IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 27 December 2023, accepted 23 February 2024, date of publication 29 February 2024, date of current version 11 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3371712

RESEARCH ARTICLE

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], (Member, IEEE)

[1]Institute of Cyber Security and Privacy (ICSP), Korea University, Seoul 02841, South Korea
[2]System LSI Business, Samsung Electronics, Hwaseong 18448, South Korea
[3]Department of Information Technology and Engineering, Jeonbuk National University, Jeonju 54896, South Korea
[4]Department of Mathematics, University of Seoul, Seoul 02504, South Korea

Corresponding author: Deukjo Hong (deukjo.hong@jbnu.ac.kr)

This work was supported in part by the Military Crypto Research Center funded by the Defense Acquisition Program Administration (DAPA) and the Agency for Defense Development (ADD) under Grant UD210027XD, and in part by the National Research Foundation of Korea (NRF) grant funded by the Korean Government [Ministry of Science and ICT (MSIT)] under Grant 2021R1A2C1005946.

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.

INDEX TERMS Multiple-of property, structural-differential property, SKINNY, AES-like cipher.

I. 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 first presented for 5-round AES [3]. Boura et al. [2] generalized the multiple-of property for a general SPN(Substitution Permutation Network) block cipher and applied it 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 for SKINNY is not only a multiple but also a fixed value. In particular, n is significantly different from the expected value for random permutation. In contrast to the previous proof of the generalization of the multiple-of property, we investigate the propagation of the set to compute the exact value of n. Furthermore, we experimentally verify that proposed property holds.

We extend this property by one round, utilizing the absence of the whitening key in SKINNY. Subsequently, we construct 6-round distinguishers based on this property. The distinguisher on 6-round SKINNY-128 distinguishes from random permutation with a total complexity of 2^{32} and a nearly 1 probability of success. Similarly, the distinguisher on

The associate editor coordinating the review of this manuscript and approving it for publication was Ramakrishnan Srinivasan.

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
Differential Cryptanalysis	64 bits	6	2^{32}	0.99	[1]
	128 bits		2^{32}	0.99	
Linear Cryptanalysis	64 bits	6	2^{38}	0.99	[1]
	128 bits		2^{38}	0.99	
Multiple-of property	64 bits	5	2^{20}	0.75	[2]
	128 bits		2^{40}	0.75	
	64 bits	5	2^{16}	0.875	Section III
	128 bits		2^{32}	0.875	
Fixed-value property	64 bits	6	2^{16}	0.99	Section V
	128 bits		2^{32}	0.99	

6-round `SKINNY-64` distinguishes from random permutation with a total complexity of 2^{16} and a nearly 1 probability of success. Our results are summarized in Table 1.

We present that this property holds for `SKINNY` but not for `AES` [4] and `MIDORI` [5]. By investigating the set propagation, we compute the exact value of n for both `AES` and `MIDORI`, similar to our approach for `SKINNY`. Furthermore, we generalize this property for `AES`-like SPN block ciphers that use matrix multiplication. In conclusion, we show that this property is related to the branch number of the MixColumns matrix.

The remainder of the paper is organized as follows: Section II provides a description of `SKINNY` and introduces basic definitions related to the multiple-of property. In Section III, subspaces and the subspace trail for `SKINNY` are defined. Section IV then presents that the number of right pairs in the multiple-of property is not only a multiple but also a fixed value for `SKINNY`. Section V extends the property one round more and constructs distinguishers for 6 rounds of `SKINNY`. Section VI shows that the property holds only for `SKINNY`, not for `AES` and `MIDORI`, and generalizes this property for `AES`-like Substitution Permutation Network (SPN) block ciphers that use matrix multiplication. Lastly, Section VII provides the conclusion.

II. PRELIMINARIES

A. 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 $l > 0$. Similarly, $\mathbb{K}^{m\times k}$ represents the set of all $m \times k$-matrices over $\mathbb{K}$ for $m, k > 0$. If $l = m \times k$, we consider $\mathbb{K}^l$ and $\mathbb{K}^{m\times k}$ as equivalent. Each element of the array are referred to as a cell.

A subspace of $\mathbb{K}^l$ is a subset $\mathbb{V} \subseteq \mathbb{K}^l$ that satisfyies non-emptiness, closure under addition and closure under scalar multiplication. The canonical basis of $\mathbb{K}^{m\times k}$, denoted by $e_{i,j}$ for $i \in \{0, \ldots, m-1\}$ and $j \in \{0, \ldots, k-1\}$, has 1 in the i-th row, j-th column, and 0 in all other cells. The linear space formed by all linear combinations with coefficients in $\mathbb{K}$ of the vectors $\mathbf{v_0}, \ldots, \mathbf{v_n} \in \mathbb{K}^l$ is denoted by $< \mathbf{v_0}, \ldots, \mathbf{v_n} >$. 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 $\mathbf{a} \in \mathbb{K}^l$, representing an affine subspace of $\mathbb{K}^l$.

B. BRIEF DESCRIPTION OF SKINNY

`SKINNY` was proposed at CRYPTO 2016 by Beierle et al. [1]. `SKINNY` is denoted by `SKINNY-64` for 64-bit block size and by `SKINNY-128` for 128-bit block size, respectively. The state vector of `SKINNY` is conveniently represented as a 4×4 array, where each cell contains a nibble (for `SKINNY-64`) or a byte (for `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). An invertible d-bit S-box is applied to each cell of the internal state,where $d = 4$ 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 internal state.
- AddRoundTweakey(ART). The first and second rows of all tweakey arrays are extracted and bitwise exclusive-ored to the corresponding rows of the internal state.
- ShiftRows(SR). The second, third, and fourth rows are rotated to the right by 1, 2 and 3 positions, respectively.
- MixColumns(MC). Each column of the 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. For a block size of 64 bits, it uses 32 rounds for $n_t = n_b$, 36 rounds for $n_t = 2n_b$, and 40 rounds for $n_t = 3n_b$. For a block size of 128 bits, 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, we omit the description of the key schedule.

C. SUBSPACE TRAIL

The concept of subspace trail cryptanalysis was introduced by Grassi et al. at ToSC 2016 [6] as a generalization of invariant

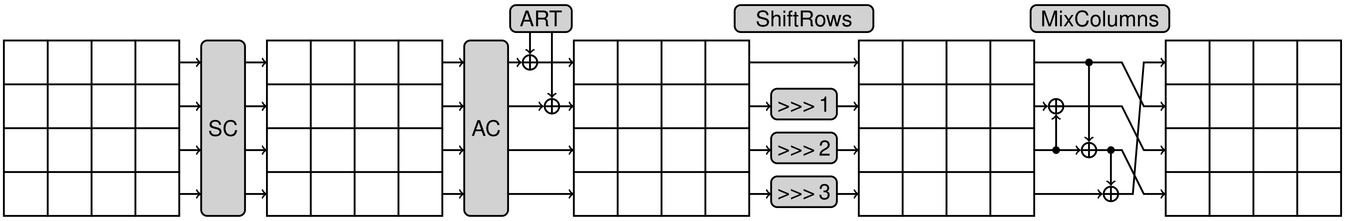


FIGURE 1. The SKINNY round function applies five different transformations: SubCells(SC), AddConstants(AC), AddRoundTweakey(ART), ShiftRows(SR), **and** MixColumns(MC).

subspace [7], [8]. It was subsequently applied to AES [4] and PRINCE [9] in [6] and [10], respectively.

Definition 1 (Subspace trail [6]): Let $\mathsf{F} : \mathbb{K}^l \rightarrow \mathbb{K}^l$ *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.

D. MULTIPLE-OF PROPERTY FOR SKINNY

The concept of the multiple-of property was introduced by Grassi et al. at EUROCRYPT 2017 [3] as an efficient method for constructing key-independent distinguisher. It was later generalized for a general SPN block cipher [2]. In this study, our focus is 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^{n_r} denotes the n_r rounds encryption function for the 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*

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

The 5-round SPN cipher is said to have the multiple-of property if n is a multiple of a natural number other than 1. We denote a right pair as an unordered pair satisfying this property.

For example, the multiple-of-8 property exists for the 5-round AES [3]. An example of the multiple-of property for SKINNY is given follow [2].

Example 1 ([2]): 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*

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

and

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

Then

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

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

III. SUBSPACE TRAIL OF SKINNY

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

Definition 3: For $i \in \{0, \ldots, 3\}$, *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*

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

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

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

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

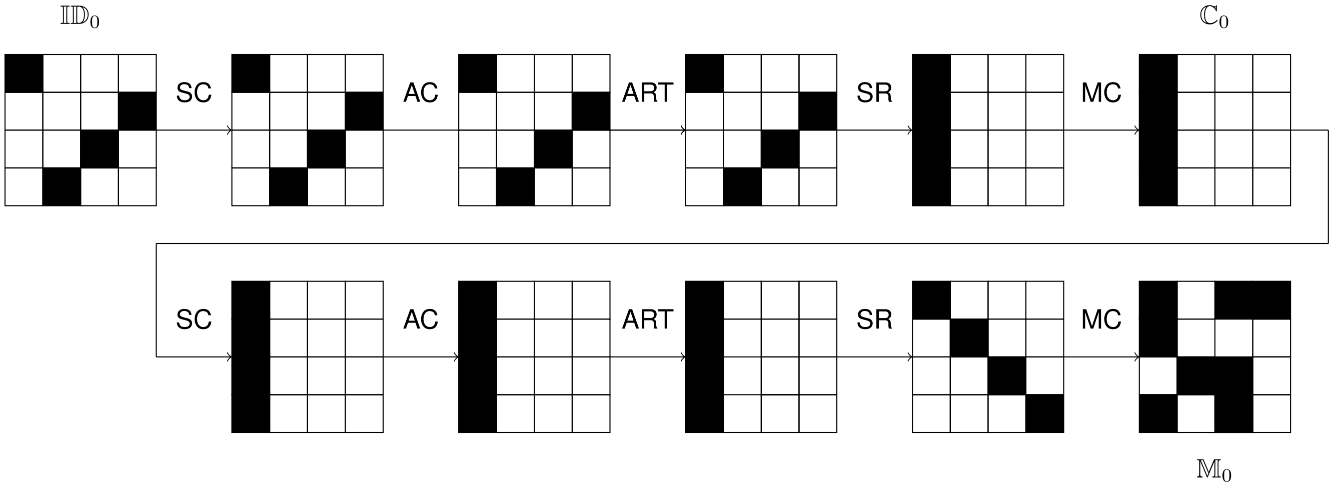


FIGURE 2. 2-round Subspace Trail of `SKINNY`.

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 an exact subspace trail for `SKINNY` using the subspaces defined in 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 where $I = \{0\}$ is illustrated in Figure 2. Lemma 1 is satisfied for both `SKINNY-64` and `SKINNY-128` simultaneously. We propose a new example of the multiple-of property for `SKINNY`, distinct from Example 1, utilizing 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 for both `SKINNY-64` and `SKINNY-128`, simultaneously. This can be used to construct 5-round distinguishers. The distinguisher for 5-round `SKINNY-64` distinguishes from a random permutation with 2^{16} chosen plaintexts and a probability of success of $(1 - 2^{-3}) = 0.875$, whereas the distinguisher for 5-round `SKINNY-128` distinguishes from a random permutation with 2^{32} chosen plaintexts and probability of success of $(1 - 2^{-3}) = 0.875$. So Example 2 achieves a higher probability of success with fewer chosen plaintexts compared to Example 1 in distinguishing between `SKINNY` and a random permutation.

IV. THE EXACT COMPUTATION OF THE MULTIPLE-OF PROPERTY FOR 5-ROUND `SKINNY`

A. THE EXACT COMPUTATION OF THE MULTIPLE-OF PROPERTY FOR 5-ROUND `SKINNY-128`

In this section, we present the exact computation of the number of right pairs, provided 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*

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

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 in a similar manner in the reverse direction: every element of $\mathbb{M}_J$ corresponds to every element of $\mathbb{ID}_J$ before 2 rounds. Therefore, proving Lemma 2 is sufficient to prove 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*

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

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

Proof: We consider only the case where $I = \{0\}$. The proofs for other cases of I follow a similar approach.

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}

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

FIGURE 3. The space after the 1-round SKINNY encryption of $\mathbb{M}_I \oplus$ a.

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

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

After the 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 shown in Figure 3. It represents one round of SKINNY encryption for $\mathbb{M}_I \oplus \mathbf{a}$.

The remainder of the proof involves counting the number n of right pairs for each case of J. We focus on the cases where $J = \{1, 2, 3\}$ and $J = \{0, 1, 2\}$. The proofs for other cases of J follow a similar approach.

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

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

The J^c inverse diagonals of $\mathsf{R}(\mathbb{M}_I \oplus a)$ can be represented as

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

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 $p^0, p^1 \in \mathbb{M}_I \oplus \mathbf{a}$, the J^c inverse diagonals of $\mathsf{R}(p^0)$ and $\mathsf{R}(p^1)$ can be represented as

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

and

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

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

$$x_0^1 \oplus z_0^2 = x_1^1 \oplus z_1^2,$$
$$w_0^1 = w_1^1.$$

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

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

Since S_8 is invertible, we have

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

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

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

Case 2 can be proven similarly to Case 1. The J^c inverse diagonals of $\mathsf{R}(\mathbb{M}_I \oplus \mathbf{a})$ are 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 integers 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 the J^c inverse diagonals of $\mathsf{R}(p^0)$ and $\mathsf{R}(p^1)$ to be the same, it must be

$$x_0^3 \oplus y_0^1 \oplus w_0^1 = x_1^3 \oplus y_1^1 \oplus w_1^1,$$
$$z_0^1 = z_1^1,$$
$$x_0^2 = x_1^2,$$
$$x_0^1 \oplus z_0^2 = x_1^1 \oplus z_1^2.$$

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

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

we have

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

Since S_8 is invertible, we have

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

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

In all cases, the resulting value of n is either $(2^{16} - 1) \cdot 2^{31}$ or $(2^8 - 1) \cdot 2^{31}$. The values of n depend on I and J and are summarized in Table 2. □

With the proof of Lemma 2, Theorem 1 is finally proven. It's worth noting that Theorem 1 specifically addresses the case $|J| = 3$, while Theorem 2 handles the case $|J| = 2$.

Theorem 2: Let $I \subseteq \{0, 1, 2, 3\}$, $J \subseteq \{0, 1, 2, 3\}$, $|I| = 1$, $|J| = 2$ and $a \in \mathbb{K}^{4\times4}$. 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 $n = 0$.

The proof of Theorem 2 follows a similar approach to that of Theorem 1. The summarized results for all cases of I and J can be found 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
$\{0\}$	$\{1,2,3\}$	$\{0\}$	$(2^{16}-1)\cdot 2^{31}$
$\{0\}$	$\{0,2,3\}$	$\{1\}$	$(2^{8}-1)\cdot 2^{31}$
$\{0\}$	$\{0,1,3\}$	$\{2\}$	$(2^{16}-1)\cdot 2^{31}$
$\{0\}$	$\{0,1,2\}$	$\{3\}$	$(2^{8}-1)\cdot 2^{31}$
$\{1\}$	$\{1,2,3\}$	$\{0\}$	$(2^{8}-1)\cdot 2^{31}$
$\{1\}$	$\{0,2,3\}$	$\{1\}$	$(2^{16}-1)\cdot 2^{31}$
$\{1\}$	$\{0,1,3\}$	$\{2\}$	$(2^{8}-1)\cdot 2^{31}$
$\{1\}$	$\{0,1,2\}$	$\{3\}$	$(2^{16}-1)\cdot 2^{31}$
$\{2\}$	$\{1,2,3\}$	$\{0\}$	$(2^{16}-1)\cdot 2^{31}$
$\{2\}$	$\{0,2,3\}$	$\{1\}$	$(2^{8}-1)\cdot 2^{31}$
$\{2\}$	$\{0,1,3\}$	$\{2\}$	$(2^{16}-1)\cdot 2^{31}$
$\{2\}$	$\{0,1,2\}$	$\{3\}$	$(2^{8}-1)\cdot 2^{31}$
$\{3\}$	$\{1,2,3\}$	$\{0\}$	$(2^{8}-1)\cdot 2^{31}$
$\{3\}$	$\{0,2,3\}$	$\{1\}$	$(2^{16}-1)\cdot 2^{31}$
$\{3\}$	$\{0,1,3\}$	$\{2\}$	$(2^{8}-1)\cdot 2^{31}$
$\{3\}$	$\{0,1,2\}$	$\{3\}$	$(2^{16}-1)\cdot 2^{31}$

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

B. THE EXACT COMPUTATION OF THE MULTIPLE-OF PROPERTY FOR 5-ROUND `SKINNY-64`

The case for `SKINNY-64` can be derived similarly to `SKINNY-128`, and the proof follows a similar process to

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

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

the proof of Theorem 1. The computations for SKINNY-64 are presented in Theorem 3 and Theorem 4, providing exact values for n.

The proofs for Theorem 3 and Theorem 4 follow a similar approach to that of Theorem 1, and hence, their details are omitted. The results for all cases of I and J are summarized in Table 4 and Table 5. Specifically, Theorem 3 addresses the case $|J| = 3$ in SKINNY-64, while Theorem 4 addresses 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*

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

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*

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

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

V. DISTINGUISHERS FOR 6-ROUND SKINNY

A. ONE ROUND EXTENSION OF THE PROPERTY

As SKINNY lacks a whitening key, we can extend the presented property by one round. This extension is achieved by altering the order of operations in the SKINNY round function and using an equivalent key.

The round function of SKINNY, denoted as R, is 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, the equivalent round tweakey is $\mathsf{MC} \circ \mathsf{SR}(rtk)$ and the equivalent constant is $\mathsf{MC} \circ \mathsf{SR}(rc)$. The round function R of SKINNY can also be expressed as $\mathsf{EqART} \circ \mathsf{EqAC} \circ \mathsf{MC} \circ \mathsf{SR} \circ \mathsf{SC}$, where EqART is the equivalent round tweakey addition operation and EqAC is the equivalent constant addition operation.

The 6-round SKINNY can be derived as follows

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

Applying $(\mathsf{EqART}\circ\mathsf{EqAC}\circ\mathsf{MC}\circ\mathsf{SR}\circ\mathsf{SC})^5\circ\mathsf{EqART}\circ\mathsf{EqAC}$ satisfies the fixed-value property for the given input subspace $\mathbb{ID}_I$ and output subspace $\mathbb{M}_J$, where $I, J \subset \{0, 1, 2, 3\}$. Since there is no secret information, the inverse of $\mathsf{MC}\circ\mathsf{SR}\circ\mathsf{SC}$ can be computed for a given subspace $\mathbb{ID}_I$, resulting in R^6 with the fixed-value property.

In conclusion, the fixed-value property for 5-round SKINNY extends smoothly to 6 rounds, and it is applicable to both SKINNY-64 and SKINNY-128, regardless of the block size.

B. 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 $|J| = 2$.

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

FIGURE 4. The space after 1-round MIDORI.

Since $\mathbb{M}_J = \mathsf{MC}(\mathbb{D}_J)$, 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 $\mathbb{D}_J$.

In the case of a 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 select 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 close to 1. This distinguisher achieves a better probability of success compared to Example 1 and Example 2, which rely on 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 [3]. This process requires $2^{33.6}$ table look-up 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}.

C. DISTINGUISHERS FOR 6-ROUND SKINNY-64

For SKINNY-64, the construction of the distinguisher follows a similar approach to 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 $\mathcal{M}_J$.

In the case of a 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 select 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 a 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 with the distinguisher for SKINNY-128, the overall complexity in time, data, and memory is 2^{16}.

VI. 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.

A. CASE OF AES

Let $\mathsf{R}_{\texttt{AES}}$ be the round function of AES and $\mathbb{M}_I^{\texttt{AES}}$ be the mixed space for AES. Then $\mathsf{R}_{\texttt{AES}}(\mathbb{M}_I^{\texttt{AES}} \oplus \mathbf{a})$ 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 cannot 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.

B. CASE OF MIDORI

Let $\mathsf{R}_{\mathtt{MI}}$ be the round function of MIDORI and $\mathbb{M}_I^{\mathtt{MI}}$ be the mixed space for MIDORI. Then $\mathsf{R}_{\mathtt{MI}}(\mathbb{M}_I^{\mathtt{MI}} \oplus \mathbf{a})$ is the set represented as a 4×4 array after one round encryption of MIDORI in mixed space. $\mathsf{R}_{\mathtt{MI}}(\mathbb{M}_I^{\mathtt{MI}} \oplus \mathbf{a})$ can be represented by Figure 4. 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 cannot 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.

C. CASE OF AES-LIKE CIPHER

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. For AES-like ciphers that use matrix multiplication linear layer, 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.

VII. CONCLUSION

In this paper, for the multiple-of property for SKINNY presented in [2], 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] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim, "The SKINNY family of block ciphers and its low-latency variant MANTIS," in *Proc. 36th Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA. Berlin, Germany: Springer, Aug. 2016, pp. 123–153.

[2] C. Boura, A. Canteaut, and D. Coggia, "A general proof framework for recent AES distinguishers," *IACR Trans. Symmetric Cryptol.*, vol. 2019, no. 1, pp. 170–191, Mar. 2019.

[3] L. Grassi, C. Rechberger, and S. Rønjom, "A new structural-differential property of 5-round AES," in *Proc. 36th Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, Paris, France. Berlin, Germany: Springer, Apr. 2017, pp. 289–317.

[4] J. Daemen and V. Rijmen, *The Design of Rijndael*, vol. 2. Berlin, Germany: Springer, 2002.

[5] S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni, "Midori: A block cipher for low energy," in *Proc. 21st Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Auckland, New Zealand. Berlin, Germany: Springer, Dec. 2015, pp. 411–436.

[6] L. Grassi, C. Rechberger, and S. Rønjom, "Subspace trail cryptanalysis and its applications to AES," *IACR Trans. Symmetric Cryptol.*, vol. 2016, no. 2, pp. 192–225, Feb. 2017.

[7] G. Leander, M. A. Abdelraheem, H. AlKhzaimi, and E. Zenner, "A cryptanalysis of PRINTCIPHER: The invariant subspace attack," in *Proc. 31st Annu. Cryptol. Conf.*, Santa Barbara, CA, USA. Berlin, Germany: Springer, Aug. 2011, pp. 206–221.

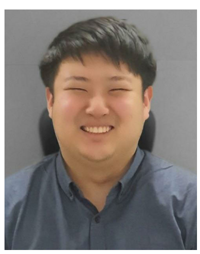
[8] G. Leander, B. Minaud, and S. Rønjom, "A generic approach to invariant subspace attacks: Cryptanalysis of Robin, iSCREAM and Zorro," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2015, pp. 254–283.

[9] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, and T. Yalçn, "PRINCE—A low-latency block cipher for pervasive computing applications," in *Proc. 18th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, Beijing, China. Berlin, Germany: Springer, Dec. 2012, pp. 208–225.

[10] L. Grassi and C. Rechberger, "Practical low data-complexity subspace-trail cryptanalysis of round-reduced prince," in *Proc. 17th Int. Conf. Cryptol.*, Kolkata, India. Berlin, Germany: Springer, Dec. 2016, pp. 322–342.

HANBEOM SHIN received the M.S. degree in information security from Korea University, in 2024, where he is currently pursuing the Ph.D. degree with the Graduate School of Cyber Security. His research interest includes symmetric cryptography.

INSUNG KIM received the B.S. degree in mathematics from the University of Seoul, in 2022. He is currently pursuing the Ph.D. degree with the Graduate School of Cyber Security, Korea University. His research interest includes symmetric cryptography.



SUNYEOP KIM received the B.S. degree in mathematics from Korea University, in 2019, where he is currently pursuing the Ph.D. degree with the Graduate School of Cyber Security. His research interest includes symmetric cryptography.

SEONGGYEOM KIM received the M.S. and Ph.D. degrees in information security from Korea University, in 2018 and 2023, respectively. He is currently a Staff Engineer with Samsung Electronics, System LSI. His research interests include cryptanalysis, IP design of cryptographic algorithm accelerators, and passive and active physical attacks, along with the corresponding countermeasures.

DEUKJO HONG received the B.S. and M.S. degrees in mathematics and the Ph.D. degree in information security from Korea University, in 1999, 2002, and 2006, respectively. From 2007 to 2015, he was employed with ETRI. He is currently an Associate Professor with the Department of Information Technology and Engineering, Jeonbuk National University. His research interest includes symmetric cryptography.

JAECHUL SUNG received the Ph.D. degree in mathematics from Korea University, in 2002. He was employed as a Senior Researcher with Korea Information Security Agency (KISA), from July 2002 to January 2004. He is currently a Professor with the Department of Mathematics, University of Seoul. His research interests include cryptography, symmetric cryptosystems, hash functions, and MACs.

SEOKHIE HONG (Member, IEEE) received the M.S. and Ph.D. degrees in mathematics from Korea University, in 1997 and 2001, respectively. He was with Security Technologies Inc., from 2000 to 2004. Subsequently, he conducted postdoctoral research with COSIC, KU Leuven, Belgium, from 2004 to 2005, after which he joined the Graduate School of Cyber Security, Korea University. His research interests include cryptography, public and symmetric cryptosystems, hash functions, and MACs.