J Cryptol (2017) 30:920–959
DOI: 10.1007/s00145-016-9240-x

Journal of
CRYPTOLOGY

Integral Cryptanalysis on Full MISTY1*

Yosuke Todo
NTT Secure Platform Laboratories, Tokyo, Japan
todo.yosuke@lab.ntt.co.jp

Kobe University, Hyogo, Japan

Communicated by Vincent Rijmen.

Received 27 December 2015 / Revised 6 July 2016
Online publication 25 August 2016

Abstract. MISTY1 is a block cipher designed by Matsui in 1997. It was well evaluated and standardized by projects, such as CRYPTREC, ISO/IEC, and NESSIE. In this paper, we propose a key recovery attack on the full MISTY1, i.e., we show that 8-round MISTY1 with 5 FL layers does not have 128-bit security. Many attacks against MISTY1 have been proposed, but there is no attack against the full MISTY1. Therefore, our attack is the first cryptanalysis against the full MISTY1. We construct a new integral characteristic by using the propagation characteristic of the division property, which was proposed in EUROCRYPT 2015. We first improve the division property by optimizing the division property for a public S-box and then construct a 6-round integral characteristic on MISTY1. Finally, we recover the secret key of the full MISTY1 with $2^{63.58}$ chosen plaintexts and 2^{121} time complexity. Moreover, if we use $2^{63.994}$ chosen plaintexts, the time complexity for our attack is reduced to $2^{108.3}$. Note that our cryptanalysis is a theoretical attack. Therefore, the practical use of MISTY1 will not be affected by our attack.

Keywords. MISTY1, Integral attack, Division property.

1. Introduction

MISTY [18] is a block cipher designed by Matsui in 1997 and is based on the theory of provable security [20,21] against the differential attack [4] and the linear attack [16]. MISTY has a recursive structure, and the component function has a unique structure, the so-called MISTY structure [17]. There are two types of MISTY, MISTY1 and MISTY2. MISTY1 adopts the Feistel structure whose F-function is designed by the recursive MISTY structure. MISTY2 does not adopt the Feistel structure and uses only the MISTY

* This paper is an extended version of [26], presented at CRYPTO 2015.

Table 1. Summary of single secret key attacks against MISTY1.

Rounds	#FL layers	Attack algorithm	Data	Time	Reference
5	0	Higher-order differential	11×2^7 CP	2^{17}	[25]
5	3	Integral	2^{34} CP	2^{48}	[14]
5	4	Higher-order differential	2^{22} CP	2^{28}	[11]
5	4	Impossible differential	2^{38} CP	$2^{46.45}$	[9]
6	4	Higher-order differential	$2^{53.7}$ CP	$2^{53.7}$	[28]
6	4	Impossible differential	2^{51} CP	$2^{123.4}$	[9]
7	0	Impossible differential	$2^{50.2}$ KP	$2^{114.1}$	[9]
7	4	Higher-order differential	$2^{54.1}$ CP	$2^{120.7}$	[28]
7	4	Higher-order differential	$2^{50.1}$ CP	$2^{100.4}$	[3]
7	5	Higher-order differential	$2^{51.4}$ CP	2^{121}	[3]
8	5	Integral by division property	$2^{63.58}$ CP	2^{121}	This paper
8	5	Integral by division property	$2^{63.994}$ CP	$2^{108.3}$	This paper

structure. Both ciphers achieve provable security against differential and linear attacks. MISTY1 is designed for practical use, and MISTY2 is designed for experimental use.

MISTY1 is a 64-bit block cipher with 128-bit key, and it has a Feistel structure with FL layers. MISTY1 is in the candidate recommended ciphers list of CRYPTREC [7], and it is standardized by ISO/IEC 18033-3 [12]. Moreover, it is a NESSIE-recommended cipher [19] and is described in RFC 2994 [22]. There are many existing attacks against reduced MISTY1, and we summarize these attacks in Table 1. A higher-order differential attack is the most powerful attack against MISTY1 [3]. However, there is no attack against the full MISTY1, i.e., 8-round MISTY1 with 5 FL layers.

1.1. *Integral Attack*

The integral attack [14] was first proposed by Daemen et al. to evaluate the security of SQUARE [8] and was then formalized by Knudsen and Wagner. There are two major techniques to construct an integral characteristic: One uses the propagation characteristic of integral properties [14] and the other estimates the algebraic degree [13,15]. We often call the second technique a "higher-order differential attack." A new technique to construct integral characteristics was proposed in EUROCRYPT 2015 [27], and it introduced a new property, the so-called division property, by generalizing the integral property [14]. It showed the propagation characteristic of the division property for any function restricted by an algebraic degree. As a result, several improved results were reported on the structural evaluation of the Feistel network and the Substitution-Permutation network. Moreover, the division property was applied to the generalized Feistel network [29].

1.2. *Our Contribution*

In [27], S-boxes are randomly chosen depending on round keys, but the algebraic degree is restricted. However, many realistic block ciphers use more efficient structures, e.g., a public S-box and a key addition. In this paper, we show that the division property

becomes more useful if an S-box is a public function. Then, we apply our technique to the cryptanalysis of MISTY1. We first evaluate the propagation characteristic of the division property for public S-boxes S_7 and S_9 and show that S_7 has a vulnerable property. We next evaluate the propagation characteristic of the division property for the FI function and then evaluate it for the FO function. Moreover, we evaluate the propagation characteristic for the FL layer. Finally, we devise an algorithm to search for integral characteristics on MISTY1 by assembling these propagation characteristics. As a result, we can construct a new 6-round integral characteristic, where the left 7-bit value of the output is balanced. We recover the round key by using the partial-sum technique [10]. As a result, the secret key of the full MISTY1 can be recovered with $2^{63.58}$ chosen plaintexts and 2^{121} time complexity. Moreover, if we can use $2^{63.994}$ chosen plaintexts, the time complexity is reduced to $2^{108.3}$. Unfortunately, we have to use almost all chosen plaintexts, and recovering the secret key by using fewer chosen plaintexts is left as an open problem.

2. MISTY1

MISTY1 is a Feistel cipher whose F-function has the MISTY structure, and the recommended parameter is 8 rounds with 5 FL layers. Figure 1 shows the structure of MISTY1. Let X_i^L (resp. X_i^R) be the left half (resp. the right half) of an i-round input. Moreover, $X_i^L[j]$ (resp. $X_i^R[j]$) denotes the jth bit of X_i^L (resp. X_i^R) from the left. MISTY1 is a 64-bit block cipher with 128-bit key, and it has a Feistel structure with FL layers, where the FO function is used in the F-function of the Feistel structure. The component function FO_i is constructed by using the 3-round MISTY structure, where $FI_{i,1}$, $FI_{i,2}$, and $FI_{i,3}$ are used as the F-function of the MISTY structure, and the four 16-bit round keys $KO_{i,1}$, $KO_{i,2}$, $KO_{i,3}$, and $KO_{i,4}$ are used. Moreover, the function $FI_{i,j}$ is constructed by using the 3-round MISTY structure, where a 9-bit S-box S_9 and a 7-bit S-box S_7 are used in the F-function, and a 16-bit round key $KI_{i,j}$ is used. Here, S_9 and S_7 are defined in "Appendix 1." The component function FL_i uses two 16-bit round keys, $KL_{i,1}$ and $KL_{i,2}$, where $\cap$ and $\cup$ denote a bitwise AND and OR, respectively. These round keys are calculated from the secret key $(K_1, K_2, \ldots, K_8)$ as follows.

Symbol	$KO_{i,1}$	$KO_{i,2}$	$KO_{i,3}$	$KO_{i,4}$	$KI_{i,1}$	$KI_{i,2}$	$KI_{i,3}$	$KL_{i,1}$	$KL_{i,2}$
Key	K_i	K_{i+2}	K_{i+7}	K_{i+4}	K'_{i+5}	K'_{i+1}	K'_{i+3}	$K_{\frac{i+1}{2}}$ (odd i) $K'_{\frac{i}{2}+2}$ (even i)	$K'_{\frac{i+1}{2}+6}$ (odd i) $K_{\frac{i}{2}+4}$ (even i)

Here, K_i and K'_i are identified with K_{i-8} and K'_{i-8}, respectively, when i exceeds 8. Moreover, K'_i is defined as the output of $FI_{i,j}$ where the input is K_i and the key is K_{i+1}.

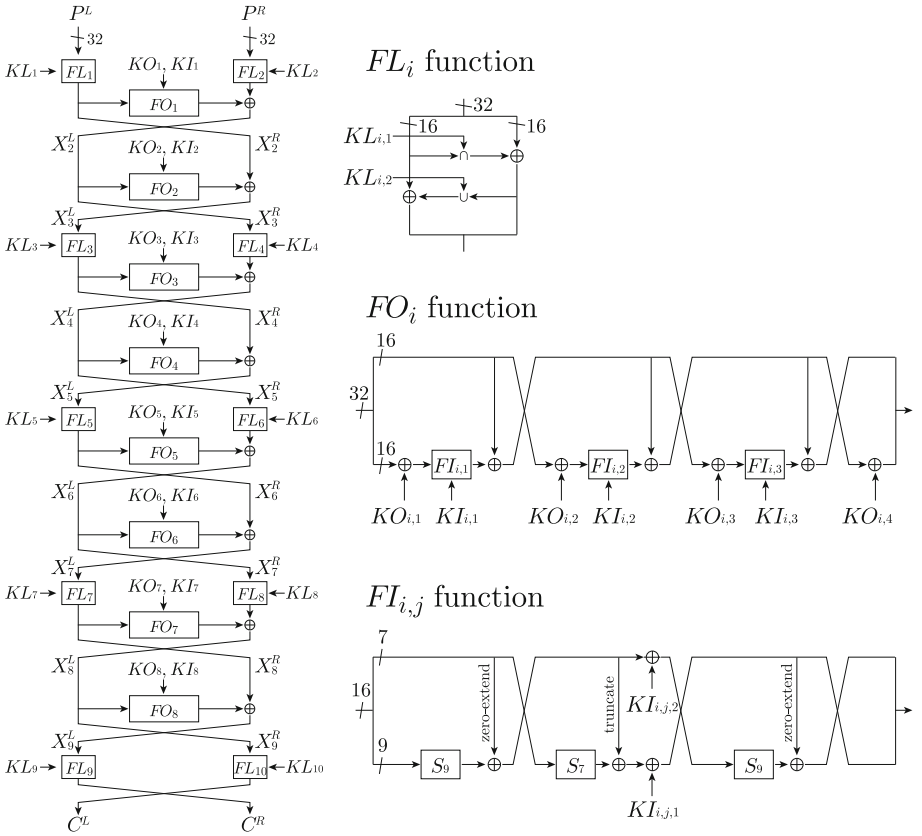

Fig. 1. Specification of MISTY1.

3. Integral Characteristic by Division Property

3.1. *Notations*

We make the distinction between the addition over $\mathbb{F}_2^n$ and the addition over $\mathbb{Z}$, and we use $\oplus$ and $+$ as the addition over $\mathbb{F}_2^n$ and the addition over $\mathbb{Z}$, respectively. For any $a \in \mathbb{F}_2^n$, the ith element is expressed as $a[i]$, and the Hamming weight $w(a)$ is calculated as $w(a) = \sum_{i=1}^{n} a[i]$. Moreover, $a[i_1, i_2, \ldots, i_j]$ denotes a j-bit substring of a as $a[i_1, i_2, \ldots, i_j] = a[i_1] \| a[i_2] \| \cdots \| a[i_j]$. Let $1^n \in \mathbb{F}_2^n$ be a value whose all elements are 1. Moreover, let $0^n \in \mathbb{F}_2^n$ be a value whose all elements are 0. For any set $\mathbb{K}$, let $|\mathbb{K}|$ be the number of elements. Moreover, let ϕ be an empty set. For any $\boldsymbol{a} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$, the vectorial Hamming weight is defined as $W(\boldsymbol{a}) = [w(a_1), w(a_2), \ldots, w(a_m)] \in \mathbb{Z}^m$, where a_i denotes the ith element of $\boldsymbol{a}$. Moreover, for any $\boldsymbol{k} \in \mathbb{Z}^m$ and $\boldsymbol{k}' \in \mathbb{Z}^m$, we define $\boldsymbol{k} \succeq \boldsymbol{k}'$ if $k_i \geq k_i'$ for all i $(1 \leq i \leq m)$. Otherwise, $\boldsymbol{k} \not\succeq \boldsymbol{k}'$.

3.1.1. *Boolean Function*

A Boolean function is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Let $\deg(f)$ be the algebraic degree of a Boolean function f. Algebraic normal form (ANF) is often used as representation of the Boolean function. Let f be any Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Then, it can be represented as

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u^f \left(\prod_{i=1}^{n} x[i]^{u[i]} \right),$$

where $a_u^f \in \mathbb{F}_2$ is a constant value depending on f and u. If $\deg(f)$ is at most d, all a_u^f satisfying $d < w(u)$ are 0. An n-bit S-box can be regarded as the collection of n Boolean functions. If the algebraic degrees of its n Boolean functions are at most d, we say the algebraic degree of the S-box is at most d.

3.2. *Integral Attack*

An integral attack [14] is one of the most powerful cryptanalyses against block ciphers. Attackers prepare N chosen plaintexts and get the corresponding ciphertexts. If the XOR of all corresponding ciphertexts is 0 for all secret keys, we say that the block cipher has an integral characteristic with N chosen plaintexts. In an integral attack, attackers first create an integral characteristic against a reduced-round block cipher. Then, they guess the round keys that are used in the last several rounds and calculate the XOR of the ciphertexts of the reduced-round block cipher. Finally, they evaluate whether or not the XOR is 0. If the XOR is not 0, they can discard the guessed round keys from the candidates of the correct key.

3.3. *Division Property*

A division property, which was proposed in [27], is used to search for integral characteristics. We first consider a set of plaintexts and evaluate the division property of the set. Then, we propagate the division property and evaluate the division property of the set of texts encrypted over one round. By repeating the propagation, we show the division property of the set of texts encrypted over some rounds. Finally, we can easily determine the existence of the integral characteristic from the propagated division property.

3.3.1. *Bit Product Function*

We first define two bit product functions π_u and $\pi_{\boldsymbol{u}}$, which are used to evaluate the division property of a multiset.[1] Let $\pi_u \colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a function for any $u \in \mathbb{F}_2^n$. Let $x \in \mathbb{F}_2^n$ be the input, and $\pi_u(x)$ be the AND of $x[i]$ satisfying $u[i] = 1$, i.e., it is defined as

[1] A multiset allows multiple instances of the elements unlike a set.

$$\pi_u(x) := \prod_{i=1}^{n} x[i]^{u[i]}.$$

Let $\pi_{\boldsymbol{u}}$: $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m}) \to \mathbb{F}_2$ be a function for any $\boldsymbol{u} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$. Let $\boldsymbol{x} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$ be the input, and $\pi_{\boldsymbol{u}}(\boldsymbol{x})$ be defined as

$$\pi_{\boldsymbol{u}}(\boldsymbol{x}) := \prod_{i=1}^{m} \pi_{u_i}(x_i).$$

3.3.2. *Definition of Division Property*

The division property is given against a multiset, and it is calculated by using the bit product function. Let $\mathbb{X}$ be an input multiset whose elements take a value of $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$. In the division property, we first evaluate a value of $\bigoplus_{\boldsymbol{x} \in \mathbb{X}} \pi_{\boldsymbol{u}}(\boldsymbol{x})$ for all $\boldsymbol{u} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$. Then, we divide the set of $\boldsymbol{u}$ into a subset whose sum is 0 and a subset whose sum becomes unknown.[2] In [27], the focus was on using the Hamming weight of $\boldsymbol{u}$ to divide the set.

Definition 1. (*Division Property*) Let $\mathbb{X}$ be a multiset whose elements take a value of $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$. Let $\mathbb{K}$ be a set whose elements take an m-dimensional vector whose ith element takes a value between 0 and n_i. When the multiset $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^{n_1,n_2,\ldots,n_m}$, it fulfills the following conditions:

$$\bigoplus_{\boldsymbol{x} \in \mathbb{X}} \pi_{\boldsymbol{u}}(\boldsymbol{x}) = \begin{cases} \text{unknown} & \text{if there exist } \boldsymbol{k} \in \mathbb{K} \text{ s.t. } W(\boldsymbol{u}) \succeq \boldsymbol{k}, \\ 0 & \text{otherwise.} \end{cases}$$

If there are $\boldsymbol{k} \in \mathbb{K}$ and $\boldsymbol{k}' \in \mathbb{K}$ satisfying $\boldsymbol{k} \succeq \boldsymbol{k}'$, $\boldsymbol{k}$ can be removed from $\mathbb{K}$ because it is redundant. Assume that the multiset $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^{n_1,n_2,\ldots,n_m}$. If there is no unit vector $\boldsymbol{e}_j$ in $\mathbb{K}$, where $\boldsymbol{e}_j$ is a vector whose jth element is 1 and the others are 0, $\bigoplus_{x \in \mathbb{X}} x_j$ is 0. See [27] to better understand the concept in detail.

Example 1. Let $\mathbb{X}$ be a multiset whose elements take a value of $\mathbb{F}_2^4$. As an example, we prepare the input multiset $\mathbb{X}$ as

$$\mathbb{X} := \{\texttt{0x0}, \texttt{0x3}, \texttt{0x3}, \texttt{0x3}, \texttt{0x5}, \texttt{0x6}, \texttt{0x8}, \texttt{0xB}, \texttt{0xD}, \texttt{0xE}\}.$$

A following table calculates the summation of $\pi_u(x)$.

[2] If we know all accurate values in a multiset, we can divide the set of $\boldsymbol{u}$ into subsets whose evaluated value is 0 or 1. However, in the application to cryptanalysis, we evaluate the multiset whose elements are texts encrypted for several rounds. Such elements change depending on the subkeys and the constant bit of plaintexts. Therefore, we consider subsets whose sum is 0 for all subkeys, and otherwise, we consider the sum as unknown.

	0x0	0x3	0x3	0x3	0x5	0x6	0x8	0xB	0xD	0xE	$\bigoplus \pi_u(x)$
	0000	0011	0011	0011	0101	0110	1000	1011	1101	1110	
$u = 0000$	1	1	1	1	1	1	1	1	1	1	0
$u = 0001$	0	1	1	1	1	0	0	1	1	0	0
$u = 0010$	0	1	1	1	0	1	0	1	0	1	0
$u = 0011$	0	1	1	1	0	0	0	1	0	0	0
$u = 0100$	0	0	0	0	1	1	0	0	1	1	0
$u = 0101$	0	0	0	0	1	0	0	0	1	0	0
$u = 0110$	0	0	0	0	0	1	0	0	0	1	0
$u = 0111$	0	0	0	0	0	0	0	0	0	0	0
$u = 1000$	0	0	0	0	0	0	1	1	1	1	0
$u = 1001$	0	0	0	0	0	0	0	1	1	0	0
$u = 1010$	0	0	0	0	0	0	0	1	0	1	0
$u = 1011$	0	0	0	0	0	0	0	1	0	0	1
$u = 1100$	0	0	0	0	0	0	0	0	1	1	0
$u = 1101$	0	0	0	0	0	0	0	0	1	0	1
$u = 1110$	0	0	0	0	0	0	0	0	0	1	1
$u = 1111$	0	0	0	0	0	0	0	0	0	0	0

For all u satisfying $w(u) < 3$, $\bigoplus_{x \in \mathbb{X}} \pi_u(x)$ is 0. Therefore, the multiset has the division property $\mathcal{D}_3^4$.

Example 2. Let $\mathbb{X}$ be a multiset whose elements take a value of $(\mathbb{F}_2^8 \times \mathbb{F}_2^8)$. Assume that the multiset $\mathbb{X}$ has the division property $\mathcal{D}^{8,8}_{\{[1,5],[3,3],[4,5],[5,1],[6,0]\}}$. In this case, if $[u_1, u_2]$ is chosen from the gray part in Fig. 2, $\bigoplus_{[x_1,x_2]\in\mathbb{X}} \pi_{[u_1,u_2]}([x_1, x_2])$ becomes unknown. For example, when $\boldsymbol{u} = [\texttt{0x3F}, \texttt{0xFC}]$ is used, we cannot determine $\bigoplus_{[x_1,x_2]\in\mathbb{X}} \pi_{[\texttt{0x3F},\texttt{0xFC}]}([x_1, x_2])$ because $W(\boldsymbol{u}) = [6, 6]$. On the other hand, if (u_1, u_2) is chosen from the white part in Fig. 2, $\bigoplus_{[x_1,x_2]\in\mathbb{X}} \pi_{[u_1,u_2]}([x_1, x_2])$ is 0. Note that the division property $\mathcal{D}^{8,8}_{\{[1,5],[3,3],[5,1],[6,0]\}}$ is the same as $\mathcal{D}^{8,8}_{\{[1,5],[3,3],[4,5],[5,1],[6,0]\}}$ because the unknown space is invariant.

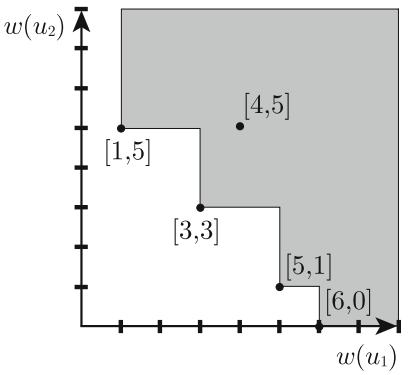

Fig. 2. Division property $\mathcal{D}^{8,8}_{\{[1,5],[3,3],[5,1],[6,0]\}}$.

A similar example is shown in [24] and may help to further understand the division property.

3.3.3. *Propagation Rules of Division Property*

Some propagation rules for the division property are proven in [27]. We summarize them as follows, and the proof is shown in "Appendix 2."

Rule 1 (*Substitution*): Let F be a function that consists of m S-boxes, where the bit length and the algebraic degree of the ith S-box is n_i bits and d_i, respectively. The input and the output take a value of $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$, and $\mathbb{X}$ and $\mathbb{Y}$ denote the input multiset and the output multiset, respectively. Assuming that the multiset $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^{n_1,n_2,\ldots,n_m}$, the multiset $\mathbb{Y}$ has the division property $\mathcal{D}_{\mathbb{K}'}^{n_1,n_2,\ldots,n_m}$, where $\mathbb{K}'$ is calculated as follows: First, $\mathbb{K}'$ is initialized to ϕ. Then, for all $\boldsymbol{k} \in \mathbb{K}$,

$$\mathbb{K}' = \mathbb{K}' \cup \left[\left\lceil \frac{k_1}{d_1} \right\rceil, \left\lceil \frac{k_2}{d_2} \right\rceil, \ldots, \left\lceil \frac{k_m}{d_m} \right\rceil \right],$$

is calculated. Here, when the ith S-box is bijective and $k_i = n_i$, the ith element of the propagated property becomes n_i not $\lceil n_i/d_i \rceil$.

Rule 2 (*Copy*): Let F be a copy function, where the input x takes a value of $\mathbb{F}_2^n$ and the output is calculated as $[y_1, y_2] = [x, x]$. Let $\mathbb{X}$ and $\mathbb{Y}$ be the input multiset and the output multiset, respectively. Assuming that the multiset $\mathbb{X}$ has the division property $\mathcal{D}_k^n$, the multiset $\mathbb{Y}$ has the division property $\mathcal{D}_{\mathbb{K}'}^{n,n}$, where $\mathbb{K}'$ is calculated as follows: First, $\mathbb{K}'$ is initialized to ϕ. Then, for all i $(0 \leq i \leq k)$,

$$\mathbb{K}' = \mathbb{K}' \cup [k - i, i],$$

is calculated.

Rule 3 (*Compression by XOR*): Let F be a function compressed by an XOR, where the input $[x_1, x_2]$ takes a value of $(\mathbb{F}_2^n \times \mathbb{F}_2^n)$ and the output is calculated as $y = x_1 \oplus x_2$. Let $\mathbb{X}$ and $\mathbb{Y}$ be the input multiset and the output multiset, respectively. Assuming that the multiset $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^{n,n}$, the division property of the multiset $\mathbb{Y}$ is $\mathcal{D}_{k'}^n$ as

$$k' = \min_{[k_1,k_2] \in \mathbb{K}} \{k_1 + k_2\}.$$

Here, if the minimum value of k' is larger than n, the propagation characteristic of the division property is aborted. Namely, a value of $\oplus_{y \in \mathbb{Y}} \pi_v(y)$ is 0 for all $v \in \mathbb{F}_2^n$.

Rule 4 (*Split*): Let F be a split function, where the input x takes a value of $\mathbb{F}_2^n$ and the output is calculated as $y_1 \| y_2 = x$, where $[y_1, y_2]$ takes a value of $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n-n_1})$. Let $\mathbb{X}$ and $\mathbb{Y}$ be the input multiset and the output multiset, respectively. Assuming that the multiset $\mathbb{X}$ has the division property $\mathcal{D}_k^n$, the multiset $\mathbb{Y}$ has the division property $\mathcal{D}_{\mathbb{K}'}^{n_1,n-n_1}$, where $\mathbb{K}'$ is calculated as follows: First, $\mathbb{K}'$ is initialized to ϕ.

Then, for all i $(0 \leq i \leq k)$,

$$\mathbb{K}' = \mathbb{K}' \cup [k-i, i],$$

is calculated. Here, $(k-i)$ is less than or equal to n_1, and i is less than or equal to $n - n_1$.

Rule 5 (*Concatenation*): Let F be a concatenation function, where the input $[x_1, x_2]$ takes a value of $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2})$ and the output is calculated as $y = x_1 \| x_2$. Let $\mathbb{X}$ and $\mathbb{Y}$ be the input multiset and the output multiset, respectively. Assuming that the multiset $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^{n_1,n_2}$, the division property of the multiset $\mathbb{Y}$ is $\mathcal{D}_{k'}^{n_1+n_2}$ as

$$k' = \min_{[k_1,k_2]\in\mathbb{K}} \{k_1 + k_2\}.$$

4. Division Property for Public Function

In an assumption of [27], attackers do not know the specification of an S-box and only know the algebraic degree of the S-box. However, many specific block ciphers usually use a public S-box and an addition of secret subkeys, where an XOR is typically used for the addition. In this paper, we show that the propagation characteristic of the division property can be improved if an S-box is a public function. The difference between [27] and this paper is shown in Fig. 3.

We consider the propagation characteristic of the division property for the function shown in the right figure in Fig. 3. The key XORing is first applied, but it does not affect the division property because it is a linear function. Therefore, when we evaluate the propagation characteristic of the division property, we can remove the key XORing. Next, a public S-box is applied, and we can determine the ANF of the S-box. Assuming that an S-box is a function from n bits to m bits, the ANF is represented as

$$\begin{aligned} y[1] &= f_1(x[1], x[2], \ldots, x[n]), \\ y[2] &= f_2(x[1], x[2], \ldots, x[n]), \\ &\vdots \\ y[m] &= f_m(x[1], x[2], \ldots, x[n]), \end{aligned}$$

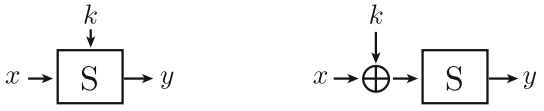

Fig. 3. Difference between [27] and this paper. The *left figure* is an assumption used in [27]. The *right one* is a new assumption used in this paper.

where $x[i]$ $(1 \le i \le n)$ is an input, $y[j]$ $(1 \le j \le m)$ is an output, and f_j $(1 \le j \le m)$ is a Boolean function. The division property evaluates the input multiset and the output one by using the bit product function π_u, and we then divide the set of u into a subset whose evaluated value is 0 and a subset whose evaluated value becomes unknown. Namely, we evaluate the equation

$$F_u(x[1], x[2], \ldots, x[n]) = \prod_{i=1}^{m} f_i(x[1], x[2], \ldots, x[n])^{u[i]}$$

and divide the set of u. In [27], a fundamental property of the product of some functions is used, i.e., the algebraic degree of F_u is at most $w(u) \times d$ if the algebraic degree of functions f_i is at most d. However, since we now know the ANF of functions $f_1, f_2, \ldots, f_m$, we can calculate the accurate algebraic degree of F_u for all $u \in \mathbb{F}_2^n$. In this case, if the algebraic degree of F_u is less than $w(u) \times d$ for all u for which $w(u)$ is constant, we can improve the propagation characteristic.

4.1. *Application to MISTY S-boxes*

4.1.1. *Evaluation of S_7*

The S_7 of MISTY is a 7-bit S-box with degree 3. We show the ANF of S_7 in "Appendix 1." We evaluate the property of $(\pi_v \circ S_7)$ to get the propagation characteristic of the division property. The algebraic degree of $(\pi_v \circ S_7)$ increases in accordance with the Hamming weight of v, and it is summarized as follows.

$w(v)$	0	1	2	3	4	5	6	7
Degree	0	3	5	5	6	6	6	7

One can easily choose a modified S-box S_7' with algebraic degree 3, such that the algebraic degree of $(\pi_v \circ S_7')$ is at least 6 with $w(v) \ge 2$. However, for the S_7, the increment of the algebraic degree is bounded by 5 when $w(v) = 2$ or $w(v) = 3$ holds.[3] Then, $\bigoplus_{x \in \mathbb{X}} (\pi_v \circ S_7)(x)$ is 0 for $w(v) \le 3$ if $\mathbb{X}$ has $\mathcal{D}_6^7$. It means that the necessary condition that $\bigoplus_{x \in \mathbb{X}} (\pi_v \circ S_7)(x)$ becomes unknown is $w(v) \ge 4$ and $\mathcal{D}_4^7$ is propagated from $\mathcal{D}_6^7$. Thus, the propagation characteristic is represented as the following.

$\mathcal{D}_k^7$ for input set $\mathbb{X}$	$\mathcal{D}_0^7$	$\mathcal{D}_1^7$	$\mathcal{D}_2^7$	$\mathcal{D}_3^7$	$\mathcal{D}_4^7$	$\mathcal{D}_5^7$	$\mathcal{D}_6^7$	$\mathcal{D}_7^7$
$\mathcal{D}_k^7$ for output set $\mathbb{Y}$	$\mathcal{D}_0^7$	$\mathcal{D}_1^7$	$\mathcal{D}_1^7$	$\mathcal{D}_1^7$	$\mathcal{D}_2^7$	$\mathcal{D}_2^7$	$\mathcal{D}_4^7$	$\mathcal{D}_7^7$

Note that all propagations except for $\mathcal{D}_6^7 \to \mathcal{D}_4^7$ are calculated by following Rule 1. If the modified S-box is applied, the division property $\mathcal{D}_2^7$ is propagated from the division

[3] This observation was also provided by Theorem 3.1 in [5].

property $\mathcal{D}_6^7$ because of Rule 1. Therefore, the deterioration of the division property for the S_7 is smaller than expected for a randomly chosen 7-bit S-box with algebraic degree 3.

4.1.2. *Evaluation of S_9*

The S_9 of MISTY is a 9-bit S-box with degree 2. We show the ANF of S_9 in "Appendix 1." We evaluate the property of $(\pi_v \circ S_9)$ to get the propagation characteristic of the division property. The algebraic degree of $(\pi_v \circ S_9)$ increases in accordance with the Hamming weight of v, and it is summarized as follows.

$w(v)$	0	1	2	3	4	5	6	7	8	9
Degree	0	2	4	6	8	8	8	8	8	9

Thus, the propagation characteristic is represented as

$\mathcal{D}_k^9$ for input set $\mathbb{X}$	$\mathcal{D}_0^9$	$\mathcal{D}_1^9$	$\mathcal{D}_2^9$	$\mathcal{D}_3^9$	$\mathcal{D}_4^9$	$\mathcal{D}_5^9$	$\mathcal{D}_6^9$	$\mathcal{D}_7^9$	$\mathcal{D}_8^9$	$\mathcal{D}_9^9$
$\mathcal{D}_k^9$ for output set $\mathbb{Y}$	$\mathcal{D}_0^9$	$\mathcal{D}_1^9$	$\mathcal{D}_1^9$	$\mathcal{D}_2^9$	$\mathcal{D}_2^9$	$\mathcal{D}_3^9$	$\mathcal{D}_3^9$	$\mathcal{D}_4^9$	$\mathcal{D}_4^9$	$\mathcal{D}_9^9$

Unlike the propagation characteristic of the division property for S_7, the one for S_9 is essentially optimal among 9-bit S-boxes with algebraic degree 2.

5. New Integral Characteristic

This section shows how to create integral characteristics for MISTY1 by using the propagation characteristic of the division property. We first evaluate the propagation characteristic for the component functions of MISTY1, i.e., the FI function, the FO function, and the FL layer. Finally, by assembling these characteristics, we devise an algorithm to search for integral characteristics on MISTY1.

5.1. *Division Property for FI Function*

We evaluate the propagation characteristic of the division property for the FI function by using those for MISTY S-boxes shown in Sect. 4.1. Since there are a zero-extended XOR and a truncated XOR in the FI function, we use a new representation, in which the internal state is expressed as two 7-bit values and one 2-bit value. Figure 4 shows the structure of the FI function with our representation, where we remove the XOR of subkeys because it does not affect the division property.

Let $\mathbb{X}_1$ be the input multiset of the FI function. We define every multiset $\mathbb{X}_2, \mathbb{X}_3, \ldots, \mathbb{X}_{11}$ in Fig. 4. Here, elements of the multiset $\mathbb{X}_1$, $\mathbb{X}_5$, $\mathbb{X}_6$, and $\mathbb{X}_{11}$ take a value of $(\mathbb{F}_2^7 \times \mathbb{F}_2^2 \times \mathbb{F}_2^7)$. Elements of the multiset $\mathbb{X}_2$, $\mathbb{X}_3$, $\mathbb{X}_8$, and $\mathbb{X}_9$ take a value of

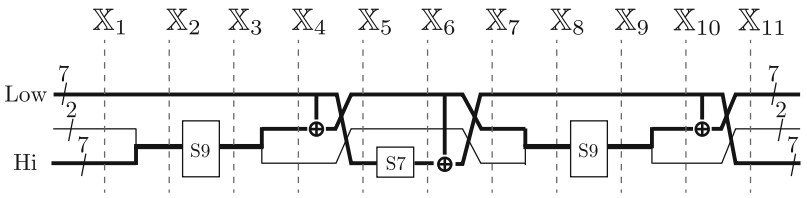

Fig. 4. Structure of FI function.

($\mathbb{F}_2^9 \times \mathbb{F}_2^7$). Elements of the multiset $\mathbb{X}_4$, $\mathbb{X}_7$, and $\mathbb{X}_{10}$ take a value of ($\mathbb{F}_2^2 \times \mathbb{F}_2^7 \times \mathbb{F}_2^7$). Since elements of $\mathbb{X}_1$ and $\mathbb{X}_{11}$ take a value of ($\mathbb{F}_2^7 \times \mathbb{F}_2^2 \times \mathbb{F}_2^7$), the propagation for the FI function is calculated on $\mathcal{D}_{\mathbb{K}}^{7,2,7}$. Here, the propagation is calculated with the following steps.

From $\mathbb{X}_1$ *to* $\mathbb{X}_2$: A 9-bit value is created by concatenating the first 7-bit value with the second 2-bit value. The propagation characteristic can be evaluated by using Rule 5.

From $\mathbb{X}_2$ *to* $\mathbb{X}_3$: The 9-bit S-box S_9 is applied to the first 9-bit value. The propagation characteristic can be evaluated by using the table shown in Sect. 4.1.

From $\mathbb{X}_3$ *to* $\mathbb{X}_4$: The 9-bit output value is split into a 2-bit value and a 7-bit value. The propagation characteristic can be evaluated by using Rule 4.

From $\mathbb{X}_4$ *to* $\mathbb{X}_5$: The second 7-bit value is XORed with the last 7-bit value, and then, the order is rotated. The propagation characteristic can be evaluated by using Rule 2 and Rule 3.

From $\mathbb{X}_5$ *to* $\mathbb{X}_6$: The 7-bit S-box S_7 is applied to the first 7-bit value. The propagation characteristic can be evaluated by using the table shown in Sect. 4.1.

From $\mathbb{X}_6$ *to* $\mathbb{X}_7$: The first 7-bit value is XORed with the last 7-bit value, and then, the order is rotated. The propagation characteristic can be evaluated by using Rule 2 and Rule 3.

From $\mathbb{X}_7$ *to* $\mathbb{X}_8$: A 9-bit value is created by concatenating the first 2-bit value with the second 7-bit value. The propagation characteristic can be evaluated by using Rule 5.

From $\mathbb{X}_8$ *to* $\mathbb{X}_{11}$: The propagation characteristic is the same as that from $\mathbb{X}_2$ to $\mathbb{X}_5$.

As an example, we show the propagation characteristic when $\mathbb{X}_1$ has the division property $\mathcal{D}_{\{[4,2,6]\}}^{7,2,7}$ in "Appendix 3." Algorithm 1 creates the propagation characteristic table for the FI function. It calls `SizeReduce`($\mathbb{K}$), where redundant vectors are eliminated, i.e., it eliminates $\boldsymbol{k}_1 \in \mathbb{K}$ if there exists $\boldsymbol{k}_2 \in \mathbb{K}$ satisfying $\boldsymbol{k}_1 \succeq \boldsymbol{k}_2$. Algorithm 1 only creates the propagation characteristic table for which the input property is represented by $\mathcal{D}_{\{\boldsymbol{k}\}}^{7,2,7}$. If any input multiset is evaluated, we need to know the propagation characteristic from $\mathcal{D}_{\mathbb{K}}^{7,2,7}$ with $|\mathbb{K}| \geq 2$. However, we do not evaluate such propagation in advance because it can be easily evaluated by the table for which the input property is represented by $\mathcal{D}_{\{\boldsymbol{k}\}}^{7,2,7}$. For example, we consider the propagation characteristic from $\mathcal{D}_{\{\boldsymbol{k},\boldsymbol{k}'\}}^{7,2,7}$ to $\mathcal{D}_{\mathbb{K}}^{7,2,7}$. We first get $\mathbb{K}_1$ and $\mathbb{K}_2$ from the propagation characteristic tables for $\mathcal{D}_{\{\boldsymbol{k}\}}^{7,2,7}$ and $\mathcal{D}_{\{\boldsymbol{k}'\}}^{7,2,7}$, respectively. Then, $\mathbb{K}$ is calculated as $\mathbb{K} = \mathbb{K}_1 \cup \mathbb{K}_2$.

Algorithm 1 Propagation for FI function

```
1: procedure FIEval(k_1, k_2, k_3)
2:     K ⇐ S9Eval(k)                          ▷ X_1 → X_5
3:     K' ⇐ S7Eval(K)                         ▷ X_5 → X_7
4:     K'' ⇐ S9Eval(K')                       ▷ X_7 → X_11
5:     return K''
6: end procedure
```

```
1: procedure S9Eval(K)
2:     K' ⇐ φ
3:     for all k ∈ K do
4:         [ℓ, c, r] ⇐ [k_1, k_2, k_3]
5:         k ⇐ ℓ + c
6:         if k < 9 then
7:             k ⇐ ⌈k/2⌉
8:         end if
9:         for c' ⇐ 0 to min(2, k) do
10:            for x ⇐ 0 to r do
11:                ℓ' ⇐ r − x
12:                r' ⇐ k − c' + x
13:                if r' ≤ 7 then
14:                    K' ⇐ K' ∪ [ℓ', c', r']
15:                end if
16:            end for
17:        end for
18:    end for
19:    return SizeReduce(K')
20: end procedure
```

```
21: procedure S7Eval(K)
22:     K' ⇐ φ
23:     for all k ∈ K do
24:         [ℓ, c, r] ⇐ [k_1, k_2, k_3]
25:         k ⇐ ℓ
26:         if k = 6 then
27:             k ⇐ 4
28:         else if k < 6 then
29:             k ⇐ ⌈k/3⌉
30:         end if
31:         for x ⇐ 0 to r do
32:             ℓ' ⇐ c
33:             c' ⇐ r − x
34:             r' ⇐ k + x
35:             if r' ≤ 7 then
36:                 K' ⇐ K' ∪ [ℓ', c', r']
37:             end if
38:         end for
39:     end for
40:     return SizeReduce(K')
41: end procedure
```

We show all propagation characteristic tables in "Appendix 6." Here, the propagation table from $\boldsymbol{k}$ to $\mathbb{K}$ is generated, and the number of entries of this table is $8 \cdot 3 \cdot 8 = 192$. Moreover, we experimentally evaluated the propagation characteristic for the FI function. In our experimental search, for any $\mathcal{D}^{7,2,7}_{\{[k_1,k_2,k_3]\}}$, we created 100 random input multisets and then evaluated the propagation characteristic. As a result, we confirmed that the experimental propagation characteristics are the same as the theoretical ones shown in "Appendix 6."

5.2. *Division Property for FO Function*

We next evaluate the propagation characteristic of the division property for the FO function by using the propagation characteristic table of the FI function. Here, we remove the XOR of subkeys because it does not affect the division property. The input and output of the FO function take the value of $(\mathbb{F}_2^7 \times \mathbb{F}_2^2 \times \mathbb{F}_2^7 \times \mathbb{F}_2^7 \times \mathbb{F}_2^2 \times \mathbb{F}_2^7)$. Therefore, the propagation for the FO function is calculated on $\mathcal{D}^{7,2,7,7,2,7}_{\mathbb{K}}$.

Similar to the one created for the FI function, we create the propagation characteristic table for the FO function (see Algorithm 2). We create only a table for which the input property is represented by $\mathcal{D}^{7,2,7,7,2,7}_{\{\boldsymbol{k}\}}$ and the output property is represented

Algorithm 2 Propagation for FO function

```
1: procedure FOEval(k1, k2, k3, k4, k5, k6)
2:     𝕂 ⇐ FORound(k)
3:     𝕂′ ⇐ FORound(𝕂)
4:     𝕂″ ⇐ FORound(𝕂′)
5:     return 𝕂″
6: end procedure

1: procedure FORound(𝕂)
2:     𝕂′ ⇐ φ
3:     for all k ∈ 𝕂 do
4:         𝕐 ⇐ FIEval(k1, k2, k3)
5:         for all y ∈ 𝕐 do
6:             for all x s.t. (x1 ≤ k4) ∧ (x2 ≤ k5) ∧ (x3 ≤ k6) do
7:                 k′ ⇐ [k4 − x1, k5 − x2, k6 − x3, y1 + x1, y2 + x2, y3 + x3]
8:                 if (k′4 ≤ 7) ∧ (k′5 ≤ 2) ∧ (k′6 ≤ 7) then
9:                     𝕂′ ⇐ 𝕂′ ∪ k′
10:                end if
11:            end for
12:        end for
13:    end for
14:    return SizeReduce(𝕂′)
15: end procedure
```

by $\mathcal{D}_{\mathbb{K}}^{7,2,7,7,2,7}$. Here, the propagation table from $\boldsymbol{k}$ to $\mathbb{K}$ is generated, and the number of entries of this table is $8 \cdot 3 \cdot 8 \cdot 8 \cdot 3 \cdot 8 = 36864$. As an example, the propagation characteristic table from $\mathcal{D}_{\{[1,1,2,3,1,5]\}}^{7,2,7,7,2,7}$ is shown in Table 2.

5.3. *Division Property for FL Layer*

MISTY1 has the FL layer, which consists of two FL functions and is applied once every two rounds. In the FL function, the right half of the input is XORed with the AND between the left half and a subkey $KL_{i,1}$. Then, the left half of the input is XORed with the OR between the right half and a subkey $KL_{i,2}$.

Since the input and the output of the FL function take the value of $(\mathbb{F}_2^7 \times \mathbb{F}_2^2 \times \mathbb{F}_2^7 \times \mathbb{F}_2^7 \times \mathbb{F}_2^2 \times \mathbb{F}_2^7)$, the propagation for the FL function is calculated on $\mathcal{D}_{\mathbb{K}}^{7,2,7,7,2,7}$. `FLEval` in Algorithm 3 calculates the propagation characteristic table for the FL function. Here, the propagation table from $\boldsymbol{k}$ to $\mathbb{K}$ is generated, and the number of entries of this table is $8 \cdot 3 \cdot 8 \cdot 8 \cdot 3 \cdot 8 = 36864$. Moreover, the FL layer consists of two FL functions. Therefore, we have to consider the propagation characteristic of the division property $\mathcal{D}_{\{\boldsymbol{k}\}}^{7,2,7,7,2,7,7,2,7,7,2,7}$, where each FL function is applied to the left half and the right one. `FLLayerEval` in Algorithm 3 calculates the propagation characteristic of the division property for the FL layer.

5.4. *New Path Search for Integral Characteristics on MISTY1*

We created the propagation characteristic table for the FI and FO functions in Sects. 5.1 and 5.2, respectively. Moreover, we showed the propagation characteristic for the FL

Table 2. Division property of input is $\mathcal{D}^{7,2,7,7,2,7}_{\{[1,1,2,3,1,5]\}}$.

$\boldsymbol{k}$ of $\mathcal{D}^{7,2,7,7,2,7}_{\{\boldsymbol{k}\}}$	$\mathbb{K}$ of $\mathcal{D}^{7,2,7,7,2,7}_{\mathbb{K}}$
[1 1 2 3 1 5]	[0 0 0 0 0 4] [0 0 0 0 1 3] [0 0 0 0 2 2] [0 0 0 1 0 3] [0 0 0 1 1 2] [0 0 0 1 2 1] [0 0 0 2 0 2] [0 0 0 2 1 1] [0 0 0 2 2 0] [0 0 0 3 0 1] [0 0 0 3 1 0] [0 0 0 5 0 0] [0 0 1 0 0 3] [0 0 1 0 1 2] [0 0 1 0 2 1] [0 0 1 1 0 2] [0 0 1 1 1 1] [0 0 1 1 2 0] [0 0 1 2 0 1] [0 0 1 2 1 0] [0 0 1 3 0 0] [0 0 2 0 0 2] [0 0 2 0 1 1] [0 0 2 0 2 0] [0 0 2 1 0 1] [0 0 2 1 1 0] [0 0 2 2 0 0] [0 0 3 0 0 1] [0 0 3 0 1 0] [0 0 3 1 0 0] [0 0 5 0 0 0] [0 1 0 0 0 3] [0 1 0 0 1 2] [0 1 0 0 2 1] [0 1 0 1 0 2] [0 1 0 1 1 1] [0 1 0 1 2 0] [0 1 0 2 0 1] [0 1 0 2 1 0] [0 1 0 3 0 0] [0 1 1 0 0 2] [0 1 1 0 1 1] [0 1 1 0 2 0] [0 1 1 1 0 1] [0 1 1 1 1 0] [0 1 1 2 0 0] [0 1 2 0 0 1] [0 1 2 0 1 0] [0 1 2 1 0 0] [0 1 4 0 0 0] [0 2 0 0 0 2] [0 2 0 0 1 1] [0 2 0 0 2 0] [0 2 0 1 0 1] [0 2 0 1 1 0] [0 2 0 2 0 0] [0 2 1 0 0 1] [0 2 1 0 1 0] [0 2 1 1 0 0] [0 2 3 0 0 0] [1 0 0 0 0 3] [1 0 0 0 1 2] [1 0 0 0 2 1] [1 0 0 1 0 2] [1 0 0 1 1 1] [1 0 0 1 2 0] [1 0 0 2 0 1] [1 0 0 2 1 0] [1 0 0 4 0 0] [1 0 1 0 0 2] [1 0 1 0 1 1] [1 0 1 0 2 0] [1 0 1 1 0 1] [1 0 1 1 1 0] [1 0 1 2 0 0] [1 0 2 0 0 1] [1 0 2 0 1 0] [1 0 2 1 0 0] [1 0 4 0 0 0] [1 1 0 0 0 2] [1 1 0 0 1 1] [1 1 0 0 2 0] [1 1 0 1 0 1] [1 1 0 1 1 0] [1 1 0 2 0 0] [1 1 1 0 0 1] [1 1 1 0 1 0] [1 1 1 1 0 0] [1 1 3 0 0 0] [1 2 0 0 0 1] [1 2 0 0 1 0] [1 2 0 1 0 0] [1 2 2 0 0 0] [2 0 0 0 0 2] [2 0 0 0 1 1] [2 0 0 0 2 0] [2 0 0 1 0 1] [2 0 0 1 1 0] [2 0 0 3 0 0] [2 0 1 0 0 1] [2 0 1 0 1 0] [2 0 1 1 0 0] [2 0 3 0 0 0] [2 1 0 0 0 1] [2 1 0 0 1 0] [2 1 0 1 0 0] [2 1 2 0 0 0] [2 2 1 0 0 0] [3 0 0 0 0 1] [3 0 0 0 1 0] [3 0 0 2 0 0] [3 0 2 0 0 0] [3 1 1 0 0 0] [3 2 0 0 0 0] [4 0 0 1 0 0] [4 0 1 0 0 0] [4 1 0 0 0 0] [6 0 0 0 0 0]

layer in Sect. 5.3. By assembling these propagation characteristics, we devise an algorithm to search for integral characteristics on MISTY1. Since the input and the output are represented as eight 7-bit values and four 2-bit values, the propagation is calculated on $\mathcal{D}^{7,2,7,7,2,7,7,2,7,7,2,7}_{\mathbb{K}}$.

The FL layer is first applied to plaintexts, and it deteriorates the propagation of the division property. Therefore, we first remove only the first FL layer and search for integral characteristics on MISTY1 without the first FL layer. The method for passing through the first FL layer is shown in the next section. Algorithm 4 shows the search algorithm for integral characteristics on MISTY1 without the first FL layer.

As a result, we find 6-round integral characteristics without the first and the last FL layers by using Algorithm 4. Each characteristic uses 2^{63} chosen plaintexts, where any one bit of the first seven bits is constant and the others take all values. Then, such input has the division property $\mathcal{D}^{7,2,7,7,2,7,7,2,7,7,2,7}_{\{[6,2,7,7,2,7,7,2,7,7,2,7]\}}$. Therefore, we use $\boldsymbol{k} = [6, 2, 7, 7, 2, 7, 7, 2, 7, 7, 2, 7]$ as the input of Algorithm 4.

We perfectly execute `SizeReduce` every round, and Table 3 shows the propagation of $\mathbb{K}$, where $\min_w(\mathbb{K})$ and $\max_w(\mathbb{K})$ are calculated as

$$\min_w(\mathbb{K}) = \min_{\boldsymbol{k}\in\mathbb{K}} \left\{ \sum_{i=1}^{12} k_i \right\}, \quad \max_w(\mathbb{K}) = \max_{\boldsymbol{k}\in\mathbb{K}} \left\{ \sum_{i=1}^{12} k_i \right\}.$$

After the 6th round function, we have 131 vectors, which are shown in "Appendix 5." Since these vectors do not contain (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0), it means that the first

Algorithm 3 Propagation for FL layer

```
1: procedure FLLayerEval(𝕂)
2:     𝕂′ ⇐ φ
3:     for all k ∈ 𝕂 do
4:         𝕃 ⇐ FlEval(k_1, k_2, ..., k_6)
5:         ℝ ⇐ FlEval(k_7, k_8, ..., k_12)
6:         for all ℓ ∈ 𝕃 do
7:             for all r ∈ ℝ do
8:                 𝕂′ ⇐ 𝕂′ ∪ [ℓ_1, ℓ_2, ℓ_3, ℓ_4, ℓ_5, ℓ_6, r_1, r_2, r_3, r_4, r_5, r_6]
9:             end for
10:        end for
11:    end for
12:    return 𝕂′
13: end procedure
```

```
1: procedure FLEval(k_1, k_2, ..., k_6)
2:     𝕂′ ⇐ φ
3:     [ℓ, c, r] ⇐ [k_1 + k_4, k_2 + k_5, k_3 + k_6]
4:     for k′_1 ⇐ 0 to min(7, ℓ) do
5:         for k′_2 ⇐ 0 to min(2, c) do
6:             for k′_3 ⇐ 0 to min(7, r) do
7:                 (k′_4, k′_5, k′_6) ⇐ (ℓ − k′_1, c − k′_2, r − k′_3)
8:                 if (k′_4 ≤ 7) ∧ (k′_5 ≤ 2) ∧ (k′_6 ≤ 7) then
9:                     𝕂′ ⇐ 𝕂′ ∪ [k′_1, k′_2, k′_3, k′_4, k′_5, k′_6]
10:                end if
11:            end for
12:        end for
13:    end for
14:    return SizeReduce(𝕂′)
15: end procedure
```

7 bits are balanced. Our algorithm is written by C++, and the execution time is about 1 day with Core i7-4770 Processor (4 cores) in 16 GB RAM. Figure 5 shows the 6-round integral characteristic, where the bit strings labeled B, i.e., the first 7 bits and last 32 bits, are balanced. Note that the 6-round characteristic becomes a 7-round characteristic if the FL layer after the 6th round function is removed. Compared with the previous 4-round characteristic [11,28], our characteristic is improved by two rounds.

As shown in Sect. 4, the S_7 of MISTY1 has the vulnerable property that $\mathcal{D}_4^7$ is provided from $\mathcal{D}_6^7$. Interestingly, assuming that S_7 does not have this property (changing lines 26–30 in `S7Eval`), our algorithm cannot construct the 6-round characteristic.

It was already shown in [25] that reduced MISTY1 has a 14th order differential characteristic, and the principle was also discussed in [1,6]. We also revisit the known characteristic for MISTY1 in "Appendix 4."

5.4.1. *Optimized Algorithm*

If we execute `SizeReduce` perfectly, it requires $O(|\mathbb{K}|^2)$ time complexity, and the execution time of Algorithm 4 is increased. Therefore, we use a more reasonable method.

Let $\mathcal{D}_{\mathbb{K}}$ be any division property, where $\mathbb{K}$ contains redundant vectors. Moreover, by executing `SizeReduce`, we get $\mathbb{K}'$ from $\mathbb{K}$. Then, as shown in Sect. 3.3, the unknown

Algorithm 4 Path search for r-round characteristics without first FL layer

```
1: procedure Misty1Eval(k_1, k_2, ..., k_12, r)
2:     K ⇐ RoundFuncEval(k)                                  ▷ 1st round
3:     for i = 1 to r do
4:         if i is even then
5:             K ⇐ FlLayerEval(K)                            ▷ FL Layer
6:         end if
7:         K ⇐ RoundFuncEval(K)                              ▷ (i+1)th round
8:     end for
9:     return K
10: end procedure
```

```
1: procedure RoundFuncEval(K)
2:     K' ⇐ φ
3:     for all k ∈ K do
4:         for all x s.t. x_j ≤ k_j for all j = 1, 2, ..., 6 do
5:             [r_1, r_2, r_3] ⇐ [k_1 − x_1, k_2 − x_2, k_3 − x_3]
6:             [r_4, r_5, r_6] ⇐ [k_4 − x_4, k_5 − x_5, k_6 − x_6]
7:             Y ⇐ FOEval(x_1, x_2, x_3, x_4, x_5, x_6)
8:             for all y ∈ Y do
9:                 [ℓ_1, ℓ_2, ℓ_3] ⇐ [k_7 + y_1, k_8 + y_2, k_9 + y_3]
10:                [ℓ_4, ℓ_5, ℓ_6] ⇐ [k_10 + y_4, k_11 + y_5, k_12 + y_6]
11:                if ℓ_{j'} ≤ 7 for j' ∈ {1, 3, 4, 6} and ℓ_{j'} ≤ 2 for j' ∈ {2, 5} then
12:                    K' ⇐ K' ∪ [ℓ_1, ℓ_2, ℓ_3, ℓ_4, ℓ_5, ℓ_6, r_1, r_2, r_3, r_4, r_5, r_6]
13:                end if
14:            end for
15:        end for
16:    end for
17:    return SizeReduce(K')
18: end procedure
```

Table 3. Propagation from $\mathcal{D}^{7,2,7,7,2,7,7,2,7,7,2,7}_{\{[6,2,7,7,2,7,7,2,7,7,2,7]\}}$.

#rounds	0 (plaintexts)	1	2	FL	3	4	FL	5	6
$\lvert\mathbb{K}\rvert$	1	1	9	16	2596	2617429	12268480	58962	131
$\max_w(\mathbb{K})$	63	63	63	63	62	55	47	27	8
$\min_w(\mathbb{K})$	63	63	61	61	43	19	19	4	1

set indicated by $\mathcal{D}_{\mathbb{K}}$ is the same as that by $\mathcal{D}_{\mathbb{K}'}$. Namely, the result of Algorithm 4 does not change even if we do not perform `SizeReduce` perfectly. Therefore, we execute a partial `SizeReduce` which performs faster. The rough `SizeReduce` first sorts every vector in $\mathbb{K}$ by using lexicographic order and obtains the following $|\mathbb{K}|$ vectors,

$$\boldsymbol{k}^{(1)}, \boldsymbol{k}^{(2)}, \ldots, \boldsymbol{k}^{(|\mathbb{K}|)}.$$

Then, there is no $(\boldsymbol{k}^{(i)}, \boldsymbol{k}^{(j)})$ satisfying $\boldsymbol{k}^{(i)} \succeq \boldsymbol{k}^{(j)}$ such that $i < j$. We initialize two indices, $i = 1$ and $j = 2$, and evaluate whether or not $\boldsymbol{k}^{(j)} \succeq \boldsymbol{k}^{(i)}$. If $\boldsymbol{k}^{(j)} \succeq \boldsymbol{k}^{(i)}$, we remove $\boldsymbol{k}^{(j)}$, and increment j. If $\boldsymbol{k}^{(j)} \not\succeq \boldsymbol{k}^{(i)}$, increment j. Moreover, if we cannot remove $\boldsymbol{k}^{(j)}$ "th" times consecutively, increment i and set $j = i + 1$. We can choose

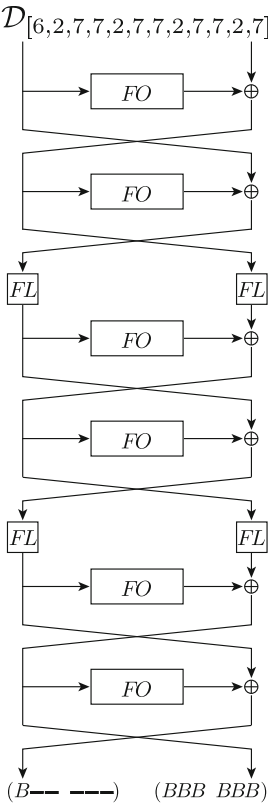

Fig. 5. New 6-round integral characteristic.

th freely. If $th = |\mathbb{K}|$, the above algorithm executes `SizeReduce` perfectly. From our experiments, $th = 10$ or $th = 100$ are reasonable parameters. We also implemented this efficient algorithm by C++, and the execution time is 12.8 min with Core i7-4770 Processor (4 cores) in 16 GB RAM.

6. Key Recovery Using New Integral Characteristic

This section shows the key recovery step of our cryptanalysis, which uses the 6-round integral characteristic shown in Sect. 5. In the characteristic, the left 7-bit value of X_7^L is balanced. Since the integral characteristic does not cover the first FL layer, we first show how to pass through the first FL layer. Then, we calculate two FL layers and one FO function by guessing round keys from ciphertexts, and we evaluate the balanced seven bits.

6.1. *Passage of First FL Layer*

Our new characteristic removes the first FL layer. Therefore, we have to create a set of chosen plaintexts to construct integral characteristics by using guessed round keys $KL_{1,1}$ and $KL_{1,2}$. Here, we have to carefully choose the set of chosen plaintexts to avoid the use of the full code book (see Figs. 6, 7, 8). In every figure, A_i denotes for which we prepare an input set that i bits are active. As an example, we consider an integral characteristic for which the first one bit is constant and the remaining 63 bits are active. Since all bits of the right half are active, we focus only on the left half. We first guess that $KL_{1,2}[1] = 1$, and we then prepare the set of plaintexts as in Fig. 6. We next guess that $(KL_{1,1}[1], KL_{1,2}[1]) = (0, 0)$, and we then prepare the set of plaintexts as in Fig. 7. Moreover, we guess that $(KL_{1,1}[1], KL_{1,2}[1]) = (1, 0)$, and we then prepare the set of plaintexts as in Fig. 8. These chosen plaintexts construct 6-round integral characteristics if the guessed key bits are correct. Note that we do not use 2^{62} chosen plaintexts of the form $(1A_{15}\ 1A_{15}\ A_{16}\ A_{16})$, i.e., we do not use chosen plaintexts satisfying $P^L[1] = P^L[16] = 1$. Thus, our integral characteristics use $2^{64} - 2^{62} \approx 2^{63.58}$ chosen plaintexts.

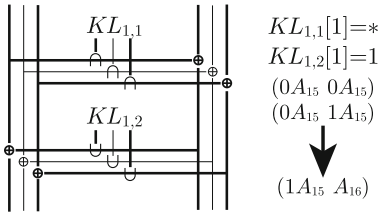

Fig. 6. $KL_{1,2} = 1$.

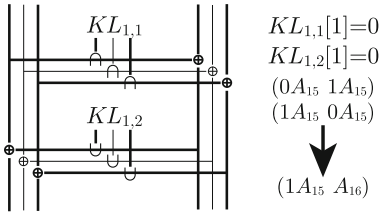

Fig. 7. $KL_{1,1} = 0, KL_{1,2} = 0$.

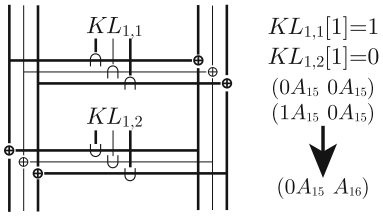

Fig. 8. $KL_{1,1} = 1, KL_{1,2} = 0$.

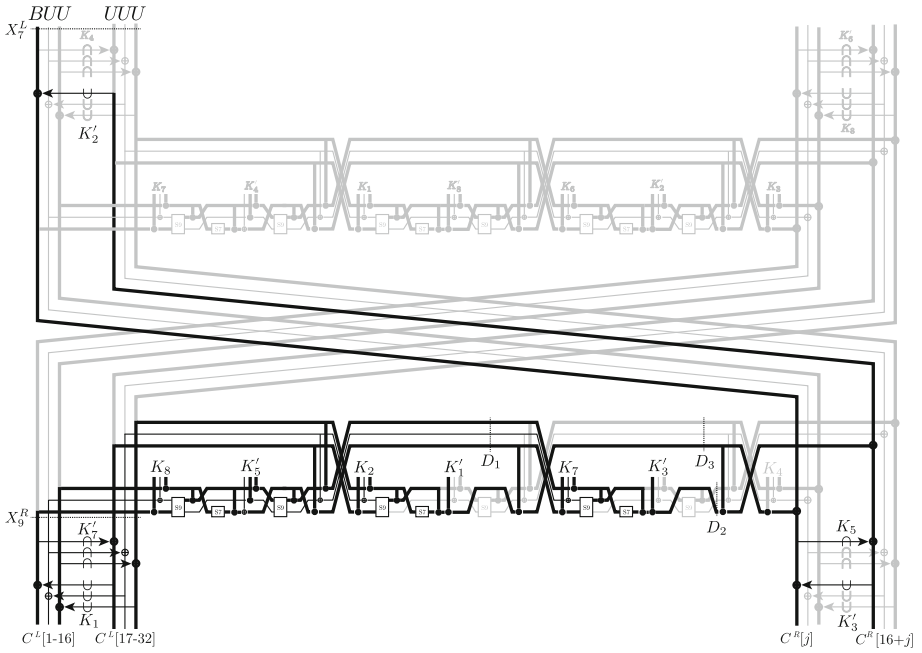

Fig. 9. Key recovery step.

6.2. *Subkey Recovery Using Partial-Sum Technique*

Figure 9 shows the structure of our key recovery step. We guess $KL_{1,1}[i]$ $(= K_1[i])$ and $KL_{1,2}[i]$ $(= K_7'[i])$ and then prepare a set of chosen plaintexts to construct an integral characteristic. In the characteristic, seven bits $X_7^L[1, \ldots, 7]$ are balanced. Therefore, we evaluate whether or not $X_7^L[j]$ is balanced for $j \in \{1, 2, \ldots, 7\}$ by using the partial-sum technique [10].

In the first step, we store the frequency of 34 bits $(C^L, C^R[j, 16 + j])$ into a voting table for $j \in \{1, 2, \ldots, 7\}$. Then, we partially guess round keys, reduce the size of the voting table, and calculate the XOR of $X_7^L[j]$. Table 4 summarizes the procedure of the key recovery step, where every value is defined in Fig. 9.

Step 1: Prepare the memory that stores how many times each 34-bit value $(C^L, C^R[j, 16+j])$ appears, and pick the values that appear an odd number of times.

Step 2: Guess 32-bit (K_1, K_7'), and calculate X_9^R from C^L. Delete the parity of the number of occurrences of C^L from the memory, and store that of X_9^R into the memory. Namely, the memory contains a 2^{34}-bit array that stores the parity of the number of occurrences of the 34-bit string $(X_9^R, C^R[j, 16 + j])$. The time complexity of Step 2 is $2^{34} \times 2^{32} = 2^{66}$.

Step 3: Additionally guess 32-bit (K_8, K_5'), and calculate D_1 from X_9^R. Delete the parity of the number of occurrences of $X_9^R[1, \ldots, 16]$ from the memory, and store that of D_1 into the memory. Namely, the memory contains a 2^{34}-bit

Table 4. Procedure of key recovery step.

Step	Guessed key	#guessed total bits	New value	Discarded values	#texts	Values in set	Complexity
1		0			2^{34}	$C^L, C^R[j, 16+j]$	
2	K_1, K_7'	32	X_9^R	C^L	2^{34}	$X_9^R, C^R[j, 16+j]$	$2^{34+32} = 2^{66}$
3	K_8, K_5'	64	D_1	$X_9^R[1, \ldots, 16]$	2^{34}	$D_1, X_9^R[17, \ldots, 32], C^R[j, 16+j]$	$2^{34+64} = 2^{98}$
4	$K_3'[j], (K_7)$	65	$D_2[j]$	D_1 w/o $D_1[j]$	2^{20}	$D_1[j], D_2[j], X_9^R[17, \ldots, 32], C^R[j, 16+j]$	$2^{34+65} = 2^{99}$
5	$K_2, (K_1'[j])$	81	$D_3[j]$	$X_9^R[17, \ldots, 32], D_1[j]$	2^4	$D_2[j], D_3[j], C^R[j, 16+j]$	$2^{20+81} = 2^{101}$
6	$K_5[j], K_2'[j]$	83	$X_7^L[j]$	$D_2[j], D_3[j], C^R[j, 16+j]$	2^1	$X_7^L[j]$	$2^{4+83} = 2^{87}$

array that stores the parity of the number of occurrences of the 34-bit string $(D_1, X_9^R[17, \ldots, 32], C^R[j, 16+j])$. The time complexity of Step 3 is $2^{34} \times 2^{64} = 2^{98}$.

Step 4: Additionally guess 1-bit $K_3'[j]$, get K_7 from (K_7', K_8), which is already guessed in Step 2 and Step 3, and calculate $D_2[j]$ from D_1. Delete the parity of the number of occurrences of D_1 without $D_1[j]$ from the memory, and store that of $D_2[j]$ into the memory. Namely, the memory contains a 2^{20}-bit array that stores the parity of the number of occurrences of the 20-bit string $(D_1[j], D_2[j], X_9^R[17, \ldots, 32], C^R[j, 16 + j])$. The time complexity of Step 4 is $2^{34} \times 2^{65} = 2^{99}$.

Step 5: Additionally guess 32-bit K_2, get $K_1'[j]$ from (K_1, K_2), which is already guessed in Step 2 and Step 5, and calculate $D_3[j]$ from $(X_9^R[17, \ldots, 32], D_1[j])$. Delete the parity of the number of occurrences of $(X_9^R[17, \ldots, 32], D_1[j])$ from the memory, and store that of $D_3[j]$ into the memory. Namely, the memory contains a 2^4-bit array that stores the parity of the number of occurrences of the 4-bit string $(D_2[j], D_3[j], C^R[j, 16+j])$. The time complexity of Step 5 is $2^{20} \times 2^{81} = 2^{101}$.

Step 6: Additionally guess 2-bit $(K_5[j], K_2'[j])$, get $K_3'[j]$, which is already guessed in Step 4, and calculate $X_7^L[j]$ from $(D_2[j], D_3[j], C^R[j, 16 + j])$. The time complexity of Step 6 is $2^4 \times 2^{83} = 2^{87}$.

The total time complexity is

$$2^{66} + 2^{98} + 2^{99} + 2^{101} + 2^{87} \approx 2^{101.5}.$$

We repeat the above six steps for $j \in \{1, 2, \ldots, 7\}$. Therefore, the time complexity of the key recovery step is $7 \times 2^{101.5} = 2^{104.3}$.

The key recovery step has to guess the 124-bit key

$$K_1, K_2, K_5[1, \ldots, 7], K_7, K_8,$$
$$K_1'[1, \ldots, 7], K_2'[1, \ldots, 7], K_3'[1, \ldots, 7], K_5', K_7'.$$

Here, K_7' and $K_1'[1, \ldots, 7]$ are uniquely determined by guessing K_7, K_8 and K_1, K_2, respectively. Thus, the guessed key material is reduced to

$$K_1, K_2, K_5[1, \ldots, 7], K_7, K_8,$$
$$K_2'[1, \ldots, 7], K_3'[1, \ldots, 7], K_5',$$

and its size becomes 101 bits. Moreover, since we already guessed 2 bits, i.e., $K_1[i]$ and $K_7'[i]$, to construct integral characteristics, the guessed key bit size is reduced to 99 bits. For wrong keys, the probability that $X_7^L[1, \ldots, 7]$ is balanced is 2^{-7}. Therefore, the number of the candidates of round keys is reduced to 2^{92}. Finally, we guess the 27 bits:

$$K_5[8, \ldots, 16], K_2'[8, \ldots, 16], K_3'[8, \ldots, 16].$$

Note that K_3, K_4, and K_6 are uniquely determined from (K_2, K_2'), (K_3, K_3'), and (K_5, K_5'), respectively. Therefore, the total time complexity is $2^{92+27} = 2^{119}$. We guess the correct key from 2^{119} candidates by using two plaintext–ciphertext pairs, and the time complexity is $2^{119} + 2^{119-64} \approx 2^{119}$. We have to execute the above procedure against $(K_1[i], K_7'[i]) = (0, 0), (0, 1), (1, 0), (1, 1)$, and the time complexity becomes $4 \times 2^{119} = 2^{121}$.

6.3. *Trade-off Between Time and Data Complexity*

In Sect. 6.2, we use only one set of chosen plaintexts, where $(2^{64} - 2^{62})$ chosen plaintexts are required. Since the probability that wrong keys are not discarded is 2^{-7}, a brute-force search is required with a time complexity of $2^{128-7} = 2^{121}$, and it is larger than the time complexity of the partial-sum technique. Therefore, if we have a higher number of characteristics, the total time complexity can be reduced.

To exploit several characteristics, we choose some constant bits from seven bits ($i \in \{1, 2, \ldots, 7\}$). If we use a characteristic with $i = 1$, we use chosen plaintexts for which plaintext P^L takes the following values

$$
\begin{aligned}
&(00A_{14}\ \ 00A_{14}), (00A_{14}\ \ 01A_{14}), (01A_{14}\ \ 00A_{14}), (01A_{14}\ \ 01A_{14}),\\
&(00A_{14}\ \ 10A_{14}), (00A_{14}\ \ 11A_{14}), (01A_{14}\ \ 10A_{14}), (01A_{14}\ \ 11A_{14}),\\
&(10A_{14}\ \ 00A_{14}), (10A_{14}\ \ 01A_{14}), (11A_{14}\ \ 00A_{14}), (11A_{14}\ \ 01A_{14}),
\end{aligned}
$$

where A_{14} denotes that all values appear the same number independently of other bits, e.g., $(00A_{14}\ \ 00A_{14})$ uses 2^{60} chosen plaintexts because P^R also takes all values. Moreover, if we use a characteristic with $i = 2$, we use chosen plaintexts for which P^L takes the following values

$$
\begin{aligned}
&(00A_{14}\ \ 00A_{14}), (00A_{14}\ \ 10A_{14}), (10A_{14}\ \ 00A_{14}), (10A_{14}\ \ 10A_{14}),\\
&(00A_{14}\ \ 01A_{14}), (00A_{14}\ \ 11A_{14}), (10A_{14}\ \ 01A_{14}), (10A_{14}\ \ 11A_{14}),\\
&(01A_{14}\ \ 00A_{14}), (01A_{14}\ \ 10A_{14}), (11A_{14}\ \ 00A_{14}), (11A_{14}\ \ 10A_{14}).
\end{aligned}
$$

When both characteristics are used, they do not require choosing plaintexts for which P^L takes $(11A_{14}\ \ 11A_{14})$. Therefore, $(2^{64} - 2^{60})$ chosen plaintexts are required, and the probability that wrong keys are not discarded becomes 2^{-14}. Similarly, when three characteristics, which require $(2^{64} - 2^{58})$ chosen plaintexts, are used, the probability that wrong keys are not discarded becomes 2^{-21}.

Table 5 summarizes the trade-off between time and data complexity. For the use of each characteristic, we have to execute four key recoveries with the partial-sum technique, i.e., for $(KL_{1,1}[1], KL_{1,2}[1]) \in \{(0, 1), (1, 1), (0, 0), (1, 0)\}$. It shows that the use of four characteristics is optimized from the perspective of time complexity. Namely, when $(2^{64} - 2^{56}) \approx 2^{63.994}$ chosen plaintexts are required, the time complexity to recover the secret key is $2^{108.3}$.

Table 5. Trade-off between time and data complexity.

#characteristics	Complexity for partial-sum	Complexity for brute-force	Total
1	$1 \times 4 \times 2^{104.3}$	2^{121}	2^{121}
2	$2 \times 4 \times 2^{104.3}$	2^{114}	2^{114}
3	$3 \times 4 \times 2^{104.3}$	2^{107}	$2^{108.5}$
4	$4 \times 4 \times 2^{104.3}$	2^{100}	$2^{108.3}$
5	$5 \times 4 \times 2^{104.3}$	2^{93}	$2^{108.6}$

6.4. *Follow-Up Results and Open Problem*

After a preliminary version [26] was published, Achiya Bar-On improved the key recovery step [2] by using the same integral characteristic shown in this paper. The improved key recovery technique uses the meet-in-the-middle technique [23] under the chosen ciphertext setting. It dramatically reduces the time complexity where the secret key is recovered, and the time complexity is $2^{69.5}$. On the other hand, it requires the full code book. When we consider the data complexity optimization, our attack, which requires 2^{121} time complexity and $2^{63.58}$ chosen plaintexts, is still the best attack. We need to construct a more efficient integral characteristic if we want to improve the data complexity, and it is left as an open problem.

7. Conclusions

In this paper, we showed a cryptanalysis of the full MISTY1. MISTY1 was well evaluated and standardized by several projects, such as CRYPTREC, ISO/IEC, and NESSIE. We constructed a new integral characteristic by using the propagation characteristic of the division property. Here, we improved the division property by optimizing the division property for a public S-box. As a result, a new 6-round integral characteristic is constructed, and we can recover the secret key of the full MISTY1 with $2^{63.58}$ chosen plaintexts and 2^{121} time complexity. If we can use $2^{63.994}$ chosen plaintexts, our attack can recover the secret key with a time complexity of $2^{108.3}$.

Appendix 1: MISTY S-boxes

The ANF of S_7 is represented as

$$
\begin{aligned}
y[0] &= x[0] \oplus x[1]x[3] \oplus x[0]x[3]x[4] \oplus x[1]x[5] \oplus x[0]x[2]x[5] \oplus x[4]x[5] \\
&\quad \oplus x[0]x[1]x[6] \oplus x[2]x[6] \oplus x[0]x[5]x[6] \oplus x[3]x[5]x[6] \oplus 1, \\
y[1] &= x[0]x[2] \oplus x[0]x[4] \oplus x[3]x[4] \oplus x[1]x[5] \oplus x[2]x[4]x[5] \oplus x[6] \oplus x[0]x[6] \\
&\quad \oplus x[3]x[6] \oplus x[2]x[3]x[6] \oplus x[1]x[4]x[6] \oplus x[0]x[5]x[6] \oplus 1, \\
y[2] &= x[1]x[2] \oplus x[0]x[2]x[3] \oplus x[4] \oplus x[1]x[4] \oplus x[0]x[1]x[4] \oplus x[0]x[5] \oplus x[0]x[4]x[5] \\
&\quad \oplus x[3]x[4]x[5] \oplus x[1]x[6] \oplus x[3]x[6] \oplus x[0]x[3]x[6] \oplus x[4]x[6] \oplus x[2]x[4]x[6], \\
y[3] &= x[0] \oplus x[1] \oplus x[0]x[1]x[2] \oplus x[0]x[3] \oplus x[2]x[4] \oplus x[1]x[4]x[5] \oplus x[2]x[6]
\end{aligned}
$$

$$
\begin{aligned}
&\oplus x[1]x[3]x[6] \oplus x[0]x[4]x[6] \oplus x[5]x[6] \oplus 1,\\
y[4] = {}& x[2]x[3] \oplus x[0]x[4] \oplus x[1]x[3]x[4] \oplus x[5] \oplus x[2]x[5] \oplus x[1]x[2]x[5] \oplus x[0]x[3]x[5]\\
&\oplus x[1]x[6] \oplus x[1]x[5]x[6] \oplus x[4]x[5]x[6] \oplus 1,\\
y[5] = {}& x[0] \oplus x[1] \oplus x[2] \oplus x[0]x[1]x[2] \oplus x[0]x[3] \oplus x[1]x[2]x[3] \oplus x[1]x[4]\\
&\oplus x[0]x[2]x[4] \oplus x[0]x[5] \oplus x[0]x[1]x[5] \oplus x[3]x[5] \oplus x[0]x[6] \oplus x[2]x[5]x[6],\\
y[6] = {}& x[0]x[1] \oplus x[3] \oplus x[0]x[3] \oplus x[2]x[3]x[4] \oplus x[0]x[5] \oplus x[2]x[5] \oplus x[3]x[5]\\
&\oplus x[1]x[3]x[5] \oplus x[1]x[6] \oplus x[1]x[2]x[6] \oplus x[0]x[3]x[6] \oplus x[4]x[6] \oplus x[2]x[5]x[6].
\end{aligned}
$$

Moreover, the ANF of S_9 is represented as

$$
\begin{aligned}
y[0] = {}& x[0]x[4] \oplus x[0]x[5] \oplus x[1]x[5] \oplus x[1]x[6] \oplus x[2]x[6] \oplus x[2]x[7] \oplus x[3]x[7] \oplus x[3]x[8]\\
&\oplus x[4]x[8] \oplus 1,\\
y[1] = {}& x[0]x[2] \oplus x[3] \oplus x[1]x[3] \oplus x[2]x[3] \oplus x[3]x[4] \oplus x[4]x[5] \oplus x[0]x[6] \oplus x[2]x[6]\\
&\oplus x[7] \oplus x[0]x[8] \oplus x[3]x[8] \oplus x[5]x[8] \oplus 1,\\
y[2] = {}& x[0]x[1] \oplus x[1]x[3] \oplus x[4] \oplus x[0]x[4] \oplus x[2]x[4] \oplus x[3]x[4] \oplus x[4]x[5] \oplus x[0]x[6]\\
&\oplus x[5]x[6] \oplus x[1]x[7] \oplus x[3]x[7] \oplus x[8],\\
y[3] = {}& x[0] \oplus x[1]x[2] \oplus x[2]x[4] \oplus x[5] \oplus x[1]x[5] \oplus x[3]x[5] \oplus x[4]x[5] \oplus x[5]x[6]\\
&\oplus x[1]x[7] \oplus x[6]x[7] \oplus x[2]x[8] \oplus x[4]x[8],\\
y[4] = {}& x[1] \oplus x[0]x[3] \oplus x[2]x[3] \oplus x[0]x[5] \oplus x[3]x[5] \oplus x[6] \oplus x[2]x[6] \oplus x[4]x[6]\\
&\oplus x[5]x[6] \oplus x[6]x[7] \oplus x[2]x[8] \oplus x[7]x[8],\\
y[5] = {}& x[2] \oplus x[0]x[3] \oplus x[1]x[4] \oplus x[3]x[4] \oplus x[1]x[6] \oplus x[4]x[6] \oplus x[7] \oplus x[3]x[7]\\
&\oplus x[5]x[7] \oplus x[6]x[7] \oplus x[0]x[8] \oplus x[7]x[8],\\
y[6] = {}& x[0]x[1] \oplus x[3] \oplus x[1]x[4] \oplus x[2]x[5] \oplus x[4]x[5] \oplus x[2]x[7] \oplus x[5]x[7] \oplus x[8]\\
&\oplus x[0]x[8] \oplus x[4]x[8] \oplus x[6]x[8] \oplus x[7]x[8] \oplus 1,\\
y[7] = {}& x[1] \oplus x[0]x[1] \oplus x[1]x[2] \oplus x[2]x[3] \oplus x[0]x[4] \oplus x[5] \oplus x[1]x[6] \oplus x[3]x[6]\\
&\oplus x[0]x[7] \oplus x[4]x[7] \oplus x[6]x[7] \oplus x[1]x[8] \oplus 1,\\
y[8] = {}& x[0] \oplus x[0]x[1] \oplus x[1]x[2] \oplus x[4] \oplus x[0]x[5] \oplus x[2]x[5] \oplus x[3]x[6] \oplus x[5]x[6]\\
&\oplus x[0]x[7] \oplus x[0]x[8] \oplus x[3]x[8] \oplus x[6]x[8] \oplus 1.
\end{aligned}
$$

Appendix 2: Proof of Propagation Rules

Proof of Rule 1 (Substitution)

Let F be a function that consists of m S-boxes, where F_i denotes the ith S-box and the bit length and the algebraic degree is n_i bits and d_i, respectively. The input and the output take a value of $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$, and $\mathbb{X}$ and $\mathbb{Y}$ denote the input multiset and the output multiset, respectively.

First, we only apply the first S-box and evaluate the division property of the multiset whose elements are represented by $[F_1(x_1), x_2, \ldots, x_m]$. Assuming that the multiset $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^{n_1,n_2,\ldots,n_m}$, the parity $\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{\boldsymbol{v}}([F_1(x_1), x_2, \ldots, x_m])$ is evaluated as follows:

$$\begin{aligned}
\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{\boldsymbol{v}}([F_1(x_1), x_2, \ldots, x_m]) &= \bigoplus_{\boldsymbol{x}\in\mathbb{X}} \left((\pi_{v_1} \circ F_1)(x_1) \times \prod_{i=2}^{m} \pi_{v_i}(x_i) \right) \\
&= \bigoplus_{\boldsymbol{x}\in\mathbb{X}} \left(\left(\bigoplus_{u_1\in\mathbb{F}_2^{n_1}} a_{u_1}^{(\pi_{v_1}\circ F_1)} \pi_{u_1}(x_1) \right) \times \left(\prod_{i=2}^{m} \pi_{v_i}(x_i) \right) \right) \\
&= \bigoplus_{u_1\in\mathbb{F}_2^{n_1}} \left(\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \left(a_{u_1}^{(\pi_{v_1}\circ F_1)} \pi_{u_1}(x_1) \times \prod_{i=2}^{m} \pi_{v_i}(x_i) \right) \right) \\
&= \bigoplus_{u_1\in\mathbb{F}_2^{n_1}} \left(a_{u_1}^{(\pi_{v_1}\circ F_1)} \bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{[u_1, v_2, v_3, \ldots, v_m]}(\boldsymbol{x}) \right).
\end{aligned}$$

Therefore, for any $\boldsymbol{v} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$, the parity $\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{\boldsymbol{v}}([F_1(x_1), x_2, \ldots, x_m])$ is 0 if

$$a_{u_1}^{(\pi_{v_1}\circ F_1)} \bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{[u_1, v_2, v_3, \ldots, v_m]}(\boldsymbol{x})$$

is 0 for all $u_1 \in \mathbb{F}_2^{n_1}$. Since the algebraic degree of $(\pi_{v_1} \circ F_1)$ is at most $w(v_1) \times d_1$, $a_{u_1}^{(\pi_{v_1}\circ F_1)} = 0$ when $w(u_1) > w(v_1) \times d_1$. Therefore, the parity becomes unknown only if we cannot determine the value of $\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{[u_1, v_2, v_3, \ldots, v_m]}(\boldsymbol{x})$ when $w(u_1) \le w(v_1) \times d_1$. Now, since the multiset $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^{n_1, n_2, \ldots, n_m}$,

$$\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{\boldsymbol{u}}(\boldsymbol{x}) = \begin{cases} \text{unknown} & \text{if there exist } \boldsymbol{k} \in \mathbb{K} \text{ s.t. } W(\boldsymbol{u}) \succeq \boldsymbol{k}, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, the necessary condition that $\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{[u_1, v_2, v_3, \ldots, v_m]}(\boldsymbol{x})$ becomes unknown is expressed as follows:

$$\begin{aligned}
&W([u_1, v_2, v_3, \ldots, v_m]) \succeq \boldsymbol{k}, \\
&\quad \Rightarrow [w(v_1) \times d_1, w(v_2), \ldots, w(v_m)] \succeq \boldsymbol{k}, \\
&\quad \Rightarrow [w(v_1), w(v_2), \ldots, w(v_m)] \succeq \left[\left\lceil \frac{k_1}{d_1} \right\rceil, k_2, k_3, \ldots, k_m \right].
\end{aligned}$$

Namely, $\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{\boldsymbol{v}}([F(x_1), x_2, \ldots, x_m])$ is unknown only if there exists $\boldsymbol{k} \in \mathbb{K}$ satisfying

$$W(v_1, v_2, v_3, \ldots, v_m) \succeq \left[\left\lceil \frac{k_1}{d_1} \right\rceil, k_2, k_3, \ldots, k_m \right].$$

Therefore, the division property of the output multiset is $\mathcal{D}^{n_1,n_2,\ldots,n_m}_{\mathbb{K}'}$, where $\mathbb{K}'$ has the following vectors

$$\left[\left\lceil\frac{k_1}{d_1}\right\rceil, k_2, \ldots, k_m\right] \quad \text{for all } \boldsymbol{k} \in \mathbb{K}.$$

Next, assume that F_1 is bijective and $k_1 = n_1$. Then, the algebraic degree of $(\pi_{v_1} \circ F_1)$ is less than n_1 for $w(v_1) < n_1$ and becomes n_1 for only $w(v_1) = n_1$. Therefore, the necessary condition that $\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{[u_1,v_2,v_3,\ldots,v_m]}(\boldsymbol{x})$ becomes unknown is $w(v_1) = n_1$. Namely, if $k_1 = n_1$, $[n_1, k_2, k_3, \ldots, k_m]$ is inserted into $\mathbb{K}'$ instead of $[\lceil k_1/d_1 \rceil, k_2, \ldots, k_m]$. Finally, Rule 1 is proven by repeating the same procedure for other S-boxes.

Proof of Rule 2 (Copy)

Let F be a copy function, where the input x takes a value of $\mathbb{F}_2^n$ and the output is calculated as $[y_1, y_2] = [x, x]$. Let $\mathbb{X}$ and $\mathbb{Y}$ be the input multiset and the output multiset, respectively.

Assuming that the multiset $\mathbb{X}$ has the division property $\mathcal{D}^n_k$, the parity $\bigoplus_{\boldsymbol{y}\in\mathbb{Y}} \pi_{\boldsymbol{v}}(\boldsymbol{y})$ is evaluated as follows:

$$\bigoplus_{\boldsymbol{y}\in\mathbb{Y}} \pi_{\boldsymbol{v}}(\boldsymbol{y}) = \bigoplus_{x\in\mathbb{X}} \pi_{[v_1,v_2]}([x,x]) = \bigoplus_{x\in\mathbb{X}} \left(\pi_{v_1}(x) \times \pi_{v_2}(x)\right) = \bigoplus_{x\in\mathbb{X}} \left(\pi_{v_1\vee v_2}(x)\right).$$

Since the multiset $\mathbb{X}$ has the division property $\mathcal{D}^n_k$,

$$\bigoplus_{x\in\mathbb{X}} \pi_u(x) = \begin{cases} \text{unknown} & w(u) \geq k, \\ 0 & w(u) < k. \end{cases}$$

When $w(v_1) + w(v_2) < k$, the parity $\bigoplus_{\boldsymbol{y}\in\mathbb{Y}} \pi_{\boldsymbol{v}}(\boldsymbol{y})$ is 0 because $w(v_1 \vee v_2) \leq w(v_1) + w(v_2) < k$. Moreover, the necessary condition that the parity becomes unknown is $w(v_1) + w(v_2) \geq k$. Therefore, the division property of $\mathbb{Y}$ is $\mathcal{D}^{n,n}_{\mathbb{K}'}$, where $\mathbb{K}'$ has the following vectors

$$[k - i, i] \quad \text{for } 0 \leq i \leq k.$$

Thus, Rule 2 is proven.

Proof of Rule 3 (Compression by XOR)

Let F be a compression function by an XOR, where the input $[x_1, x_2]$ takes a value of $(\mathbb{F}_2^n \times \mathbb{F}_2^n)$ and the output is calculated as $y = x_1 \oplus x_2$. Let $\mathbb{X}$ and $\mathbb{Y}$ be the input multiset and the output multiset, respectively.

Assuming that the multiset $\mathbb{X}$ has the division property $\mathcal{D}^{n,n}_{\mathbb{K}}$, the parity $\bigoplus_{y\in\mathbb{Y}}\pi_v(y)$ is evaluated as follows:

$$\begin{aligned}\bigoplus_{y\in\mathbb{Y}}\pi_v(y) = \bigoplus_{[x_1,x_2]\in\mathbb{X}}\pi_v(x_1\oplus x_2) &= \bigoplus_{[x_1,x_2]\in\mathbb{X}}\left(\prod_{i=1}^{n}(x_1[i]\oplus x_2[i])^{v[i]}\right)\\ &= \bigoplus_{[x_1,x_2]\in\mathbb{X}}\left(\bigoplus_{\boldsymbol{w}\in\{1,2\}^n}\left(\prod_{i=1}^{n}x_{w_i}[i]^{v[i]}\right)\right)\\ &= \bigoplus_{\boldsymbol{w}\in\{1,2\}^n}\left(\bigoplus_{[x_1,x_2]\in\mathbb{X}}\left(\prod_{i=1}^{n}x_{w_i}[i]^{v[i]}\right)\right)\\ &= \bigoplus_{\boldsymbol{w}\in\{1,2\}^n}\left(\bigoplus_{[x_1,x_2]\in\mathbb{X}}\left(\pi_{\delta_1(v,\boldsymbol{w})}(x_1)\times\pi_{\delta_2(v,\boldsymbol{w})}(x_2)\right)\right),\end{aligned}$$

where

$$\delta_j(v,\boldsymbol{w})[i] = \begin{cases}1 & v[i]=1 \text{ and } w_i = j,\\ 0 & \text{otherwise.}\end{cases}$$

Since the multiset $\mathbb{X}$ has the division property $\mathcal{D}^{n,n}_{\mathbb{K}}$,

$$\bigoplus_{\boldsymbol{x}\in\mathbb{X}}\pi_{[u_1,u_2]}(\boldsymbol{x}) = \begin{cases}\text{unknown} & \text{if there exist } [k_1,k_2]\in\mathbb{K} \text{ s.t. } [w(u_1),w(u_2)]\succeq[k_1,k_2],\\ 0 & \text{otherwise.}\end{cases}$$

When $w(v) = w(\delta_1(v,\boldsymbol{w})) + w(\delta_2(v,\boldsymbol{w})) < \min_{\boldsymbol{k}\in\mathbb{K}}\{k_1+k_2\}$, the parity $\bigoplus_{y\in\mathbb{Y}}\pi_v(y)$ is 0 because there is not $[k_1,k_2]\in\mathbb{K}$ satisfying $[w(\delta_1(v,\boldsymbol{w})), w(\delta_2(v,\boldsymbol{w}))]\succeq[k_1,k_2]$. Moreover, the necessary condition that the parity becomes unknown is $w(v)\geq \min_{\boldsymbol{k}\in\mathbb{K}}\{k_1+k_2\}$. Therefore, the division property of $\mathbb{Y}$ is $\mathcal{D}^n_{k'}$, where $k' = \min_{\boldsymbol{k}\in\mathbb{K}}\{k_1+k_2\}$. Note that the parity is 0 for all v if k' is greater than n. Thus, Rule 3 is proven.

Proof of Rule 4 (Split)

Let F be a split function, where the input x takes a value of $\mathbb{F}_2^n$ and the output is calculated as $y_1\|y_2 = x$, where $[y_1,y_2]$ takes a value of $(\mathbb{F}_2^{n_1}\times\mathbb{F}_2^{n-n_1})$. Let $\mathbb{X}$ and $\mathbb{Y}$ be the input multiset and the output multiset, respectively.

Assuming that the multiset $\mathbb{X}$ has the division property $\mathcal{D}^n_k$, the parity $\bigoplus_{\boldsymbol{y}\in\mathbb{Y}}\pi_{\boldsymbol{v}}(\boldsymbol{y})$ is evaluated as follows:

$$\bigoplus_{\boldsymbol{y}\in\mathbb{Y}}\pi_{\boldsymbol{v}}(\boldsymbol{y}) = \bigoplus_{x\in\mathbb{X}}\pi_{[v_1\|v_2]}(x).$$

Since the multiset $\mathbb{X}$ has the division property $\mathcal{D}_k^n$,

$$\bigoplus_{x\in\mathbb{X}} \pi_u(x) = \begin{cases} \text{unknown} & w(u) \geq k, \\ 0 & w(u) < k. \end{cases}$$

When $w(v_1) + w(v_2) < k$, the parity $\bigoplus_{\boldsymbol{y}\in\mathbb{Y}} \pi_{\boldsymbol{v}}(\boldsymbol{y})$ is 0 because $w(v_1\|v_2) = w(v_1) + w(v_2) < k$. Moreover, the necessary condition that the parity becomes unknown is $w(v_1) + w(v_2) \geq k$. Therefore, the division property of $\mathbb{Y}$ is $\mathcal{D}_{\mathbb{K}'}^{n_1, n-n_1}$, where $\mathbb{K}'$ has the following vectors

$$[k-i, i] \quad \text{for } 0 \leq i \leq k.$$

Note that we cannot choose more than n_1 and $n - n_1$ bits from y_1 and y_2, respectively. Thus, Rule 4 is proven.

Proof of Rule 5 (Concatenation)

Let F be a concatenation function, where the input $[x_1, x_2]$ takes a value of $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2})$ and the output is calculated as $y = x_1\|x_2$. Let $\mathbb{X}$ and $\mathbb{Y}$ be the input multiset and the output multiset, respectively.

Assuming that the multiset $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^{n_1,n_2}$, the parity $\bigoplus_{y\in\mathbb{Y}} \pi_v(y)$ is evaluated as follows:

$$\bigoplus_{y\in\mathbb{Y}} \pi_v(y) = \bigoplus_{[x_1,x_2]\in\mathbb{X}} \pi_{v_1\|v_2}(x_1\|x_2) = \bigoplus_{[x_1,x_2]\in\mathbb{X}} \pi_{[v_1,v_2]}([x_1, x_2]),$$

where $v = v_1\|v_2$, and the bit length of v_1 and that of v_2 is n_1 and n_2, respectively. Since the multiset $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^{n_1,n_2}$,

$$\bigoplus_{\boldsymbol{x}\in\mathbb{X}} \pi_{[u_1,u_2]}(\boldsymbol{x}) = \begin{cases} \text{unknown} & \text{if there exist } [k_1, k_2] \in \mathbb{K} \text{ s.t. } [w(u_1), w(u_2)] \succeq [k_1, k_2], \\ 0 & \text{otherwise.} \end{cases}$$

When $w(v) = w(v_1) + w(v_2) < \min_{\boldsymbol{k}\in\mathbb{K}}\{k_1 + k_2\}$, the parity $\bigoplus_{y\in\mathbb{Y}} \pi_v(y)$ is 0 because there is not $[k_1, k_2] \in \mathbb{K}$ satisfying $[w(v_1), w(v_2)] \succeq [k_1, k_2]$. Moreover, the necessary condition that the parity becomes unknown is $w(v) \geq \min_{\boldsymbol{k}\in\mathbb{K}}\{k_1 + k_2\}$. Therefore, the division property of $\mathbb{Y}$ is $\mathcal{D}_{k'}^n$, where $k' = \min_{\boldsymbol{k}\in\mathbb{K}}\{k_1 + k_2\}$. Thus, Rule 5 is proven.

Appendix 3: Example—Propagation from $\mathcal{D}_{\{[4,2,6]\}}^{7,2,7}$ for FI Function

We consider the propagation characteristic of the division property for the FI function (see Fig. 4). Assume that $\mathbb{X}_1$ has the division property $\mathcal{D}_{\{[4,2,6]\}}^{7,2,7}$.

From $\mathbb{X}_1$ *to* $\mathbb{X}_2$: Since the first 7-bit value and the second 2-bit value are concatenated, Rule 5 is applied. Thus, the multiset $\mathbb{X}_2$ has the division property $\mathcal{D}_{\{[6,6]\}}^{9,7}$.

From $\mathbb{X}_2$ *to* $\mathbb{X}_3$: The 9-bit S-box S_9 is applied. Thus, the multiset $\mathbb{X}_3$ has the division property $\mathcal{D}^{9,7}_{\{[3,6]\}}$.

From $\mathbb{X}_3$ *to* $\mathbb{X}_4$: Since the first 9-bit value is split to 2-bit and 7-bit values, Rule 4 is applied. Thus, the multiset $\mathbb{X}_4$ has the division property $\mathcal{D}^{2,7,7}_{\{[0,3,6],[1,2,6],[2,1,6]\}}$.

From $\mathbb{X}_4$ *to* $\mathbb{X}_5$: Since the second 7-bit value is XORed with the last 7-bit value, Rule 2 and Rule 3 are applied. In this case, the propagation of the division property is calculated as

$$
\begin{aligned}
&[0, 3, 6] \Rightarrow [0, 3, 6], [0, 4, 5], [0, 5, 4], [0, 6, 3], [0, 7, 2],\\
&[1, 2, 6] \Rightarrow [1, 2, 6], [1, 3, 5], [1, 4, 4], [1, 5, 3], [1, 6, 2], [1, 7, 1],\\
&[2, 1, 6] \Rightarrow [2, 1, 6], [2, 2, 5], [2, 3, 4], [2, 4, 3], [2, 5, 2], [2, 6, 1], [2, 7, 0].
\end{aligned}
$$

The position is rotated, and then, the division property of $\mathbb{X}_5$ has $\mathcal{D}^{7,2,7}_{\mathbb{K}}$, where $\mathbb{K}$ has 18 vectors as

$$
\begin{aligned}
&[6, 0, 3], [5, 0, 4], [4, 0, 5], [3, 0, 6], [2, 0, 7],\\
&[6, 1, 2], [5, 1, 3], [4, 1, 4], [3, 1, 5], [2, 1, 6], [1, 1, 7],\\
&[6, 2, 1], [5, 2, 2], [4, 2, 3], [3, 2, 4], [2, 2, 5], [1, 2, 6], [0, 2, 7].
\end{aligned}
$$

From $\mathbb{X}_5$ *to* $\mathbb{X}_6$: The 7-bit S-box S_7 is applied. Here, we exploit the vulnerable property of S_7. Thus, the following 18 vectors

$$
\begin{aligned}
&[4, 0, 3], [2, 0, 4], [2, 0, 5], [1, 0, 6], [1, 0, 7],\\
&[4, 1, 2], [2, 1, 3], [2, 1, 4], [1, 1, 5], [1, 1, 6], [1, 1, 7],\\
&[4, 2, 1], [2, 2, 2], [2, 2, 3], [1, 2, 4], [1, 2, 5], [1, 2, 6], [0, 2, 7],
\end{aligned}
$$

are calculated. For example, the vector $[2, 0, 5]$ is removed because $[2, 0, 5] \succ [2, 0, 4]$. Similarly, after removing redundant vectors, and the division property of $\mathbb{X}_6$ has $\mathcal{D}^{7,2,7}_{\mathbb{K}}$, where $\mathbb{K}$ has 10 vectors as

$$
\begin{aligned}
&[0, 2, 7], [1, 0, 6], [1, 1, 5], [1, 2, 4], [2, 0, 4],\\
&[2, 1, 3], [2, 2, 2], [4, 0, 3], [4, 1, 2], [4, 2, 1].
\end{aligned}
$$

From $\mathbb{X}_6$ *to* $\mathbb{X}_7$: Since the first 7-bit value is XORed with the last 7-bit value, Rule 2 and Rule 3 are applied. In this case, the propagation of the division property is calculated as

$$
\begin{aligned}
&[0, 2, 7] \Rightarrow [0, 2, 7], [1, 2, 6], [2, 2, 5], [3, 2, 4], [4, 2, 3], [5, 2, 2], [6, 2, 1], [7, 2, 0],\\
&[1, 0, 6] \Rightarrow [1, 0, 6], [2, 0, 5], [3, 0, 4], [4, 0, 3], [5, 0, 2], [6, 0, 1], [7, 0, 0],\\
&[1, 1, 5] \Rightarrow [1, 1, 5], [2, 1, 4], [3, 1, 3], [4, 1, 2], [5, 1, 1], [6, 1, 0],\\
&[1, 2, 4] \Rightarrow [1, 2, 4], [2, 2, 3], [3, 2, 2], [4, 2, 1], [5, 2, 0],\\
&[2, 0, 4] \Rightarrow [2, 0, 4], [3, 0, 3], [4, 0, 2], [5, 0, 1], [6, 0, 0],\\
&[2, 1, 3] \Rightarrow [2, 1, 3], [3, 1, 2], [4, 1, 1], [5, 1, 0],
\end{aligned}
$$

$[2, 2, 2] \Rightarrow [2, 2, 2], [3, 2, 1], [4, 2, 0],$
$[4, 0, 3] \Rightarrow [4, 0, 3], [5, 0, 2], [6, 0, 1], [7, 0, 0],$
$[4, 1, 2] \Rightarrow [4, 1, 2], [5, 1, 1], [6, 1, 0],$
$[4, 2, 1] \Rightarrow [4, 2, 1], [5, 2, 0].$

After removing redundant vectors, the position is rotated and then the division property of $\mathbb{X}_7$ has $\mathcal{D}_{\mathbb{K}}^{2,7,7}$, where $\mathbb{K}$ has 16 vectors as

$$[0, 0, 6], [0, 1, 5], [0, 2, 4], [0, 3, 3], [0, 4, 2], [0, 6, 1], [1, 0, 5], [1, 1, 4],$$
$$[1, 2, 3], [1, 3, 2], [1, 5, 1], [2, 0, 4], [2, 1, 3], [2, 2, 2], [2, 4, 1], [2, 7, 0].$$

From $\mathbb{X}_7$ *to* $\mathbb{X}_8$: Since the first 2-bit value and the second 7-bit value are concatenated, Rule 5 is applied. Then, the following 16 vectors

$$[0, 6], [1, 5], [2, 4], [3, 3], [4, 2], [6, 1], [1, 5], [2, 4],$$
$$[3, 3], [4, 2], [6, 1], [2, 4], [3, 3], [4, 2], [6, 1], [9, 0],$$

are calculated. After removing redundant vectors, the division property of $\mathbb{X}_8$ has $\mathcal{D}_{\mathbb{K}}^{9,7}$, where $\mathbb{K}$ has 7 vectors as

$$[0, 6], [1, 5], [2, 4], [3, 3], [4, 2], [6, 1], [9, 0].$$

From $\mathbb{X}_8$ *to* $\mathbb{X}_9$: The 9-bit S-box S_9 is applied. Then, the following 7 vectors

$$[0, 6], [1, 5], [1, 4], [2, 3], [2, 2], [3, 1], [9, 0],$$

are calculated. After removing redundant vectors, the division property of $\mathbb{X}_9$ has $\mathcal{D}_{\mathbb{K}}^{9,7}$, where $\mathbb{K}$ has 5 vectors as

$$[0, 6], [1, 4], [2, 2], [3, 1], [9, 0].$$

From $\mathbb{X}_9$ *to* $\mathbb{X}_{10}$: Since the first 9-bit value is split to 2-bit and 7-bit values, Rule 4 is applied. Thus, the multiset $\mathbb{X}_{10}$ has the division property $\mathcal{D}_{\mathbb{K}}^{2,7,7}$, where $\mathbb{K}$ has 10 vectors as

$$[0, 6] \Rightarrow [0, 0, 6],$$
$$[1, 4] \Rightarrow [0, 1, 4], [1, 0, 4],$$
$$[2, 2] \Rightarrow [0, 2, 2], [1, 1, 2], [2, 0, 2],$$
$$[3, 1] \Rightarrow [0, 3, 1], [1, 2, 1], [2, 1, 1],$$
$$[9, 0] \Rightarrow [2, 7, 0].$$

From $\mathbb{X}_{10}$ *to* $\mathbb{X}_{11}$: Since the second 7-bit value is XORed with the last 7-bit value, Rule 2 and Rule 3 are applied. In this case, the propagation of the division property is calculated as

$[0, 0, 6] \Rightarrow [0, 0, 6], [0, 1, 5], [0, 2, 4], [0, 3, 3], [0, 4, 2], [0, 5, 1], [0, 6, 0],$
$[0, 1, 4] \Rightarrow [0, 1, 4], [0, 2, 3], [0, 3, 2], [0, 4, 1], [0, 5, 0],$
$[1, 0, 4] \Rightarrow [1, 0, 4], [1, 1, 3], [1, 2, 2], [1, 3, 1], [1, 4, 0],$
$[0, 2, 2] \Rightarrow [0, 2, 2], [0, 3, 1], [0, 4, 0],$
$[1, 1, 2] \Rightarrow [1, 1, 2], [1, 2, 1], [1, 3, 0],$
$[2, 0, 2] \Rightarrow [2, 0, 2], [2, 1, 1], [2, 2, 0],$
$[0, 3, 1] \Rightarrow [0, 3, 1], [0, 4, 0],$
$[1, 2, 1] \Rightarrow [1, 2, 1], [1, 3, 0],$
$[2, 1, 1] \Rightarrow [2, 1, 1], [2, 2, 0],$
$[2, 7, 0] \Rightarrow [2, 7, 0].$

After removing redundant vectors, the position is rotated, and then the division property of $\mathbb{X}_{11}$ has $\mathcal{D}_{\mathbb{K}}^{7,2,7}$, where $\mathbb{K}$ has 12 vectors as

$$[0, 0, 4], [0, 1, 3], [0, 2, 2], [1, 0, 3], [1, 1, 2], [1, 2, 1],$$
$$[2, 0, 2], [2, 1, 1], [2, 2, 0], [4, 0, 1], [4, 1, 0], [6, 0, 0].$$

Algorithm 1 can automatically search for the propagation characteristic of the division property from any $\mathcal{D}_{\{\boldsymbol{k}\}}^{7,2,7}$. We create the propagation characteristic tables, which are shown in "Appendix 6", by implementing Algorithm 1.

Appendix 4: Revisiting Known Characteristic for MISTY1

It was already shown in [25] that reduced MISTY1 has a 14th order differential characteristic, and the principle was also discussed in [1,6]. In the 14th order differential characteristic, 14 bits $P^R[10, \ldots, 16, 26, \ldots, 32]$ are active and the others are constant. Then, the first seven bits of X_5^R are balanced. We evaluate the principle of the characteristic by using the propagation characteristic of the division property. We search for the integral characteristics by using Algorithm 4 with perfect `SizeReduce`. We use $\boldsymbol{k} = [0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 0, 7]$ as the input of Algorithm 4, and Table 6 shows the propagation of $\mathbb{K}$. The output of the 4th round function has the division property $\mathcal{D}_{\mathbb{K}}^{7,2,7,7,2,7,7,2,7,7,2,7}$, where $\mathbb{K}$ has 12 vectors as follows:

Table 6. Propagation from $\mathcal{D}_{\{[6,2,7,7,2,7,7,2,7,7,2,7]\}}^{0,0,0,0,0,0,0,0,7,0,0,7}$.

#rounds	0 (plaintexts)	1	2	FL	3	4	FL
$\lvert\mathbb{K}\rvert$	1	1	460	400	125	12	12
$\max_w(\mathbb{K})$	14	14	14	14	4	2	1
$\min_w(\mathbb{K})$	14	14	4	4	1	1	1

[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] [0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] [0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0] [0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0] [0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0] [0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0] [0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0] [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0] [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0]

This result implies the existence of a 14th order differential characteristic, where the left seven bits of X_5^R are balanced.

The 14th order differential characteristic is extended to a 46th order differential characteristic, where 14 bits $P^L[10, \ldots, 16, 26, \ldots, 32]$ and 32 bits P^R are active and the others are constant. Then, the first seven bits of X_5^L are balanced. We also revisit the 46th order differential characteristic. Namely, we evaluate the propagation characteristic of the division property, where the input set has the division property $\mathcal{D}^{7,2,7,7,2,7,7,2,7,7,2,7}_{\{[0,0,7,0,0,7,7,2,7,7,2,7]\}}$. As a result, we can get an integral characteristic that the first 16 bits of X_5^L are balanced. In the simple extension shown in [11] and [28], only the first 7 bits are balanced. Thus, our method proves that the number of balanced bits is extended from 7 bits to 16 bits.

Appendix 5: Propagation from $\mathcal{D}^{7,2,7,7,2,7,7,2,7,7,2,7}_{\{[6,2,7,7,2,7,7,2,7,7,2,7]\}}$

When the input set has the division property $\mathcal{D}^{7,2,7,7,2,7,7,2,7,7,2,7}_{\{[6,2,7,7,2,7,7,2,7,7,2,7]\}}$, the division property of the set of texts encrypted 6 rounds without the first and the last FL layers is represented as $\mathcal{D}^{7,2,7,7,2,7,7,2,7,7,2,7}_{\mathbb{K}}$. Here, $\mathbb{K}$ has 131 vectors as follows:

[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4] [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 3] [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2] [0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 3]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 2] [0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 2, 1] [0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 2] [0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 1, 1]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 0] [0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 1] [0, 0, 0, 0, 0, 0, 0, 0, 0, 3, 1, 0] [0, 0, 0, 0, 0, 0, 0, 0, 0, 4, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 3] [0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 2] [0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 2, 1] [0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 2]
[0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1] [0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 2, 0] [0, 0, 0, 0, 0, 0, 0, 0, 1, 2, 0, 1] [0, 0, 0, 0, 0, 0, 0, 0, 1, 2, 1, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 1, 3, 0, 0] [0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 2] [0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 1, 1] [0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 2, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 2, 1, 0, 1] [0, 0, 0, 0, 0, 0, 0, 0, 2, 1, 1, 0] [0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 0, 0] [0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 0, 1]
[0, 0, 0, 0, 0, 0, 0, 0, 3, 0, 1, 0] [0, 0, 0, 0, 0, 0, 0, 0, 4, 1, 0, 0] [0, 0, 0, 0, 0, 0, 0, 0, 7, 0, 0, 0] [0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 3]
[0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 2] [0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 2, 1] [0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 2] [0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1]
[0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 2, 0] [0, 0, 0, 0, 0, 0, 0, 1, 0, 2, 0, 1] [0, 0, 0, 0, 0, 0, 0, 1, 0, 2, 1, 0] [0, 0, 0, 0, 0, 0, 0, 1, 0, 3, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 2] [0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1] [0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 2, 0] [0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1]
[0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0] [0, 0, 0, 0, 0, 0, 0, 1, 1, 2, 0, 0] [0, 0, 0, 0, 0, 0, 0, 1, 2, 0, 0, 1] [0, 0, 0, 0, 0, 0, 0, 1, 2, 0, 1, 0]
[0, 0, 0, 0, 0, 0, 0, 1, 2, 1, 0, 0] [0, 0, 0, 0, 0, 0, 0, 1, 5, 0, 0, 0] [0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 2] [0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 1, 1]
[0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 2, 0] [0, 0, 0, 0, 0, 0, 0, 2, 0, 1, 0, 1] [0, 0, 0, 0, 0, 0, 0, 2, 0, 1, 1, 0] [0, 0, 0, 0, 0, 0, 0, 2, 0, 2, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 2, 1, 0, 0, 1] [0, 0, 0, 0, 0, 0, 0, 2, 1, 0, 1, 0] [0, 0, 0, 0, 0, 0, 0, 2, 1, 1, 0, 0] [0, 0, 0, 0, 0, 0, 0, 2, 4, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 3] [0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 2] [0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 2, 1] [0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 2]
[0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1] [0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 2, 0] [0, 0, 0, 0, 0, 0, 1, 0, 0, 2, 0, 1] [0, 0, 0, 0, 0, 0, 1, 0, 0, 2, 1, 0]
[0, 0, 0, 0, 0, 0, 1, 0, 0, 3, 0, 0] [0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 2] [0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1] [0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 2, 0]
[0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1] [0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0] [0, 0, 0, 0, 0, 0, 1, 0, 1, 2, 0, 0] [0, 0, 0, 0, 0, 0, 1, 0, 2, 0, 0, 1]
[0, 0, 0, 0, 0, 0, 1, 0, 2, 0, 1, 0] [0, 0, 0, 0, 0, 0, 1, 0, 2, 1, 0, 0] [0, 0, 0, 0, 0, 0, 1, 0, 5, 0, 0, 0] [0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 2]
[0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1] [0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 2, 0] [0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1] [0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 0]
[0, 0, 0, 0, 0, 0, 1, 1, 0, 2, 0, 0] [0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1] [0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0] [0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0]

[0, 0, 0, 0, 0, 0, 1, 1, 4, 0, 0, 0] [0, 0, 0, 0, 0, 0, 1, 2, 0, 0, 0, 1] [0, 0, 0, 0, 0, 0, 1, 2, 0, 0, 1, 0] [0, 0, 0, 0, 0, 0, 1, 2, 0, 1, 0, 0]
[0, 0, 0, 0, 0, 0, 1, 2, 3, 0, 0, 0] [0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 2] [0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 1, 1] [0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 2, 0]
[0, 0, 0, 0, 0, 0, 2, 0, 0, 1, 0, 1] [0, 0, 0, 0, 0, 0, 2, 0, 0, 1, 1, 0] [0, 0, 0, 0, 0, 0, 2, 0, 0, 2, 0, 0] [0, 0, 0, 0, 0, 0, 2, 0, 1, 0, 0, 1]
[0, 0, 0, 0, 0, 0, 2, 0, 1, 0, 1, 0] [0, 0, 0, 0, 0, 0, 2, 0, 1, 1, 0, 0] [0, 0, 0, 0, 0, 0, 2, 0, 4, 0, 0, 0] [0, 0, 0, 0, 0, 0, 2, 1, 0, 0, 0, 1]
[0, 0, 0, 0, 0, 0, 2, 1, 0, 0, 1, 0] [0, 0, 0, 0, 0, 0, 2, 1, 0, 1, 0, 0] [0, 0, 0, 0, 0, 0, 2, 1, 3, 0, 0, 0] [0, 0, 0, 0, 0, 0, 2, 2, 2, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 3, 0, 0, 0, 0, 1] [0, 0, 0, 0, 0, 0, 3, 0, 0, 0, 1, 0] [0, 0, 0, 0, 0, 0, 3, 0, 3, 0, 0, 0] [0, 0, 0, 0, 0, 0, 3, 1, 2, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 3, 2, 1, 0, 0, 0] [0, 0, 0, 0, 0, 0, 4, 0, 0, 1, 0, 0] [0, 0, 0, 0, 0, 0, 5, 0, 2, 0, 0, 0] [0, 0, 0, 0, 0, 0, 5, 1, 1, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 5, 2, 0, 0, 0, 0] [0, 0, 0, 0, 0, 0, 7, 0, 1, 0, 0, 0] [0, 0, 0, 0, 0, 0, 7, 1, 0, 0, 0, 0] [0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0] [0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0] [0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0] [0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1] [1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0] [1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0] [1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0]
[1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0] [1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0] [2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

Assume that $\mathbb{X}$ has the division property $\mathcal{D}_{\mathbb{K}}^{7,2,7,7,2,7,7,2,7,7,2,7}$. Let $e_i \in \mathbb{Z}^{12}$ be a unit vector whose ith element is one and the others are zero. When there do not exist e_i in $\mathbb{K}$, $\bigoplus_{\boldsymbol{x}\in\mathbb{X}} x_i = 0$. Since the vector $[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$ is not included in 131 vectors, we are certain that the first 7 bits are balanced.

Appendix 6: Propagation Characteristic Table for FI Function

See Tables 7, 8, 9, 10, 11, 12, 13 and 14.

Table 7. Propagation from $\mathcal{D}_{\{[0,*,*]\}}^{7,2,7}$ to $\mathcal{D}_{\mathbb{K}}^{7,2,7}$.

k	$\mathbb{K}$
[0 0 0]	[0 0 0]
[0 0 1]	[0 0 1] [0 1 0] [1 0 0]
[0 0 2]	[0 0 1] [0 1 0] [1 0 0]
[0 0 3]	[0 0 1] [0 2 0] [1 0 0]
[0 0 4]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[0 0 5]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [2 0 0]
[0 0 6]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [3 0 0]
[0 0 7]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[0 1 0]	[0 0 1] [0 1 0] [1 0 0]
[0 1 1]	[0 0 1] [0 1 0] [2 0 0]
[0 1 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[0 1 3]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[0 1 4]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[0 1 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [3 0 0]
[0 1 6]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[0 1 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[0 2 0]	[0 0 1] [0 1 0] [1 0 0]
[0 2 1]	[0 0 1] [0 1 0] [2 0 0]
[0 2 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[0 2 3]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[0 2 4]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[0 2 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [3 0 0]
[0 2 6]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[0 2 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]

Table 8. Propagation from $\mathcal{D}^{7,2,7}_{\{[1,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$.

$\boldsymbol{k}$	$\mathbb{K}$
[1 0 0]	[0 0 1] [0 1 0] [1 0 0]
[1 0 1]	[0 0 1] [0 1 0] [2 0 0]
[1 0 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[1 0 3]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[1 0 4]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[1 0 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [3 0 0]
[1 0 6]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[1 0 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[1 1 0]	[0 0 1] [0 1 0] [1 0 0]
[1 1 1]	[0 0 1] [0 1 0] [2 0 0]
[1 1 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[1 1 3]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[1 1 4]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[1 1 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [3 0 0]
[1 1 6]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[1 1 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[1 2 0]	[0 0 1] [0 1 0] [2 0 0]
[1 2 1]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[1 2 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[1 2 3]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[1 2 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[1 2 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[1 2 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[1 2 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]

Table 9. Propagation from $\mathcal{D}^{7,2,7}_{\{[2,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$.

$\boldsymbol{k}$	$\mathbb{K}$
[2 0 0]	[0 0 1] [0 1 0] [1 0 0]
[2 0 1]	[0 0 1] [0 1 0] [2 0 0]
[2 0 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[2 0 3]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [2 0 0]
[2 0 4]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[2 0 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [3 0 0]
[2 0 6]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[2 0 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[2 1 0]	[0 0 1] [0 1 0] [2 0 0]
[2 1 1]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[2 1 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[2 1 3]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[2 1 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[2 1 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[2 1 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[2 1 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[2 2 0]	[0 0 1] [0 1 0] [2 0 0]
[2 2 1]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[2 2 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[2 2 3]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]

Table 9. continued.

k	$\mathbb{K}$
[2 2 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[2 2 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[2 2 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[2 2 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]

Table 10. Propagation from $\mathcal{D}^{7,2,7}_{\{[3,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$.

k	$\mathbb{K}$
[3 0 0]	[0 0 1] [0 1 0] [2 0 0]
[3 0 1]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[3 0 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[3 0 3]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[3 0 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[3 0 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[3 0 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[3 0 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[3 1 0]	[0 0 1] [0 1 0] [2 0 0]
[3 1 1]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[3 1 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[3 1 3]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[3 1 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[3 1 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[3 1 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[3 1 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[3 2 0]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[3 2 1]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[3 2 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[3 2 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[3 2 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[3 2 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[3 2 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[3 2 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]

Table 11. Propagation from $\mathcal{D}^{7,2,7}_{\{[4,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$.

k	$\mathbb{K}$
[4 0 0]	[0 0 1] [0 1 0] [2 0 0]
[4 0 1]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[4 0 2]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[4 0 3]	[0 0 2] [0 1 1] [1 0 1] [1 1 0] [3 0 0]
[4 0 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 0 5]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 0 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[4 0 7]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[4 1 0]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]

Table 11. continued.

$\boldsymbol{k}$	$\mathbb{K}$
[4 1 1]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 1 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 1 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 1 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[4 1 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[4 1 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[4 1 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[4 2 0]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[4 2 1]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 2 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 2 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[4 2 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[4 2 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[4 2 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[4 2 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]

Table 12. Propagation from $\mathcal{D}^{7,2,7}_{\{[5,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$.

$\boldsymbol{k}$	$\mathbb{K}$
[5 0 0]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[5 0 1]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[5 0 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[5 0 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[5 0 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[5 0 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[5 0 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[5 0 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[5 1 0]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[5 1 1]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[5 1 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[5 1 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[5 1 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[5 1 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[5 1 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[5 1 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[5 2 0]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[5 2 1]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[5 2 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[5 2 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[5 2 4]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[5 2 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[5 2 6]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[5 2 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [4 0 2] [4 1 1] [4 2 0] [6 0 1] [6 1 0]

Table 13. Propagation from $\mathcal{D}^{7,2,7}_{\{[6,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$.

k	$\mathbb{K}$
[6 0 0]	[0 0 2] [0 1 1] [0 2 0] [1 0 1] [1 1 0] [3 0 0]
[6 0 1]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[6 0 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[6 0 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [2 0 1] [2 1 0] [4 0 0]
[6 0 4]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 0 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 0 6]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[6 0 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[6 1 0]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[6 1 1]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 1 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 1 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 1 4]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[6 1 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[6 1 6]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[6 1 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [4 0 2] [4 1 1] [4 2 0] [6 0 1] [6 1 0]
[6 2 0]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[6 2 1]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 2 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 2 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[6 2 4]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[6 2 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[6 2 6]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[6 2 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [4 0 2] [4 1 1] [4 2 0] [6 0 1] [6 1 0]

Table 14. Propagation from $\mathcal{D}^{7,2,7}_{\{[7,*,*]\}}$ to $\mathcal{D}^{7,2,7}_{\mathbb{K}}$.

k	$\mathbb{K}$
[7 0 0]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[7 0 1]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[7 0 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[7 0 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[7 0 4]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[7 0 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[7 0 6]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[7 0 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [4 0 2] [4 1 1] [4 2 0] [6 0 1] [6 1 0]
[7 1 0]	[0 0 2] [0 1 1] [0 2 0] [2 0 1] [2 1 0] [4 0 0]
[7 1 1]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[7 1 2]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]
[7 1 3]	[0 0 3] [0 1 2] [0 2 1] [1 0 2] [1 1 1] [1 2 0] [3 0 1] [3 1 0] [5 0 0]

Table 14. continued.

k	$\mathbb{K}$
[7 1 4]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[7 1 5]	[0 0 4] [0 1 3] [0 2 2] [1 0 3] [1 1 2] [1 2 1] [2 0 2] [2 1 1] [2 2 0] [4 0 1] [4 1 0] [6 0 0]
[7 1 6]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [3 0 2] [3 1 1] [3 2 0] [5 0 1] [5 1 0] [7 0 0]
[7 1 7]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [2 0 3] [2 1 2] [2 2 1] [4 0 2] [4 1 1] [4 2 0] [6 0 1] [6 1 0]
[7 2 0]	[0 0 5] [0 1 4] [0 2 3] [1 0 4] [1 1 3] [1 2 2] [3 0 3] [3 1 2] [3 2 1] [5 0 2] [5 1 1] [5 2 0] [7 0 1] [7 1 0]
[7 2 1]	[0 0 6] [0 1 5] [0 2 4] [1 0 5] [1 1 4] [1 2 3] [2 0 4] [2 1 3] [2 2 2] [4 0 3] [4 1 2] [4 2 1] [6 0 2] [6 1 1] [6 2 0]
[7 2 2]	[0 0 6] [0 1 5] [0 2 4] [1 0 5] [1 1 4] [1 2 3] [2 0 4] [2 1 3] [2 2 2] [4 0 3] [4 1 2] [4 2 1] [6 0 2] [6 1 1] [6 2 0]
[7 2 3]	[0 0 6] [0 1 5] [0 2 4] [1 0 5] [1 1 4] [1 2 3] [2 0 4] [2 1 3] [2 2 2] [4 0 3] [4 1 2] [4 2 1] [6 0 2] [6 1 1] [6 2 0]
[7 2 4]	[0 0 7] [0 1 6] [0 2 5] [1 0 6] [1 1 5] [1 2 4] [2 0 5] [2 1 4] [2 2 3] [3 0 4] [3 1 3] [3 2 2] [5 0 3] [5 1 2] [5 2 1] [7 0 2] [7 1 1] [7 2 0]
[7 2 5]	[0 0 7] [0 1 6] [0 2 5] [1 0 6] [1 1 5] [1 2 4] [2 0 5] [2 1 4] [2 2 3] [3 0 4] [3 1 3] [3 2 2] [5 0 3] [5 1 2] [5 2 1] [7 0 2] [7 1 1] [7 2 0]
[7 2 6]	[0 2 7] [1 1 7] [1 2 6] [2 0 7] [2 1 6] [2 2 5] [3 0 6] [3 1 5] [3 2 4] [4 0 5] [4 1 4] [4 2 3] [5 0 4] [5 1 3] [5 2 2] [7 0 3] [7 1 2] [7 2 1]
[7 2 7]	[7 2 7]

References

[1] S. Babbage, L. Frisch, On MISTY1 higher order differential cryptanalysis, in *ICISC*. LNCS, vol. 2015, ed. by D. Won (Springer, 2000), pp. 22–36

[2] A. Bar-On, A 2^{70} attack on the full MISTY1. IACR Cryptology ePrint Archive 2015, 746 (2015). http://eprint.iacr.org/2015/746

[3] A. Bar-On, Improved higher-order differential attacks on MISTY1, in *FSE* (2015)

[4] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, in *CRYPTO*. LNCS, vol. 537, ed. by A. Menezes, S.A. Vanstone (Springer, 1990), pp. 2–21

[5] C. Boura, A. Canteaut, On the influence of the algebraic degree of f^{-1} on the algebraic degree of $G \circ F$. *IEEE Trans. Inf. Theory* **59**(1), 691–702 (2013)

[6] A. Canteaut, M. Videau, Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis, in *EUROCRYPT*. LNCS, vol. 2332, ed. by L.R. Knudsen (Springer, 2002), pp. 518–533

[7] CRYPTREC, Specifications of e-government recommended ciphers (2013). http://www.cryptrec.go.jp/english/method.html

[8] J. Daemen, L.R. Knudsen, V. Rijmen, The block cipher square, in *FSE*. LNCS, vol. 1267, ed. by E. Biham (Springer, 1997), pp. 149–165

[9] O. Dunkelman, N. Keller, An improved impossible differential attack on MISTY1, in *ASIACRYPT*. LNCS, vol. 5350, ed. by J. Pieprzyk (Springer, 2008), pp. 441–454

[10] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, D. Whiting, Improved cryptanalysis of Rijndael, in *FSE*. LNCS, vol. 1978, ed. by B. Schneier (Springer, 2000), pp. 213–230

[11] Y. Hatano, H. Tanaka, T. Kaneko, Optimization for the algebraic method and its application to an attack of MISTY1. *IEICE Trans.* **87-A**(1), 18–27 (2004)

[12] ISO/IEC: JTC1: ISO/IEC 18033, Security techniques—encryption algorithms—part 3: block ciphers (2005)

[13] L.R. Knudsen, Truncated and higher order differentials, in *FSE*. LNCS, vol. 1008, ed. by B. Preneel (Springer, 1994), pp. 196–211
[14] L.R. Knudsen, D. Wagner, Integral cryptanalysis, in *FSE*. LNCS, vol. 2365, ed. by J. Daemen, V. Rijmen (Springer, 2002), pp. 112–127
[15] X. Lai, Higher order derivatives and differential cryptanalysis, in *Communications and Cryptography. The Springer International Series in Engineering and Computer Science*, vol. 276 (1994), pp. 227–233
[16] M. Matsui, Linear cryptanalysis method for DES cipher, in *EUROCRYPT*. LNCS, vol. 765, ed. by T. Helleseth (Springer, 1993), pp. 386–397
[17] M. Matsui, New structure of block ciphers with provable security against differential and linear cryptanalysis, in *FSE*. LNCS, vol. 1039, ed. by D. Gollmann (Springer, 1996), pp. 205–218
[18] M. Matsui, New block encryption algorithm MISTY, in *FSE*. LNCS, vol. 1267, ed. by E. Biham (Springer, 1997), pp. 54–68
[19] NESSIE: New European schemes for signatures, integrity, and encryption (2004). https://www.cosic.esat.kuleuven.be/nessie/
[20] K. Nyberg, Linear approximation of block ciphers, in *EUROCRYPT*. LNCS, vol. 950, ed. by A.D. Santis (Springer, 1994), pp. 439–444
[21] K. Nyberg, L.R. Knudsen, Provable security against a differential attack. *J. Cryptol*. **8**(1), 27–37 (1995)
[22] H. Ohta, M. Matsui, A description of the MISTY1 encryption algorithm (2000). https://tools.ietf.org/html/rfc2994
[23] Y. Sasaki, L. Wang, Meet-in-the-middle technique for integral attacks against Feistel ciphers, in *SAC*. vol. 7707, ed. by L.R. Knudsen, H. Wu (Springer, 2012), pp. 234–251
[24] B. Sun, X. Hai, W. Zhang, L. Cheng, Z. Yang, New observation on division property. IACR Cryptology ePrint Archive, 459 (2015). http://eprint.iacr.org/2015/459
[25] H. Tanaka, K. Hisamatsu, T. Kaneko, Strength of MISTY1 without FL function for higher order differential attack, in *AAECC-13*. LNCS, vol. 1719, ed. by M.P.C. Fossorier, H. Imai, S. Lin, A. Poli (Springer, 1999), pp. 221–230
[26] Y. Todo, Integral cryptanalysis on full MISTY1, in *CRYPTO Part I*. LNCS, vol. 9215, ed. by R. Gennaro, M. Robshaw (Springer, 2015), pp. 413–432
[27] Y. Todo, Structural evaluation by generalized integral property, in *EUROCRYPT Part I*. LNCS, vol. 9056, ed. by E. Oswald, M. Fischlin (Springer, 2015b), pp. 287–314
[28] Y. Tsunoo, T. Saito, M. Shigeri, T. Kawabata, Higher order differential attacks on reduced-round MISTY1, in *ICISC*. LNCS, vol. 5461, ed. by P.J. Lee, J.H. Cheon (Springer, 2008), pp. 415–431
[29] H. Zhang, W. Wu, Structural evaluation for generalized Feistel structures and applications to LBlock and TWINE, in *INDOCRYPT*. LNCS, vol. 9462, ed. by A. Biryukov, V. Goyal (Springer, 2015), pp. 218–237