New Insights on AES-Like SPN Ciphers ⋆

Bing Sun[1,2,3], Meicheng Liu[3,4], Jian Guo[3], Longjiang Qu[1], Vincent Rijmen[5]

[1] College of Science, National University of Defense Technology,
Changsha, Hunan, P.R.China, 410073
happy_come@163.com, qlj_happy@163.com
[2] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, P.R. China, 100878
[3] Nanyang Technological University, Singapore
meicheng.liu@gmail.com, ntu.guo@gmail.com
[4] State Key Laboratory of Information Security, Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, P.R. China, 100093
[5] Dept. Electrical Engineering (ESAT), KU Leuven and iMinds, Belgium
vincent.rijmen@esat.kuleuven.be

Abstract. It has been proved in Eurocrypt 2016 that if the details of the S-boxes are not exploited, an impossible differential and a zero-correlation hull can extend over at most 4 rounds of the AES. This paper concentrates on distinguishing attacks on AES-like SPN ciphers by investigating the details of both the S-boxes and the MDS matrices and illustrates some new insights on the security of these schemes. Firstly, we construct several types of 5-round zero-correlation linear hulls for AES-like ciphers that adopt *identical S-boxes* to construct the round function and that have *two identical elements in a column of the inverse of their MDS matrices*. We then use these linear hulls to construct 5-round integrals provided that the difference of two sub-key bytes is known. Furthermore, we prove that we can always distinguish 5 rounds of such ciphers from random permutations even when the difference of the sub-keys is unknown. Secondly, the constraints for the S-boxes and special property of the MDS matrices can be removed if the cipher is used as a building block of the Miyaguchi-Preneel hash function. As an example, we construct two types of 5-round distinguishers for the hash function Whirlpool. Finally, we show that, in the chosen-ciphertext mode, there exist some nontrivial distinguishers for 5-round AES. To the best of our knowledge, this is the longest distinguishing attack for the round-reduced AES in the secret-key setting. Since the 5-round distinguisher for the AES can only be constructed in the chosen-ciphertext mode, *the security margin for the round-reduced AES under the chosen-plaintext attack may be different from that under the chosen-ciphertext attack.*

⋆ The work in this paper is supported by the National Basic Research Program of China (973 Program) (2013CB338002), the National Natural Science Foundation of China(No: 61272484, 61303258, 61402515, 61572016), and the Program for New Century Excellent Talents in University.
IACR 2016. This article is the final version submitted by the authors to the IACR and to Springer-Verlag on May 30, 2016. The version published by Springer-Verlag is available at DOI***.

Keywords: Distinguishing attack, AES, Whirlpool, Zero correlation linear, Integral

1 Introduction

Block ciphers are among the most important primitives in constructing symmetric cryptographic schemes such as encryption algorithms, hash functions, authentication schemes and pseudo-random number generators. The Advanced Encryption Standard (AES) [12] is currently the most interesting candidate to build different schemes. For example, in the on-going Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) [10], among many others, the permutation of PRIMATEs [1] is designed based on an AES-like SPN structure, AEGIS [39] uses 4 AES round-functions in the state update functions, ELmD [13] recommends to use some round-reduced AES including the 5-round AES to partially encrypt the data, and 4-round AES is adopted to build the AESQ permutation in PAEQ [5]. Although the security of these candidates does not completely depend on the underlying primitives, we believe that security of the round-reduced AES could give some new insights to both the design and cryptanalysis of the authenticated encryption algorithms.

1.1 Distinguishing Attacks

The aim of a distinguishing attack is to find some properties of a cipher that random permutations do not have thus we can distinguish a cipher from random permutations. For example, in *differential cryptanalysis* [4], one always finds an r-round differential characteristic with high probability while for random permutations such a differential characteristic does not exist.

In [11], Daemen *et al.* proposed a new method that can break more rounds of SQUARE than differential and linear cryptanalysis, which is named the SQUARE attack consequently. Some similar ideas such as the saturation attack [29], the multi-set attack [6], and the higher-order differential attack [26, 22] have also been proposed. In [25], Knudsen and Wagner proposed the integral cryptanalysis as a generalized case of these attacks. In an integral attack, with some special inputs, one checks whether the sum of the corresponding ciphertexts is zero or not. Integral attacks on the round-reduced AES are based on the following distinguisher:

Property 1. [12, 17] Let 15 bytes of the input be constants and the remaining byte take all possible values from $\mathbb{F}_{2^8}$. Such a set is called a Λ-set. Then, the sum of each byte of the output of the third round is 0. Furthermore, let the 4 bytes in the diagonal of the state take all possible values from $\mathbb{F}_{2^8}^4$ and the other 12 bytes be constants, then the output of 1-round AES can be divided into 2^{24} Λ-sets. Therefore, the sum of each byte of the output of the fourth round is 0.

Gilbert and Minier showed that the set of functions mapping one active byte to one byte after 3 rounds depends on 9-byte parameters [20]. Therefore, the whole set can be described by using a table of 2^{72} entries of 256-byte sequences. This idea was later generalized by Demirci and Selçuk in [14] using meet-in-the-middle techniques. They showed that on 4 rounds, the value of each byte of the ciphertext can be described by a function of the active byte parameterized by 25 in [14] and 24 8-bit parameters in [15].

Property 2. [15] The set of functions mapping one active byte to one byte after 4 rounds AES depends on 24 one-byte parameters.

Knudsen [23] and Biham *et al.* [3] independently proposed impossible-differential cryptanalysis. The main idea of impossible-differential cryptanalysis is to use differentials that hold with probability zero to discard the wrong keys that lead to the impossible differential. Now, it is one of the most effective methods towards many different ciphers. One of the 4-round impossible differentials is shown as follows:

Property 3. [33, 30, 31] The differential, where there is only one nonzero (active) byte of the input difference and output difference, respectively, is a 4-round impossible differential of the AES.

Zero-correlation linear cryptanalysis was proposed by Bogdanov and Rijmen in [9]. They try to construct some linear hulls with correlation exactly zero. The 4-round zero correlation linear hull of the AES is shown as follows:

Property 4. [9] If there is only one nonzero (active) byte of the input mask and output mask, respectively, then the correlation of 4-round AES is 0.

In summary, although there exist some 5-round distinguishers for AES-192 and AES-256 [16], the known distinguishers for all version of the AES only cover at most 4 rounds.

All the above distinguishers are in the secret-key setting, which were used in key recovery attacks. At Asiacrypt 2007, Knudsen and Rijmen proposed the *known-key distinguisher* for block ciphers [24]. In the setting that the key is public to the attacker, one can construct 7-round known-key distinguisher for the AES, which was improved to 8-round and 10-round in [19]. Allowing even more degrees of freedom to attackers so that they can even choose keys, distinguishers of 9-round AES were proposed [18] in the *chosen-key setting*. In this paper, we restrict ourselves to the secret-key setting, and the distinguishers to be presented are natural extensions of those used in key recovery attacks.

1.2 Key-Recovery Attacks

The aim of a key-recovery attack is to recover some roundkeys of a cipher. Usually, the attack is applied once some distinguishing attack against the reduced-round block cipher has been found. Up to date, the biclique attack can recover some subkeys of the full round AES with slightly less than exhaustive complexity [7]. We briefly list some results of the key-recovery attacks against round-reduced AES as in Table 1, together with the number of rounds of the underlying distinguishers used.

Table 1. Some Key-Recovery Attacks against AES-128

Rounds	Technique	Data	Memory	Time	Reference	Rounds of distinguisher
6	integral	6×2^{32}	2^{8}	2^{72}	[17]	4
7	integral	$2^{127.997}$	2^{64}	2^{120}	[17]	4
7	impossible differential	$2^{112.2}$	$2^{112.2}$	$2^{117.2}$	[30]	4
7	impossible differential	$2^{106.2}$	$2^{90.2}$	$2^{110.2}$	[31]	4
7	meet-in-the-middle	2^{105}	2^{90}	2^{99}	[16]	4
7	meet-in-the-middle	2^{97}	2^{98}	2^{99}	[16]	4

1.3 Details of the Components of a Cipher

If we choose the parameters carefully, the dedicated cipher based on the AES-like structure can be resilient to both differential [4] and linear cryptanalysis [32]. For example, based on the fact that the branch number of the MixColumns is 5, it is proved in [12] that the number of active S-boxes of 4-round AES is at least 25. Since the maximal differential probability of the S-box is 2^{-6}, there does not exist any differential characteristic of 4-round AES with probability larger than 2^{-128}.

In most cases, especially in the cryptanalysis of AES, we do not need to investigate the details of the S-boxes. Thus, the corresponding results are independent of the non-linear components. In other words, if we choose some other S-boxes with similar differential/linear properties in a cipher, the corresponding cryptanalytic results remain almost the same. To characterize what "being independent of the choice of the S-boxes" means, in [36], Sun *et al.* proposed the conception of *Structure* of a block cipher. By structural evaluation, we mean the domain of cryptography that analyzes a cryptosystem in terms of generic constructions which keep the linear parts of the cipher and omit the details of the non-linear components.

The influence of the choices of S-boxes in constructing integral distinguishers has been studied in [21, 28, 34]. For example, if ARIA adopts only one S-box, more balanced bytes could be determined and if the order of different S-boxes is changed (There are 4 different S-boxes in ARIA), we will get different integral distinguishers from the one constructed in [28]. In [34], the authors pointed that in some cases, the key-recovery attack based on the integral distinguisher may be failed. Very recently, Todo proposed the division property [37] by which one could build longer integral distinguishers provided the algebraic degree of the S-boxes is known. For example, a 6-round integral for MISTY1 was built in [38] based on which the first cryptanalysis result against the full MISTY1 was given.

Although we already have 4-round impossible differentials and zero-correlation linear hulls for the AES, the effort to find new impossible differentials and zero-correlation linear hulls that cover more rounds has never stopped. In EURO-

CRYPT 2016, Sun *et al.* proved that, unless the details of the S-boxes are exploited, one cannot find any impossible differential or zero-correlation linear hull of the AES that covers 5 or more rounds:

Property 5. [35] There does not exist any impossible differential or zero-correlation linear hull of $\mathcal{E}^{\text{AES}}$ which covers $r \geq 5$ rounds. Or equivalently, there does not exist any 5-round impossible differential or zero-correlation linear hull of the AES unless the details of the S-boxes are considered.

To increase the performance of a block cipher, one usually uses an MDS (Maximal Distance Seperatable) matrix whose elements always have low hamming weights to reduce the workload for the multiplication over finite fields. Furthermore, it is noticed that not only the MDS matrices are always circulant, but also there are identical elements in each row. For example, in AES, the first row of the MDS matrix is $(\texttt{02}, \texttt{03}, \texttt{01}, \texttt{01})$. However, most known techniques have not made use of these observations and there is little literature concentrating on the choices of these matrices in constructing distinguishers for the round-reduced AES. Since known impossible differentials and zero-correlation linear hulls of round-reduced AES are constructed based on the fact that the branch number of the MixColumns is 5, these two kinds of distinguishers still hold even if another 4×4 MDS matrix over $\mathbb{F}_{2^8}$ is used. Furthermore, since the inverse of an MDS matrix also has the MDS property, these distinguishers not only hold in the *chosen-plaintext* setting, but also hold in the *chosen-ciphertext* setting.

1.4 Our Contributions

This paper concentrates on the details of both the S-boxes and MDS matrices that are used in AES-like SPN structures. Denote by M_{MC} the MDS matrix used in a cipher. If there are two identical elements in a row of $(M_{\mathsf{MC}}^{-1})^{\mathrm{T}}$ and if the cipher adopts identical S-boxes, then we can construct a 5-round distinguisher. This implies that applied to AES, our distinguisher covers the most rounds up till now:

(1) If the difference of two sub-key bytes is known, we can construct several types of 5-round zero-correlation linear hulls for such ciphers *without* MixColumns operation in the last round which could be turned into 5-round integrals both *with* and *without* MixColumns operations in the last round. Furthermore, we not only prove that 5 rounds of such ciphers *with* MixColumns operation in the last round can be distinguished from a random permutation, but also that some sub-keys can be recovered from the distinguisher directly.

(2) In a hash function setting, where an AES-like SPN structure is used as a building block and the chaining value acts as the key, there always exist 5-round distinguishers. As proof of concept, we give two types of 5-round distinguishers for the hash function Whirlpool.

For the AES, every row of $(M_{\mathsf{MC}}^{-1})^{\mathrm{T}}$ contains 4 different elements. Thus we cannot apply the results to the AES directly. However, for the decryption of the AES, every row of $(M_{\mathsf{MC}}^{-1})^{\mathrm{T}}$ contains twice the same element, therefore we can construct a 5-round distinguisher for the AES in a chosen-ciphertext mode:

(3) For 5-round AES, divide the whole plaintext-ciphertext pairs into the following 2^8 subsets:
$$A_\Delta = \{(p,c)|c_{0,0} \oplus c_{1,3} = \Delta\}.$$
Then, there always exists a Δ such that $\sum_{(p,c)\in A_\Delta} p = 0$, while for random permutations, this happens with probability $1-(1-2^{-128})^{2^8} \approx 2^{-120}$. Furthermore, we can deduce $k_{0,0} \oplus k_{1,3} = \Delta$ from the distinguisher.

Since this property only applies in the chosen-ciphertext setting, we conclude that the security margin of the AES under the chosen-plaintext setting may be different from the one under the chosen-ciphertext setting. Furthermore, since we have proved that 5-round AES can be distinguished from a random permutation, more attention should be paid when round-reduced AES is used as a building block of some new cryptographic scheme.

Though we have already found some 5-round distinguisher, we leave as an open problem whether we could mount more efficient key-recovery attack against round-reduced AES or other AES-based schemes.

2 Preliminaries

Before proceeding to our results, we first introduce some notations here on both boolean functions and the ciphers we are analyzing.

2.1 Boolean Functions

Given a boolean function $G : \mathbb{F}_2^n \to \mathbb{F}_2$, the *correlation* of G is defined by
$$c(G(x)) \triangleq \frac{1}{2^n} \sum_{x\in\mathbb{F}_2^n} (-1)^{G(x)}.$$

Given a vectorial function $H : \mathbb{F}_2^n \to \mathbb{F}_2^k$, the *correlation* of the linear approximation for a k-bit output mask b and an n-bit input mask a is defined by
$$c(a \cdot x \oplus b \cdot H(x)) \triangleq \frac{1}{2^n} \sum_{x\in\mathbb{F}_2^n} (-1)^{a\cdot x \oplus b\cdot H(x)},$$

where "$\cdot$" is the inner product of two elements. If $c(a \cdot x \oplus b \cdot H(x)) = 0$, then $a \to b$ is called a *zero-correlation linear hull* of H, following the same definition in [9]. Let $A \subseteq \mathbb{F}_2^n$, $B \subseteq \mathbb{F}_2^k$, if for all $a \in A$, $b \in B$, $c(a \cdot x \oplus b \cdot H(x)) = 0$, then $A \to B$ is called a *zero-correlation linear hull* of H.

In this paper, we denote by $\mathrm{circ}(a_0, a_1, \ldots, a_{n-1})$ a *circulant matrix* defined as follows:
$$\mathrm{circ}(a_0, a_1, \ldots, a_{n-1}) = \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & \ldots & a_{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}.$$

For any vector $v = (v_0, v_1, \dots, v_{n-1}) \in \mathbb{F}_{2^b}^n$, the *Hamming Weight* of v is defined as the number of non-zero components of v:

$$\mathrm{wt}(v) = \#\{i | v_i \neq 0, i = 0, 1, \dots, n-1\}.$$

Let $P \in \mathbb{F}_{2^b}^{n \times n}$. Then the *branch number* of P is defined as

$$\mathcal{B}(P) = \min_{0 \neq x \in \mathbb{F}_{2^b}^n} \{\mathrm{wt}(x) + \mathrm{wt}(Px)\}.$$

Obviously, for any $x \in \mathbb{F}_{2^b}^n$, we always have $\mathrm{wt}(Px) \leq n$. Therefor we can choose x such that $\mathrm{wt}(x) = 1$ which indicates that $\mathcal{B}(P) \leq n+1$. A matrix $P \in \mathbb{F}_{2^b}^{n \times n}$ is called *Maximum Distance Separable* (MDS) matrix if and only if $\mathcal{B}(P) = n+1$. In the proof of the security of a cipher against differential and linear cryptanalysis, one can use the branch number to calculate the number of active S-boxes. Since a larger branch number usually gives more active S-boxes, MDS matrices are widely used in modern block ciphers.

2.2 SPN and AES-Like SPN Ciphers

To keep our results as general as possible, we are going to give a generic description of the Substitution-Permutation Network (SPN) ciphers and AES-like ciphers, respectively. We assume that the input can be viewed as an $n \times n$ square matrix over $\mathbb{F}_{2^b}$, which implies that both the input (plaintext) and output (ciphertext) of the block ciphers count $n^2 b$ bits. The cipher successively applies R round functions, and we denote respectively by $s^{(r)}$ and $k^{(r)}$ the input and subkey states of the r-th round. The state $s^{(0)}$ is initialized with the input plaintext. One round function is composed of the following layers: a key addition layer (KA) where an n^2b-bit roundkey $k^{(r-1)}$ is xored to $s^{(r-1)}$, a block cipher permutation layer BC that updates the n^2b-bit current state of the block cipher after addition of the subkey, i.e. $s^{(r)} = \mathsf{BC}(s^{(r-1)} \oplus k^{(r-1)})$. For an SPN cipher, the permutation BC is composed of SubBytes (SB) which applies non-linear transformations to the n^2 b-bit bytes in parallel, and then a layer P which is linear over $\mathbb{F}_2^{n^2 b}$, i.e. $\mathsf{BC} = \mathsf{P} \circ \mathsf{SB}$. The final ciphertext is then defined as $s^{(r)} \oplus k^{(r)}$. In the following, we will simply use $\mathcal{E}(n, b, r)$ to denote an r-round AES-like SPN cipher which operates on $n \times n$ b-bit bytes.

In the case of AES-like ciphers, the internal state of BC can be viewed as a square matrix of b-bit cells with n rows and n columns. A cell of $s^{(r)}$ is denoted by $s_{i,j}^{(r)}$, where i is its row position and j its column position in the square matrix, starting counting from 0. Then, the linear layer itself is composed of the ShiftRows transformation (SR), which can be defined as a permutation $\pi_{\mathsf{SR}} = (l_0, l_1, \dots, l_{n-1})$ on $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ that moves cell $s_{i,j}^{(r)}$ by l_i positions to the left in its own row, and the MixColumns transformation (MC), which linearly mixes all the columns of the matrix. Overall, for AES-like ciphers, we always have $\mathsf{BC} = P \circ S = \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SB}$.

The AES Block Cipher. AES only uses a single S-box which is based on the inverse function over $\mathbb{F}_{2^8}$ to construct the round function. The SR and the MC of AES are defined as follows:

$$\pi_{\mathsf{SR}} = (0, 1, 2, 3),$$
$$M_{\mathsf{MC}} = \begin{pmatrix} \mathsf{02} & \mathsf{03} & \mathsf{01} & \mathsf{01} \\ \mathsf{01} & \mathsf{02} & \mathsf{03} & \mathsf{01} \\ \mathsf{01} & \mathsf{01} & \mathsf{02} & \mathsf{03} \\ \mathsf{03} & \mathsf{01} & \mathsf{01} & \mathsf{02} \end{pmatrix} = \mathrm{circ}(\mathsf{02}, \mathsf{03}, \mathsf{01}, \mathsf{01}).$$

Since we do not investigate the key-recovery attack, please refer to [12] for the details of the key schedule.

3 Zero-Correlation Linear Cryptanalysis of AES-Like SPN Ciphers

3.1 Zero-Correlation Linear Hull of 4-round AES-Like Ciphers

In zero-correlation linear cryptanalysis, we construct some linear hulls with correlation exactly zero. One of the most efficient methods to construct zero correlation linear hulls is based on the miss-in-the-middle technique, i.e., we start from the beginning and the end of the cipher, partially encrypt the plaintext and decrypt the ciphertext, respectively. Then some contradiction could be found in the middle round of the cipher. For example, the 4-round zero-correlation linear hull of the AES is built as follows [9] (see Fig.1): if only the first byte of the input mask is active, then after 1 round, all the 4 bytes in the first column of the output mask are active. Thus in each column of the input mask to the second MixColumns, the number of active bytes is 1. Using the same technique, we find that if there is only 1 active byte in the output mask of the forth round, in each column of the output mask to the second MixColumns round, the number of active bytes is 1. Since the branch number of MixColumns is 5, we find a contradiction which indicates that the correlation of such a linear hull is 0.

To enhance the performance of a cipher, designers usually use identical S-boxes and a diffusion layer whose elements often have relatively low hamming weights, which not necessarily but often cause some weakness as shown in the following.

3.2 New Cryptanalysis of 5-round AES-Like Ciphers

Though it has been proven that the longest zero-correlation linear hull of the AES only covers 4 rounds if we do not investigate the details of the S-box, we can improve this results by exploiting these details.

In this section, we are going to use the miss-in-the-middle technique to construct some novel distinguishers of AES-like SPN ciphers, provided that the difference of two sub-keys bytes is known. Firstly, we recall the following propositions for the propagation for input-output masks/differentials of linear functions:

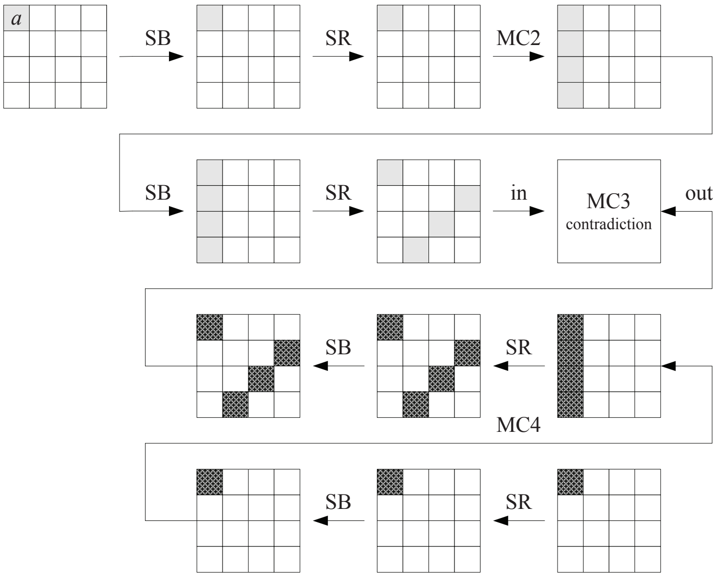

Fig. 1. 4-round zero-correlation linear hull of the AES

Proposition 1. *Let $\mathcal{L}$ be a linear transformation defined on $\mathbb{F}_2^T$, and $L \in \mathbb{F}_2^{t\times t}$ be the matrix representation of $\mathcal{L}$. Then,*

(1) For any input-output mask $\Gamma_I \to \Gamma_O$, if the correlation is nonzero, we always have $\Gamma_O = (L^{-1})^T \Gamma_I$.
(2) For any input-output difference $\Delta_I \to \Delta_O$, if the differential probability is nonzero, we always have $\Delta_O = L\Delta_I$.

Since ShiftRows in the first round does not influence the results, in this section, we omit SR in the first round. Denote by $(M_{\mathsf{MC}}^{-1})^{\mathrm{T}} = (m^*_{i,j})$ the transpose of the inverse of M_{MC}. We assume that an AES-like SPN cipher $\mathcal{E}(n, b, r)$ satisfies the following conditions:

(1) There exists a triple (i, j_0, j_1) such that $m^*_{i,j_0} = m^*_{i,j_1}$ where $j_0 \neq j_1$;
(2) Without loss of generality, the S-boxes used at positions $(j_0, 0)$ and $(j_1, 0)$ are identical.

Lemma 1. *Let $\mathcal{E}(n, b, r)$ be an AES-like SPN cipher satisfying conditions (1) and (2). Define*

$$V = \{(s_{i,j}) \in \mathbb{F}_{2^b}^{n\times n} | s_{j_0,0} \oplus s_{j_1,0} = k_{j_0,0} \oplus k_{j_1,0}\}.$$

For any $0 \neq a \in \mathbb{F}_{2^b}$, let the input mask be

$$\Gamma_I = (\alpha_{i,j})_{0\le i,j\le n-1}, \quad \alpha_{i,j} = \begin{cases} a & (i,j) = (j_0, 0), (j_1, 0), \\ 0 & otherwise, \end{cases}$$

and the output mask be $\Gamma_O = (\beta_{i,j}) \in \mathbb{F}_{2^b}^{n\times n}$. *Then, if the correlation* $\Gamma_I \rightarrow \Gamma_O$ *of* $\mathcal{E}(n,b,1)$ *on* V *is non-zero, we have*

$$wt(\beta_{0,0,}, \beta_{1,0}, \ldots, \beta_{n-1,0}) = n - 1,$$

$\beta_{i,j} = 0$ *for* $j \geq 1$, *and the absolute value of the correlation is* 1.

Proof. Let the output mask of the SB layer be

$$\Gamma_{\mathsf{SB}} = (\gamma_{i,j}) \in \mathbb{F}_{2^b}^{n\times n}.$$

To make the correlation non-zero, $\gamma_{i,j} = 0$ should hold if $\alpha_{i,j} = 0$. Next, we will show $\gamma_{j_0,0} = \gamma_{j_1,0}$. Since $s_{j_0,0} \oplus s_{j_1,0} = k_{j_0,0} \oplus k_{j_1,0}$, denote by

$$x = s_{j_0,0} \oplus k_{j_0,0} = s_{j_1,0} \oplus k_{j_1,0},$$

then

$$\begin{aligned}\Gamma_I \cdot X \oplus \Gamma_{\mathsf{SB}} \cdot S(X) &= a \cdot x \oplus a \cdot x \oplus \gamma_{j_0,0} \cdot S(x) \oplus \gamma_{j_1,0} \cdot S(x)\\ &= (\gamma_{j_0,0} \oplus \gamma_{j_1,0}) \cdot S(x),\end{aligned}$$

Since $S(x)$ is a permutation on $\mathbb{F}_{2^b}$, if $\gamma_{j_0,0} \oplus \gamma_{j_1,0} \neq 0$, the correlation of $(\gamma_{j_0,0} \oplus \gamma_{j_1,0}) \cdot S(x)$ is always 0. On the other hand, if $\gamma_{j_0,0} \oplus \gamma_{j_1,0} = 0$, the correlation is always 1.

Therefore, to make the correlation non-zero, according to Proposition 1, the output mask of $\mathcal{E}(n,b,1)$ should be

$$\Gamma_O = (M_{\mathsf{MC}}^{-1})^{\mathrm{T}} \Gamma_{\mathsf{SB}}.$$

Taking this into consideration, the absolute value of the correlation is always 1 which ends our proof. □

Lemma 2. *Let* $\mathcal{E}(n,b,r)$ *be an AES-like SPN cipher satisfying conditions (1) and (2). Let* $\Delta = k_{j_0,0}^{(0)} \oplus k_{j_1,0}^{(0)}$, *and define*

$$V_\Delta = \{(s_{i,j}^{(0)}) \in \mathbb{F}_{2^b}^{n\times n} | s_{j_0,0}^{(0)} \oplus s_{j_1,0}^{(0)} = \Delta\}.$$

For any $0 \neq a \in \mathbb{F}_{2^b}$, *let the input mask be*

$$\Gamma_I = (\alpha_{i,j})_{0\leq i,j\leq n-1}, \quad \alpha_{i,j} = \begin{cases} a & (i,j) = (j_0,0), (j_1,0),\\ 0 & \textit{otherwise}, \end{cases}$$

and for any $0 \neq d \in \mathbb{F}_{2^b}$, $(u,v) \in \mathbb{Z}_n \times \mathbb{Z}_n$, *let the output mask be*

$$\Gamma_O^{(u,v)} = (\beta_{i,j})_{0\leq i,j\leq n-1}, \quad \beta_{i,j} = \begin{cases} d & (i,j) = (u,v),\\ 0 & \textit{otherwise.} \end{cases}$$

Then for $\mathcal{E}(n,b,5)$ *without MixColumns in the last round, the correlation for* $\Gamma_I \rightarrow \Gamma_O^{(u,v)}$ *on* V_Δ *is always* 0.

Proof. The proof is divided into 2 halves (Fig.2 gives the procedure of the proof for the case $n = 4$ and $\pi_{\mathsf{SR}} = (0, 3, 2, 1)$):

Firstly, from the encryption direction, let the input mask be Γ_I as defined above. According to Lemma 1, the output mask of the first round has the following properties: there are $n - 1$ non-zero elements in the first column and all of the elements in other columns are zero.

Then, in the second round, the output mask of the SB layer keeps the pattern of the input mask and SR shifts the $n - 1$ non-zero elements to $n - 1$ different columns. Since MC has the MDS property, we can conclude that the output mask of the second round has the following properties: there exists 1 column such that all elements in this columns are 0's, and all elements in the other columns are non-zero.

In the third round, the output mask of the SB layer keeps the pattern of the input mask and SR shifts the $n-1$ zero elements to $n-1$ different columns, i.e., there are $n - 1$ non-zero elements in each column of the input mask of MC in the third round.

Using the same technique, we can find that from the decryption direction, there is only 1 non-zero element in each column of the output mask of MC in the third round.

Since the MC has the MDS property, i.e., the sum of the non-zero elements from both the input and output mask of MC is at least $n + 1$, the correlation of $\Gamma_I \to \Gamma_O^{(u,v)}$ is 0. □

4 Integrals for the AES-Like SPN Ciphers

Links between integrals and zero correlation linear hulls were first studied by Bogdanov *et al.* at Asiacrypt 2012 [8], and then refined at CRYPTO 2015 [36]. In [36], Sun *et al.* proved that a zero correlation linear hull of a block cipher always implies the existence of an integral distinguisher which gives a novel way to construct integrals of a cipher. For example, the 4-round zero-correlation linear hull of the AES implies the following distinguisher: Let 15 bytes of the input take all possible values from $\mathbb{F}_{2^8}^{15}$ and the other 1 byte be constant, then each byte of the output before the MixColumns operation in the forth round takes each value from $\mathbb{F}_{2^8}$ exactly 2^{112} times.

This section mainly discusses the integral properties of the AES-like ciphers based on the links between zero correlation linear hulls and integrals. It was pointed at CRYPTO 2015 [36] that a zero-correlation linear hull always implies the existence of an integral, based on which we can get the following results.

Corollary 1. *Let $\mathcal{E}(n, b, r)$ be an AES-like SPN cipher satisfying conditions (1) and (2). Let $\Delta = k^{(0)}_{j_0,0} \oplus k^{(0)}_{j_1,0}$ and the input set be*

$$V_\Delta = \{(s^{(0)}_{i,j})_{0\le i,j\le n-1} \in \mathbb{F}_{2^b}^{n\times n} | s^{(0)}_{j_0,0} \oplus s^{(0)}_{j_1,0} = \Delta\}.$$

Then for each output byte of $\mathcal{E}(n, b, 5)$ without MixColumns, every value of $\mathbb{F}_{2^b}$ appears exactly $2^{(n^2-2)b}$ times, and the sum of every output byte of $\mathcal{E}(n, b, 5)$ with MixColumns is 0.

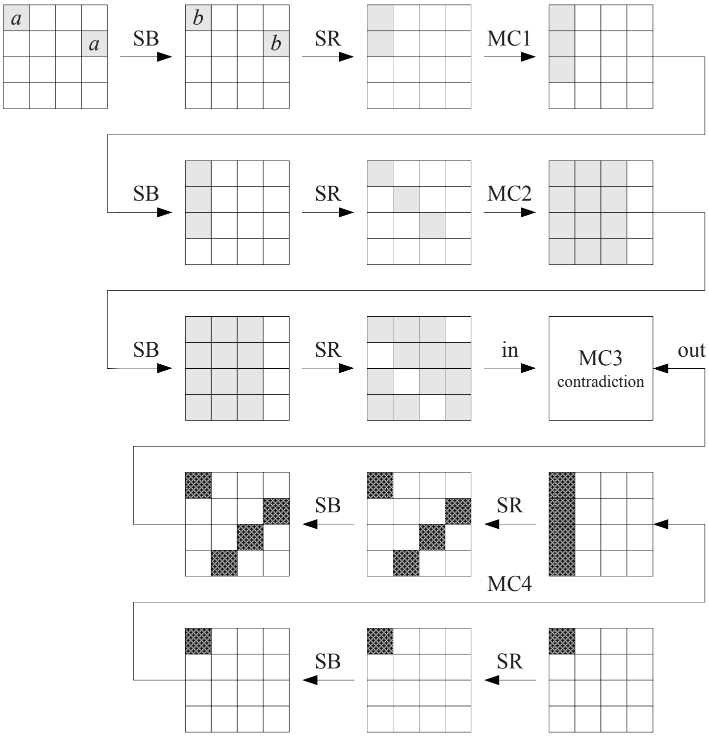

Fig. 2. Proof for the zero correlation linear hull of $\mathcal{E}(n, b, 5)$

Since there exists exactly one value in $\{0, 1, \cdots, 2^b - 1\}$ which is equal to $\delta = k^{(0)}_{j_0,0} \oplus k^{(0)}_{j_1,0}$, we have:

Theorem 1. *Denote by $\mathcal{E}(n, b, r)$ an r-round AES-like SPN cipher with MixColumns in the last round, where b and n are the sizes of the S-boxes and the MDS matrix, respectively. Let $(M^{-1}_{\mathsf{MC}})^T = (m^*_{i,j}) \in \mathbb{F}^{n\times n}_{2^b}$ be the transpose of the inverse of M_{MC}. Assume that there exists a triple (i, j_0, j_1) such that $m^*_{i,j_0} = m^*_{i,j_1}$. Then $\mathcal{E}(n, b, 5)$ can be distinguished from a random permutation $\mathcal{R}$ as follows: for $F \in \{\mathcal{E}(n, b, 5), \mathcal{R}\}$ and $\Delta = 0, 1, \ldots, 2^b - 1$, divide the whole input-output space into the following 2^b subsets:*

$$A^F_\Delta = \{(p, c)|c = F(p), p_{j_0,a_0} \oplus p_{j_1,a_1} = \Delta\},$$

where SR moves p_{j_0,a_0} and p_{j_1,a_1} to the same column, and let

$$T^F_\Delta = \sum_{(p,c)\in A^F_\Delta} c.$$

If the S-boxes applied to p_{j_0,a_0} and p_{j_1,a_1} are identical, there always exists a Δ such that $T^{\mathcal{E}(n,b,5)}_\Delta = 0$, while for random permutations, this happens with *probability* $1-(1-2^{-n^2b})^{2^b} \approx 2^{-(n^2-1)b}$. *Furthermore, we can deduce that the value of* $k_{j_0,a_0} \oplus k_{j_1,a_1}$ *is* Δ.

This theorem can be clearly deduced from Corollary 1 above. We can further give a direct proof as follows.

Proof. Without loss of generality, let $(M_{\mathsf{MC}}^{-1})^{\mathrm{T}} = (m_{i,j}^*)$ and $m_{0,0}^* = m_{0,1}^* = \mathtt{01}$. Let the input and output of the MixColumns operation be $(x_0, x_0, x_1, \ldots, x_{n-2})^{\mathrm{T}}$ and $(y_0, y_1, \ldots, y_{n-1})^{\mathrm{T}}$, respectively. Then we have

$$\begin{pmatrix} x_0 \\ x_0 \\ x_1 \\ \vdots \\ x_{n-2} \end{pmatrix} = \begin{pmatrix} \mathtt{01} * \cdots * * \\ \mathtt{01} * \cdots * * \\ * \ * \cdots * * \\ \cdots \\ * \ * \cdots * * \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{n-1} \end{pmatrix},$$

which implies

$$x_0 = y_0 \oplus l_1(y_1, \ldots, y_{n-1}) = y_0 \oplus l_2(y_1, \ldots, y_{n-1}),$$

where l_1 and l_2 are different linear functions on $(y_1, \ldots, y_{n-1})$. Accordingly, we always have

$$(l_1 \oplus l_2)(y_1, \ldots, y_{n-1}) = 0.$$

Since the dimension of the input is $n-1$, we conclude that y_0 is independent of $y_1, \ldots, y_{n-1}$, i.e., the number of possible values for $(y_1, \ldots, y_{n-1})$ is $2^{(n-2)b}$. Thus the output of the first round can be divided into the following $2^{(n-2)b}$ subsets: the last $n-1$ bytes of the first columns are fixed to $(y_1, \ldots, y_{n-1})$ and the other n^2-n+1 bytes take all possible value from $\mathbb{F}_{2^b}^{n^2-n+1}$. Taking the 4-round integral distinguisher into consideration, we conclude that the sum of the output of the fifth round with MixColumns is 0. □

Since a lot of AES-based ciphers adopt circulant MDS matrices, now we will list a result when a cipher uses a circulant MDS matrix:

Corollary 2. *Let* $\mathcal{E}(n,b,r)$ *be an AES-like SPN cipher which uses a circulant MDS matrix* $M_{\mathsf{MC}} = circ(m_0, m_1, \ldots, m_{n-1}) \in \mathbb{F}_{2^b}^{n\times n}$. *Denote by* $(M_{\mathsf{MC}}^{-1})^T = circ(m_0^*, m_1^*, \ldots, m_{n-1}^*)$ *the transpose of the inverse of* M_{MC}. *If there exists a* (j_0, j_1) *where* $j_0 \neq j_1$ *such that* $m_{j_0}^* = m_{j_1}^*$, *then the plaintext-ciphertext space of* $\mathcal{E}(n,b,5)$ *can be divided into* 2^{nb} *subsets* A_Δ *and* $|A_\Delta| = 2^{(n^2-n)b}$, *and there exists a* Δ *such that the sum of ciphertexts in* A_Δ *is* 0. *Moreover, some sub-keys can also be deduced from the partition.*

5 Application to Hashing Schemes

To apply these results to block ciphers directly, we need to know the difference of the corresponding sub-key bytes which is impossible in most cases. However, if the cipher is used as a building block of a hash function and the chain value acts as the key, we can always get a new distinguisher of the hash function based on these new observations. We use Whirlpool [2] as an example in this section.

5-Round Distinguisher for Whirlpool. Whirlpool [2] is a hash function proposed by Barreto and Rijmen as a candidate for the NESSIE project. It iterates the Miyaguchi-Preneel hashing scheme over t padded message blocks m_i, $0 \leq i \leq t-1$, using the dedicated 512-bit block cipher W:

$$H_i = W_{H_{i-1}}(m_{i-1}) \oplus H_{i-1} \oplus m_{i-1}, \quad i = 1, 2, \ldots, t.$$

The W block cipher only employs one S-box, and the SR and the MC are defined as follows:

$$\begin{aligned} \pi_{\mathsf{SR}} &= (0, 1, 2, 3, 4, 5, 6, 7), \\ M_{\mathsf{MC}} &= \mathrm{circ}(\mathtt{01}, \mathtt{01}, \mathtt{04}, \mathtt{01}, \mathtt{08}, \mathtt{05}, \mathtt{02}, \mathtt{09}). \end{aligned}$$

Notice that the SR of Whirlpool applies to columns and MC applies to rows, respectively.

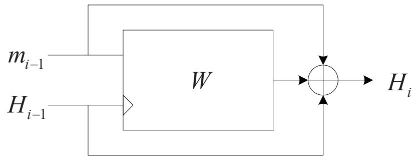

Fig. 3. The structure of Whirlpool Hash Function.

Noting that the matrix

$$(M_{\mathsf{MC}}^{-1})^{\mathrm{T}} = \mathrm{circ}(\mathtt{04}, \mathtt{3E}, \mathtt{CB}, \mathtt{C2}, \mathtt{C2}, \mathtt{A4}, \mathtt{0E}, \mathtt{AE}),$$

has two identical elements in each row, according to Theorem 1, we have the following distinguishing property for Whirlpool:

Corollary 3. *Let* $V_1 = \{(p_{i,j}) \in \mathbb{F}_{2^8}^{8\times 8} | p_{0,3} \oplus p_{0,4} = h_{0,3}^{(0)} \oplus h_{0,4}^{(0)}\}$. *Then for Whirlpool reduced to* 5 *rounds, the sum of all the outputs is* 0.

Although this distinguisher covers less rounds than the rebound attack [27], our result shows some new features of Whirlpool that could be exploited in the future. From the direct proof of Theorem 1, the key point is that the outputs of the first round could be divided into some known structures which lead to 4-round integrals. Therefore we have the following property:

Corollary 4. *Let* $V_2 = \{(p_{i,j}) \in \mathbb{F}_{2^8}^{8\times 8} | \mathtt{AE} \cdot S(p_{0,0} \oplus h_{0,0}^{(0)}) = \mathtt{04} \cdot S(p_{1,1} \oplus h_{1,1}^{(0)})\}$. *Then for Whirlpool reduced to* 5 *rounds, the sum of all the outputs is* 0.

Proof. Let the input of the first column to the first MixColumns be $X = (x_0, \ldots, x_7)^{\mathrm{T}}$ and $Y = (y_0, \ldots, y_7)^{\mathrm{T}}$ be the corresponding output. Then $x_0 =$

$S(p_{0,0} \oplus h_{0,0}^{(0)})$, $x_1 = S(p_{1,1} \oplus h_{1,1}^{(0)})$ and we have $\texttt{AE} \cdot x_0 = \texttt{04} \cdot x_1$. Since $X = M_{\mathsf{MC}}^{-1} Y$, therefore,

$$\begin{cases} x_0 = \texttt{04} \cdot y_0 \oplus \texttt{3E} \cdot y_1 \oplus \texttt{CB} \cdot y_2 \oplus \texttt{C2} \cdot y_3 \oplus \texttt{C2} \cdot y_4 \oplus \texttt{A4} \cdot y_5 \oplus \texttt{0E} \cdot y_6 \oplus \texttt{AE} \cdot y_7 \\ x_1 = \texttt{AE} \cdot y_0 \oplus \texttt{04} \cdot y_1 \oplus \texttt{3E} \cdot y_2 \oplus \texttt{CB} \cdot y_3 \oplus \texttt{C2} \cdot y_4 \oplus \texttt{C2} \cdot y_5 \oplus \texttt{A4} \cdot y_6 \oplus \texttt{0E} \cdot y_7. \end{cases}$$

Consequently,

$$\begin{aligned} &\texttt{AE}(\texttt{3E} \cdot y_1 \oplus \texttt{CB} \cdot y_2 \oplus \texttt{C2} \cdot y_3 \oplus \texttt{C2} \cdot y_4 \oplus \texttt{A4} \cdot y_5 \oplus \texttt{0E} \cdot y_6 \oplus \texttt{AE} \cdot y_7) \\ =\ &\texttt{04}(\texttt{04} \cdot y_1 \oplus \texttt{3E} \cdot y_2 \oplus \texttt{CB} \cdot y_3 \oplus \texttt{C2} \cdot y_4 \oplus \texttt{C2} \cdot y_5 \oplus \texttt{A4} \cdot y_6 \oplus \texttt{0E} \cdot y_7), \end{aligned}$$

which implies that there exists a linear function l such that

$$y_4 = l(y_1, y_2, y_3, y_5, y_6, y_7).$$

Since the dimension of the input is $n - 1$, we know that y_0 is independent of $y_1, \ldots, y_7$. On the other hand, as in the AES, we always have a 4-round integral for Whirlpool. Therefore, we conclude that the sum of the outputs is 0. □

Furthermore, we can extend the results to the structures with different S-boxes and no constraints on the elements of $(M_{\mathsf{MC}}^{-1})^{\mathrm{T}}$.

Theorem 2. *In a Miyaguchi-Preneel hashing mode, if the block cipher adopts a* 5*-round AES-like structure, there always exists a subset* V *such that when the input takes all possible value in* V*, the sum of output is* 0.

Let the first two elements in the first column of the inverse MDS matrix be a_0 and a_1, and the input to these two positions be $S_0(p_{0,0} \oplus h_{0,0})$ and $S_1(p_{1,1} \oplus h_{1,1})$. For any $p_{0,0}$, we can always choose $p_{1,1}$ such that

$$a_1 S_0(p_{0,0} \oplus h_{0,0}) = a_0 S_1(p_{1,1} \oplus h_{1,1}).$$

Then the conclusion follows from the proof of Corollary 4.

6 Application to AES

AES is one of the most widely used block ciphers since 2000, and many cryptographic primitives adopt round-reduced AES as a building block. The first known integral distinguisher for the AES covers 3 rounds [12] which was later improved to a 4-round higher-order integral [17]. However, the technique that improved the 3-round integral to a 4-round one cannot be directly used to improve the integral from 4 rounds to 5 rounds. In the following, we will show that the improvement is possible provided the difference of some sub-key bytes is known.

Since for M_{MC} adopted in the AES, we have

$$(M_{\mathsf{MC}}^{-1})^{\mathrm{T}} = \begin{pmatrix} \texttt{0E} & \texttt{09} & \texttt{0D} & \texttt{0B} \\ \texttt{0B} & \texttt{0E} & \texttt{09} & \texttt{0D} \\ \texttt{0D} & \texttt{0B} & \texttt{0E} & \texttt{09} \\ \texttt{09} & \texttt{0D} & \texttt{0B} & \texttt{0E} \end{pmatrix} = \mathrm{circ}(\texttt{0E}, \texttt{09}, \texttt{0D}, \texttt{0B}),$$

i.e., the elements in each row are different from each other, it seems that we cannot construct such distinguishers for 5-round AES. However, since there are two 1's in each columns of $M_{\mathsf{MC}} = \mathrm{circ}(\mathtt{02}, \mathtt{03}, \mathtt{01}, \mathtt{01})$, we can construct a distinguisher for AES^{-1}, i.e., we can turn the chosen-plaintext distinguishers shown in Theorem 1 into a chosen-ciphertext one.

Lemma 3. *Let* $V = \{(x_{i,j}) \in \mathbb{F}_{2^8}^{4\times 4} | x_{0,0} \oplus x_{1,3} = k_{0,0} \oplus k_{1,3}\}$ *be the input set. Then for each output byte of* 5*-round* AES^{-1} *without MixColumns operation in the last round, every value of* $\mathbb{F}_{2^8}$ *appears* 2^{112} *times and the sum of every output byte of the* 5*-round* AES^{-1} *with MixColumns operation in the last round is* 0.

Theorem 3. 5*-round AES with MixColumns in the last round can be distinguished from a random permutations as follows. Divide the whole input-output space into the following* 2^8 *subsets:*

$$A_{\Delta} = \{(p, c) | c_{0,0} \oplus c_{1,3} = \Delta\},$$

and let

$$T_{\Delta} = \sum_{(p,c)\in A_{\Delta}} p.$$

Then there exists a Δ *such that* $k_{0,0} \oplus k_{1,3} = \Delta$ *and* $T_{\Delta} = 0$*. For random permutations, this happens with probability* $1 - (1 - 2^{-128})^{2^8} \approx 2^{-120}$.

To the best of our knowledge, Theorem 3 gives the best distinguisher of the AES with respect to the rounds it covers. Since the AES adopts a circulant MDS matrix, we can get many other different distinguishers by dividing the whole set into different subsets. For example,

Corollary 5. 5*-round AES with MixColumns in the last round can be distinguished from a random permutation as follows. Divide the whole input-output space into the following* 2^{32} *subsets:*

$$A_{\alpha,\beta,\gamma,\phi} = \{(p, c) | c_{0,0} \oplus c_{1,3} = \alpha, c_{0,1} \oplus c_{3,2} = \beta, c_{1,2} \oplus c_{2,1} = \gamma, c_{2,0} \oplus c_{3,3} = \phi\},$$

and let

$$T_{\alpha,\beta,\gamma,\phi} = \sum_{(p,c)\in A_{\alpha,\beta,\gamma,\phi}} p.$$

Then there exists an $(\alpha, \beta, \gamma, \phi) \in \mathbb{F}_{2^8}^4$ *such that* $T_{\alpha,\beta,\gamma,\phi} = 0$*. For random permutations, this happens with probability* $1 - (1 - 2^{-128})^{2^{32}} \approx 2^{-96}$.

7 Conclusion

Distinguishing attacks on AES-like SPN structures are covered extensively in the literature. For example, we already have 4-round zero-correlation linear hulls for AES-like structures without MixColumns in the last round and 4-round integral distinguishers for AES-like structures with MixColumns in the last round. Note that these distinguishers do not depend on which S-box and MDS matrix are used in the cipher. This paper gives some new insights on such ciphers especially with detailed S-boxes and MDS matrices.

Firstly, we observe that if there are two identical elements in a row of the transpose of the inverse matrix of the MixColumns operation, and the S-boxes used in these two positions are identical, then we can construct some 5-round zero-correlation linear hull for a 5-round AES-like SPN structure provided some differences of the sub-key bytes are known. Then, under the same setting, and based on the link between zero-correlation linear hulls and integrals, we construct 5-round integrals for such AES-like SPN structures both with and without the MixColumns operation in the last round. These results show that such 5-round AES-like SPN structures can be theoretically distinguished from random permutations.

Secondly, in a hashing scheme where the chaining value serves as the secret key in block ciphers, we can further remove the constraint on the matrices and S-boxes. We apply the new results to the Whirlpool hash function and construct 5-round integral-like distinguishers.

Furthermore, since these results do not apply to the AES directly, we find that although we cannot build a distinguisher in a chosen-plaintext mode, we can construct a 5-round distinguisher for the AES in the chosen-ciphertext mode which is the best distinguishing attack for the AES with respect to the number of rounds it covers.

Our results show that despite the key schedule, there may be some difference between the security margins of round-reduced AES under chosen-plaintext attacks and under chosen-ciphertext attacks. Since we can distinguish 5-round AES from random permutations, some dedicated cryptographic schemes should be carefully investigated to guarantee the security claims. Furthermore, when we design an AES-like cipher, it is better to choose those MDS matrices M_{MC} such that both M_{MC} and M_{MC}^{-1} do not have identical elements in the same columns.

Now that we get some new features of 5-round AES, we leave as an open problem whether one could mount better key-recovery attack against round-reduced AES or some other schemes based on the AES-like SPN structure.

Acknowledgment

The authors would like to thank the anonymous reviewers for their useful comments, and Ruilin Li, Shaojing Fu, Wentao Zhang and Ming Duan for fruitful discussions.

References

1. E. Andreeva, B. Bilgin, A. Bogdanov, A. Luykx, F. Mendel, B. Mennink, N. Mouha, Q. Wang, K. Yasuda. PRIMATEs v1.02 Submission to the CAESAR Competition. http://competitions.cr.yp.to/round2/primatesv102.pdf

2. P. Barreto, V. Rijmen. NESSIE proposal: WHIRLPOOL (2000). `https://www.cosic.esat.kuleuven.be/nessie/`
3. E. Biham, A. Biryukov, A. Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. EUROCRYPT 1999, LNCS 1592, pp. 12–23, Springer-Verlag, 1999.
4. E. Biham, A. Shamir: Differential Cryptanalysis of the Data Encryption Standard. Springer–Verlag, 1993.
5. A. Biryukov, D. Khovratovich. PAEQ v1. `http://competitions.cr.yp.to/round1/paeqv1.pdf`
6. A. Biryukov, A. Shamir: Structural Cryptanalysis of SASAS. Advances in Cryptology — EUROCRYPT 2001, LNCS 2045, pp. 394–405, Springer–Verlag, 2001.
7. A. Bogdanov, D. Khovratovich, C. Rechberger: Biclique Cryptanalysis of the Full AES. In: D. H. Lee, X. Wang(eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 344–371. Springer, Heidelberg (2011)
8. A. Bogdanov, G. Leander, K. Nyberg and M. Wang. Integral and Multidimensional Linear Distinguishers with Correlation Zero. ASIACRYPT 2012, LNCS 7658, pp. 244–261, Springer–Verlag, 2012.
9. A. Bogdanov, V. Rijmen. Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. Designs, Codes and Cryptography, 70(3), pp. 369–383, 2014.
10. CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness. `http://competitions.cr.yp.to/caesar.html`
11. J. Daemen, L. R. Knudsen, V. Rijmen. The Block Cipher Square. Fast Software Encryption 1997, LNCS 1267, pp. 149–165, Springer–Verlag, 1997.
12. J. Daemen, V. Rijmen: The design of Rijndael: AES—the Advanced Encryption Standard. Springer, Heidelberg (2002)
13. N. Datta, M. Nandi. ELmD v2.0. `http://competitions.cr.yp.to/round2/elmdv20.pdf`
14. H. Demirci, A. Selçuk: A Meet-in-the-Middle Attack on 8-Round AES. In: K. Nyberg (ed.) FSE 2008. LNCS, vol. 5086, pp. 116–126. Springer, Heidelberg (2008)
15. H. Demirci, İ. Taşkın, M. Çoban, A. Baysal: Improved Meet-in-the-Middle Attacks on AES. In: Roy, B., Sendrier, N. (eds.) INDOCRYPT 2009. LNCS, vol. 5922, pp. 144–156. Springer, Heidelberg (2009)
16. P. Derbez, P.A. Fouque, J. Jean. Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting. EUROCRYPT 2013, LNCS 7881, pp. 371–387, 2013.
17. N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, D. Whiting: Improved Cryptanalysis of Rijndael. FSE 2000, LNCS 1978, pp. 213–230, Springer-Verlag, 2001.
18. P. Fouque, J. Jean, T. Peyrin: Structural Evaluation of AES and Chosen-Key Distinguisher of 9-Round AES-128. In R. Canetti and J. A. Garay (Eds.): CRYPTO 2013, LNCS, Vol. 8042, pp. 183–203, Springer, Heidelberg (2013).
19. H. Gilbert. A Simplified Representation of AES. In P. Sarkar and T. Iwata (Eds.): ASIACRYPT 2014, PART I, LNCS 8873, pp. 200–222, 2014.
20. H. Gilbert, M. Minier: A Collision Attack on 7 Rounds of Rijndael. In: AES Candidate Conference, pp. 230–241 (2000)
21. Y. Hatano, H. Sekine, T. Kaneko. Higher Order Differential Attack of Camellia(II). SAC 2002, LNCS 2595, pp. 129–146, 2003.
22. L.R. Knudsen. Truncated and Higher Order Differentials. Fast Software Encryption 1994, LNCS 1008, pp. 196–211. Springer, Heidelberg (1995)

23. L.R. Knudsen. DEAL — A 128-bit Block Cipher. Department of Informatics, University of Bergen, Norway. Technical report, 1998.
24. L.R. Knudsen, V. Rijmen. Known-Key Distinguishers for Some Block Ciphers. In K. Kurosawa (Ed.): ASIACRYPT 2007, LNCS 4833, pp. 315–324, 2007.
25. L.R. Knudsen, D. Wagner. Integral Cryptanalysis. FSE 2002, LNCS 2365, pp. 112–127, Springer–Verlag, 2002.
26. X. Lai. Higher Order Derivatives and Differential Cryptanalysis. Communications and Cryptography: Two Sides of One Tapestry, 227 (1994)
27. M. Lamberger, F. Mendel, M. Schläffer, C. Rechberger, V. Rijmen: The Rebound Attack and Subspace Distinguishers: Application to Whirlpool. J. Cryptology (JOC) 28(2): 257–296 (2015)
28. P. Li, B. Sun, C. Li.: Integral Cryptanalysis of ARIA. Inscrypt 2009, LNCS 6151, pp. 1–14, 2010.
29. S. Lucks: The Saturation Attack — A Bait for Twofish. FSE 2001, LNCS 2355, pp. 1–15, Springer–Verlag, 2002.
30. J. Lu, O. Dunkelman, N. Keller, J. Kim: New Impossible Differential Attacks on AES. In: D.R. Chowdhury, V. Rijmen, A. Das (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 279–293. Springer, Heidelberg (2008)
31. H. Mala, M. Dakhilalian, V. Rijmen, M. Modarres-Hashemi: Improved Impossible Differential Cryptanalysis of 7-Round AES-128. In: G. Gong, K.C. Gupta (eds.) INDOCRYPT 2010. LNCS, vol. 6498, pp. 282–291. Springer, Heidelberg (2010)
32. M. Matsui. Linear Cryptanalysis Method for DES Cipher. EUROCRYPT 1993, LNCS 765, pp. 386–397, Springer–Verlag, 1993.
33. R. Phan. Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES). 33–38, Information Processing Letters, Volume 91, Number 1, 16 July 2004.
34. B. Sun, R. Li, L. Qu, C. Li. SQUARE Attack on Block Ciphers with Low Algebraic Degree. Science China Information Sciences 53(10), pp. 1988–1995, 2010.
35. B. Sun, M. Liu, J. Guo, V. Rijmen, R. Li.: Provable Security Evaluation of Structures against Impossible Differential and Zero Correlation Linear Cryptanalysis. EUROCRYPT 2016, Part I, LNCS 9665, pp. 196–213, 2016.
36. B. Sun, Z. Liu, V. Rijmen, R. Li, L. Cheng, Q. Wang, H. Alkhzaimi, C. Li.: Links Among Impossible Differential, Integral and Zero Correlation Linear Cryptanalysis. CRYPTO 2015, Part I, LNCS 9215, pp. 95–115, 2015.
37. Y. Todo: Structural Evaluation by Generalized Integral Property. EUROCRYPT 2015. LNCS 9056, pp. 287–314, 2015.
38. Y. Todo. Integral Cryptanalysis on Full MISTY1. CRYPTO 2015, Part I, LNCS 9215, pp. 413–432, 2015.
39. H. Wu, B. Preneel. A Fast Authenticated Encryption Algorithm. `http://competitions.cr.yp.to/round1/aegisv1.pdf`