On the provable security against truncated impossible differential cryptanalysis for AES in the master-key setting

Xueping Yan, Lin Tan, Hong Xu, and Wenfeng Qi

PLA Strategic Support Force Information Engineering University, China
yanxueping163@163.com, tanlin100@163.com, xuhong0504@163.com, wenfeng.qi@263.net

Abstract. Impossible differential cryptanalysis is a powerful cryptanalysis technique of block ciphers. Length of impossible differentials is important for the security evaluation of a block cipher against impossible differential cryptanalysis. Many previous studies on finding impossible differentials of AES assumed that round keys are independent and uniformly random. There are few results on security evaluation of AES in the master-key setting. In ASIACRYPT 2020, Hu et al. redefined impossible differential with the key schedule considered, and showed that there exists no one-byte active input and one-byte active output impossible differential for 5-round AES-128 even considering the relations of 3-round keys. In this paper, we prove theoretically that even though the relations of all round keys are considered, there do not exist three kinds of truncated impossible differentials for 5-round AES: (1) the input truncated differences are nonzero only in any diagonal and the output truncated differences are nonzero only in any inverse diagonal; (2) the input truncated differences are nonzero only in any two diagonals and the output truncated differences are nonzero only in any inverse diagonal; (3) the input truncated differences are nonzero only in any diagonal and the output truncated differences are nonzero only in any two inverse diagonals. Furthermore, for any given truncated differentials of these three kinds, the lower bounds of the number of master keys such that the truncated differentials are possible for 5-round AES-128 are presented.

Keywords: AES · Truncated impossible differential · Provable security · Master-key setting

1 Introduction

Impossible differential cryptanalysis [4,20] is a powerful cryptanalysis technique of block ciphers. The differentials with probability 0 are used to distinguish round-reduced block ciphers and discard the wrong keys in the key recovery attack. Truncated impossible differentials are usually used in the impossible differential cryptanalysis of block ciphers, such as AES [1,5,6,9,13,21,28], Crypton [6, 9], Camellia [6, 7], SIMON [7], CLEFIA [7, 25] and XTEA [8]. AES is

the most widely used block cipher and its security has been studied worldwide in the last twenty years. Many cryptanalysis techniques have been applied to distinguish or attack the round-reduced variants of AES, such as integral [12], impossible differential [6], zero-correlation linear [17,23], subspace trail [15], mixture differential [2, 14], multiple-of-8 [16], meet-in-the-middle [10], yoyo [22], exchange [3] and boomerang [11]. The first impossible differential distinguisher on 4-round AES was proposed to attack 5-round AES in [5]. Then based on 4-round impossible differential distinguishers, many impossible differential attacks on 6 rounds and 7 rounds of AES were proposed [1, 6, 9, 21, 28]. As we know, the best key recovery attacks on AES-128 in the secret-key model cover 7 rounds. In EUROCRYPT 2021, Gaëtan et al. [13] gave new representations of the AES key schedule and improved the impossible differential attack on 7-round AES-128. The length of truncated impossible differentials used in these known attacks is 4 rounds. To some extent, the longer truncated impossible differentials can be found, the more rounds can be attacked. Whether there exist 5-round truncated impossible differentials is one of important problems for the security evaluation of AES.

In [24], Sun et al. proved that there exists no 5-round impossible differential for the AES structure, where the details of S-boxes are not considered. Under the assumption that round keys are independent and uniformly random, Wang et al. showed that there exists no 5-round truncated impossible differential even considering the details of the AES S-box [26], and further proved that any concrete differential is possible for 5-round AES [27]. These results are not true for the real AES, because the round keys are dependent under the key schedule. In ASIACRYPT 2020, Hu et al. [18] redefined impossible differential with the key schedule considered, and proposed a SAT-based automatic search tool for impossible differentials. With the help of the automatic search tool, it was shown that there exists no one-byte active input and one-byte active output impossible differential for 5-round AES even taking the relations of the middle 3-round keys into account. It is the first result on the provable security evaluation of AES against impossible differential cryptanalysis with the key schedule considered.

In this paper, we study three kinds of truncated differentials for 5-round AES in the master-key setting.

-**Set 1**: the input truncated differences are nonzero only in any diagonal and the output truncated differences are nonzero only in any inverse diagonal.

-**Set 2**: the input truncated differences are nonzero only in any two diagonals and the output truncated differences are nonzero only in any inverse diagonal.

-**Set 3**: the input truncated differences are nonzero only in any diagonal and the output truncated differences are nonzero only in any two inverse diagonals.

By investigating the properties of the key schedule, we prove theoretically that there do not exist the three kinds of truncated impossible differentials for 5-round AES even considering the relations of all round keys. Furthermore, for any given truncated differentials in the three sets, the lower bounds of the number of master keys such that the truncated differentials are possible for 5-round AES-128 are presented.

This paper is organized as follows. In Section 2, the description of AES and the definitions related to truncated differential are recalled. In Section 3, three kinds of truncated differentials for 5-round AES in the master-key setting are studied. Section 4 concludes the paper.

2 Preliminaries

2.1 Brief description of AES

AES is a Substitution-Permutation Network cipher with 128-bit block. The 128-bit state can be described as a 4×4 matrix over the finite field $\mathbb{F}_{2^8}$, and the order of bytes in the state matrix is showed in Fig. 1. The number of rounds N_r depends on the length of master key, that is, $N_r = 10$ for 128-bit key, $N_r = 12$ for 192-bit key and $N_r = 14$ for 256-bit key. The round transformation of AES consists of the following four operations.

1. *SubBytes*(SB) : applies the same 8-bit S-box to 16 bytes of the state parallelly. The S-box is composed of the multiplicative inverse transformation over $\mathbb{F}_{2^8}$ and an affine function over $\mathbb{F}_2$, i.e., $S(x) = L(x^{-1}) + b$, $x \in \mathbb{F}_{2^8}$.
2. *ShiftRows*(SR) : shifts the i-th row by i bytes to the left circularly for $i = 0, 1, 2, 3$.
3. *MixColumns*(MC) : multiplies each column by the following MDS matrix over $\mathbb{F}_{2^8}$.
$$\begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix}$$
4. *AddRoundKey*(AK) : XORs the state with a 128-bit round key, which is generated from a master key by the key schedule.

An additional AK is applied before the first round and the MC is omitted in the last round. Let K_r denote the r-th round key, and AK_r denote the AddRoundKey operation with K_r. The r-th round transformation can be written as $AK_r \circ MC \circ SR \circ SB$. When interchanging the order of MC and AK, we can get the equivalent round transformation $MC \circ AK'_r \circ SR \circ SB$, where AK'_r denotes XORing the equivalent round key $K'_r = MC^{-1}(K_r)$. Denote by $K_{r,j}$ the j-th byte of K_r. When considering several bytes $j_1, j_2, ..., j_n$ of K_r simultaneously, we denote by $K_{r,\{j_1,j_2,...,j_n\}}$. In this paper, we focus on AES-128. The key schedule of AES-128 can be described as follows.

$$\begin{aligned} K_{r,0} &= K_{r-1,0} + S(K_{r-1,13}) + C_r, \\ K_{r,1} &= K_{r-1,1} + S(K_{r-1,14}), \\ K_{r,2} &= K_{r-1,2} + S(K_{r-1,15}), \\ K_{r,3} &= K_{r-1,3} + S(K_{r-1,12}), \\ K_{r,j} &= K_{r-1,j} + K_{r,j-4}, \quad 4 \le j \le 15, \end{aligned}$$

where K_0 is the master key, and C_r is the round constant, $1 \le r \le 10$.

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

Fig. 1. The order of bytes in the state matrix

2.2 Definitions

Definition 1. *Given a vectorial Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$, for an input difference $\Delta X \in \mathbb{F}_2^n$ and an output difference $\Delta Y \in \mathbb{F}_2^n$, the differential probability is defined as*

$$DP(\Delta X \xrightarrow{f} \Delta Y) = \frac{1}{2^n} \# \left\{ X \in \mathbb{F}_2^n \mid f(X) + f(X + \Delta X) = \Delta Y \right\}.$$

Definition 2. *Given a keyed function $f_K : \mathbb{F}_2^n \times K \to \mathbb{F}_2^n$, for an input difference $\Delta X \in \mathbb{F}_2^n$ and an output difference $\Delta Y \in \mathbb{F}_2^n$, the expected differential probability over all keys is defined as*

$$EDP(\Delta X \xrightarrow{f_K} \Delta Y) = \frac{1}{\# K} \sum_{k \in K} DP(\Delta X \xrightarrow{f_k} \Delta Y).$$

If $EDP(\Delta X \xrightarrow{f_K} \Delta Y)$ is too small to distinguish f_K from random permutations for any differential $\Delta X \to \Delta Y$, then f_K is provably secure against differential cryptanalysis. If $EDP(\Delta X \xrightarrow{f_K} \Delta Y) = 0$, then $\Delta X \to \Delta Y$ is called an impossible differential of f_K. In the following we recall the definitions related to truncated differential introduced in [19].

Definition 3. *For $x \in \mathbb{F}_{2^m}$, define the function χ as*

$$\chi(x) = \begin{cases} 0, & if\ x = 0; \\ 1, & if\ x \neq 0. \end{cases}$$

For $X = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_{2^m}^n$, define $\chi(X) = (\chi(x_1), \chi(x_2), \ldots, \chi(x_n))$.

Definition 4. *Given a function $f : \mathbb{F}_{2^m}^n \to \mathbb{F}_{2^m}^n$, for an input truncated difference $\overline{\Delta X} \in \mathbb{F}_2^n$ and an output truncated difference $\overline{\Delta Y} \in \mathbb{F}_2^n$, the truncated differential probability is defined as*

$$DP(\overline{\Delta X} \xrightarrow{f} \overline{\Delta Y}) = \frac{\sum\limits_{\substack{\Delta X, \Delta Y \in \mathbb{F}_{2^m}^n, \\ \chi(\Delta X) = \overline{\Delta X}, \chi(\Delta Y) = \overline{\Delta Y}}} DP(\Delta X \xrightarrow{f} \Delta Y)}{\# \left\{ \Delta X \in \mathbb{F}_{2^m}^n \mid \chi(\Delta X) = \overline{\Delta X} \right\}}.$$

Definition 5. *Given a keyed function* $f_K : \mathbb{F}_{2^m}^n \times K \to \mathbb{F}_{2^m}^n$*, for an input truncated difference* $\overline{\Delta X} \in \mathbb{F}_2^n$ *and an output truncated difference* $\overline{\Delta Y} \in \mathbb{F}_2^n$*, the expected truncated differential probability over all keys is defined as*

$$EDP(\overline{\Delta X} \xrightarrow{f_K} \overline{\Delta Y}) = \frac{1}{\#K} \sum_{k \in K} DP(\overline{\Delta X} \xrightarrow{f_k} \overline{\Delta Y}).$$

If $EDP(\overline{\Delta X} \xrightarrow{f_K} \overline{\Delta Y}) = 0$, then $\overline{\Delta X} \to \overline{\Delta Y}$ is called a truncated impossible differential of f_K. To prove that truncated differential $\overline{\Delta X} \to \overline{\Delta Y}$ is possible for f_K, we need to find at least a key $k \in K$ and a differential $\Delta X \to \Delta Y$ such that $\chi(\Delta X) = \overline{\Delta X}$, $\chi(\Delta Y) = \overline{\Delta Y}$, and $DP(\Delta X \xrightarrow{f_k} \Delta Y) > 0$.

3 Main results

Let $\overline{\Delta X}, \overline{\Delta W} \in \mathbb{F}_2^{4\times 4}$ be the input and output truncated differences respectively. In this section, we reveal some properties of the key schedule of AES-128, and prove theoretically that in the master-key setting there do not exist the following three kinds of truncated impossible differentials for 5-round AES.

-**Set 1**: $\overline{\Delta X}$ is nonzero only in any diagonal and $\overline{\Delta W}$ is nonzero only in any inverse diagonal;

-**Set 2**: $\overline{\Delta X}$ is nonzero only in any two diagonals and $\overline{\Delta W}$ is nonzero only in any inverse diagonal;

-**Set 3**: $\overline{\Delta X}$ is nonzero only in any diagonal and $\overline{\Delta W}$ is nonzero only in any two inverse diagonals.

We note that the input (output) truncated differences being nonzero in some diagonals (inverse diagonals) means that there exists at least a nonzero bit in each corresponding diagonal (inverse diagonal).

Five rounds of AES can be written as

$$AK_5 \circ SR \circ SB \circ AK_4 \circ G \circ AK_1' \circ SR \circ SB \circ AK_0,$$

where $G = MC \circ SR \circ SB \circ AK_3 \circ MC \circ SR \circ SB \circ MC \circ AK_2' \circ SR \circ SB \circ MC$. To prove the results, it is sufficient to prove that the following three kinds of truncated differentials $\overline{\Delta X'} \to \overline{\Delta W'}$ are all possible for G even considering the relation of K_2' and K_3.

1. $\overline{\Delta X'}$ is nonzero only in any column and $\overline{\Delta W'}$ is nonzero only in any column;
2. $\overline{\Delta X'}$ is nonzero only in any two columns and $\overline{\Delta W'}$ is nonzero only in any column;
3. $\overline{\Delta X'}$ is nonzero only in any column and $\overline{\Delta W'}$ is nonzero only in any two columns.

Since SB and SR are applied on each byte independently, we can interchange their order in the last $SR \circ SB$ of G. Then decompose G as

$$G = f \circ (SR \circ AK_3) \circ g \circ (AK_2' \circ SR) \circ h,$$

where $h = SB \circ MC$, $g = MC \circ SR \circ SB \circ MC$, and $f = MC \circ SB$ are key-independent.

Lemma 1. *For any nonzero truncated difference* $\overline{\Delta y} \in \mathbb{F}_2^4$*, there exists difference* $\Delta x \in (\mathbb{F}_{2^8}^*)^4$ *such that* $\chi(MC(\Delta x)) = \overline{\Delta y}$*, where* $\mathbb{F}_{2^8}^*$ *denotes the multiplicative group of nonzero elements of* $\mathbb{F}_{2^8}$*.*

Proof. Let c be the Hamming weight of $\overline{\Delta y}$. If $c = 1$, then for any Δy with $\chi(\Delta y) = \overline{\Delta y}$, we have $MC^{-1}(\Delta y) \in (\mathbb{F}_{2^8}^*)^4$ since the MC matrix is MDS. If $2 \le c \le 4$, then the number of Δy such that $\chi(\Delta y) = \overline{\Delta y}$ is 255^c. But the number of Δy such that $\chi(\Delta y) = \overline{\Delta y}$ and $MC^{-1}(\Delta y) \notin (\mathbb{F}_{2^8}^*)^4$ is at most $4 \cdot (255)^{c-1}$. Therefore, there exists difference $\Delta x \in (\mathbb{F}_{2^8}^*)^4$ such that $\chi(MC(\Delta x)) = \overline{\Delta y}$. □

Lemma 2. (See [27].) *If* $SB \circ MC$ *is regarded as a function on* $\mathbb{F}_{2^8}^4$*, then for any nonzero input truncated difference* $\overline{\Delta x} \in \mathbb{F}_2^4$ *and any output difference* $\Delta y \in (\mathbb{F}_{2^8}^*)^4$*, there exists input difference* Δx *such that* $\chi(\Delta x) = \overline{\Delta x}$ *and*

$$SB \circ MC(x) + SB \circ MC(x + \Delta x) = \Delta y$$

for some $x \in \mathbb{F}_{2^8}^4$*.*

Lemma 3. *Suppose the master keys of AES-128 are independent and uniformly random. Then any inverse diagonal of* K'_r *and any diagonal of* K_{r+1} *are independent, and for any given values of the eight bytes there are* 2^{64} *master keys under the key schedule of AES-128,* $0 \le r \le 9$*.*

Proof. By the assumption, the 16 bytes of K_r are independent and uniformly random. Let $(p, q, s, t) \in \{(0, 7, 10, 13), (1, 4, 11, 14), (2, 5, 8, 15), (3, 6, 9, 12)\}$ be any inverse diagonal. Since $K'_r = MC^{-1}(K_r)$, four bytes in the p-th inverse diagonal of K'_r can be represented by the bytes of K_r as follows.

$$\begin{aligned} K'_{r,p} &= a_0 K_{r,0} + a_1 K_{r,1} + a_2 K_{r,2} + a_3 K_{r,3}, \\ K'_{r,q} &= a_4 K_{r,4} + a_5 K_{r,5} + a_6 K_{r,6} + a_7 K_{r,7}, \\ K'_{r,s} &= a_8 K_{r,8} + a_9 K_{r,9} + a_{10} K_{r,10} + a_{11} K_{r,11}, \\ K'_{r,t} &= a_{12} K_{r,12} + a_{13} K_{r,13} + a_{14} K_{r,14} + a_{15} K_{r,15}, \end{aligned} \tag{1}$$

where $a_j \in \{0B, 0D, 0E, 09\}$ is a constant dependent on (p, q, s, t), $0 \le j \le 15$. From the key schedule, the four diagonals of K_{r+1} can be represented by the bytes of K_r as the following four systems of equations respectively.

$$\begin{aligned} K_{r+1,0} &= K_{r,0} + S(K_{r,13}) + C_{r+1}, \\ K_{r+1,5} &= K_{r,5} + K_{r,1} + S(K_{r,14}), \\ K_{r+1,10} &= K_{r,10} + K_{r,6} + K_{r,2} + S(K_{r,15}), \\ K_{r+1,15} &= K_{r,15} + K_{r,11} + K_{r,7} + K_{r,3} + S(K_{r,12}). \end{aligned} \tag{2}$$

$$\begin{aligned} K_{r+1,3} &= K_{r,3} + S(K_{r,12}), \\ K_{r+1,4} &= K_{r,4} + K_{r,0} + S(K_{r,13}) + C_{r+1}, \\ K_{r+1,9} &= K_{r,9} + K_{r,5} + K_{r,1} + S(K_{r,14}), \\ K_{r+1,14} &= K_{r,14} + K_{r,10} + K_{r,6} + K_{r,2} + S(K_{r,15}). \end{aligned} \tag{3}$$

$$\begin{aligned} K_{r+1,2} &= K_{r,2} + S(K_{r,15}), \\ K_{r+1,7} &= K_{r,7} + K_{r,3} + S(K_{r,12}), \\ K_{r+1,8} &= K_{r,8} + K_{r,4} + K_{r,0} + S(K_{r,13}) + C_{r+1}, \\ K_{r+1,13} &= K_{r,13} + K_{r,9} + K_{r,5} + K_{r,1} + S(K_{r,14}). \end{aligned} \tag{4}$$

$$\begin{aligned} K_{r+1,1} &= K_{r,1} + S(K_{r,14}), \\ K_{r+1,6} &= K_{r,6} + K_{r,2} + S(K_{r,15}), \\ K_{r+1,11} &= K_{r,11} + K_{r,7} + K_{r,3} + S(K_{r,12}), \\ K_{r+1,12} &= K_{r,12} + K_{r,8} + K_{r,4} + K_{r,0} + S(K_{r,13}) + C_{r+1}. \end{aligned} \tag{5}$$

We claim that for any given values of $K'_{r,\{p,q,s,t\}}$ and any diagonal of K_{r+1}, the number of solutions of K_r is 2^{64}. For $K_{r+1,\{0,5,10,15\}}$, we can take the eight bytes $K_{r,\{0,1,4,6,9,11,14,15\}}$ as free variables in the system of (1) and (2). When the free variables are determined the other eight bytes of K_r have unique solution. Similarly, for $K_{r+1,\{3,4,9,14\}}$, we also take $K_{r,\{0,1,4,6,9,11,14,15\}}$ as free variables in the system of (1) and (3). For $K_{r+1,\{2,7,8,13\}}$, we take $K_{r,\{0,2,4,5,9,11,12,13\}}$ as free variables in the system of (1) and (4). For $K_{r+1,\{1,6,11,12\}}$, we take $K_{r,\{0,2,4,5,9,11,14,15\}}$ as free variables in the system of (1) and (5). Since $K'_{r,\{p,q,s,t\}}$ and any diagonal of K_{r+1} can take arbitrary values, they are independent. Furthermore, for their any given values there are 2^{64} master keys under the key schedule of AES-128. □

Theorem 1. *For any input truncated difference $\overline{\Delta X}$ with one diagonal nonzero and any output truncated difference $\overline{\Delta W}$ with one inverse diagonal nonzero, there are at least 2^{66} master keys such that $\overline{\Delta X} \to \overline{\Delta W}$ is possible for 5-round AES-128.*

Proof. It is sufficient to prove that for any input truncated difference $\overline{\Delta X'}$ with one column nonzero and any output truncated difference $\overline{\Delta W'}$ with one column nonzero, there are at least 2^{66} master keys such that

$$DP(\overline{\Delta X'} \xrightarrow{G} \overline{\Delta W'}) > 0.$$

Let the i-th column of $\overline{\Delta X'}$ and the j-th column of $\overline{\Delta W'}$ be nonzero, $0 \le i, j \le 3$. From the definition of truncated differential probability, we just need to find a differential $\Delta X' \to \Delta W'$ such that $\chi(\Delta X') = \overline{\Delta X'}$, $\chi(\Delta W') = \overline{\Delta W'}$, and

$$DP(\Delta X' \xrightarrow{G} \Delta W') > 0.$$

The propagation of the differential is shown in Fig. 2. We recall

$$G = f \circ (SR \circ AK_3) \circ g \circ (AK'_2 \circ SR) \circ h,$$

where $h = SB \circ MC$, $g = MC \circ SR \circ SB \circ MC$, and $f = MC \circ SB$.

From Lemma 1, there exist ΔZ with only four bytes in the j-th column nonzero and $\Delta W'$ with $\chi(\Delta W') = \overline{\Delta W'}$ such that $f(Z) + f(Z + \Delta Z) = \Delta W'$, where $Z \in \mathbb{F}_{2^8}^{4\times 4}$ and the bytes except the j-th column of Z can take arbitrary

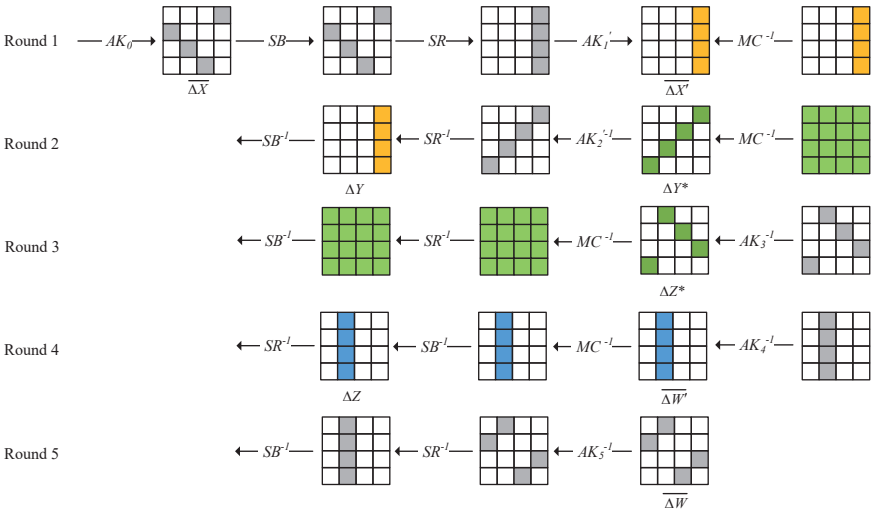

Fig. 2. The propagation of the differential in Set 1

values. Let $\Delta Z^* = SR^{-1}(\Delta Z)$, then $SR^{-1} \circ MC^{-1}(\Delta Z^*) \in (\mathbb{F}_{2^8}^*)^{4\times 4}$. From Lemma 2, there exists input difference ΔY^* with only four bytes in the i-th inverse diagonal nonzero such that $g(Y^*) + g(Y^* + \Delta Y^*) = \Delta Z^*$ for some $Y^* \in \mathbb{F}_{2^8}^{4\times 4}$. Let $\Delta Y = SR^{-1}(\Delta Y^*)$. From Lemma 2 again, there exists input difference $\Delta X'$ such that $\chi(\Delta X') = \overline{\Delta X'}$ and $h(X') + h(X' + \Delta X') = \Delta Y$, where $X' \in \mathbb{F}_{2^8}^{4\times 4}$ and the bytes except the i-th column of X' can take arbitrary values. Denote $Y = h(X')$, then the bytes except the i-th column of Y can take arbitrary values.

Taking $K_2' = SR(Y) + Y^*$ or $K_2' = SR(Y) + Y^* + \Delta Y^*$, the output states of $SR \circ h$ and the input states of g are connected. Because the bytes except the i-th column of Y can take arbitrary values, the bytes except the i-th inverse diagonal of K_2' can take arbitrary values. Denote $Z^* = g(Y^*)$. Taking $K_3 = Z^* + SR^{-1}(Z)$ or $K_3 = Z^* + SR^{-1}(Z) + \Delta Z^*$, the output states of g and the input states of $f \circ SR$ are connected. Since the bytes except the j-th column of Z can take arbitrary values, the bytes except the j-th diagonal of K_3 can take arbitrary values.

The i-th inverse diagonal of K_2' and the j-th diagonal of K_3 have at least two possible values respectively. From Lemma 3, for any given values of these eight bytes, there are 2^{64} master keys under the key schedule of AES-128. Thus there are at least 2^{66} master keys such that $\overline{\Delta X'} \to \overline{\Delta W'}$ is possible for G. This completes the proof. □

Lemma 4. *Suppose the master keys of AES-128 are independent and uniformly random. Then any two inverse diagonals of K_r' and any diagonal of K_{r+1} are independent, and for any given values of the twelve bytes there are 2^{32} master keys under the key schedule of AES-128, $0 \le r \le 9$.*

Proof. The bytes of K_r are independent and uniformly random. Let (p, q, s, t), $(p', q', s', t') \in \{(0, 7, 10, 13), (1, 4, 11, 14), (2, 5, 8, 15), (3, 6, 9, 12)\}$ are any two inverse diagonals. Since $K'_r = MC^{-1}(K_r)$, $K'_{r,\{p,p',q,q',s,s',t,t'\}}$ can be represented by the bytes of K_r as follows.

$$\begin{aligned}
K'_{r,p} &= a_0K_{r,0} + a_1K_{r,1} + a_2K_{r,2} + a_3K_{r,3},\\
K'_{r,p'} &= a'_0K_{r,0} + a'_1K_{r,1} + a'_2K_{r,2} + a'_3K_{r,3},\\
K'_{r,q} &= a_4K_{r,4} + a_5K_{r,5} + a_6K_{r,6} + a_7K_{r,7},\\
K'_{r,q'} &= a'_4K_{r,4} + a'_5K_{r,5} + a'_6K_{r,6} + a'_7K_{r,7},\\
K'_{r,s} &= a_8K_{r,8} + a_9K_{r,9} + a_{10}K_{r,10} + a_{11}K_{r,11},\\
K'_{r,s'} &= a'_8K_{r,8} + a'_9K_{r,9} + a'_{10}K_{r,10} + a'_{11}K_{r,11},\\
K'_{r,t} &= a_{12}K_{r,12} + a_{13}K_{r,13} + a_{14}K_{r,14} + a_{15}K_{r,15},\\
K'_{r,t'} &= a'_{12}K_{r,12} + a'_{13}K_{r,13} + a'_{14}K_{r,14} + a'_{15}K_{r,15}.
\end{aligned} \tag{6}$$

where $a_j, a'_j \in \{0B, 0D, 0E, 09\}$ are constants dependent respectively on (p, q, s, t) and (p', q', s', t'), $0 \le j \le 15$. Note that four diagonals of K_{r+1} are represented by the bytes of K_r in (2),(3),(4) and (5). We combine (6) with (2),(3),(4) and (5) respectively, and $K_{r,\{4,5,12,13\}}$ can be taken as free variables in the four combined systems of equations. When the free variables are determined the other twelve bytes of K_r have unique solution. Thus, for any given values of $K'_{r,\{p,p',q,q',s,s',t,t'\}}$ and any diagonal of K_{r+1}, the number of solutions of K_r is 2^{32}. Since the twelve bytes can take arbitrary values, they are independent. Furthermore, for any given values of the twelve bytes there are 2^{32} master keys under the key schedule of AES-128. □

Theorem 2. *For any input truncated difference $\overline{\Delta X}$ with two diagonals nonzero and any output truncated difference $\overline{\Delta W}$ with one inverse diagonal nonzero, there are at least 2^{34} master keys such that $\overline{\Delta X} \to \overline{\Delta W}$ is possible for 5-round AES-128.*

Proof. It is sufficient to prove that for any input truncated difference $\overline{\Delta X'}$ with two columns nonzero and any output truncated difference $\overline{\Delta W'}$ with one column nonzero, there are at least 2^{34} master keys such that

$$DP(\overline{\Delta X'} \xrightarrow{G} \overline{\Delta W'}) > 0.$$

Let the i_1-th and i_2-th columns of $\overline{\Delta X'}$ and the j-th column of $\overline{\Delta W'}$ be nonzero, $i_1 \ne i_2$, $0 \le i_1, i_2, j \le 3$. We need to find a differential $\Delta X' \to \Delta W'$ such that $\chi(\Delta X') = \overline{\Delta X'}$, $\chi(\Delta W') = \overline{\Delta W'}$, and

$$DP(\Delta X' \xrightarrow{G} \Delta W') > 0.$$

The propagation of the differential is shown in Fig. 3. Similar to the proof of Theorem 1, there exist ΔZ with only four bytes in the j-th column nonzero and $\Delta W'$ with $\chi(\Delta W') = \overline{\Delta W'}$ such that $f(Z) + f(Z + \Delta Z) = \Delta W'$, where

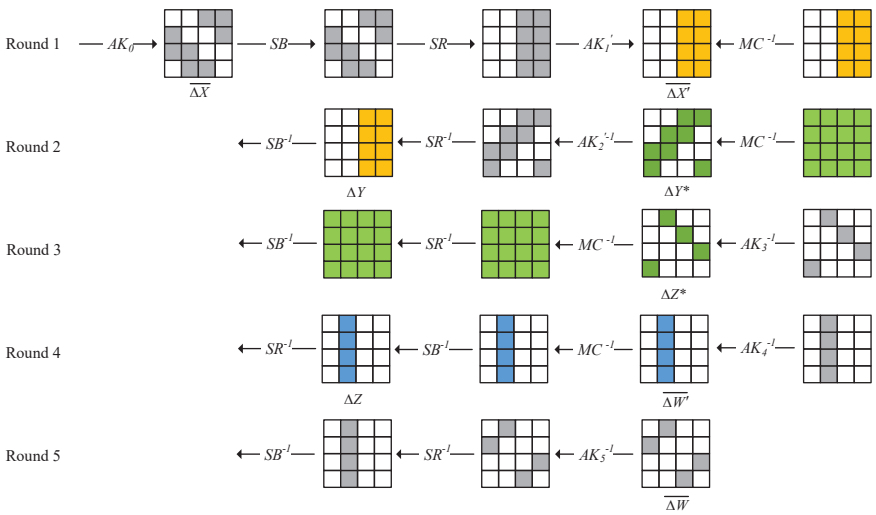

Fig. 3. The propagation of the differential in Set 2

$Z \in \mathbb{F}_{2^8}^{4\times 4}$ and the bytes except the j-th column of Z can take arbitrary values. Let $\Delta Z^* = SR^{-1}(\Delta Z)$, and then $SR^{-1} \circ MC^{-1}(\Delta Z^*) \in (\mathbb{F}_{2^8}^*)^{4\times 4}$. From Lemma 2, there exists ΔY^* with only eight bytes in the i_1-th and i_2-th inverse diagonals nonzero such that $g(Y^*) + g(Y^* + \Delta Y^*) = \Delta Z^*$ for some $Y^* \in \mathbb{F}_{2^8}^{4\times 4}$. Let $\Delta Y = SR^{-1}(\Delta Y^*)$. By Lemma 2 again, there exists input difference $\Delta X'$ such that $\chi(\Delta X') = \overline{\Delta X'}$ and $g(X') + g(X' + \Delta X') = \Delta Y$, where $X' \in \mathbb{F}_{2^8}^{4\times 4}$ and the bytes except the i_1-th and i_2-th columns of X' can take arbitrary values. Denote $Y = h(X')$, the bytes except the i_1-th and i_2-th columns of Y can take arbitrary values.

Taking $K_2' = SR(Y) + Y^*$ or $K_2' = SR(Y) + Y^* + \Delta Y^*$, then the output states of $SR \circ h$ and the input states of g are connected. The bytes except the i_1-th and i_2-th inverse diagonals of K_2' can take arbitrary values. Denote $Z^* = g(Y^*)$. Taking $K_3 = Z^* + SR^{-1}(Z)$ or $K_3 = Z^* + SR^{-1}(Z) + \Delta Z^*$, then the output states of g and the input states of $f \circ SR$ are connected. The bytes except the j-th diagonal of K_3 can take arbitrary values. From Lemma 4, for any given values of the i_1-th and i_2-th inverse diagonals of K_2' and the j-th diagonal of K_3, there are 2^{32} master keys under the key schedule of AES-128. Thus there are at least 2^{34} master keys such that $\overline{\Delta X'} \to \overline{\Delta W'}$ is possible for G. □

Lemma 5. *Suppose the master keys of AES-128 are independent and uniformly random. Then any inverse diagonal of K_r' and any two diagonals of K_{r+1} are independent, and for any given values of the twelve bytes there are 2^{32} master keys under the key schedule of AES-128, $0 \le r \le 9$.*

Proof. By the assumption, the 16 bytes of K_r are independent and uniformly random. Let $(p, q, s, t) \in \{(0, 7, 10, 13), (1, 4, 11, 14), (2, 5, 8, 15), (3, 6, 9, 12)\}$ be any inverse diagonal. Then $K'_{r,\{p,q,s,t\}}$ can be represented by the bytes of K_r in (1). Note that four diagonals of K_{r+1} are represented by the bytes of K_r in (2), (3), (4) and (5) respectively. We combine (1) with any two of (2), (3), (4) and (5) to form 6 systems of equations. For each system, there are four bytes of K_r that can be taken as free variables. That is, $K_{r,\{5,6,12,13\}}$ are free variables in the system of (1), (2) and (3). $K_{r,\{7,13,14,15\}}$ are free variables in the system of (1), (2) and (4). $K_{r,\{2,7,12,13\}}$ are free variables in the system of (1), (2) and (5). $K_{r,\{1,5,12,14\}}$ are free variables in the system of (1), (3) and (4). $K_{r,\{0,12,13,14\}}$ are free variables in the system of (1), (3) and (5). $K_{r,\{0,4,13,14\}}$ are free variables in the system of (1), (4) and (5). When the free variables are determined the other bytes of K_r have unique solution in each combined system of equations. Since $K'_{r,\{p,q,s,t\}}$ and any two diagonals of K_{r+1} can take arbitrary values, they are independent. Furthermore, for their any given values there are 2^{32} master keys under the key schedule of AES-128. □

Theorem 3. *For any input truncated difference $\overline{\Delta X}$ with one diagonal nonzero and any output truncated difference $\overline{\Delta W}$ with two inverse diagonals nonzero, there are at least 2^{34} master keys such that $\overline{\Delta X} \to \overline{\Delta W}$ is possible for 5-round AES-128.*

Proof. It is sufficient to prove that for any input truncated difference $\overline{\Delta X'}$ with one column nonzero and any output truncated difference $\overline{\Delta W'}$ with two columns nonzero, there are at least 2^{34} master keys such that

$$DP(\overline{\Delta X'} \xrightarrow{G} \overline{\Delta W'}) > 0.$$

Let the i-th column of $\overline{\Delta X'}$ and the j_1-th and j_2-th columns of $\overline{\Delta W'}$ be nonzero, $j_1 \neq j_2$, $0 \leq i, j_1, j_2 \leq 3$. We just need to find a differential $\Delta X' \to \Delta W'$ such that $\chi(\Delta X') = \overline{\Delta X'}$, $\chi(\Delta W') = \overline{\Delta W'}$, and

$$DP(\Delta X' \xrightarrow{G} \Delta W') > 0.$$

The propagation of the differential is shown in Fig. 4. From Lemma 1, there exists $\Delta W'$ such that $\chi(\Delta W') = \overline{\Delta W'}$ and the eight bytes in the j_1-th and j_2-th columns of $MC^{-1}(\Delta W')$ are nonzero. Let $f(Z) + f(Z + \Delta Z) = \Delta W'$, where $Z \in \mathbb{F}_{2^8}^{4\times 4}$ and the bytes except the j_1-th and j_2-th columns of Z can take arbitrary values. By the differential distribution of S-box, each byte in the j_1-th and j_2-th columns of ΔZ has 127 possible values. Denote $\Delta Z^* = SR^{-1}(\Delta Z)$, then each column of ΔZ^* has two nonzero bytes and each nonzero byte has 127 possible values. That is, the number of ΔZ^* is 127^8. But the number of ΔZ^* such that $MC^{-1}(\Delta Z^*) \notin (\mathbb{F}_{2^8}^*)^{4\times 4}$ is at most $(127 \cdot 4)^4$. So there exists ΔZ^* such that $MC^{-1}(\Delta Z^*) \in (\mathbb{F}_{2^8}^*)^{4\times 4}$, and then $SR^{-1} \circ MC^{-1}(\Delta Z^*) \in (\mathbb{F}_{2^8}^*)^{4\times 4}$. From Lemma 2, there exists input difference ΔY^* with only four bytes in the i-th inverse diagonal nonzero such that $g(Y^*) + g(Y^* + \Delta Y^*) = \Delta Z^*$ for some $Y^* \in \mathbb{F}_{2^8}^{4\times 4}$. Let $\Delta Y = SR^{-1}(\Delta Y^*)$. From Lemma 2 again, there exists input

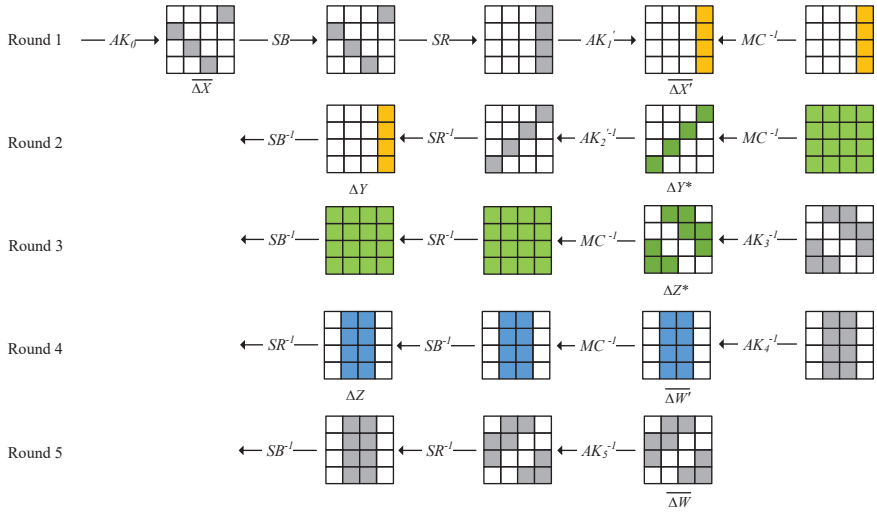

Fig. 4. The propagation of the differential in Set 3

difference $\Delta X'$ such that $\chi(\Delta X') = \overline{\Delta X'}$ and $h(X') + h(X' + \Delta X') = \Delta Y$, where $X' \in \mathbb{F}_{2^8}^{4\times 4}$ and the bytes except the i-th column of X' can take arbitrary values. Denote $Y = h(X')$, then the bytes except the i-th column of Y can take arbitrary values.

Taking $K_2' = SR(Y) + Y^*$ or $K_2' = SR(Y) + Y^* + \Delta Y^*$, the output states of $SR \circ h$ and the input states of g are connected. Denote $Z^* = g(Y^*)$. Taking $K_3 = Z^* + SR^{-1}(Z)$ or $K_3 = Z^* + SR^{-1}(Z) + \Delta Z^*$, then the output states of g and the input states of $f \circ SR$ are connected. The bytes except the i-th inverse diagonal of K_2' as well as the bytes except the j_1-th and j_2-th diagonals of K_3 can take arbitrary values. From Lemma 5, for any given values of the i-th inverse diagonal of K_2' and the j_1-th and j_2-th diagonals of K_3, there are 2^{32} master keys under the key schedule of AES-128. Thus there are at least 2^{34} master keys such that $\overline{\Delta X'} \to \overline{\Delta W'}$ is possible for G. □

From the view of provable security, we can get the following theorem. The result also holds for AES-192 and AES-256 because their master keys have larger degrees of freedom.

Theorem 4. *There do not exist truncated impossible differentials in Set* 1*, Set* 2 *and Set* 3 *for* 5*-round AES even considering the key schedule. That is, for any truncated differential* $\overline{\Delta X} \to \overline{\Delta W}$ *in Set* 1*, Set* 2 *or Set* 3*, we have*

$$EDP(\overline{\Delta X} \xrightarrow{5-round\ AES} \overline{\Delta W}) > 0.$$

4 Conclusion

In this paper, we prove theoretically that there do not exist three kinds of truncated impossible differentials for 5-round AES in the master-key setting. Furthermore, for any given truncated differentials of the three kinds, the lower bounds of the number of master keys such that the truncated differentials are possible for 5-round AES-128 are given. The lower bounds could be improved by more detailed analysis. These results improve the provable security evaluation of the real AES. It seems difficult to study the differentials in the master-key setting, because the dependence of round keys affects the propagation of states. Thanks to the simple algebraic relation of consecutive two-round keys in the key schedule, we prove the independence between the key bytes involved for the three kinds of truncated differentials. And for any given values of the key bytes involved, the number of master keys under the key schedule of AES-128 are also presented by analysing the number of solutions of the corresponding systems of algebraic equations. In the master-key setting, the nonexistence of r-round impossible differentials can not lead to the nonexistence of $(r+1)$-round impossible differentials. There are still many problems that need to be studied in the future. For example, it is not clear that whether other kinds of truncated differentials are impossible for 5-round AES in the master-key setting. When the concrete differentials are considered, whether they are impossible for round-reduced AES in the master-key setting.

Acknowledgements. The authors are grateful to the anonymous reviewers for their helpful comments and suggestions. This work was supported by the National Cryptography Development Fund of China under grant numbers MMJJ20170103 and MMJJ20180204.

References

1. Bahrak, B., Aref, M.R.: Impossible differential attack on seven-round AES-128. IET Inf. Secur. **2**(2), 28-32 (2008).
2. Bar-On, A., Dunkelman, O., Keller, N., Ronen, E., Shamir, A.: Improved key recovery attacks on reduced-round AES with practical data and memory complexities. J. Cryptol. **33**(3), 1003-1043 (2020).
3. Bardeh, N.G., Rønjom, S.: The exchange attack: How to distinguish six rounds of AES with $2^{88.2}$ chosen plaintexts. In: ASIACRYPT 2019. Lecture Notes in Computer Science, vol. 11923, pp. 347-370. Springer (2019).
4. 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 (1999).
5. Biham, E., Keller, N.: Cryptanalysis of reduced variants of Rijndael. In: The 3rd AES Conference (2000).
6. Boura, C., Lallemand, V., Naya-Plasencia, M., Suder, V.: Making the impossible possible. J. Cryptol. **31**(1), 101-133 (2018).

7. Boura, C., Naya-Plasencia, M., Suder, V.: Scrutinizing and improving impossible differential attacks: Applications to CLEFIA, Camellia, LBlock and SIMON. In: ASIACRYPT 2014. Lecture Notes in Computer Science, vol. 8873, pp. 179-199. Springer (2014).
8. Chen, J., Wang, M., Preneel, B.: Impossible differential cryptanalysis of the lightweight block ciphers TEA, XTEA and HIGHT. In: AFRICACRYPT 2012. Lecture Notes in Computer Science, vol. 7374, pp. 117-137. Springer (2012).
9. Cheon, J.H., Kim, M., Kim, K., Jung-Yeun, L., Kang, S.: Improved impossible differential cryptanalysis of Rijndael and Crypton. In: ICISC 2001. Lecture Notes in Computer Science, vol. 2288, pp. 39-49. Springer (2002).
10. Derbez, P., Fouque, P., Jean, J.: Improved key recovery attacks on reduced-round AES in the single-key setting. In: EUROCRYPT 2013. Lecture Notes in Computer Science, vol. 7881, pp. 371-387. Springer (2013).
11. Dunkelman, O., Keller, N., Ronen, E., Shamir, A.: The retracing boomerang attack. In: EUROCRYPT 2020. Lecture Notes in Computer Science, vol 12105, pp. 280-309. Springer (2020).
12. 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 (2001).
13. Gaëtan, L., Clara, P.: New representations of the AES key schedule. In: EUROCRYPT 2021, accepted.
14. Grassi, L.: Mixture differential cryptanalysis: New approaches for distinguishers and attacks on round-reduced AES. IACR Trans. Symmetric Cryptol. **2018**(2), 133-160 (2018).
15. Grassi, L., Rechberger, C., Rønjom, S.: Subspace trail cryptanalysis and its applications to AES. IACR Trans. Symmetric Cryptol. **2016**(2), 192-225 (2016).
16. Grassi, L., Rechberger, C., Rønjom, S.: A new structural-differential property of 5-round AES. In: EUROCRYPT 2017. Lecture Notes in Computer Science, vol. 10211, pp. 289-317. Springer (2017).
17. Hu, K., Cui, T., Gao, C., Wang, M.: Towards key-dependent integral and impossible differential distinguishers on 5-round AES. In: SAC 2018. Lecture Notes in Computer Science, vol. 11349, pp. 139-162. Springer (2019).
18. Hu, X., Li, Y., Jiao, L., Tian, S., Wang, M.: Mind the propagation of states: New automatic search tool for impossible differentials and impossible polytopic transitions. In: ASIACRYPT 2020. Lecture Notes in Computer Science, vol. 12491, pp. 415-445. Springer (2020).
19. Kanda, M., Matsumoto, T.: Security of Camellia against truncated differential cryptanalysis. In: FSE 2001. Lecture Notes in Computer Science, vol. 2355, pp. 286-299. Springer (2002).
20. Knudsen, L.R.: DEAL - a 128-bit cipher. Technical Report, Department of Informatics, University of Bergen, Norway (1998).
21. Mala, H., Dakhilalian, M., Rijmen, V., Modarres-Hashemi, M.: Improved impossible differential cryptanalysis of 7-round AES-128. In: INDOCRYPT 2010. Lecture Notes in Computer Science, vol. 6498, pp. 282-291. Springer (2010).
22. Rønjom, S., Bardeh, N.G., Helleseth, T.: Yoyo tricks with AES. In: ASIACRYPT 2017. Lecture Notes in Computer Science, vol. 10624, pp. 217-243. Springer (2017).
23. Sun, B., Liu, M., Guo, J., Qu, L., Rijmen, V.: New insights on AES-like SPN ciphers. In: CRYPTO 2016. Lecture Notes in Computer Science, vol. 9814, pp. 605-624. Springer (2016).

24. Sun, B., Liu, M., Guo, J., Rijmen, V., Li, R.: Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis. In: EUROCRYPT 2016. Lecture Notes in Computer Science, vol. 9665, pp. 196-213. Springer (2016).
25. Tsunoo, Y., Tsujihara, E., Shigeri, M., Saito, T., Suzaki, T., Kubo, H.: Impossible differential cryptanalysis of CLEFIA. In: FSE 2008. Lecture Notes in Computer Science, vol. 5086, pp. 398-411. Springer (2008).
26. Wang, Q., Jin, C.: Upper bound of the length of truncated impossible differentials for AES. Des. Codes Cryptogr. **86**(7), 1541-1552 (2018).
27. Wang, Q., Jin, C.: More accurate results on the provable security of AES against impossible differential cryptanalysis. Des. Codes Cryptogr. **87**(12), 3001-3018 (2019).
28. 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 (2007).