4\times 8} = 2^{147}$ ciphertext quartets for every subkey guess after Step 2. In Step 3(a), a ciphertext quartet meets the condition with probability 2^{-24}, and thus after Step 3(a) there remain $2^{147} \times 2^{-24} = 2^{123}$ ciphertext quartets for every subkey guess. In Step 3(b), a ciphertext quartet meets the condition with probability 2^{-24} as well, so $2^{123} \times 2^{-24} = 2^{99}$ ciphertext quartets are expected to pass Step 3(b) for every subkey guess. In Step 4(a), a ciphertext quartet meets the condition with probability 2^{-24}, and thus after Step 4(a) there remain $2^{99} \times 2^{-24} = 2^{75}$ ciphertext quartets for every subkey guess. In Step 4(b), a ciphertext quartet meets the condition with probability 2^{-24} as well, so $2^{75} \times 2^{-24} = 2^{51}$ ciphertext quartets are expected to pass Step 4(b) for every subkey guess. In Step 5 a ciphertext quartet meets the condition with probability 2^{-24}, so about $2^{51} \times 2^{-24} = 2^{27}$ ciphertext quartets are expected to pass Step 5 for every subkey guess. In Step 6(a), a ciphertext quartet meets the condition with probability $\binom{4}{1} \times 2^{-8} = 2^{-6}$, so it is expected that after Step 5(a) there remain $2^{27} \times 2^{-6} = 2^{21}$ ciphertext quartets for every subkey guess. In Step 6(b), a ciphertext quartet meets the condition with probability $\binom{3}{1} \times 2^{-16} = 2^{-14.42}$, and thus after analysing the remaining 2^{21} ciphertext quartets we get that there remain only $2^{224} \times (1 - 2^{-14.42})^{2^{21}} \approx 2^{86.24}$ guessed values for $(K_{0,1}, K_{0,2}, K_{0,6}, K_{0,7}, K_{0,8}, K_{0,11}, K_{0,12}, K_{0,13}, K_{9,0}, K^B_{9,2}, K_{9,3}, K^B_{9,5}, K_{9,6}, K_{9,7}, K^B_{9,8}, K_{9,9}, K_{9,10}, K_{9,12}, K_{9,13}, K^B_{9,15}, \widehat{K}^A_{8,0}, \widehat{K}^A_{8,7}, \widehat{K}^B_{8,0}, \widehat{K}^B_{8,7}, \widehat{K}^B_{8,10}, \Delta K_{9,10}, \Delta K_{9,12}, \Delta K_{9,13})$. Therefore, it is expected that we can find the correct key using $2^{86.24} \times 2^{136} = 2^{222.24}$ trial encryptions in Step 7.

Step 1 has a time complexity of 2^{123} 9-round AES-256 encryptions. Step 2 takes $2 \times 2^{64} \times 2^{122} \times \frac{8}{16} \times \frac{1}{9} + 2^{123} \approx 2^{182.84}$ 9-round AES-256 encryptions, and a simple implementation using a hash table takes $2^{122} \times 2^{64} = 2^{186}$ memory accesses to obtain the useful ciphertext quartets. Step 3 has a time complexity of $2 \times 2^{96} \times 2^{147} \times \frac{4}{16} \times \frac{1}{9} + 2 \times 2^{112} \times 2^{123} \times \frac{4}{16} \times \frac{1}{9} \approx 2^{238.84}$ 9-round AES-256 encryptions. Step 4 has a time complexity of $2 \times 2^{144} \times 2^{99} \times \frac{4}{16} \times \frac{1}{9} + 2 \times 2^{152} \times 2^{75} \times \frac{4}{16} \times \frac{1}{9} \approx 2^{238.84}$ 9-round AES-256 encryptions. Step 5 has a time complexity of $2 \times 2^{184} \times 2^{51} \times \frac{4}{16} \times \frac{1}{9} \approx 2^{230.84}$ 9-round AES-256 encryptions. Step 6(a) has a time complexity of $2 \times 2^{200} \times 2^{27} \times \frac{2}{16} \times \frac{1}{9} \approx 2^{221.84}$ 9-round AES-256 encryptions. Step 6(b) has a time complexity of $2 \times 2^{224} \times [1 + (1 - 2^{-14.42}) + \cdots + (1 - 2^{-14.42})^{2^{21}}] \times \frac{1}{16} \times \frac{1}{9} \approx 2^{232.26}$ 9-round AES-256 encryptions. Therefore, the attack has a total time complexity of approximately $2^{239.9}$ 9-round AES-256 encryptions.

6 Conclusions

In this paper we have proposed a new cryptanalytic technique, called the impossible boomerang attack, and have given an extension of this attack which applies in a related-key attack scenario. The impossible boomerang attack can break 6-round AES-128, 7-round AES-192 and 7-round AES-256 in the single-key attack scenario, and the related-key impossible boomerang attack can break 8-round AES-192 and 9-round AES-256 in the two-key related-key attack scenario. Note that trade-off versions between time and memory can be easily obtained from these attacks by using the technique described in [36,39]. The presented cryptanalytic results suggest a perspective never addressed before to look at the security of AES, exhibiting some merits. The related-key impossible boomerang attack on 9-round AES-256 was the first to achieve this amount of attacked rounds in the two-key related-key attack scenario, and in this particular attack scenario the related-key impossible boomerang attacks on 8-round AES-192 and 9-round AES-256 match the best currently known results for AES-192/256 in terms of the numbers of attacked rounds.

The (related-key) impossible boomerang attack is a general cryptanalytic technique, and can potentially be used to cryptanalyse other block ciphers except AES. Block cipher designers should pay attention to this technique when designing ciphers.

Acknowledgments The author is very grateful to Prof. Chris Mitchell and the anonymous referees for their comments on earlier versions of this paper, and also very grateful to the editor for his/her editorial efforts during the review of this paper.

References

1. Bahrak B., Aref M.R.: Impossible differential attack on seven-round AES-128. IET Inform. Secur. **2**(2), 28–32 (2008).
2. Biham E.: New types of cryptanalytic attacks using related keys. In: EUROCRYPT 1993. Lecture Notes in Computer Science, vol. 765, pp. 398–409. Springer, Heidelberg (1993).
3. Biham E., Biryukov A., Shamir A.: Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In: EUROCRYPT 1999. Lecture Notes in Computer Science, vol. 1592, pp. 12–23. Springer, Heidelberg (1999).
4. Biham E., Biryukov A., Shamir A.: Miss in the middle attacks on IDEA and Khufu. In: FSE 1999. Lecture Notes in Computer Science, vol. 1636, pp. 124–138. Springer, Heidelberg (1999).

5. Biham E., Dunkelman O., Keller N.: The rectangle attack—rectangling the Serpent. In: EUROCRYPT 2001. Lecture Notes in Computer Science, vol. 2045, pp. 340–357. Springer, Heidelberg (2001).
6. Biham E., Dunkelman O., Keller N.: Enhancing differential-linear cryptanalysis. In: ASIACRYPT 2002. Lecture Notes in Computer Science, vol. 2501, pp. 254–266. Springer, Heidelberg (2002).
7. Biham E., Dunkelman O., Keller N.: New combined attacks on block ciphers. In: FSE 2005. Lecture Notes in Computer Science, vol. 3557, pp. 126–144. Springer, Heidelberg (2005).
8. Biham E., Dunkelman O., Keller N.: Related-key boomerang and rectangle attacks. In: EUROCRYPT 2005. Lecture Notes in Computer Science, vol. 3494, pp. 507–525. Springer, Heidelberg (2005).
9. Biham E., Dunkelman O., Keller N.: A related-key rectangle attack on the full KASUMI. In: ASIACRYPT 2005. Lecture Notes in Computer Science, vol. 3788, pp. 443–461. Springer, Heidelberg (2005).
10. Biham E., Dunkelman O., Keller N.: Related-key impossible differential attacks on 8-round AES-192. In: CT-RSA 2006. Lecture Notes in Computer Science, vol. 3860, pp. 21–33. Springer, Heidelberg (2006).
11. Biham E., Shamir A.: Differential cryptanalysis of DES-like cryptosystems. In: CRYPTO 1990. Lecture Notes in Computer Science, vol. 537, pp. 2–21. Springer, Heidelberg (1990).
12. Biryukov A.: The boomerang attack on 5 and 6-round reduced AES. In: AES 2004. Lecture Notes in Computer Science, vol. 3373, pp. 11–15. Springer, Heidelberg (2005).
13. Biryukov A., Dunkelman O., Keller N., Khovratovich D., Shamir A.: Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. In: EUROCRYPT 2010. Lecture Notes in Computer Science, vol. 6110, pp. 299–319. Springer, Heidelberg (2010).
14. Biryukov A., Khovratovich D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: ASIACRYPT 2009. Lecture Notes in Computer Science, vol. 5912, pp. 1–18. Springer, Heidelberg (2009).
15. Biryukov A., Khovratovich D, Nikolic I.: Distinguisher and related-key attack on the full AES-256. In: CRYPTO 2009. Lecture Notes in Computer Science, vol. 5677, pp. 231–249. Springer, Heidelberg (2009).
16. Cheon J., Kim M., Kim K., Lee J.: Improved impossible differential cryptanalysis of Rijndael and Crypton. In: ICISC 2001. Lecture Notes in Computer Science, vol. 2288, pp. 39–49. Springer, Heidelberg (2001).
17. Daemen J., Knudsen L.R., Rijmen V.: The block cipher Square. In: FSE 1997. Lecture Notes in Computer Science, vol. 1267, pp. 149–165. Springer, Heidelberg (1997).
18. Daemen J., Rijmen V.: AES proposal: rijndael. In: The First Advanced Encryption Standard Candidate Conference. NIST, Ventura, CA (1998).
19. Demirci H., Selcuk A.A.: A meet-in-the-middle attack on 8-round AES. In: FSE 2008. Lecture Notes in Computer Science, vol. 5086, pp. 116–126. Springer, Heidelberg (2008).
20. Dunkelman O., Keller N.: An improved impossible differential attack on MISTY1. In: Advances in Cryptology—ASIACRYPT 2008. Lecture Notes in Computer Science, vol. 5350, pp. 441–454. Springer, Heidelberg (2008).
21. Ferguson N., Kelsey J., Lucks S., Schneier B., Stay M., Wagner D., Whiting D.: Improved cryptanalysis of Rijndael. In: FSE 2000. Lecture Notes in Computer Science, vol. 1978, pp. 213–230. Springer, Heidelberg (2001).
22. Fleischmann E., Gorski M., Lucks S.: Attacking 9 and 10 rounds of AES-256. In: ACISP 2009. Lecture Notes in Computer Science, vol. 5594, pp. 60–72. Springer, Heidelberg (2009).
23. Gilbert H., Minier M.: A collision attack on 7 rounds of Rijndael. In: The Third Advanced Encryption Standard Candidate Conference, pp. 230–241. NIST, Ventura, CA (2000).
24. Hong S., Kim J., Lee S., Preneel B.: Related-key rectangle attacks on reduced versions of SHACAL-1 and AES-192. In: FSE 2005. Lecture Notes in Computer Science, vol. 3557, pp. 368–383. Springer, Heidelberg (2005).
25. International Organization for Standardization (ISO): ISO/IEC 18033-3:2005: Information technology—Security techniques—Encryption algorithms—Part 3: block ciphers. ISO, Geneva (2005).
26. Jakimoski G., Desmedt Y.: Related-key differential cryptanalysis of 192-bit key AES variants. In: SAC 2003. Lecture Notes in Computer Science, vol. 3006, pp. 208–221. Springer, Heidelberg (2004).
27. Kelsey J., Kohno T., Schneier B.: Amplified boomerang attacks against reduced-round MARS and Serpent. In: FSE 2000. Lecture Notes in Computer Science, vol. 1978, pp. 75–93. Springer, Heidelberg (2001).
28. Kelsey J., Schneier B., Wagner D.: Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In: CRYPTO 1996. Lecture Notes in Computer Science, vol. 1109, pp. 237–251. Springer, Heidelberg (1996).
29. Kim J., Hong S., Preneel B.: Related-key rectangle attacks on reduced AES-192 and AES-256. In: FSE 2007. Lecture Notes in Computer Science, vol. 4593, pp. 225–241. Springer, Heidelberg (2007).
30. Kim J., Kim G., Hong S., Lee S., Hong D.: The related-key rectangle attack—application to SHACAL-1. In: ACISP 2004. Lecture Notes in Computer Science, vol. 3108, pp. 123–136. Springer, Heidelberg (2004).

31. Knudsen L.R.: Cryptanalysis of LOKI91. In: AUSCRYPT 1992. Lecture Notes in Computer Science, vol. 718, pp. 196–208. Springer, Heidelberg (1993).
32. Knudsen L.R.: Trucated and higher order differentials. In: FSE 1994. Lecture Notes in Computer Science, vol. 1008, pp. 196–211. Springer, Heidelberg (1995).
33. Knudsen L.R.: DEAL—a 128-bit block cipher. Technical report, Department of Informatics, University of Bergen, Norway (1998).
34. Langford S.K., Hellman M.E.: Differential-linear cryptanalysis. In: CRYPTO 1994. Lecture Notes in Computer Science, vol. 839, pp. 17–25. Springer, Heidelberg (1994).
35. Lu J.: Cryptanalysis of block ciphers. PhD Thesis, The University of London, UK (2008). A copy is available online as Technical Report RHUL-MA-2008-19, Department of Mathematics, Royal Holloway, University of London, UK. http://www.ma.rhul.ac.uk/static/techrep/2008/RHUL-MA-2008-19.pdf (2008).
36. Lu J., Dunkelman O., Keller N., Kim J.: New impossible differential attacks on AES, In: INDOCRYPT 2008. Lecture Notes in Computer Science, vol. 5365, pp. 279–293. Springer, Heidelberg (2008).
37. Lu J., Kim J.: Attacking 44 rounds of the SHACAL-2 block cipher using related-key rectangle cryptanalysis. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **91**(A), 2588–2596 (2008).
38. Lu J., Kim J., Keller N., Dunkelman O.: Related-key rectangle attack on 42-round SHACAL-2. In: ISC 2006. Lecture Notes in Computer Science, vol. 4176, pp. 85–100. Springer, Heidelberg (2006).
39. Lu J., Kim J., Keller N., Dunkelman O.: Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1. In: CT-RSA 2008. Lecture Notes in Computer Science, vol. 4964, pp. 370–386. Springer, Heidelberg (2008).
40. Lucks S.: Attacking seven rounds of Rijndael under 192-bit and 256-bit keys. In: The Third Advanced Encryption Standard Candidate Conference, pp. 215–229. NIST, Ventura, CA (2000).
41. Matsui M.: Linear cryptanalysis method for DES cipher. In: EUROCRYPT 1993. Lecture Notes in Computer Science, vol. 765, pp. 386–397. Springer, Heidelberg (1994).
42. Murphy S.: The return of the boomerang. Technical Report RHUL-MA-2009-20, Department of Mathematics, Royal Holloway, University of London, UK. http://www.ma.rhul.ac.uk/static/techrep/2009/RHUL-MA-2009-20.pdf (2009).
43. National Institute of Standards and Technology (NIST). Advanced Encryption Standard (AES). FIPS-197 (2001).
44. NIST: National Institute of Standards and Technology. http://www.nist.gov.
45. Phan R.: Impossible differential cryptanalysis of 7-round advanced encryption standard (AES). Inform. Process. Lett. 91(1), 33–38 (2004).
46. Wagner D.: The boomerang attack. In: FSE 1999. Lecture Notes in Computer Science, vol. 1636, pp. 156–170. Springer, Heidelberg (1999).
47. Wang G., Keller N., Dunkelman O.: The delicate issues of addition with respect to XOR differences. In: SAC 2007. Lecture Notes in Computer Science, vol. 4876, pp. 212–231. Springer, Heidelberg (2007).
48. Zhang W., Wu W., Zhang L., Feng D.: Improved related-key impossible differential attacks on reduced-round AES-192. In: SAC 2006. Lecture Notes in Computer Science, vol. 4356, pp. 15–27. Springer, Heidelberg (2007).
49. Zhang W., Wu W., Zhang L.: Related-key impossible differential attacks on reduced-round AES-256. J. Softw. 18(11), 2893–2901. http://www.lois.cn/LOIS-AES/data/AES-256.pdf (2007).
50. Zhang W., Wu W., Feng D.: New results on impossible differential cryptanalysis of reduced AES. In: ICISC 2007. Lecture Notes in Computer Science, vol. 4817, pp. 239–250. Springer, Heidelberg (2007).
51. Zhang W., Zhang L., Wu W., Feng D.: Related-key differential-linear attacks on reduced AES-192. In: INDOCRYPT 2007. Lecture Notes in Computer Science, vol. 4859, pp. 73–85. Springer, Heidelberg (2007).