Revisiting The Multiple-of Property for SKINNY: The Exact Computation of the number of right pairs

Hanbeom Shin[1], Insung Kim[1], Sunyeop Kim[1], Seonggyeom Kim[2], Deukjo Hong[3] Jaechul Sung[4], and Seokhie Hong[1]

[1] Korea University, Seoul 02841, South Korea
[2] Samsung Electronics, Hwaseong 18448, South Korea
[3] Jeonbuk National University, Jeonju 54896, South Korea
[4] University of Seoul, Seoul 02504, South Korea

Abstract. At EUROCRYPT 2017, Grassi et al. proposed the multiple-of-8 property for 5-round AES, where the number n of right pairs is a multiple of 8. At ToSC 2019, Boura et al. generalized the multiple-of property for a general SPN block cipher and applied it to block cipher SKINNY.
In this paper, we present that n is not only a multiple but also a fixed value for SKINNY. Unlike the previous proof of generalization of multiple-of property using equivalence class, we investigate the propagation of the set to compute the exact number n. We experimentally verified that presented property holds. We extend this property one round more using the lack of the whitening key on the SKINNY and use this property to construct 6-round distinguisher on SKINNY-64 and SKINNY-128. The probability of success of both distinguisher is almost 1 and the total complexities are 2^{16} and 2^{32} respectively. We verified that this property only holds for SKINNY, not for AES and MIDORI, and provide the conditions under which it exists for AES-like ciphers.

Keywords: Multiple-of Property · Structural-Differential Property · SKINNY · AES-like cipher.

1 Introduction

SKINNY is a lightweight tweakable block cipher presented at CRYPTO 2016 [1]. It has flexible block, tweak size and has a structure which internal state is represented as a 4 × 4 square array of cells. It provides good performance on both hardware and software implementations. It can also benefit from very efficient threshold implementations for side-channel protection.

The multiple-of property states that the number n of right pairs is multiple of a natural number other than 1 and was presented first for 5-round AES [8]. Boura et al. [4] generalized the multiple-of property for general SPN(Substitution

Table 1. Comparisons of Distinguishers on 6-Round SKINNY-64 and SKINNY-128

Cryptanalysis	Block Size	Distinguished Rounds	Total Complexity	Probability of Success of the Distinguisher	Source
Multiple-of property	64-bit	5	2^{20}	0.75	[4]
	128-bit		2^{40}	0.75	
	64-bit	5	2^{16}	0.875	Section 3
	128-bit		2^{32}	0.875	
Fixed-value property	64-bit	6	2^{16}	0.99	Section 5
	128-bit		2^{32}	0.99	

Permutation Network) block cipher and applied to various SPN block ciphers. Their work also showed that the multiple-of property holds for 5-round SKINNY.

In this paper, we present that the number n of right pairs in the multiple-of property is not only a multiple but also a fixed value for SKINNY. In particular, n is significantly different from the expected value for random permutation. Unlike the previous proof of generalization of multiple-of property, we investigate the propagation of the set to compute the exact n. Furthermore, we experimentally verified that proposed property holds.

We extend this property by one round, utilizing the absence of the whitening key on the SKINNY. Then, we construct 6-round distinguishers based on this property. The distinguisher on 6-round SKINNY-128 distinguishes from random permutation with 2^{32} total complexity and a probability of success of this distinguisher of almost 1, and the distinguisher on 6-round SKINNY-64 distinguishes from random permutation with 2^{16} total complexity and a probability of success of this distinguisher of almost 1. Our results are summarized in Table 1.

We present that this property holds for SKINNY but not for AES and MIDORI. We also investigate the propagation of the set to compute the exact n for AES and MIDORI. We generalize this property for AES-like SPN block cipher which use matrix multiplication. In conclusion, we show that this property is related to the branch number of the MixColumns matrix.

The rest of the paper is organized as follows. A description of the SKINNY and basic definitions on the multiple-of property are recalled in Section 2. Section 3 defines subspaces and the subspace trail for SKINNY. Section 4 then present that the number of right pairs in the multiple-of property is not only a multiple but also a fixed value for SKINNY. Section 5 constructs distinguishers on 6 rounds of SKINNY. Section 6 shows that the property hold only for SKINNY but not for AES and MIDORI, and generalize this property for AES-like SPN block cipher which use matrix multiplication. Lastly, the conclusion is given in Section 7.

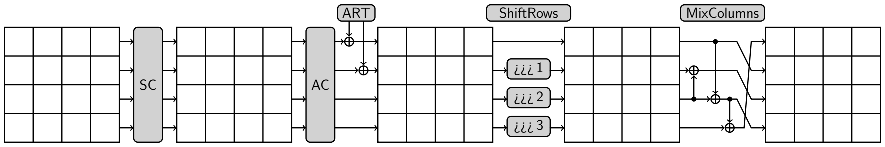

Fig. 1. The SKINNY round function applies five different transformations: SubCells(SC), AddConstants(AC), AddRoundTweakey(ART), ShiftRows(SR), and MixColumns(MC)

2 Preliminaries

2.1 Symbols and Notations

We denote the size of S-box by d. Let $\mathbb{K} = \mathbb{F}_2^d$. We define $\mathbb{K}^l$ as the set of all l-vectors over $\mathbb{K}$ for $l > 0$. We define $\mathbb{K}^{m \times k}$ as the set of all $m \times k$-matrices over $\mathbb{K}$ for $m, k > 0$. If $l = m \times k$, we consider that $\mathbb{K}^l$ and $\mathbb{K}^{m \times k}$ are equivalent. We call the element of the array a cell.

A subspace of $\mathbb{K}^l$ is a subset $\mathbb{V} \subseteq \mathbb{K}^l$ satisfying: non-emptiness, closure under addition and closure under scalar multiplication. We denote the canonical basis of $\mathbb{K}^{m \times k}$ with 1 in the i-th row, j-th column and 0 in all other cells by $e_{i,j}$ for $i \in \{0, ..., m-1\}$ and $j \in \{0, ..., k-1\}$. We denote the linear space formed by all linear combinations with coefficients in $\mathbb{K}$ of the vectors $\mathbf{v_0}, ..., \mathbf{v_n} \in \mathbb{K}^l$ by $< \mathbf{v_0}, ..., \mathbf{v_n} >$. A coset of $\mathbb{V} \subseteq \mathbb{K}^l$ is a set of the form $\mathbb{V} \oplus \mathbf{a} = \{\mathbf{v} \oplus \mathbf{a} \mid \mathbf{v} \in \mathbb{V}\}$ where $\mathbf{a} \in \mathbb{K}^l$, i.e., affine subspace of $\mathbb{K}^l$.

2.2 SKINNY

SKINNY was proposed at CRYPTO 2016 [2]. SKINNY is denoted by SKINNY-64 for 64-bit block size and by SKINNY-128 for 128-bit block size, respectively. It is convenient to represent a state vector of SKINNY as a 4×4 array whose each cell is a nibble (in SKINNY-64) or a byte (in SKINNY-128).

The round function of SKINNY is consisted of five operations in the following order: SubCells, AddConstants, AddRoundTweakey, ShiftRows and MixColumns (see Figure 1).

SubCells(SC). A d-bit invertible S-box is applied to every cell of the cipher internal state($d = 4$ for SKINNY-64 and $d = 8$ for SKINNY-128).

AddConstants(AC). Round constants are bitwise exclusive-ored to first, second and third cells of the first column of the cipher internal state.

AddRoundTweakey(ART). The first and second rows of all tweakey arrays are extracted and bitwise exclusive-ored to first and second rows of the cipher internal state.

ShiftRows(SR). Second, third, and fourth rows are rotated by 1, 2 and 3 positions to the right, respectively.

MixColumns(MC). Each column of internal state is multiplied by the following binary matrix M:

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

The number of rounds depends on the block size n_b and the tweakey size n_t. When $n_b = 64$, it uses 32 rounds for $n_t = n_b$, 36 rounds for $n_t = 2n_b$ and 40 rounds for $n_t = 3n_b$, and when $n_b = 128$, it uses 40 rounds for $n_t = n_b$, 48 rounds for $n_t = 2n_b$ and 56 rounds for $n_t = 3n_b$.

Since the property proposed in this paper are independent of the key schedule, the description of the key schedule is omitted.

2.3 Subspace Trail

The notion of the subspace trail cryptanalysis was proposed by Grassi et al. at ToSC 2016 [7] as a generalization of invariant subsapce [9] [10] and was applied to `AES` [5] and `PRINCE` [3] in [7] and [6] respectively.

Definition 1 (Subspace trail [7]). *Let $\mathsf{F} : \mathbb{K}^l \to \mathbb{K}^l$ be any map. Two linear subspaces $\mathbb{U}, \mathbb{V} \subseteq \mathbb{K}^l$ form a subspace trail if*

$$\forall \mathbf{a} \in \mathbb{K}^l, \exists \mathbf{b} \in \mathbb{K}^l : \mathsf{F}(\mathbb{U} \oplus \mathbf{a}) \subseteq \mathbb{V} \oplus \mathbf{b},$$

which is denoted by $\mathbb{U} \overset{\mathsf{F}}{\rightrightarrows} \mathbb{V}$. We call exact subspace trail if

$$\forall \mathbf{a} \in \mathbb{K}^l, \exists \mathbf{b} \in \mathbb{K}^l : \mathsf{F}(\mathbb{U} \oplus \mathbf{a}) = \mathbb{V} \oplus \mathbf{b}.$$

For example, we have trivial subspace trails $\{0\} \overset{\mathsf{F}}{\rightrightarrows} \{0\}$ and $\mathbb{U} \overset{\mathsf{F}}{\rightrightarrows} \mathbb{K}^l$. In this paper, we only consider exact subspace trails.

2.4 Multiple-of Property for `SKINNY`

The notion of the multiple-of property was proposed by Grassi et al. at EUROCRYPT 2017 [8] as an efficient method for constructing key independent distinguishers, and was subsequently generalized for a general SPN block cipher [4]. In this study, we focus on the multiple-of property for a general SPN block cipher.

Let $\mathbb{U}$ and $\mathbb{W}$ be subspaces of $\mathbb{K}^l$ and R be the round function of the block cipher. R^5 means 5-round encryption function for block cipher. For any 5-round SPN block cipher, the multiple-of property is defined as follows.

Definition 2 (Multiple-of property). *Let $\mathbf{a} \in \mathbb{K}^l$. We define*

$$n = \#\{\{p^0, p^1\} \mid \forall p^0, p^1 \in \mathbb{U} \oplus \mathbf{a}, \mathsf{R}^5(p^0) \oplus \mathsf{R}^5(p^1) \in \mathbb{W}\}.$$

If n is a multiple of a natural number other than 1, then the 5-round SPN cipher is called to have the multiple-of property. We denote a right pair as an unordered pair that satisfies this property.

For example, the multiple-of-8 property exists for the 5-round AES [8]. An example of multiple-of property for SKINNY is given follow [4].

Example 1 ([4]). Let R be the round function of SKINNY. There exist two 2-round subspace trails, $\mathbb{U}_i \overset{\mathsf{R}}{\rightrightarrows} \mathbb{V}_i \overset{\mathsf{R}}{\rightrightarrows} \mathbb{W}_i$ for $i \in \{0, 1\}$ where

$$\begin{aligned} \mathbb{U}_0 &= < \mathbf{e}_{\mathbf{1},\mathbf{1}}, \mathbf{e}_{\mathbf{1},\mathbf{2}}, \mathbf{e}_{\mathbf{1},\mathbf{3}}, \mathbf{e}_{\mathbf{3},\mathbf{1}}, \mathbf{e}_{\mathbf{3},\mathbf{3}} >, \\ \mathbb{V}_0 &= \mathsf{R}(\mathbb{U}_0), \\ \mathbb{W}_0 &= \mathsf{R}(\mathbb{V}_0) \end{aligned}$$

and

$$\begin{aligned} \mathbb{U}_1 &= < \mathbf{e}_{\mathbf{0},\mathbf{3}}, \mathbf{e}_{\mathbf{1},\mathbf{0}}, \mathbf{e}_{\mathbf{1},\mathbf{2}}, \mathbf{e}_{\mathbf{1},\mathbf{3}}, \mathbf{e}_{\mathbf{2},\mathbf{1}}, \mathbf{e}_{\mathbf{2},\mathbf{3}}, \mathbf{e}_{\mathbf{3},\mathbf{0}}, \mathbf{e}_{\mathbf{3},\mathbf{1}}, \mathbf{e}_{\mathbf{3},\mathbf{2}}, \mathbf{e}_{\mathbf{3},\mathbf{3}} >, \\ \mathbb{V}_1 &= \mathsf{R}(\mathbb{U}_1), \\ \mathbb{W}_1 &= \mathsf{R}(\mathbb{V}_1). \end{aligned}$$

Then

$$\#\{\{p^0, p^1\} \mid \forall p^0, p^1 \in \mathbb{U}_0 \oplus \mathbf{a},\ \mathsf{R}^5(p^0) \oplus \mathsf{R}^5(p^1) \in \mathbb{W}_1\} \equiv 0 \mod 4.$$

Example 1 is satisfied with both SKINNY-64 and SKINNY-128 respectively. This can be used to construct 5-round distinguisher on SKINNY. The distinguisher on 5-round SKINNY-64 distinguishes from random permutation with 2^{20} chosen plaintexts and probability of success of this distinguisher $(1-2^{-2}) = 0.75$, whereas the distinguisher on 5-round SKINNY-128 distinguishes from random permutation with 2^{40} chosen plaintexts and probability of success of this distinguisher $(1 - 2^{-2}) = 0.75$.

3 Subspace trail of SKINNY

In this Section, we define subspaces of $\mathbb{K}^{4\times4}$ for SKINNY. Moreover, we propose subspace trail for SKINNY to compute the exact number n of right pairs.

Definition 3. *For $i \in \{0, ..., 3\}$, with indices computed modulo 4, the column spaces $\mathbb{C}_i$, the diagonal spaces $\mathbb{D}_i$, the inverse-diagonal spaces $\mathbb{ID}_i$ and are mixed spaces $\mathbb{M}_i$ are defined as*

$$\begin{aligned} \mathbb{C}_i &= < \mathbf{e}_{\mathbf{0},\mathbf{i}}, \mathbf{e}_{\mathbf{1},\mathbf{i}}, \mathbf{e}_{\mathbf{2},\mathbf{i}}, \mathbf{e}_{\mathbf{3},\mathbf{i}} >, \\ \mathbb{D}_i &= \mathit{SR}(\mathbb{C}_i) = < \mathbf{e}_{\mathbf{0},\mathbf{i}}, \mathbf{e}_{\mathbf{1},\mathbf{i+1}}, \mathbf{e}_{\mathbf{2},\mathbf{i+2}}, \mathbf{e}_{\mathbf{3},\mathbf{i+3}} >, \\ \mathbb{ID}_i &= \mathit{SR}^{-1}(\mathbb{C}_i) = < \mathbf{e}_{\mathbf{0},\mathbf{i}}, \mathbf{e}_{\mathbf{1},\mathbf{i-1}}, \mathbf{e}_{\mathbf{2},\mathbf{i-2}}, \mathbf{e}_{\mathbf{3},\mathbf{i-3}} >, \\ \mathbb{M}_i &= \mathit{MC}(\mathbb{D}_i). \end{aligned}$$

For example, if $x_0, x_1, x_2, x_3 \in \mathbb{K}$,

$$\begin{bmatrix} x_0 & 0 & 0 & 0 \\ x_1 & 0 & 0 & 0 \\ x_2 & 0 & 0 & 0 \\ x_3 & 0 & 0 & 0 \end{bmatrix} \in \mathbb{C}_0, \begin{bmatrix} x_0 & 0 & 0 & 0 \\ 0 & x_1 & 0 & 0 \\ 0 & 0 & x_2 & 0 \\ 0 & 0 & 0 & x_3 \end{bmatrix} \in \mathbb{D}_0, \begin{bmatrix} x_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x_1 \\ 0 & 0 & x_2 & 0 \\ 0 & x_3 & 0 & 0 \end{bmatrix} \in \mathbb{ID}_0, \begin{bmatrix} x_0 & 0 & x_2 & x_3 \\ 0 & 0 & 0 & 0 \\ x_0 & x_1 & x_2 & 0 \\ x_0 & 0 & x_2 & 0 \end{bmatrix} \in \mathbb{M}_0.$$

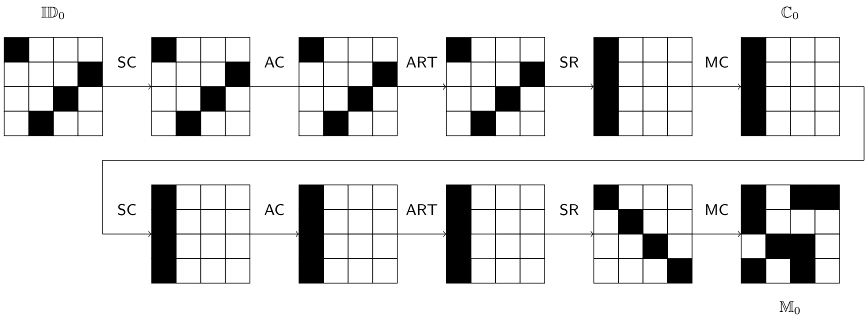

Fig. 2. 2-round Subspace Trail of SKINNY

If $I \subseteq \{0,1,2,3\}$,

$$\mathbb{C}_I = \bigoplus_{i \in I} \mathbb{C}_i, \mathbb{D}_I = \bigoplus_{i \in I} \mathbb{D}_i, \mathbb{ID}_I = \bigoplus_{i \in I} \mathbb{ID}_i, \mathbb{M}_I = \bigoplus_{i \in I} \mathbb{M}_i.$$

We propose the exact subspace trail for SKINNY by using the subspaces of Definition 3.

Lemma 1. *Let $I \subseteq \{0,1,2,3\}$ and R be the round function of SKINNY. Then*

$$\mathbb{ID}_I \overset{\mathsf{R}}{\rightrightarrows} \mathbb{C}_I \overset{\mathsf{R}}{\rightrightarrows} \mathbb{M}_I$$

is exact subspace trail for SKINNY.

For example, a case of $I = \{0\}$ can see in Figure 2. Lemma 1 is satisfied with both SKINNY-64 and SKINNY-128, simultaneously. We propose the new example of the multiple-of property for SKINNY that is different from Example 1 by using Definition 3.

Example 2. Let $I \subseteq \{0,1,2,3\}$, $J \subseteq \{0,1,2,3\}$, $|I| = 1$, $1 \leq |J| \leq 3$ and $\mathbf{a} \in \mathbb{K}^{4\times 4}$. Let R be the round function of SKINNY. Then we can have

$$\#\{\{p^0, p^1\} \mid \forall p^0, p^1 \in \mathbb{ID}_I \oplus \mathbf{a}, \mathsf{R}^5(p^0) \oplus \mathsf{R}^5(p^1) \in \mathbb{M}_J\} \equiv 0 \mod 8.$$

Example 2 is also satisfied with both SKINNY-64 and SKINNY-128, simultaneously. This can be used to construct 5-round distinguisher. The distinguisher on 5-round SKINNY-64 distinguishes from random permutation with 2^{16} chosen plaintexts and probability of success of this distinguisher $(1 - 2^{-3}) = 0.875$, whereas the distinguisher on 5-round SKINNY-128 distinguishes from random permutation with 2^{32} chosen plaintexts and probability of success of this distinguisher $(1 - 2^{-3}) = 0.875$. So Example 2 can distinguish between SKINNY and random permutation with a higher probability of success and fewer chosen plaintexts than Example 1.

4 The Exact Computation of the multiple-of property for 5-round `SKINNY`

4.1 The Exact Computation of the multiple-of property for 5-round `SKINNY-128`

In this section, we provide the exact computation of the number of right pairs. The computations are given in Theorem 1 and Theorem 2.

Theorem 1. *Let $I \subseteq \{0,1,2,3\}$, $J \subseteq \{0,1,2,3\}$, $|I| = 1$, $|J| = 3$ and $\mathbf{a} \in \mathbb{K}^{4\times 4}$. Let R be the round function of `SKINNY-128`. We define*

$$n = \#\{\{p^0, p^1\} \mid \forall p^0, p^1 \in \mathbb{ID}_I \oplus a, \mathsf{R}^5(p^0) \oplus \mathsf{R}^5(p^1) \in \mathbb{M}_J\}.$$

Then $n = (2^{16} - 1) \cdot 2^{31}$ or $n = (2^8 - 1) \cdot 2^{31}$.

By Lemma 1, every element of a coset of $\mathbb{ID}_I$ corresponds to every element of a coset of $\mathbb{M}_I$ after 2 rounds. This statement holds also in the similar way in the reverse direction: every element of $\mathbb{M}_J$ corresponds to every element of $\mathbb{ID}_J$ before 2 rounds. Thus it is sufficient to prove Lemma 2 in order to prove the Theorem 1.

Lemma 2. *Let $I \subseteq \{0,1,2,3\}$, $J \subseteq \{0,1,2,3\}$, $|I| = 1$, $|J| = 3$ and $\mathbf{a} \in \mathbb{K}^{4\times 4}$. Let R be the round function of `SKINNY-128`. We define*

$$n = \#\{\{p^0, p^1\} \mid \forall p^0, p^1 \in \mathbb{M}_I \oplus \mathbf{a}, \mathsf{R}(p^0) \oplus \mathsf{R}(p^1) \in \mathbb{ID}_J\}.$$

Then $n = (2^{16} - 1) \cdot 2^{31}$ or $n = (2^8 - 1) \cdot 2^{31}$.

Proof. *We consider only the case of $I = \{0\}$. The other cases of I can be proved in the similar way.*

Since $\mathbb{M}_I \oplus \mathbf{a} = \mathsf{MC}(\mathbb{D}_I \oplus \mathbf{b})$ for $\mathbf{b} = \mathsf{MC}^{-1}(\mathbf{a})$, considering all elements of $\mathbb{M}_I \oplus \mathbf{a}$ is equivalent to considering all elements of $\mathbb{D}_I \oplus \mathbf{b}$. We define X, Y, Z and W as the set that has all 2^8 possible 8-bit elements. We define c^i as constant element for $i > 0$. Then, $\mathbb{D}_I \oplus \mathbf{b}$, composed of 2^{32} elements, can be represented by

$$\begin{bmatrix} X & c^4 & c^7 & c^{10} \\ c^1 & Y & c^8 & c^{11} \\ c^2 & c^5 & Z & c^{12} \\ c^3 & c^6 & c^9 & W \end{bmatrix}.$$

After MC operation, $\mathbb{M}_I \oplus \mathbf{a} = \mathsf{MC}(\mathbb{D}_I \oplus \mathbf{b})$ can be represented by

$$\begin{bmatrix} X \oplus c^{13} & c^{17} & Z \oplus c^{21} & W \oplus c^{25} \\ X \oplus c^{14} & c^{18} & c^{22} & c^{26} \\ c^{15} & Y \oplus c^{19} & Z \oplus c^{23} & c^{27} \\ X \oplus c^{16} & c^{20} & Z \oplus c^{24} & c^{28} \end{bmatrix}.$$

Let S_8 be a S-box of `SKINNY-128`. For $i > 0$, we define X^i, Y^i, Z^i and W^i as the set which depends on X, Y, Z and W, respectively. For example, $X^1 = \mathsf{S}_8(X \oplus c^{13})$. After SC operation, $\mathsf{SC}(\mathbb{M}_I \oplus \mathbf{a})$ can be represented by

$$\begin{bmatrix} X^1 & c^{30} & Z^1 & W^1 \\ X^2 & c^{31} & c^{33} & c^{34} \\ c^{29} & Y^1 & Z^2 & c^{35} \\ X^3 & c^{32} & Z^3 & c^{36} \end{bmatrix}.$$

Because AC adds round constants to only first, second and third cells of first column and ART adds round tweakey to only first and second rows, after AC and ART operation, $\mathsf{ART} \circ \mathsf{AC} \circ \mathsf{SC}(\mathbb{M}_I \oplus \mathbf{a})$ can be represented by

$$\begin{bmatrix} X^1 \oplus c^{37} & c^{40} & Z^1 \oplus c^{42} & W^1 \oplus c^{43} \\ X^2 \oplus c^{38} & c^{41} & c^{43} & c^{45} \\ c^{39} & Y^1 & Z^2 & c^{35} \\ X^3 & c^{32} & Z^3 & c^{36} \end{bmatrix}.$$

After SR operation, $\mathsf{SR} \circ \mathsf{ART} \circ \mathsf{AC} \circ \mathsf{SC}(\mathbb{M}_I \oplus \mathbf{a})$ can be represented by

$$\begin{bmatrix} X^1 \oplus c^{37} & c^{40} & Z^1 \oplus c^{42} & W^1 \oplus c^{43} \\ c^{45} & X^2 \oplus c^{38} & c^{41} & c^{43} \\ Z^2 & c^{35} & c^{39} & Y^1 \\ c^{32} & Z^3 & c^{36} & X^3 \end{bmatrix}.$$

So after MC operation, $\mathsf{R}(\mathbb{M}_I \oplus \mathbf{a}) = \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{ART} \circ \mathsf{AC} \circ \mathsf{SC}(\mathbb{M}_I \oplus \mathbf{a})$ can be represented as

$$\begin{bmatrix} X^1 \oplus Z^2 \oplus c^{46} & Z^3 \oplus c^{50} & Z^1 \oplus c^{54} & X^3 \oplus Y^1 \oplus W^1 \oplus c^{58} \\ X^1 \oplus c^{47} & c^{51} & Z^1 \oplus c^{55} & W^1 \oplus c^{59} \\ Z^2 \oplus c^{48} & X^2 \oplus c^{52} & c^{56} & Y^1 \oplus c^{60} \\ X^1 \oplus Z^2 \oplus c^{49} & c^{53} & Z^1 \oplus c^{57} & Y^1 \oplus c^{61} \end{bmatrix}.$$

It is one round `SKINNY` encryption of $\mathbb{M}_I \oplus \mathbf{a}$.

The remainder of the proof is to count the number n of right pairs for each case of J. We consider only the cases of $J = \{1, 2, 3\}$ and $J = \{0, 1, 2\}$. The other cases of J can be proved in the similar way.

Let $J^c = \{0, 1, 2, 3\} - J$. For $\mathsf{R}(p^0) \oplus \mathsf{R}(p^1) \in \mathbb{ID}_J$, J^c inverse diagonals of $\mathsf{R}(p^0) \oplus \mathsf{R}(p^1)$ is zero. To be this, J^c inverse diagonals of $\mathsf{R}(p^0)$ and $\mathsf{R}(p^1)$ must be the same.

***Case 1** : $J = \{1, 2, 3\}$.*

J^c inverse diagonals of $\mathsf{R}(\mathbb{M}_I \oplus a)$ is represented by

$$(X^1 \oplus Z^2 \oplus c^{46}, W^1 \oplus c^{59}, c^{56}, c^{53}).$$

Let $x_0^1, x_1^1 \in X^1$, $z_0^2, z_1^2 \in Z^2$ and $w_0^1, w_1^1 \in W^1$. For $p^0, p^1 \in \mathbb{M}_I \oplus \mathbf{a}$, J^c inverse diagonals of $\mathsf{R}(p^0)$ and $\mathrm{R}(p^1)$ can be represented by

$$(x_0^1 \oplus z_0^2 \oplus c^{46}, w_0^1 \oplus c^{59}, c^{56}, c^{53})$$

and

$$(x_1^1 \oplus z_1^2 \oplus c^{46}, w_1^1 \oplus c^{59}, c^{56}, c^{53}).$$

For J^c inverse diagonal of $\mathsf{R}(p^0)$ and $\mathsf{R}(p^1)$ to be the same, it must be

$$\begin{aligned} x_0^1 \oplus z_0^2 =& x_1^1 \oplus z_1^2, \\ w_0^1 =& w_1^1. \end{aligned}$$

Let $x_0, x_1 \in X$, $z_0, z_1 \in Z$ and $w_0, w_1 \in W$. For $i \in \{0,1\}$, since $x_i^1 = \mathsf{S}_8(x_i \oplus c^{13})$, $z_i^2 = \mathsf{S}_8(z_i \oplus c^{23})$ and $w_i^1 = \mathsf{S}_8(w_i \oplus c^{25})$, we have

$$\begin{aligned} \mathsf{S}_8(x_0 \oplus c^{13}) \oplus \mathsf{S}_8(z_0 \oplus c^{23}) =& \mathsf{S}_8(x_1 \oplus c^{13}) \oplus \mathsf{S}_8(z_1 \oplus c^{23}), \\ \mathsf{S}_8(w_0 \oplus c^{25}) =& \mathsf{S}_8(w_0 \oplus c^{25}). \end{aligned}$$

Since S_8 is invertible, we have

$$\begin{aligned} \mathsf{S}_8(x_0 \oplus c^{13}) \oplus \mathsf{S}_8(z_0 \oplus c^{23}) =& \mathsf{S}_8(x_1 \oplus c^{13}) \oplus \mathsf{S}_8(z_1 \oplus c^{23}), \\ w_0 =& w_1. \end{aligned} \tag{1}$$

For any element (x_0, y_0, z_0, w_0) of set (X, Y, Z, W), there are exactly $2^{16} - 1$ other elements (x_1, y_1, z_1, w_1) that satisfy (1). There are 2^{32} possible values for (x_0, y_0, z_0, w_0) and except for reordering, the number of right pairs is always $(2^{16} - 1) \cdot 2^{31}$.

***Case 2** : $J = \{0, 1, 2\}$.*

Case 2 can also be proved by the similar way with Case 1. J^c inverse diagonals of $\mathsf{R}(\mathbb{M}_I \oplus \mathbf{a})$ is represented by

$$(X^3 \oplus Y^1 \oplus W^1 \oplus c^{58}, Z^1 \oplus c^{55}, X^2 \oplus c^{52}, X^1 \oplus Z^2 \oplus c^{49}).$$

For positive integer i and j, let $x_i^j \in X^j$, $y_i^j \in Y^j$, $z_i^j \in Z^j$ and $w_i^j \in W^j$. For $p^0, p^1 \in \mathbb{M}_I \oplus \mathbf{a}$, J^c inverse diagonals of $\mathsf{R}(p^0)$ and $\mathsf{R}(p^1)$ can be represented by

$$(x_0^3 \oplus y_0^1 \oplus w_0^1 \oplus c^{58}, z_0^1 \oplus c^{55}, x_0^2 \oplus c^{52}, x_0^1 \oplus z_0^2 \oplus c^{49})$$

and

$$(x_1^3 \oplus y_1^1 \oplus w_1^1 \oplus c^{58}, z_1^1 \oplus c^{55}, x_1^2 \oplus c^{52}, x_1^1 \oplus z_1^2 \oplus c^{49}).$$

For J^c inverse diagonals of $\mathsf{R}(p^0)$ and $\mathsf{R}(p^1)$ to be the same, it must be

$$\begin{aligned} x_0^3 \oplus y_0^1 \oplus w_0^1 =& x_1^3 \oplus y_1^1 \oplus w_1^1, \\ z_0^1 =& z_1^1, \\ x_0^2 =& x_1^2, \\ x_0^1 \oplus z_0^2 =& x_1^1 \oplus z_1^2. \end{aligned}$$

For $i \in \{0,1\}$, let $x_i \in X$, $y_i \in Y$, $z_i \in Z$ and $w_i \in W$. Since

$$\begin{aligned}
x_i^1 =& \mathsf{S}_8(x_i \oplus c^{13}),\\
x_i^2 =& \mathsf{S}_8(x_i \oplus c^{14}),\\
x_i^3 =& \mathsf{S}_8(x_i \oplus c^{16}),\\
y_i^1 =& \mathsf{S}_8(y_i \oplus c^{19}),\\
z_i^1 =& \mathsf{S}_8(z_i \oplus c^{21}),\\
z_i^2 =& \mathsf{S}_8(z_i \oplus c^{23}),\\
w_i^1 =& \mathsf{S}_8(w_i \oplus c^{25}),
\end{aligned}$$

we have

$$\begin{aligned}
\mathsf{S}_8(x_0 \oplus c^{16}) \oplus \mathsf{S}_8(y_0 \oplus c^{19}) \oplus \mathsf{S}_8(w_0 \oplus c^{25}) =& \mathsf{S}_8(x_1 \oplus c^{16}) \oplus \mathsf{S}_8(y_1 \oplus c^{19}) \oplus \mathsf{S}_8(w_1 \oplus c^{25}),\\
\mathsf{S}_8(z_0 \oplus c^{21}) =& \mathsf{S}_8(z_1 \oplus c^{21}),\\
\mathsf{S}_8(x_0 \oplus c^{14}) =& \mathsf{S}_8(x_1 \oplus c^{14}),\\
\mathsf{S}_8(x_0 \oplus c^{13}) \oplus \mathsf{S}_8(z_0 \oplus c^{23}) =& \mathsf{S}_8(x_1 \oplus c^{13}) \oplus \mathsf{S}_8(z_1 \oplus c^{23}).
\end{aligned}$$

Since S_8 is invertible, we have

$$\begin{aligned}
x_0 =& x_1,\\
z_0 =& z_1,\\
\mathsf{S}_8(y_0 \oplus c^{19}) \oplus \mathsf{S}_8(w_0 \oplus c^{25}) =& \mathsf{S}_8(y_1 \oplus c^{19}) \oplus \mathsf{S}_8(w_1 \oplus c^{25}).
\end{aligned} \tag{2}$$

For any element (x_0, y_0, z_0, w_0) of set (X, Y, Z, W), there are exactly $2^8 - 1$ other elements (x_1, y_1, z_1, w_1) that satisfy (2). There are 2^{32} possible values for (x_0, y_0, z_0, w_0) and except for reordering, the number of right pairs is always $(2^8 - 1) \cdot 2^{31}$.

In all cases, as a result, $n = (2^{16} - 1) \cdot 2^{31}$ or $n = (2^8 - 1) \cdot 2^{31}$. Values of n depends on I and J are summarized in Table 2.

Since Lemma 2 is proved, this finally proves the Theorem 1. Theorem 1 is for the case $|J| = 3$, whereas Theorem 2 is for the case $|J| = 2$.

Theorem 2. *Let $I \subseteq \{0,1,2,3\}$, $J \subseteq \{0,1,2,3\}$, $|I| = 1$, $|J| = 2$ and $a \in \mathbb{K}^{4\times 4}$. Let R be the round function of `SKINNY-128`. We define*

$$n = \#\{\{p^0, p^1\} \mid \forall p^0, p^1 \in \mathbb{D}_I \oplus \mathbf{a}, \mathsf{R}^5(p^0) \oplus \mathsf{R}^5(p^1) \in \mathbb{M}_J\}.$$

Then $n = (2^8 - 1) \cdot 2^{31}$ or $n = 0$.

Theorem 2 can be proved in a similar way with the proof of Theorem 1. All results of the cases of I and J are summarized in Table 3.

Table 2. The number n of right pairs for given I, J with $|I| = 1$, $|J| = 3$ for SKINNY-128

I	J	J^c	n
$\{0\}$	$\{1,2,3\}$	$\{0\}$	$(2^{16}-1)\cdot 2^{31}$
$\{0\}$	$\{0,2,3\}$	$\{1\}$	$(2^{8}-1)\cdot 2^{31}$
$\{0\}$	$\{0,1,3\}$	$\{2\}$	$(2^{16}-1)\cdot 2^{31}$
$\{0\}$	$\{0,1,2\}$	$\{3\}$	$(2^{8}-1)\cdot 2^{31}$
$\{1\}$	$\{1,2,3\}$	$\{0\}$	$(2^{8}-1)\cdot 2^{31}$
$\{1\}$	$\{0,2,3\}$	$\{1\}$	$(2^{16}-1)\cdot 2^{31}$
$\{1\}$	$\{0,1,3\}$	$\{2\}$	$(2^{8}-1)\cdot 2^{31}$
$\{1\}$	$\{0,1,2\}$	$\{3\}$	$(2^{16}-1)\cdot 2^{31}$
$\{2\}$	$\{1,2,3\}$	$\{0\}$	$(2^{16}-1)\cdot 2^{31}$
$\{2\}$	$\{0,2,3\}$	$\{1\}$	$(2^{8}-1)\cdot 2^{31}$
$\{2\}$	$\{0,1,3\}$	$\{2\}$	$(2^{16}-1)\cdot 2^{31}$
$\{2\}$	$\{0,1,2\}$	$\{3\}$	$(2^{8}-1)\cdot 2^{31}$
$\{3\}$	$\{1,2,3\}$	$\{0\}$	$(2^{8}-1)\cdot 2^{31}$
$\{3\}$	$\{0,2,3\}$	$\{1\}$	$(2^{16}-1)\cdot 2^{31}$
$\{3\}$	$\{0,1,3\}$	$\{2\}$	$(2^{8}-1)\cdot 2^{31}$
$\{3\}$	$\{0,1,2\}$	$\{3\}$	$(2^{16}-1)\cdot 2^{31}$

4.2 The Exact Computation of the multiple-of property for 5-round SKINNY-64

The case for SKINNY-64 can be derived similarly to the case for SKINNY-128. It can be proved in the similar way as Theorem 1, only that the size of set is different from SKINNY-128 and hence the value of n changes accordingly. The exact computations for SKINNY-64 that we present in this section are Theorem 3 and Theorem 4.

Theorem 3 and Theorem 4 can be proved in the similar way as Theorem 1, so we omit their proofs. All results of their cases of I and J are summarized in Table 4 and Table 5. Theorem 3 is for the case $|J| = 3$ in SKINNY-64, whereas Theorem 4 is for the case $|J| = 2$ in SKINNY-64.

Theorem 3. *Let $I \subseteq \{0,1,2,3\}$, $J \subseteq \{0,1,2,3\}$, $|I| = 1$, $|J| = 3$ and $a \in \mathbb{K}^{4\times 4}$. Let R denote the round function of SKINNY-64. We define*

$$n = \#\{\{p^0, p^1\} \mid \forall p^0, p^1 \in \mathbb{D}_I \oplus \mathbf{a}, \mathsf{R}^5(p^0) \oplus \mathsf{R}^5(p^1) \in \mathbb{M}_J\}.$$

Then $n = (2^8 - 1)\cdot 2^{15}$ or $n = (2^4 - 1)\cdot 2^{15}$.

Theorem 4. *Let $I \subseteq \{0,1,2,3\}$, $J \subseteq \{0,1,2,3\}$, $|I| = 1$, $|J| = 2$ and $a \in \mathbb{K}^{4\times 4}$. Let R denote the round function of SKINNY-64. We define*

$$n = \#\{\{p^0, p^1\} \mid \forall p^0, p^1 \in \mathbb{D}_I \oplus \mathbf{a}, \mathsf{R}^5(p^0) \oplus \mathsf{R}^5(p^1) \in \mathbb{M}_J\}.$$

Then $n = (2^4 - 1)\cdot 2^{15}$ or $n = 0$.

Table 3. The number n of right pairs for given I, J with $|I| = 1$, $|J| = 2$ for `SKINNY-128`

I	J	J^c	n
$\{0\}$	$\{2,3\}$	$\{0,1\}$	0
$\{0\}$	$\{1,3\}$	$\{0,2\}$	0
$\{0\}$	$\{1,2\}$	$\{0,3\}$	0
$\{0\}$	$\{0,3\}$	$\{1,2\}$	$(2^8-1)\cdot 2^{31}$
$\{0\}$	$\{0,2\}$	$\{1,3\}$	0
$\{0\}$	$\{0,1\}$	$\{2,3\}$	0
$\{1\}$	$\{2,3\}$	$\{0,1\}$	0
$\{1\}$	$\{1,3\}$	$\{0,2\}$	0
$\{1\}$	$\{1,2\}$	$\{0,3\}$	0
$\{1\}$	$\{0,3\}$	$\{1,2\}$	0
$\{1\}$	$\{0,2\}$	$\{1,3\}$	0
$\{1\}$	$\{0,1\}$	$\{2,3\}$	$(2^8-1)\cdot 2^{31}$
$\{2\}$	$\{2,3\}$	$\{0,1\}$	0
$\{2\}$	$\{1,3\}$	$\{0,2\}$	0
$\{2\}$	$\{1,2\}$	$\{0,3\}$	$(2^8-1)\cdot 2^{31}$
$\{2\}$	$\{0,3\}$	$\{1,2\}$	0
$\{2\}$	$\{0,2\}$	$\{1,3\}$	0
$\{2\}$	$\{0,1\}$	$\{2,3\}$	0
$\{3\}$	$\{2,3\}$	$\{0,1\}$	$(2^8-1)\cdot 2^{31}$
$\{3\}$	$\{1,3\}$	$\{0,2\}$	0
$\{3\}$	$\{1,2\}$	$\{0,3\}$	0
$\{3\}$	$\{0,3\}$	$\{1,2\}$	0
$\{3\}$	$\{0,2\}$	$\{1,3\}$	0
$\{3\}$	$\{0,1\}$	$\{2,3\}$	0

Table 4. The number n of right pairs for given I, J with $|I| = 1$, $|J| = 3$ for SKINNY-64

I	J	J^c	n
$\{0\}$	$\{1,2,3\}$	$\{0\}$	$(2^8 - 1) \cdot 2^{15}$
$\{0\}$	$\{0,2,3\}$	$\{1\}$	$(2^4 - 1) \cdot 2^{15}$
$\{0\}$	$\{0,1,3\}$	$\{2\}$	$(2^8 - 1) \cdot 2^{15}$
$\{0\}$	$\{0,1,2\}$	$\{3\}$	$(2^4 - 1) \cdot 2^{15}$
$\{1\}$	$\{1,2,3\}$	$\{0\}$	$(2^4 - 1) \cdot 2^{15}$
$\{1\}$	$\{0,2,3\}$	$\{1\}$	$(2^8 - 1) \cdot 2^{15}$
$\{1\}$	$\{0,1,3\}$	$\{2\}$	$(2^4 - 1) \cdot 2^{15}$
$\{1\}$	$\{0,1,2\}$	$\{3\}$	$(2^8 - 1) \cdot 2^{15}$
$\{2\}$	$\{1,2,3\}$	$\{0\}$	$(2^8 - 1) \cdot 2^{15}$
$\{2\}$	$\{0,2,3\}$	$\{1\}$	$(2^4 - 1) \cdot 2^{15}$
$\{2\}$	$\{0,1,3\}$	$\{2\}$	$(2^8 - 1) \cdot 2^{15}$
$\{2\}$	$\{0,1,2\}$	$\{3\}$	$(2^4 - 1) \cdot 2^{15}$
$\{3\}$	$\{1,2,3\}$	$\{0\}$	$(2^4 - 1) \cdot 2^{15}$
$\{3\}$	$\{0,2,3\}$	$\{1\}$	$(2^8 - 1) \cdot 2^{15}$
$\{3\}$	$\{0,1,3\}$	$\{2\}$	$(2^4 - 1) \cdot 2^{15}$
$\{3\}$	$\{0,1,2\}$	$\{3\}$	$(2^8 - 1) \cdot 2^{15}$

5 Distinguishers for 6-round SKINNY

5.1 One round extension of the property

As is well known, SKINNY does not have the whitening key. Then we can extend the property we presented by one round. This can be achieved by changing the order of operations in the SKINNY round function and using equivalent key.

The round function of SKINNY R can be represented as $\mathsf{MC} \circ \mathsf{SR} \circ \mathsf{ART} \circ \mathsf{AC} \circ \mathsf{SC}$. For a round tweakey rtk and a round constant rc, let the equivalent round tweakey be $\mathsf{MC} \circ \mathsf{SR}(rtk)$ and the equivalent constant be $\mathsf{MC} \circ \mathsf{SR}(rc)$. Let EqART be the equivalent round tweakey addition operation and EqAC be the equivalent constant addition operation. Then, The round function R of SKINNY also can be represented as $\mathsf{EqART} \circ \mathsf{EqAC} \circ \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SC}$.

The 6-round SKINNY can be derived as follows

$$\begin{aligned} \mathsf{R}^6 =& (\mathsf{EqART} \circ \mathsf{EqAC} \circ \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SC})^6 \\ =& (\mathsf{EqART} \circ \mathsf{EqAC} \circ \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SC})^5 \\ & \circ \mathsf{EqART} \circ \mathsf{EqAC} \circ \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SC}. \end{aligned}$$

Here, $(\mathsf{EqART} \circ \mathsf{EqAC} \circ \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SC})^5 \circ \mathsf{EqART} \circ \mathsf{EqAC}$ satisfies the fixed-value property we presented for input subspace $\mathbb{D}_I$ and output subspace $\mathbb{M}_J$ where $I, J \subset \{0, 1, 2, 3\}$. For a given subspace $\mathbb{D}_I$, the inverse of $\mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SC}$ can be computed because there is no secret information, so R^6 has the fixed-value property.

Table 5. The number n of right pairs for given I, J with $|I| = 1$, $|J| = 2$ for `SKINNY-64`

I	J	J^c	n
$\{0\}$	$\{2,3\}$	$\{0,1\}$	0
$\{0\}$	$\{1,3\}$	$\{0,2\}$	0
$\{0\}$	$\{1,2\}$	$\{0,3\}$	0
$\{0\}$	$\{0,3\}$	$\{1,2\}$	$(2^4-1)\cdot 2^{15}$
$\{0\}$	$\{0,2\}$	$\{1,3\}$	0
$\{0\}$	$\{0,1\}$	$\{2,3\}$	0
$\{1\}$	$\{2,3\}$	$\{0,1\}$	0
$\{1\}$	$\{1,3\}$	$\{0,2\}$	0
$\{1\}$	$\{1,2\}$	$\{0,3\}$	0
$\{1\}$	$\{0,3\}$	$\{1,2\}$	0
$\{1\}$	$\{0,2\}$	$\{1,3\}$	0
$\{1\}$	$\{0,1\}$	$\{2,3\}$	$(2^4-1)\cdot 2^{15}$
$\{2\}$	$\{2,3\}$	$\{0,1\}$	0
$\{2\}$	$\{1,3\}$	$\{0,2\}$	0
$\{2\}$	$\{1,2\}$	$\{0,3\}$	$(2^4-1)\cdot 2^{15}$
$\{2\}$	$\{0,3\}$	$\{1,2\}$	0
$\{2\}$	$\{0,2\}$	$\{1,3\}$	0
$\{2\}$	$\{0,1\}$	$\{2,3\}$	0
$\{3\}$	$\{2,3\}$	$\{0,1\}$	$(2^4-1)\cdot 2^{15}$
$\{3\}$	$\{1,3\}$	$\{0,2\}$	0
$\{3\}$	$\{1,2\}$	$\{0,3\}$	0
$\{3\}$	$\{0,3\}$	$\{1,2\}$	0
$\{3\}$	$\{0,2\}$	$\{1,3\}$	0
$\{3\}$	$\{0,1\}$	$\{2,3\}$	0

Thus, the fixed-value property for 5-round SKINNY can be extended to 6 rounds, and it holds for both SKINNY-64 and SKINNY-128, regardless of block size.

5.2 Distinguishers for 6-round SKINNY-128

By combining Theorem 1 and Theorem 2 with one round extension each, we can construct distinguishers for 6-round SKINNY-128. We can choose 2^{32} plaintexts that are active on one inverse diagonal and constant on the other inverse diagonal after one round. Since the matrix M of MC is binary matrix, plaintexts are easy to choose. Then, for 2^{32} ciphertexts after 6-round SKINNY encryption corresponding to 2^{32} chosen plaintexts, the number of pairs whose difference is an element of $\mathbb{M}_J$ is $(2^{16}-1)\cdot 2^{31}$ or $(2^8-1)\cdot 2^{31}$ when $|J|=3$, and $(2^8-1)\cdot 2^{31}$ or 0 when $|J|=2$.

Since $\mathbb{M}_{\mathbb{J}} = \mathsf{MC}(\mathbb{D}_J)$, an easy way to check that the difference of a pair of ciphertexts is an element of $\mathbb{M}_J$ is to check that the difference of the values of applying the MC^{-1} operation to each ciphertext is an element of $\mathbb{D}_J$.

For the random permutation, the expected value of n is 2^{31} when $|J|=3$ and 2^{-1} when $|J|=2$. To construct a distinguisher with high probability of success, we choose a J such that n is $(2^{16}-1)\cdot 2^{31}$ when $|J|=3$ and n is $(2^8-1)\cdot 2^{31}$ when $|J|=2$. Then we can construct a distinguisher that distinguishes SKINNY-128 from the random permutation with a probability of success of almost 1. This distinguisher can distinguish SKINNY-128 from the random permutation with more better probability of success than Example 1 and Example 2 which use the multiple-of property.

Time Complexity. First, since 2^{32} one round SKINNY-128 round functions are used to form the plaintext structure, this process requires a time complexity of $\frac{1}{6}\cdot 2^{32} \approx 2^{29.4}$ 6-round SKINNY-128 encryption. Second, encrypting 2^{32} plaintexts requires 2^{32} 6-round SKINNY-128 encryption. Third, we need to find the number of right pairs, which was presented in [8]. This process requires $2^{33.6}$ table lookup complexity, which is equivalent to 2^{27} 6-round SKINNY-128 encryption(using the approximation 16 table look-ups $\approx$ one round SKINNY-128 encryption). So the overall time complexity is 2^{32} 6-round SKINNY-128 encryption.

Data Complexity. To do this, we need 2^{32} chosen plaintexts.

Memory Complexity. First, to create the plaintext structure, we need memory to store 2^{32} 128-bit texts. Second, since we need to store 2^{32} ciphertexts to count the number of right pairs, we need as much memory as 2^{32} 128-bit texts. Since the two events do not occur simultaneously, the overall memory complexity is 2^{32} 128-bit texts.

So the overall complexity in time, data, and memory is 2^{32}.

5.3 Distinguishers for 6-round SKINNY-64

For SKINNY-64, the distinguisher can be constructed in a similar way as for SKINNY-128. By combining Theorem 3 and Theorem 4 with one round extension each, we can construct distinguishers for SKINNY-64. We can choose 2^{16}

plaintexts that are active on one inverse diagonal and constant on the other inverse diagonal after one round. Since the matrix M of MC is binary matrix, plaintexts are easy to choose. Then, for 2^{16} ciphertexts after 6 rounds of SKINNY encryption corresponding to 2^{16} chosen plaintexts, the number of pairs whose difference is an element of $\mathcal{M}_J$ is $(2^8-1)\cdot 2^{15}$ or $(2^4-1)\cdot 2^{15}$ when $|J|=3$, and $(2^4-1)\cdot 2^{15}$ or 0 when $|J|=2$. As in the case of SKINNY-128, we can easily check that the difference of a pair of ciphertexts is an element of $\mathcal{M}_J$.

For the random permutation, the expected value of n is 2^{15} when $|J|=3$ and 2^{-1} when $|J|=2$. To construct a distinguisher with high probability of success, we choose a J such that n is $(2^8-1)\cdot 2^{15}$ when $|J|=3$ and n is $(2^4-1)\cdot 2^{15}$ when $|J|=2$. Then we can construct a distinguisher that distinguishes SKINNY-64 from the random permutation with a probability of success of almost 1.

As in the case of SKINNY-128, this distinguisher can distinguish SKINNY-64 from the random permutation with better probability of success than Example 1 and Example 2 which use the multiple-of property.

Complexity. The complexity of the distinguisher for SKINNY-64 can be calculated similarly to the case of the distinguisher for SKINNY-128. This results in a time complexity of 2^{16} 6-round SKINNY-64 encryptions, a data complexity of 2^{16} chosen plaintexts, and a memory complexity of 2^{16} 64-bit texts. So, as in the case of the distinguisher for SKINNY-128, the overall complexity in time, data, and memory is 2^{16}.

6 Discussion

AES and MIDORI have a similar structure (AES-like) to SKINNY and satisfies the multiple-of property for 5 rounds. Thus we tried to take a similar approach to the proof of Lemma 2 in the case of AES and MIDORI. An important part of the proof of Lemma 2 is how the set is represented as a 4×4 array after one round encryption of a mixed space. If equations for the difference of a pair to be an element of the subspace have a fixed number of solutions, then the proposed property is satisfied.

So, for the case of AES and MIDORI, we check how the set is represented as a 4×4 array after one round encryption in mixed space. We then check that whether or not the number of solutions of equations for the difference of a pair to be an element of the subspace is fixed. In the process, we check under what conditions the number of solutions is determined for general SPN block cipher.

6.1 AES

Let $\mathsf{R}_{\mathtt{AES}}$ be the round function of AES and $\mathbb{M}_I^{\mathtt{AES}}$ be the mixed space for AES. Then $\mathsf{R}_{\mathtt{AES}}(\mathbb{M}_I^{\mathtt{AES}}\oplus\mathbf{a})$ is the set represented as a 4×4 array after one round encryption of AES in mixed space. All cells of $\mathsf{R}_{\mathtt{AES}}(\mathbb{M}_I^{\mathtt{AES}}\oplus\mathbf{a})$ are represented by

$$aX^{i_0}\oplus bY^{i_1}\oplus cZ^{i_2}\oplus dW^{i_3}\oplus c^{i_4}$$

for $j \in \{0, 1, 2, 3, 4\}$, $i_j > 0$ and $a, b, c, d \in \{1, 2, 3\}$. Then the number of solutions of equations for the difference of a pair to be an element of the subspace can not be determined. In the case of AES, right pairs exist probabilistically, so it is impossible for n to be a constant. And we confirmed this experimentally.

6.2 MIDORI

Let $\mathsf{R}_{\texttt{MI}}$ be the round function of MIDORI and $\mathbb{M}_I^{\texttt{MI}}$ be the mixed space for MIDORI. Then $\mathsf{R}_{\texttt{MI}}(\mathbb{M}_I^{\texttt{MI}} \oplus \mathbf{a})$ is the set represented as a 4×4 array after one round MIDORI encryption for mixed space. $\mathsf{R}_{\texttt{MI}}(\mathbb{M}_I^{\texttt{MI}} \oplus \mathbf{a})$ can be represented as

$$\begin{bmatrix} Y^1 \oplus Z^1 \oplus W^1 \oplus c^1 & X^1 \oplus Z^2 \oplus W^2 \oplus c^5 & X^2 \oplus Y^2 \oplus Z^3 \oplus c^9 & X^3 \oplus Y^3 \oplus W^3 \oplus c^{13} \\ Y^1 \oplus Z^1 \oplus c^2 & X^1 \oplus W^2 \oplus c^6 & Y^2 \oplus Z^3 \oplus c^{10} & X^3 \oplus W^3 \oplus c^{14} \\ Y^1 \oplus W^1 \oplus c^3 & X^1 \oplus Z^2 \oplus c^7 & X^2 \oplus Z^3 \oplus c^{11} & Y^3 \oplus W^3 \oplus c^{15} \\ Z^1 \oplus W^1 \oplus c^4 & Z^2 \oplus W^2 \oplus c^8 & X^2 \oplus Y^2 \oplus c^{12} & X^3 \oplus Y^3 \oplus c^{16} \end{bmatrix}.$$

In the case of MIDORI, it is important to determining the cells that need to be solved simultaneously through the new subspace introduced by ShuffleCell. Then, as in the case of AES, the number of solutions of equations for the difference of a pair to be an element of the subspace can not be determined in the case of MIDORI. Right pairs exist probabilistically, so it is impossible for n to be a constant. And we confirmed this experimentally.

6.3 Relation to branch number

We verified that the property only holds for SKINNY, but not for AES and MIDORI. The important thing is that the array representation does not determine how many solutions of the equations are derived for the difference of a pair to be an element of the subspace. As each cell is combined into more sets, the more likely it is that the number of solutions is undetermined. It is related to the branch number of MixColumns. The branch number of SKINNY MC is 2, AES MixColumns is 5 because it uses an MDS matrix, and MIDORI MixColumns is 4. If the branch number is greater than or equal to 3, the property that n is a fixed value does not occur because every cell is represented as a combination of several sets.

7 Conclusion

In this paper, for the multiple-of property for SKINNY presented in [4], we provide the exact computation of n and show that n is always the same value for certain subspace indices. We also show that n is a much larger value than when it is a random permutation. We prove this by investigating the propagation of the set. It is not only proved theoretically, but also confirmed experimentally. We use the lack of the whitening key on the SKINNY to extend the property one round more. Using this property, we construct 6-round distinguishers for SKINNY and it is able to distinguish with more better probability of success than the previous distinguisher which uses multiple-of property. We also show that the property does not hold for AES and MIDORI, but only for SKINNY, and it is related to the branch number.

References

1. Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., Regazzoni, F.: Midori: A block cipher for low energy. In: Advances in Cryptology–ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29–December 3, 2015, Proceedings, Part II 21. pp. 411–436. Springer (2015)
2. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The skinny family of block ciphers and its low-latency variant mantis. In: Advances in Cryptology–CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II 36. pp. 123–153. Springer (2016)
3. Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., et al.: Prince–a low-latency block cipher for pervasive computing applications. In: Advances in Cryptology–ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings 18. pp. 208–225. Springer (2012)
4. Boura, C., Canteaut, A., Coggia, D.: A general proof framework for recent aes distinguishers. IACR Transactions on Symmetric Cryptology pp. 170–191 (2019)
5. Daemen, J., Rijmen, V.: The design of Rijndael, vol. 2. Springer (2002)
6. Grassi, L., Rechberger, C.: Practical low data-complexity subspace-trail cryptanalysis of round-reduced prince. In: Progress in Cryptology–INDOCRYPT 2016: 17th International Conference on Cryptology in India, Kolkata, India, December 11-14, 2016, Proceedings 17. pp. 322–342. Springer (2016)
7. Grassi, L., Rechberger, C., Rønjom, S.: Subspace trail cryptanalysis and its applications to aes. Cryptology ePrint Archive (2016)
8. Grassi, L., Rechberger, C., Rønjom, S.: A new structural-differential property of 5-round aes. In: Advances in Cryptology–EUROCRYPT 2017: 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30–May 4, 2017, Proceedings, Part II. pp. 289–317. Springer (2017)
9. Leander, G., Abdelraheem, M.A., AlKhzaimi, H., Zenner, E.: A cryptanalysis of printcipher: the invariant subspace attack. In: Advances in Cryptology–CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings 31. pp. 206–221. Springer (2011)
10. Leander, G., Minaud, B., Rønjom, S.: A generic approach to invariant subspace attacks: Cryptanalysis of robin, iscream and zorro. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 254–283. Springer (2015)