Noname manuscript No.
(will be inserted by the editor)

Structure Evaluation of AES-like Ciphers against Mixture Differential Cryptanalysis

Xiaofeng Xie · Tian Tian

Received: date / Accepted: date

Abstract In ASIACRYPT 2017, Rønjom et al. analyzed AES with yoyo attack. Inspired by their 4-round AES distinguisher, Grassi proposed the mixture differential cryptanalysis as well as a key recovery attack on 5-round AES, which was shown to be better than the classical square attack in computation complexity. After that, Bardeh et al. combined the exchange attack with the 4-round mixture differential distinguisher of AES, leading to the first secret-key chosen plaintext distinguisher for 6-round AES. Unlike the attack on 5-round AES, the result of 6-round key-recovery attack on AES has extremely large complexity, which implies the weakness of mixture difference to a certain extent. Our work aims at evaluating the security of AES-like ciphers against mixture differential cryptanalysis. We propose a new structure called a boomerang struncture and illustrate that a differential distinguisher of a boomerang struncture just corresponds to a mixture differential distinguisher for AES-like ciphers. Based on the boomerang structure, it is shown that the mixture differential cryptanalysis is not suitable to be applied to AES-like ciphers with high round number. In specific, we associate the primitive index with our framework built on the boomerang structure and give the upper bound for the length of mixture differentials with probability 1 on AES-like ciphers. It can be directly deduced from our framework that there is no mixture differential distinguisher for 6-round AES.

Keywords Mixture differential attacks · Boomerange attacks · AES-like ciphers

1 Introduction

Block ciphers are typical iterative ciphers, which are built by iterating a simple round function many times to ensure that they behave like random permutations.

X.-F. Xie · T. Tian
PLA Strategic Support Force Information Engineering University, Zhengzhou 450001, China.
Tian Tian
E-mail: tiantian_d@126.com

Xiaofeng Xie
E-mail: xiaofengxie514@126.com

The characteristic that is different from a random permutation can always be utilized as a secret-key distinguisher or be applied in key recovery. Differential cryptanalysis and linear cryptanalysis are among the best known cryptanalysis of block ciphers. The designers of block ciphers always take the security against these cryptanalysis into consideration. The Advanced Encryption Standard (AES) [1] is the best known and most widely used block cipher which has been proved to be secure against differential cryptanalysis by "wide trail". Since the proposal of AES, evaluating its security is one of the most important problems in cryptanalysis.

Yoyo game cryptanalysis was introduced by Biham et.al for cryptanalysis of SKIPJACK [2]. In ASIACRYPT 2017, the authors of [3] presented a deterministic 4-round property based on Yoyo game cryptanalysis, see Theorem 1 in Section 2.2. With this property, they achieved a key recovery attack on 5-round AES with data complexity $2^{11.3}$ and computational complexity 2^{31}. At EUROCRYPT 2017, Grassi presented a new property of AES called "multiple-of-8" [4], leading to the first secret-key distinguisher for 5-round AES. Although the work of [3] and [4] analyzed AES in terms of key recovery attack and secret-key distinguisher respectively, the core ideas of them are very similar. After that, the 4-round yoyo property has gained much attention in the literature. The authors of [5] explored the 4-round yoyo property of AES and re-described it with the notation of subspace trails. A new key-recovery attack on 5-round AES with $2^{33.6}$ chosen plaintexts and $2^{33.28}$ computational cost was set up in [5]. As presented in [6], the pairs of texts used in [5] were constructed directly from the chosen plaintexts when attacking 5-round AES, which was different from the yoyo attack. Thus the authors renamed this method as "mixture differential cryptanalysis". Later the 4-round mixture differential distinguisher of AES is widely used in the cryptanalysis. With this distinguisher, the authors of [6] broke the record for 5-round AES attacks which was held by the classical Square attack, and the authors of [7] presented a 6-round secret-key distinguisher with 2^{88} complexity. Actually, the 6-round distinguisher in [7] utilized a 5-round mixture differential distinguisher. In EUROCRYPT 2020 [8], Dunkelman et al. illustrated the relation between the mixture differential and the boomerang attack. They also proposed a new variant of boomerang attack called retracing boomerang attack, which covered the yoyo attack and the mixture differential cryptanalysis [8].

In this paper, we aim at evaluating the security of AES-like ciphers against mixture differential cryptanalysis. We convert the construction of mixture differential distinguishers into the problem of searching differential distinguishers for a new structure called "boomerang structure". The differential distinguishers utilized in the boomerang structure could be differential distinguishers, truncated differential distinguishers, and impossible differential distinguishers. We also show the reason why high order differential cryptanalysis could not combine with the mixture differential. With the boomerang structure, we could reasonably compare the effect of mixture differential distinguishers with differential cryptanalysis, truncated differential cryptanalysis, and impossible differential cryptanalysis against an AES-like cipher for the same number of rounds. It is shown that the mixture differential attack is not suitable for cryptanalysis against AES-like ciphers with high round number, since the mixture differential distinguisher is always weaker than truncated differential distinguisher. We illustrate this statement by proving that for an AES-like cipher with the branch number more than 3, when the round number of mixture differential is more than 10, there always exists a truncated differential covering the same round number with a higher probability.

In Section 2, we introduce some concepts used in the following paper, including but not limited to the SPN and AES-like ciphers, mixture differential distinguishers, and some notations. Section 3 investigate the precondition of mixture differential distinguishers and reviews the previous distinguishers in our new insights. Section 4 evaluates the security of AES-like ciphers against mixture differential. Section 5 concludes this paper.

Throughout the paper we use the following notations. Let $\mathbb{Z}$ denote the set of integers and $\mathbb{F}_2$ denote the finite field of two elements. For positive integers m_1, m_2, n, the set of all $m_1 \times m_2$ matrices over $\mathbb{Z}$ is denoted by $\mathbb{Z}^{m_1 \times m_2}$, and the n-dimensional vector space over $\mathbb{F}_2$ is denoted by $\mathbb{F}_2^n$.

2 Preliminaries

In this section, we briefly introduce SPN ciphers, some basics of mixture differentials and impossible differentials against SPN ciphers.

2.1 SPN and AES-like ciphers

For an SPN block cipher, its intermediate state can typically be loaded into an n-dimensional vector $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{F}_2^{n \times b}$, where $\alpha_i \in \mathbb{F}_2^b$ for $0 \le i < n$. The round function of an SPN cipher is composed of Sub-Bytes layer(SB), Linear layer(L) and AddKey(AK). The Sub-Bytes layer is formed by concatenating n parallel S-boxes s over $\mathbb{F}_2^b$, and the Linear layer is a linear function over $\mathbb{F}_2^{n \times b}$. The AddKey operation xor the $(n \times b)$-bit round-key with the intermediate state α. Overall, the round function of an SPN cipher can be described as $R = AK \circ L \circ SB$.

AES-like ciphers are SPN ciphers. In particular, the n-dimensional intermediate state α of an AES-like cipher is treated as an $m_1 \times m_2$ matrix over $\mathbb{F}_2^b$ where $m_1 \times m_2 = n$. Thus, for the sake of discussion, the set of AES-like ciphers with the above framework is denoted by $\varepsilon(m_1, m_2, b)$. The linear layer of an AES-like cipher consists of a position permutation of cells (SC) and a MixColumn transformation (MC), i.e., $L = MC \circ SC$. For the intermediate state $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$, the position permutation SC permutes the cells of the state as follows:

$$(\alpha_0, \alpha_1, \ldots, \alpha_n) \leftarrow (\alpha_{l_0}, \alpha_{l_1}, \ldots, \alpha_{l_{n-1}}).$$

In the following paper, we define the index set $SC(I) = \{l_i | i \in I\}$, where $I \subset \{0, 1, \ldots, n-1\}$, and the index set $Col(J) = \{i | \alpha_i \text{ belong to the } j\text{-th column}, j \in J\}$. The MixColumn transformation MC mixes each column by a matrix M. Thus, the round function of an AES-like cipher can be written as

$$R = AK \circ MC \circ SC \circ SB.$$

Since the key addition does not influence the value of a difference, we omit AK when discussing differentials. For an AES-like cipher with round function R, we denote E_n as r-round encryption without the last MC in the following paper, i.e., $E_n = SC \circ SB \circ R^{n-1} = MC^{-1} \circ R^n$.

2.2 Yoyo distinguishers and mixture differentials

Before introducing the yoyo distinguisher of AES, we give the definitions of exchange words operation and difference pattern as follows.

Definition 1 (Exchange words) Let $\alpha, \beta \in \mathbb{F}_2^{n\times b}$, where $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}), \beta = (\beta_0, \beta_1, \ldots, \beta_{n-1})$, and $I \subseteq \{0, 1, \ldots, n-1\}$. The exchange words function $\rho^I(\alpha, \beta)$ is defined as follow:

$$\rho^I(\alpha,\beta)_i = \begin{cases} \beta_i,\ i \in I, \\ \alpha_i,\ otherwise. \end{cases}$$

For an index set $I \subseteq \{0, 1, \ldots, n-1\}$ we define (α', β) as an exchange pair of (α, β) on index I, where $\alpha' = \rho^I(\alpha, \beta),\ \beta' = \rho^I(\beta, \alpha)$.

Definition 2 (Difference pattern [3]) Let $\alpha, \beta \in \mathbb{F}_2^{n\times b}$, where $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}), \beta = (\beta_0, \beta_1, \ldots, \beta_{n-1})$. The difference pattern $v(\alpha \oplus \beta) \in \mathbb{F}_2^n$ is defined as follow:

$$v(\alpha \oplus \beta)_i = \begin{cases} 1,\ \alpha_i \oplus \beta_i \neq 0, \\ 0,\ \alpha_i \oplus \beta_i = 0. \end{cases}$$

The main idea of yoyo attacks is to divide the plaintext pairs into different subsets according to the definition of exchange word operation, and the ciphertext pairs in each subset has the same difference pattern after rounds of encryption. It is obvious that for the difference of state pair (α, β) and their exchange pair (α', β'), the equality $\alpha' \oplus \beta' = \beta \oplus \alpha$ always holds. The generic yoyo distinguishers of SPN ciphers have been illustrated in [3] where authors discussed the relation of original pairs and their exchange pairs after encryption of Sub-Bytes layer and Linear layer. As a result, they gave the following lemma.

Lemma 1 *[3] Let $\alpha, \beta \in \mathbb{F}_2^{n\times b}$ be a plaintext pair of an SPN cipher and S be a permutation over $\mathbb{F}_2^b$. Then*

$$L \circ S(\alpha) \oplus L \circ S(\beta) = L \circ S(\rho^I(\alpha, \beta)) \oplus L \circ S(\rho^I(\beta, \alpha))$$

holds for every $I \subseteq \{0, 1, \ldots, n-1\}$.

According to the above lemma, they gave the following theorem, which describes a generic distinguisher for the 2-round SPN structure.

Theorem 1 *[3] Let $\alpha, \beta \in \mathbb{F}_2^{n\times b}$ and S be a permutation over $\mathbb{F}_2^b$. Then*

$$v(S \circ L \circ S(\alpha) \oplus S \circ L \circ S(\beta)) = v(S \circ L \circ S(\rho^I(\alpha, \beta)) \oplus S \circ L \circ S(\rho^I(\beta, \alpha)))$$

holds for every $I \subseteq \{0, 1, \ldots, n-1\}$.

As shown in [3], the 2-round AES can be written as

$$R^2 = (MC \circ SR) \circ (SB \circ MC \circ SR \circ SB).$$

The first part of the function $(SB \circ MC \circ SR \circ SB)$ can be divided into four independent Super S-boxes, and the second part $(MC \circ SR)$ is a linear function. Let $\alpha, \beta \in \mathbb{F}_2^{16\times 8}$. Then for $J \subset \{0, 1, 2, 3\}$ we have

$$R^2(\alpha) \oplus R^2(\beta) = R^2(\rho^I(\alpha, \beta)) \oplus R^2(\rho^I(\beta, \alpha)),$$

where $I = SR(Col(J))$. As a result, the 4-round AES encryption that omit the first and the last SR, say

$$R^4 = SB \circ MC \circ SR \circ SB \circ MC \circ SR \circ SB \circ MC \circ SB,$$

has the following yoyo property

$$\upsilon(R^4(\alpha) \oplus R^4(\beta)) = \upsilon(R^4(\rho^I(\alpha, \beta)) \oplus R^4(\rho^I(\beta, \alpha))), \tag{1}$$

where $I = Col(J),\ J \subset \{0, 1, 2, 3\}$.

Inspired by the 4-round yoyo property, authors in [5] proposed the mixture differential. The mixture differential cryptanalysis only exchanges the pairs in one side(output pairs or input pairs), which is different from yoyo attacks.

2.3 Truncated differentials

For a function F: $\mathbb{F}_2^n \to \mathbb{F}_2^n$, the differential probability for an input difference δ and an output difference $\varDelta$ is defined as

$$\Pr[\delta \xrightarrow{F} \triangle] = \frac{|\{x \in \mathbb{F}_2^n | F(x) \oplus F(x \oplus \delta) = \triangle\}|}{2^n}.$$

If $\Pr[\delta \xrightarrow{F} \triangle] = 0$, then the differential trail $\delta \to \triangle$ is called an impossible differential of F [9]. For the case that $A \subset \mathbb{F}_2^n$ and $B \subset \mathbb{F}_2^n$, we say

$$A \xrightarrow{F} B = \{\delta \to \triangle \ |\text{there exists } x \in \mathbb{F}_2^n, F(x \oplus \delta) \oplus F(x) = \triangle, \delta \in A, \triangle \in B\}$$

is a truncated differential trail of F. Define

$$\Pr[A \xrightarrow{F} B] = \Pr[F(x) \oplus F(x \oplus \delta) \in B | \delta \in A]$$

as the probability of $A \xrightarrow{F} B$. If $\Pr[A \xrightarrow{F} B] = 0$, then we also say that $A \xrightarrow{F} B$ is an impossible differential for F.

In EUROCRYPT 2016, Sun et al. associated the primitive index with the characteristic matrix to bound the length of impossible differentials [10]. The definitions of the primitive index and the characteristic matrix of a linear layer P is as follows.

Definition 3 (Characteristic matrix [10]) For $P = (p_{ij}) \in \mathbb{F}_{2^b}^{m_1 \times m_2}$, the characteristic matrix of P is defined as $P^* = (p^*_{ij}) \in \mathbb{Z}^{m_1 \times m_2}$, where $p^*_{ij} = 0$ if $p_{ij} = 0$ and $p^*_{ij} = 1$ otherwise.

It is obvious that, if the element with position (i, j) in the characteristic matrix is positive, then the value of i-th output byte is relate to the j-th input byte. Thus, if all elements of a characteristic matrix P^* is positive, then the encryption with linear layer P is a full diffusion. As a result, to indicate an encryption is a full diffusion, Sun et. defined the matrices whose elements are all positive as positive matrix [10].

Definition 4 (Primitive index [10]) Let $P \in \mathbb{F}_{2^b}^{m\times m}$ and P^* be the characteristic matrix of P. Set

$$f_t(x) = x^t$$

$$g_t(x) = \begin{cases} \sum\limits_{t=0}^{h} x^{2i} & t = 2h \\ \sum\limits_{t=0}^{h} x^{2i-1} & t = 2h-1. \end{cases}$$

Then the minimal integer t that makes $f_t(P^*)$ a positive matrix is called Type 1 primitive index of P, and the minimal integer t such that $g_t(P^*)$ is positive is called Type 2 primitive index of P.

Remark 1 In the following paper, we denote Type 1 primitive index of P by $L_1(P)$.

3 New insights into mixture differential cryptanalysis

In [5], the authors emphasized the similarity between the truncated differentials and their 5-round AES distinguisher. In this section, we attempt to indicate the further relationship between mixture differentials and truncated differentials, and convert the mixture differential distinguishers into differential distinguishers or impossible differential distinguishers. As the first thing, we discuss the basic of mixture differential cryptanalysis.

3.1 The basic of mixture differential cryptanalysis

For a function $F : \mathbb{F}_{2^q}^n \to \mathbb{F}_{2^q}^n$ and an index set $I = \{i_0, i_1, \ldots, i_m\}$, denote the component functions about the index set I by $F_I = (F_{i_0}, F_{i_1}, \ldots, F_{i_m})$ where $i_j \in I$ and $i_j < i_{j+1}$, $0 \le j < m$. Similarly, denote the input vector about the index set I as $x_I = (x_{i_0}, x_{i_1}, \ldots, x_{i_m})$ where $i_j \in I$ and $i_j < i_{j+1}$, $0 \le j < m$. Denote $Var(F_i)$ as the set of all variables appearing in F_i and $Var(F_I)$ as the set of all variables appearing in F_I. We are concerned with whether an r-round encryption could be divided into several independent small permutations. We provide a necessary and sufficient condition for this.

Definition 5 For a permutation $F : \mathbb{F}_{2^q}^n \to \mathbb{F}_{2^q}^n$, define the relation $\mathcal{R}_F$ on the set of input words $\{x_0, x_1, \ldots, x_{n-1}\}$ such that $(x_i, x_j) \in \mathcal{R}_F$ if and only if there exist Boolean functions $F_{t_0}, F_{t_1}, \ldots, F_{t_m}$ satisfying two conditions:

(1) $x_i \in Var(F_{t_0}), x_j \in Var(F_{t_m})$;
(2) $Var(F_{t_k}) \cap Var(F_{t_{k+1}}) \neq \varnothing$ for $0 \le k < m$ if $m > 0$.

For a permutation $F : \mathbb{F}_{2^q}^n \to \mathbb{F}_{2^q}^n$, $\mathcal{R}_F$ is an equivalence relation on the set $\{x_0, x_1, \ldots, x_{n-1}\}$ since $\mathcal{R}_F$ is reflexive, symmetric and transitive. For convenience, we denote $\mathcal{R}_F$ by $\overset{F}{\sim}$. For $0 \le j \le n-1$, the equivalence class of x_j under $\overset{F}{\sim}$ is denoted by $\overline{x}_j$. Notice that if $Var(F_i) \cap \overline{x}_j \neq \varnothing$ with $0 \le i, j < n$, then $Var(F_i) \subset \overline{x}_j$, and so either $Var(F_i) \subset \overline{x}_j$ or $Var(F_i) \cap \overline{x}_j = \varnothing$. Furthermore, if $(x_i, x_j) \in \mathcal{R}_F$ and $F_{t_0}, F_{t_1}, \ldots, F_{t_m}$ satisfies (2), then $Var(F_{t_k}) \subset \overline{x}_i$ for all $0 \le k \le m$.

Example 1 For Midori64, the MixColumn matrix is given by

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

Let $x = (x_0, x_1, \ldots, x_{15}) \in \mathbb{F}_{2^4}^{16}$ and $F = MC(x)$. Then

$$Var(F_0) = \{x_1, x_2, x_3\} \text{ and } Var(F_1) = \{x_0, x_2, x_3\}.$$

Considering the relation $\mathcal{R}_F$, since $Var(F_0) = \{x_1, x_2, x_3\}$, we have $x_1 \overset{F}{\sim} x_2 \overset{F}{\sim} x_3$. Furthermore, since $Var(F_1) = \{x_0, x_2, x_3\}$, we have $x_0 \overset{F}{\sim} x_1 \overset{F}{\sim} x_2 \overset{F}{\sim} x_3$.

Theorem 2 *Let $F = (F_0, F_1, \ldots, F_{n-1})$ be a permutation on $\mathbb{F}_{2^q}^n$. Then F can be divided into m independent permutations if and only if there are at least m equivalence classes of the set $\{x_0, x_1, \ldots, x_{n-1}\}$ under the equivalence relation $\mathcal{R}_F$.*

Proof If F can be divided into m independent permutations given by $F_{J_0}, F_{J_1}, \ldots, F_{J_{m-1}}$, then $\{Var(F(J_i))|0 \leq i \leq m-1\}$ is a partition of $\{x_0, x_1, \ldots, x_{n-1}\}$. It follows that if $x_a \in Var(F_{J_i})$ for $0 \leq a \leq n-1$ and $0 \leq i \leq m-1$, then $\overline{x}_a \subset Var(F_{J_i})$. Thus there are at least m equivalent classes under $\mathcal{R}_F$.

Conversely, if $\overline{x}_{l_0}, \overline{x}_{l_1}, \ldots, \overline{x}_{l_{m'-1}}$ be all equivalence classes under $\mathcal{R}_F$ with $m' \geq m$. For $0 \leq i \leq m'-1$, let $J_i = \{j|Var(F_j) \subset \overline{x}_{l_i}\}$. Since $\overline{x}_{l_i} \cap \overline{x}_{l_j} = \emptyset$ for $0 \leq i \neq j \leq m'-1$, it follows that F can be divided into m independent functions given by

$$F_{J_0}, F_{J_1}, \ldots, F_{J_{m-2}}, F_{\cup_{m-1 \leq i \leq m'-1} J_i}.$$

Since F is a permutation, it follows that $F_{J_1}, F_{J_2}, \ldots, F_{J_{m-2}}, F_{\cup_{m-1 \leq i \leq m'-1} J_i}$ are all permutations.

Since the cancellation of an input variable rarely happens during the iteration of rounds in block ciphers, in the following paper we assume that an input variable will not be eliminated during the encryption of a block cipher. For example, if $F : \mathbb{F}_{2^q}^n \to \mathbb{F}_{2^q}^n$, $x_0 \in Var(F_0)$, $x_0 \in Var(F_1)$ and $G : \mathbb{F}_{2^q}^2 \to \mathbb{F}_{2^q}$, then $x_0 \in Var(G(F_0, F_1))$.

Lemma 2 *Let $F : \mathbb{F}_{2^q}^n \to \mathbb{F}_{2^q}^n$ and $G : \mathbb{F}_{2^q}^n \to \mathbb{F}_{2^q}^n$ be two permutations. If $(x_i, x_j) \in \mathcal{R}_F$, then $(x_i, x_j) \in \mathcal{R}_{G \circ F}$.*

Proof Since $(x_i, x_j) \in \mathcal{R}_F$, there exist $F_{t_0}, F_{t_1}, \ldots, F_{t_m}$ satisfying $x_i \in Var(F_{t_0})$, $x_j \in Var(F_{t_m})$, and $Var(F_{t_k}) \cap Var(F_{t_{k+1}}) \neq \varnothing$ for $0 \leq k < m$. Since G is invertible, for every x_{t_k}, there exists G_{l_k} satisfies $x_{t_k} \in Var(G_{l_k})$. Let $H = G \circ F$. It is clear that $Var(F_{t_k}) \subset Var(H_{l_k})$. Thus $(x_i, x_j) \in \mathcal{R}_{G \circ F}$.

Theorem 3 *Let $F : \mathbb{F}_{2^q}^n \to \mathbb{F}_{2^q}^n$ and $G : \mathbb{F}_{2^q}^n \to \mathbb{F}_{2^q}^n$ be two permutations and $(x_i, x_j) \in \mathcal{R}_G$. Then for every $(x_{l_1}, x_{l_0}) \in \mathcal{R}_F$ and $(x_{k_1}, x_{k_0}) \in \mathcal{R}_F$ with $x_{l_0} \in Var(F_i)$ and $x_{k_0} \in Var(F_j)$, we have $(x_{l_1}, x_{k_1}) \in \mathcal{R}_{G \circ F}$.*

Proof Since $(x_i, x_j) \in \mathcal{R}_G$, there exist $G_{t_0}, G_{t_1}, \ldots, G_{t_m}$ satisfying $x_i \in Var(G_{t_0})$, $x_j \in Var(G_{t_m})$, and $Var(G_{t_k}) \cap Var(G_{t_{k+1}}) \neq \varnothing$ for $0 \leq k < m$. Let $H = G \circ F$. Since $x_i \in Var(G_{t_0})$, it follows that $Var(F_i) \subset Var(H_{t_0})$. Thus $x_{l_0} \in Var(H_{t_0})$. Similarly, $x_{k_0} \in Var(H_{t_m})$. Because $Var(G_{t_k}) \cap Var(G_{t_{k+1}}) \neq \varnothing$, we have $Var(H_{t_k}) \cap Var(H_{t_{k+1}}) \neq \varnothing$. As a result, $(x_{l_0}, x_{k_0}) \in \mathcal{R}_{G \circ F}$. By Lemma 2, we have $(x_{l_1}, x_{k_1}) \in \mathcal{R}_{G \circ F}$.

For most of AES-like ciphers in $\boldsymbol{\varepsilon}(4,4,b)$, the following result is useful which immediately follows from Theorem 3.

Corollary 1 *Let $R = MC \circ SC \circ SB$ be the round function of an AES-like cipher which belongs to $\boldsymbol{\varepsilon}(4,4,b)$. If the linear layer satisfies the following two conditions:*

(1) the MixColumn matrix M could not be transformed into the following form

$$M = \begin{pmatrix} A & O \\ O & B \end{pmatrix}$$

where A is an $n_0 \times n_1$ matrix and B is an $n_2 \times n_3$ matrix with $n_0 + n_2 = n_1 + n_3 = 4$ by changing column positions and row positions,

(2) $\#\{i|SC^{-1}(Col(\{j\})) \cap Col(\{i\}) \neq \varnothing,\ 0 \leq i < 4\} > 2$ for every $0 \leq j < 4$, that is to say, the words in each column are shifted from more than 2 different columns.

then the 2-round encryption R^2 could not be divided into more than one independent functions.

Proof Let $x = (x_0, x_1, \ldots x_{15}) \in \mathbb{F}_{2^b}^{16}$, and $y = R(x)$. Then $R^2(x) = R(y)$. Without loss of generality, we assume that y_0, y_1, y_2, y_3 are input words that be shifted to the j-th column after SC. Condition 1 implies that all 4 input words of MC are belong to the same equivalence class under $\overset{MC}{\sim}$, it follows that $y_0 \overset{R}{\sim} y_1 \overset{R}{\sim} y_2 \overset{R}{\sim} y_3$. Assume y_0, y_1, y_2, y_3 are shifted from columns indexed by $I = \{i|SC(Col(\{j\})) \cap Col(\{i\}) \neq \varnothing\}$, then we can deduce from Theorem3 that elements in $\{x_i|i \in SC^{-1}(Col(I))\}$ are belong to the same equivalence class under $\overset{R^2}{\sim}$. From Condition 2 we know that $|I| > 2$ which implies that $\#\{x_i|i \in SC^{-1}(Col(I))\} \geq 12$. Thus, every equivalence class of $\overset{R^2}{\sim}$ has more than 12 elements. Since there are only 16 input words for R^2, there is only 1 equivalence class under $\overset{R^2}{\sim}$.

For a generic AES-like cipher in $\boldsymbol{\varepsilon}(m_1, m_2, b)$ with $m_1 \times m_2 = n$ and round function R, it is clear that R^t is a permutation on $\mathbb{F}_{2^b}^n$ for a positive integer t. Let us denote the least positive integer t such that the input set $\{x_0, x_1, \ldots, x_{n-1}\}$ has only one equivalence class under $\overset{F}{\sim}$ with $F = R^t$ by $L_2(R)$. Set $\kappa = L_2(R)$. Then it follows from Theorem 2 that R^κ could not be divided into more than one independent permutations. Assume $R^{\kappa-1}$ can be divided into m independent functions where $m > 1$. Because the nonlinear layer SB works on words individually, the function $SB \circ R^{\kappa-1}$ can also be divided into m independent functions. Thus, the κ-round encryption R^κ can be written as $R^\kappa = G \circ F$, where G is a linear function and $F = SB \circ R^{\kappa-1}$ can be divided into m independent permutations given by

$$F_{J_0}(x_{I_0}), F_{J_1}(x_{I_1}), \ldots, F_{J_{m-1}}(x_{I_{m-1}}).$$

Based on this representation, we give the following theorem.

Theorem 4 *Let $K \subset \{0, 1, \ldots m-1\}$, $I = \bigcup_{i \in K} I_i$, $p^0, p^1 \in \mathbb{F}_{2^b}^n$ and $p'^0 = \rho^I(p^0, p^1)$, $p'^1 = \rho^I(p^1, p^0)$. Then*

$$R^\kappa(p^0) \oplus R^\kappa(p^1) = R^\kappa(p'^0) \oplus R^\kappa(p'^1).$$

Proof The κ-round encryption R^κ can be rewritten as

$$R^\kappa(x) = G \circ F(x) = G \circ (F_{J_0}(x_{I_0}), F_{J_1}(x_{I_1}), \dots, F_{J_{m-1}}(x_{I_{m-1}})).$$

Take $I = I_0$ as an example. Since the exchange operation only exchanges the words indexed by I_0, we have

$$\begin{aligned}&F(p'^0) \oplus F(p'^1)\\ =&(F_{J_0}(p^1_{I_0}), F_{J_1}(p^0_{I_1}) \dots, F_{J_{m-1}}(p^0_{I_{m-1}})) \oplus (F_{J_0}(p^0_{I_0}), F_{J_1}(p^1_{I_1}) \dots, F_{J_{m-1}}(p^1_{I_{m-1}}))\\ =&F(p^0) \oplus F(p^1).\end{aligned}$$

Since G is a linear function, it follows that

$$G \circ F(p'^0) \oplus G \circ F(p'^1) = G(F(p'^0) \oplus G(F(p'^1)) = G \circ F(p^0) \oplus G \circ F(p^1).$$

This completes the proof.

Now we are going to illustrate the idea of constructing mixture differential distinguishers using the property given by Theorem 4. We know that for an input pair (p^0, p^1) and its exchanged pair (p'^0, p'^1), the equality

$$R^\kappa(p^0) \oplus R^\kappa(p^1) = R^\kappa(p'^0) \oplus R^\kappa(p'^1)$$

holds. For an integer $a \geq 0$, let $c^0 = R^{\kappa+a}(p^0), c^1 = R^{\kappa+a}(p^1), c'^0 = R^{\kappa+a}(p'^0), c'^1 = R^{\kappa+a}(p'^1)$ and $\gamma = R^\kappa(p^0) \oplus R^\kappa(p'^0) = R^\kappa(p^1) \oplus R^\kappa(p'^1)$. Then we have

$$c'^0 = R^a(R^\kappa(p'^0)) = R^a(\gamma \oplus R^\kappa(p^0)) = R^a(\gamma \oplus R^{-a}(c^0)).$$

Similarly, we have

$$c'^1 = R^a(\gamma \oplus R^{-a}(c^1)).$$

We define the encryption $R^a(\gamma \oplus R^{-a}(x))$ as follow.

Definition 6 (Boomerang structure) Let n be an integer not less than κ. The function $B_n = R^{n-\kappa} \circ AC \circ R^{-(n-\kappa)}$ is called the boomerang structure of R^n, where AC represents constant addition operation.

6

Let n be an integer not less than κ. For a ciphertext pair (c^0, c^1), and its plaintext pairs (p^0, p^1) where $p^0 = R^{-(n)}(c^0)$ and $p^1 = R^{-(n)}(c^1)$, let (p'^0, p'^1) be the exchange pair of (p^0, p^1) and $(c'^0, c'^1) = (R^n(p'^0), R^n(p'^1))$. Then

$$\begin{aligned}c'^0 &= R^{n-\kappa} \circ AC \circ R^{-(n-\kappa)}(c^0),\\ c'^1 &= R^{n-\kappa} \circ AC \circ R^{-(n-\kappa)}(c^1).\end{aligned}$$

It can be seen that if there is a differential trail or an impossible differential of boomerang structure $B_n = R^{n-\kappa} \circ AC \circ R^{-(n-\kappa)}$, then the propagation of difference $c^0 \oplus c^1 \to c'^0 \oplus c'^1$ also has the same probability, i.e.,

$$\Pr[B_n(x \oplus \alpha) \oplus B_n(x) = \beta] = \Pr[c'^0 \oplus c'^1 = \beta \mid c^0 \oplus c^1 = \alpha],$$

and

$$\Pr[B_n(x) \oplus B_n(x \oplus \delta) \in B \mid \delta \in A] = \Pr[c'^0 \oplus c'^1 \in B \mid c^0 \oplus c^1 \in A]$$

Since the output pair (c^0, c^1) is alternative, this property can be easily used in cryptanalysis. Thus, based on this observation, we convert the mixture differential distinguisher construction of R^{r+a} into searching differential distinguishers of boomerang structure E. Note that for different pair (c^0, c^1), the constant γ is different, which implies that the constant in AC is continually changing. Although the value of constant does not influence the propagation of difference, we could not analyze the boomerang structure with high order differential cryptanalysis since the constant is not fixed.

3.2 Previous distinguishers in the new framework

In the following of this paper, we denote the boomerang structure of r-round AES-like cipher as B_r. We are going to review the previous mixture differential distinguishers from the point of view of boomerang structure. First of all, we divide the mixture differential distinguishers into three types.

(1) Type 1: distinguishers utilizing impossible differentials in boomerang structure;
(2) Type 2: distinguishers utilizing truncated differentials in boomerang structure;
(3) Type 3: distinguishers utilizing traditional differentials in boomerang structure.

For the AES round function $R = MC \circ SR \circ SB$, we have $L_2(R) = 2$. Thus, the boomerang structure of 4-round AES is

$$B_4 = SR \circ SB \circ MC \circ SR \circ SB \circ AC \circ SB^{-1} \circ SR^{-1} \circ MC^{-1} \circ SB^{-1} \circ SR^{-1}.$$

Since SR and SB are commutative, B_4 can be writed as

$$B_4 = SR \circ SB \circ MC \circ SB \circ AC \circ SB^{-1} \circ MC^{-1} \circ SB^{-1} \circ SR^{-1}.$$

It can be seen that there is a truncated differential distinguisher with probability 1 for B_4 given by

$$\Pr[\upsilon(SR(x \oplus x')] = \upsilon(SR^{-1}(B_4(x) \oplus B_4(x')))] = 1,$$

where $x, x' \in \mathbb{F}_{2^8}^{16}$. This distinguisher is utilized in the 4-round Type 2 distinguisher described by Equation (1). Moreover, it can also be extended to a series of Type 1 distinguishers, which are usually used to filter wrong key guesses. In [7], the 6-round distinguisher is based on a Type2 distinguisher for 5-round AES. We describe the truncated difference for B_5 used in this distinguisher in Fig.1. In [3], the authors presented Type 1 mixture differential distinguishers for 5-round and 6-round AES respectively. The boomerang structure of 5-round AES is

$$B_5 = F \circ F \circ SB \circ AC \circ SB^{-1} \circ F^{-1} \circ F^{-1},$$

where $F = SR \circ SB \circ MC$. The impossible differential distinguisher utilized in the 5-round Type 1 distinguisher is presented by Fig.2. This distinguisher only covers the following encryption

$$E_5' = F \circ SB \circ AC \circ SB^{-1} \circ F^{-1} \circ F^{-1},$$

and the distinguisher can be described as

$$\Pr[\upsilon(SR(E_5'(x) \oplus E_5'(x'))) \leq 2 | wt(x_i \oplus x_i') \leq 2] = 0$$

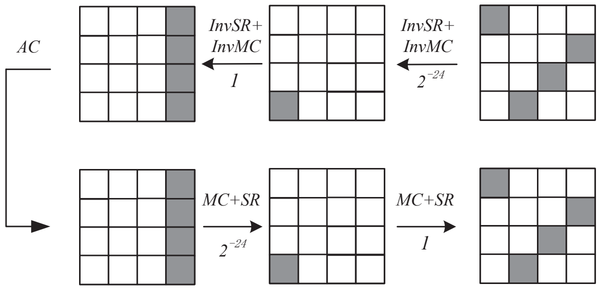

Fig. 1: Truncated differential for boomerang structure of 5-round AES

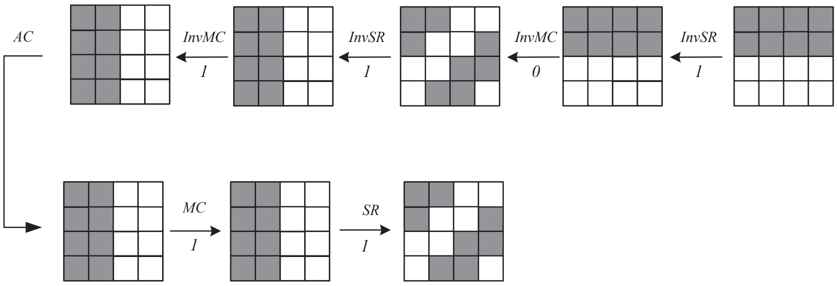

Fig. 2: Impossible differential for boomerang structure of 5-round AES

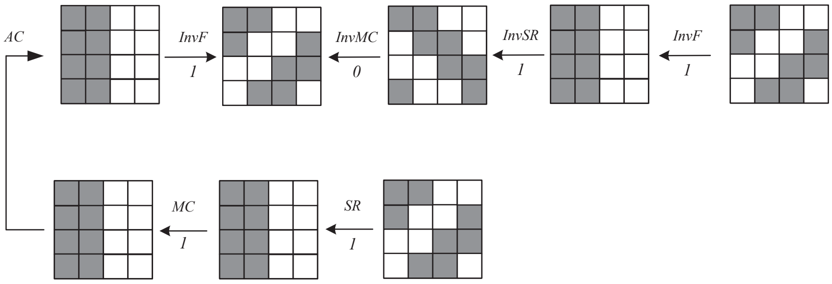

Fig. 3: Impossible differential for boomerang structure of 6-round AES

for $x, x' \in \mathbb{F}_{2^8}^{16}$ and $0 \leq i < 4$. The 6-round Type 1 distinguisher of AES does not cover the whole boomerang structure either. Let

$$E'_6 = F \circ SB \circ AC \circ SB^{-1} \circ F^{-1} \circ F^{-1} \circ F^{-1}.$$

The impossible differential of E'_6 utilized in 6-round Type 1 distinguisher is

$$\Pr[\upsilon(SR(E'_6(x) \oplus E'_6(x'))) \leq 2 | \upsilon(SR(x_i \oplus x'_i)) \leq 2] = 0, \text{where } x, x' \in \mathbb{F}_{2^8}^{16}.$$

which is presented in Fig3.

It is difficult to apply these distinguishers to distinguish AES, since they do not cover the whole boomerang structure, and the difficulty lies in that the difference pattern of intermediate state is unknown. Take Algorithm 4 in [3] as an example. Recall that this algorithm uses a truncated differential to figure out the difference pattern of intermediate states. Thus the algorithm combines an impossible differential with a truncated differential whose probability is less than 1, which makes the 5-round distinguisher invalid. As a result, the probability that a wrong pair is judged as a right pair is $(1-2^{-11.4})^{2^{11.4}} \approx e^{-1} \approx 0.368$. Since there are nearly $2^{13.4}$ wrong pairs to be checked, the probability that at least a wrong pair is judged as a right pair is $1-(1-0.368)^{2^{13.4}} \approx 1$, which means the probability that a random permutation is judged as AES is 1. To verify our deduction, we apply Algorithm 4 on some block ciphers, including full round AES128, Midori128, SIMON128 [11] and Spring128 [12]. All these block ciphers are identified as 6-round AES. The code of the experiments are presented at https://github.com/BLOCKCIPHERS702702. It is also difficult to apply the distinguishers that do not cover the whole boomerang structure to key-recovery attack against AES. As a result, we mainly focus on the distinguishers covering the whole boomerang structure.

4 Security evaluation of AES-like ciphers against mixture differential

In this section, we are going to evaluate the security of AES-like cipher against the three types of distinguishers, especially the security against Type 1 and Type 2 distinguishers.

4.1 Security evaluation against Type 1 distinguisher

In the previous mixture differential cryptanalysis against AES, the 4-round Type 2 distinguisher with probability 1 played a very important role. The following proposition illustrate the relation between this kind of distinguishers and Type 1 distinguisher.

Proposition 1 *For a boomerang structure, if there is a deterministic truncated difference, then there exists an impossible difference.*

According to Proposition 1, if there is no impossible difference for a boomerang structure, there is no deterministic truncated difference either. As a result, if we can give the upper bound of round number r for Type 1 distinguisher, then we know there is no r-round Type 2 distinguisher with probability 1. In [3], the upper bound of impossible differential distinguisher is well studied using “primitive index” and the characteristic matrix. Based on these methods, we give the following theorem.

Theorem 5 *For an AES-like cipher with the round function $R = MC \circ SC \circ SB$, let $F = SC \circ SB \circ MC$, $P = MC^{-1} \circ SC^{-1}$, and $r = L_1(P)$. There is no impossible differential distinguisher for $F^r \circ SB \circ AC \circ SB \circ F^{-r}$.*

Proof Let m be the length of input vectors. For a vector $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{m-1})$, denote $H(\alpha) = \#\{\alpha_i | \alpha_i \neq 0\}$. It follows from Lemma 1 in [3] that for $\alpha \neq 0$ with $H(\alpha) = 1$, there exists a vector $\beta = (\beta_0, \beta_1, \ldots, \beta_{m-1})$ such that $H(\beta) = m$ and $\alpha \to \beta$ is a possible differential for F^r. Thus, for any α, α' and corresponding β, β' satisfying $H(\alpha) = H(\alpha') = 1$, $H(\beta) = H(\beta') = m$. Since $v(\beta) = v(\beta')$, we have $\alpha \to \alpha'$ is a possible differential for $F^r \circ SB \circ F^{-r}$. Notice that $H(\alpha) = H(\alpha') = 1$, by the Theorem 1 in [3], there is no impossible differential for $F^r \circ SB \circ AC \circ SB \circ F^{-r}$.

Theorem 6 *For an AES-like cipher with the round function $R = MC \circ SC \circ SB$ and $P = MC^{-1} \circ SC^{-1}$, let $r = L_1(P) + L_2(R)$. There is no Type 1 distinguisher for more than r-round encryption.*

Proof Let $F = SC \circ SB \circ MC$ and $\kappa = L_2(R)$. The boomerang structure of $(r+1)$-round encryption is $B_r = F^{\kappa} \circ SB \circ AC \circ SB \circ F^{-\kappa}$. By Theorem 5, there is no impossible differential for B_r. Thus, there is no Type 1 distinguisher for more than r-round encryption.

The following corollary immediately follows from Theorem 6.

Corollary 2 *For an AES-like cipher with the round function R and the linear layer P. Let $r = L_1(P) + L_2(R)$. There is no Type 2 distinguisher with probability 1 for r-round encryption E_r. For an AES-like cipher with round function $R = MC \circ SC \circ SB$. Let $P = MC^{-1} \circ SC^{-1}$ and $r = L_1(P) + L_2(R)$. There is no Type 1 distinguisher for more than r-round encryption.*

For AES, since $L_1(P) = 2$, $L_2(R) = 2$, it can be deduced from Corollary2 that there is no Type 2 distinguisher with probability 1 for 5-round AES.

4.2 Security evaluation against Type 2 distinguisher

The point of constructing a Type 2 distinguisher for AES-like ciphers is searching a truncated differential for boomerang structure. At the state of the art, there are following two frameworks to construct truncated differentials: adopting the branch property of linear layer [13] and employing multiple differentials [14]. The truncated differentials adopting branch property of linear layer can be searched by automatic search method easily [15]. We analysis the security of AES-like ciphers against these two kind of distinguishers respectively.

For an AES-like cipher belonging to $\varepsilon(4, 4, b)$, let R be the round function. Based on Corollary 1, we give a reasonable assumption that $L_2(R) = 2$ which is the worst situation. Let $F = SC \circ SB \circ MC$. Then, for an integer $n \geq 3$, the boomerang structure of this n-round encryption is

$$B_n = F^{n-3} \circ SB \circ AC \circ SB^{-1} \circ F^{3-n}$$

and the n-round encryption can be rewritten as

$$E_n = F^{n-3} \circ SC \circ SB \circ R^2.$$

These equations split the B_n and E_n into two parts respectively, where the second part of B_n and E_n are both F^{n-3}. We remark that a truncated differential distinguisher for B_n is equal to a mixture differential distinguisher. It can be seen that with the increasing of n, it is more difficult to search differential distinguishers for B_n than E_n since F^{3-n} consists of much more operations than R^2. To give a bound on n that multiple differences exist, we propose the following proposition.

Proposition 2 *Let $R = MC \circ SR \circ SB$ be the round function of an AES-like cipher belonging to $\varepsilon(4, 4, b)$. Assume that SR shifts the words in every column into 4 different columns, and the branch number of MC is $\mathcal{B}$. Denote N the least active S-boxes for differential trails of $F^3 \circ SB$. Then $N \geq \mathcal{B}^2$.*

Proof Note that there are 3 Mixcolumns in $F^3 \circ SB$. Let $\alpha^i = (\alpha_0^i, \alpha_1^i, \ldots, \alpha_{15}^i)$ and $\beta^i = (\beta_0^i, \beta_1^i, \ldots, \beta_{15}^i)$ be the input difference and output difference of the i-th MC. Without loss of generality, assume that $(\alpha_0^1, \alpha_4^1, \alpha_8^1, \alpha_{12}^1)$ is one active column of α^1. Since $\alpha^1 = SR \circ SB \circ MC(\alpha^0)$, the active S-boxes in $(\alpha_0^1, \alpha_4^1, \alpha_8^1, \alpha_{12}^1)$ are shifted from different columns of α^0. Denote a_i as the number of active column for α^i. It follows that

$$a_0 \geq \upsilon(\alpha_0^1, \alpha_4^1, \alpha_8^1, \alpha_{12}^1).$$

Similarly, the active S-boxes in $(\beta_0^1, \beta_4^1, \beta_8^1, \beta_{12}^1)$ will be shifted to different columns, and so $a_2 \geq \upsilon(\beta_0^1, \beta_4^1, \beta_8^1, \beta_{12}^1)$. Thus we have

$$a_0 + a_2 \geq \upsilon(\alpha_0^1, \alpha_4^1, \alpha_8^1, \alpha_{12}^1) + \upsilon(\beta_0^1, \beta_4^1, \beta_8^1, \beta_{12}^1) \geq \mathcal{B}.$$

This implies that the number of active S-boxes for every differential trail satisfies $N \geq a_0 \times \mathcal{B} + a_2 \times \mathcal{B} \geq \mathcal{B}^2$.

It can be deduced from Proposition 2 that, for

$$E_6 = F^3 \circ SB \circ AC \circ SB^{-1} \circ F^{-3},$$

there are more than $2 \times \mathcal{B}^2$ active S-boxes for every differential trail. Now, we can illustrate the security of E_6 against multiple difference. Let A, B be the set of input and output differences of E_6, respectively. Let $N_1 = |A|$ and $N_2 = |B|$. Then the probability of multiple difference satisfies

$$P(A \to B) = \sum_{\alpha \in A, \beta \in B} P(\alpha \to \beta) \leq N_1 \times N_2 \times p^{2 \times \mathcal{B}^2}$$

where p is the max differential probability of S-box. For the random case, the probability that output difference falls in B is $P_{rand} = N_2 \times 2^{-16 \times b}$. Since $N_1 \leq 2^{16 \times b}$, it follows that if $p^{2 \times \mathcal{B}^2} \leq 2^{-32 \times b}$, then we have

$$P(A \to B) \leq N_1 \times N_2 \times p^{2 \times \mathcal{B}^2} \leq N_2 \times 2^{-16 \times b} = P_{rand},$$

which means the truncated difference $A \to B$ can not be a distinguisher. Since A and B are arbitrary, there is no multiple difference for E_6. Similarly, for E_{10}, the number of active S-boxes for every differential trail satisfies $N \geq 4 \times \mathcal{B}^2$. It follows that if $p^{4 \times \mathcal{B}^2} \leq 2^{32 \times b}$, then there is no multiple difference for E_{10}. We apply these analysis on some block ciphers, and the results are presented in Table 1, where the bound n in Table 1 means there is no n round multiple difference.

We also apply the MILP (Mixed-Integer Linear Programming) method that exploits the branch property on AES-like ciphers. That is modeling the branch property of Mixcolumn to MILP problem, and so we can search distinguishers by

Table 1: Bound of multiple differences for boomerang structure

Ciphers	Cell size(b)	Branch number($\mathcal{B}$)	Max probability of S-box(p)	Bound of multiple difference(n)
AES	8	5	2^{-6}	6
Midori64	4	4	2^{-2}	10
Midori128	8	4	2^{-2}	16

Table 2: Bound of truncated differences for boomerang structure based on MILP

Ciphers	Bound of truncated differences
AES	6
Midori64	7
Midori128	7
Skinny	9

automatic search tools. The detail of building MILP models is presented in 15. We only focus on the least round number that no distinguisher could be found. Results on AES, Midori64, Midori128 and Skinny are given in Table 2.

We remark that from Tables 1 and 2, it can be seen that there is no mixture differential distinguish for 6-round AES. Thus, there is no need to find a mixture differential distinguish for 6-round AES in practice.

5 Conclusions

This paper studies the security evaluation of AES-like ciphers against mixture differential cryptanalysis. The boomerang structure which associates the mixture differential distinguishers with other types of differential distinguishers is firstly proposed. Based on the boomerang structure, an upperbound on the number of rounds for an AES-like cipher to resist mixture differential cryptanalysis could be estimated. It is shown that there is no mixture difference distinguishers for 6-, 10-, 16- and 9-round AES, Midori64, Midori128 and Skinny, respectively.

References

1. Joan Daemen and Vincent Rijmen. *The Design of Rijndael - The Advanced Encryption Standard (AES), Second Edition.* Information Security and Cryptography. Springer, 2020.
2. Eli Biham, Alex Biryukov, Orr Dunkelman, Eran Richardson, and Adi Shamir. Initial observations on skipjack: Cryptanalysis of skipjack-3xor. In Stafford E. Tavares and Henk Meijer, editors, *Selected Areas in Cryptography '98, SAC'98, Kingston, Ontario, Canada, August 17-18, 1998, Proceedings*, volume 1556 of *Lecture Notes in Computer Science*, pages 362–376. Springer, 1998.
3. Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth. Yoyo tricks with AES. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017*, volume 10624 of *LNCS*, pages 217–243. Springer, 2017.
4. Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. A new structural-differential property of 5-round AES. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017*, volume 10211 of *LNCS*, pages 289–317, 2017.
5. Lorenzo Grassi. Mixture differential cryptanalysis: a new approach to distinguishers and attacks on round-reduced AES. *IACR Trans. Symmetric Cryptol.*, 2018(2):133–160, 2018.

6. Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. Improved key recovery attacks on reduced-round AES with practical data and memory complexities. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018*, volume 10992 of *LNCS*, pages 185–212. Springer, 2018.
7. Navid Ghaedi Bardeh and Sondre Rønjom. The exchange attack: How to distinguish six rounds of AES with 2ˆ88.2 chosen plaintexts. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019*, volume 11923 of *LNCS*, pages 347–370. Springer, 2019.
8. Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. The retracing boomerang attack. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020*, volume 12105 of *LNCS*, pages 280–309. Springer, 2020.
9. Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In Jacques Stern, editor, *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*, volume 1592 of *Lecture Notes in Computer Science*, pages 12–23. Springer, 1999.
10. Bing Sun, Meicheng Liu, Jian Guo, Vincent Rijmen, and Ruilin Li. Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016*, volume 9665 of *Lecture Notes in Computer Science*, pages 196–213. Springer, 2016.
11. Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. SIMON and SPECK: block ciphers for the internet of things. *IACR Cryptol. ePrint Arch.*, 2015:585, 2015.
12. Tian Tian, Wenfeng Qi, Chendong Ye, and Xiaofeng Xie. Spring: A family of small hardware-oriented block ciphers based on NFSRs. *Journal of Cryptologic Research*, 2019(6(6)):815–834, 2019.
13. Zhenzhen Bao, Jian Guo, and Eik List. Extended truncated-differential distinguishers on round-reduced AES. *IACR Trans. Symmetric Cryptol.*, 2020(3):197–261, 2020.
14. Céline Blondeau and Benoît Gérard. Multiple differential cryptanalysis: Theory and practice. In Antoine Joux, editor, *Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers*, volume 6733 of *Lecture Notes in Computer Science*, pages 35–54. Springer, 2011.
15. Amirhossein Ebrahimi Moghaddam and Zahra Ahmadian. New automatic search method for truncated-differential characteristics application to midori, SKINNY and CRAFT. *Comput. J.*, 63(12):1813–1825, 2020.