HCIS | Human-centric Computing and Information Sciences

RESEARCH (Research Manuscript) **Open Access**

Human-centric Computing and Information Sciences (2023) 12:03
DOI: https://doi.org/10.22967/HCIS.2023.13.003
Received: April 18, 2022; Accepted: April 24, 2022; Published: January 30, 2023

Related-Key Amplified Boomerang Attack on Full-Round MM-128

Hyejin Eom, Byoungjin Seok, and Changhoon Lee*

Abstract

Recently, the use of open platforms with various network functions and hardware interfaces has been increasing in various fields such as the Internet of Things, smart buildings, and industrial automation. In this new device environment, data-dependent operation (DDO) usage-based cryptographic design based on the control element have been introduced, which is suitable for ensuring high-efficiency performance and network security of the CIA (confidentiality, integrity, accessibility) security model. Among them, the MM-128 proposed by Hieu and his colleagues is a high-speed block cipher that uses the latest FPGA devices to increase the hardware implementation efficiency of block ciphers. It is composed of 9 rounds and uses a 256-bit key. However, most data-dependent permutation (DDP), DDO, and switchable data-dependent operation (SDDOS)-based block ciphers are vulnerable to related-key attacks owing to their simple key scheduling processes, including this paper's target algorithm MM-128. This paper presents a related-key amplified boomerang attack that is more efficient than an exhaustive attack as the first known result. The attack on MM-128 requires $2^{72.5}$ related-key chosen plaintexts and $2^{132.5}$ encryptions. In future research, this work is expected to be extended and improved with the latest boomerang connectivity table (BCT) and differential-linear connectivity table (DLCT) techniques to obtain better cryptanalytic results.

Keywords

Block Cipher, MM-128, Related-key Amplified Boomerang Attack, Controlled Substitution-Permutation Network (CSPN), Data-Dependent Operations (DDOs)

1. Introduction

As a result of the rapid development of Internet of Things (IoT) technology, sensor networks, healthcare, distributed control systems and virtual physical systems, which belong to related industrial fields, are growing together. The majority of devices that use IoT technology in these fields are small computing devices used in everyday life. These IoT devices risk exposure to various types of hacking and cracking because they use big data such as the sensitive personal information of users, voice/video DB, and various life information in order to provide users with convenient and useful services. However, since the available resources of IoT devices are limited, it is difficult to secure safety with the encryption algorithm used in the existing server or the PC environment as it is.

***Corresponding Author:** Changhoon Lee (chlee@seoultech.ac.kr)
Department of Computer Science and Engineering Seoul National University of Science and Technology, Seoul, Korea

Therefore, in a restricted IoT environment, the network not only handles unauthorized access to systems and data, but also requires specific security requirements to ensure suitability, portability and applicability for software and hardware performance when operating and integrating in these environments. In addition, the need for encryption algorithms that can guarantee an appropriate level of safety and efficiency at a lower cost than existing algorithms is increasing, and this is becoming increasingly important as IoT technology continues to develop. To address such issues, the most prominent solution focuses on improving the protection of cipher designs by distinct switch operations and functions; for example, data-dependent permutation (DDP)-based constructions such as CIKS-1 [1], Cobra-H64/128 [2] and SCO-family [3]; advanced data-dependent operations (DDO) designs such as CIKS-1 [1], CIKS-128 [4], MD-64 [5], DDP-64 [6], TMN-64, and TMN-128 [7]; or switchable data-dependent operations (SDDO) designs such as XO-64 [8] and BM123-64 [9].

Because these algorithms use a very simple key schedule, they are highly efficient when applied to an environment in which the secret key is frequently changed. However, most algorithms are vulnerable to differential cryptanalysis attacks due to the linearity and simply designed key schedule of DDPs [10–17].

To overcome these problems, Hieu et al. [18] proposed a new DDO-based block cipher, MM-128, which has a block size of 128 bits and consists of a 256-bit secret key and 9 rounds. It was designed by combining new concepts in an attempt to obtain better capabilities and properties in DDO and CSPN (controlled substitution-permutation network) frameworks. The authors introduced a new class of $F_{2/4}$ type CE (controlled elements) as cryptographic primitives suitable for the design of FPGA-efficient DDO boxes. $F_{2/4}$ shows higher nonlinearity and improved hardware implementation efficiency.

However, this paper shows that their simple key schedules and structural weaknesses make this cipher vulnerable to related-key attacks. The proposed amplified boomerang attack requires about $2^{72.5}$ in terms of the complexity of data, $2^{76.5}$ memory bytes and $2^{132.5}$ encryptions for MM-128. This cryptanalytic result means that the MM-128 constructions, as in existing studies of DDP-based or DDO-based schemes, are still vulnerable to and insecure against related-key differential cryptanalysis.

This paper is organized as follows. Section 2 describes the related-key amplified boomerang attack; Section 3 briefly introduces the block cipher, MM-128; Sections 4 and 5 introduces the extended associated key boomerang attack on MM-128; and, finally, Section 6 presents the conclusion.

2. Related-Key Amplified Boomerang Attack

The related-key differential cryptanalysis was introduced by Biham [19]. It is an upgraded model of the related key boomerang attack developed by Wagner [20] and Biham et al. [21] as a pure adaptive chosen-plaintext attack. In particular, it has become an effective cryptographic analysis technique, and has been applied to a variety of cryptographic mechanisms, as the target of the attack aims to exploit two uniquely related key differential properties to find the correct quartet with a high probability. This attack scenario provides high efficiency and high probability for certain DDO-based ciphers, such as DDO-64 [6], XO-64 [8], MD-64 [5], BM123-64 [9],TMN-64 [7], and TMN-128 [7].

The related-key amplified boomerang attack treats a block cipher $E: \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$ as a cascade of two subciphers $E = E^1 \cdot E^0$. It is assumed that $\alpha \rightarrow \beta$ is a related-key differential for E^0 with probability p using key difference $\triangle K$, and that $\gamma \rightarrow \delta$ is another related-key differential for E^1 with probability q using key difference $\triangle K'$. With the related keys $K, K^*, K', \ and\ K'^*$ where $K' \oplus K'^* = \triangle K$ and $K^* \oplus K'^* = \triangle K'$, the attack can be implemented as follows (Fig. 1).

(1) Choose two random n-bit plaintexts $\boldsymbol{P}, \boldsymbol{P'}$ and compute two other plaintexts

$$\boldsymbol{P^*} = \boldsymbol{P} \oplus \boldsymbol{\alpha} \text{ and } \boldsymbol{P'^*} = \boldsymbol{P'} \oplus \boldsymbol{\alpha} \text{ for a constant } \boldsymbol{\alpha}.$$

(2) With a chosen plaintext attack scenario, obtain the corresponding cipher texts

$$\boldsymbol{C} = \boldsymbol{E_k(p)}, \boldsymbol{C^*} = \boldsymbol{E_{K^*}(P^*)}, \boldsymbol{C'} = \boldsymbol{E_{K'}(P')} \textbf{ and } \boldsymbol{C'^*} = \boldsymbol{E_{K'^*}(P'^*)},$$

where $\boldsymbol{K} \oplus \boldsymbol{K^*} = \boldsymbol{K'} \oplus \boldsymbol{K'^*} = \triangle \boldsymbol{K} \neq \boldsymbol{0}, \boldsymbol{K} \oplus \boldsymbol{K^*} = \boldsymbol{K'} \oplus \boldsymbol{K'^*} = \triangle \boldsymbol{K'} \neq \boldsymbol{0}$, $\triangle \boldsymbol{K} \neq \triangle \boldsymbol{K'}$ and $\triangle \boldsymbol{K}$, $\triangle \boldsymbol{K'}$ are the differences in the secret key chosen by the attacker.

(3) Check whether or not $\boldsymbol{C}\oplus\boldsymbol{C'} = \boldsymbol{C}^{*}\oplus\boldsymbol{C'}^{*} = \boldsymbol{\delta}$.

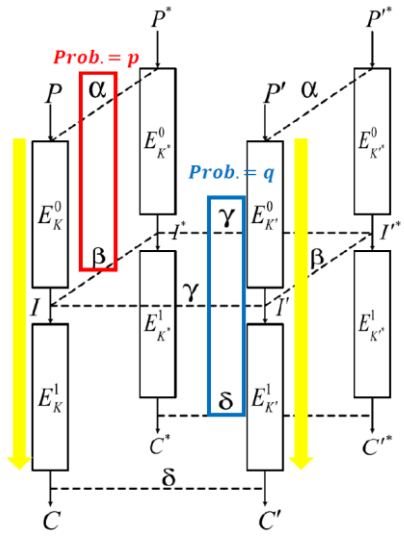


Fig. 1. Related-key amplified boomerang distinguisher.

If the plaintext quartet ($\boldsymbol{P}$, $\boldsymbol{P}^{*}$, $\boldsymbol{P'}$, $\boldsymbol{P'}^{*}$) goes through three steps, the related key amplified boomerang attack model outputs the correct quartet.

A correct plaintext quartet must satisfy the following four conditions for a delta test:

(1) $\boldsymbol{P}\oplus\boldsymbol{P}^{*} = \boldsymbol{P'}\oplus\boldsymbol{P'}^{*} = \boldsymbol{\alpha}$

(2) $\boldsymbol{I}\oplus\boldsymbol{I}^{*} = \boldsymbol{I'}\oplus\boldsymbol{I'}^{*} = \boldsymbol{\beta}$(for some $\boldsymbol{\beta}$)

(3) $\boldsymbol{I} \oplus \boldsymbol{I'} = \boldsymbol{\gamma}$(for some $\boldsymbol{\gamma}$)

(4) $\boldsymbol{C}\oplus\boldsymbol{C}^{*} = \boldsymbol{C'}\oplus\boldsymbol{C'}^{*} = \boldsymbol{\delta}$

Conditions 2 and 3 mean that $\boldsymbol{I'}\oplus\boldsymbol{I'}^{*} = \boldsymbol{\gamma}$ and if all four conditions are satisfied, such a quartet ($\boldsymbol{P}$, $\boldsymbol{P}^{*}$, $\boldsymbol{P'}$, $\boldsymbol{P'}^{*}$) is termed a right quartet.

We select $\boldsymbol{m_1}$ pairs of ($\boldsymbol{P}$, $\boldsymbol{P}^{*}$) and $\boldsymbol{m_2}$ pairs of ($\boldsymbol{P'}$, $\boldsymbol{P'}^{*}$) as the difference $\boldsymbol{\alpha}$. We also assume that $\boldsymbol{\alpha} \rightarrow \boldsymbol{\beta}$ is the first related-key derivative with respect to $\boldsymbol{E^0}$ in the probability of $\boldsymbol{p}$ using the key difference $\triangle \boldsymbol{K}$, and that $\boldsymbol{\gamma} \rightarrow \boldsymbol{\delta}$ is the second related-key derivative of $\boldsymbol{E^1}$ in the probability of $\boldsymbol{q}$ using the key difference $\triangle \boldsymbol{K'}$. There are a number of pairs ($\boldsymbol{m_1}\cdot \boldsymbol{p}$) and ($\boldsymbol{m_2}\cdot \boldsymbol{p}$) that satisfy the first related-key derivative $\boldsymbol{\alpha} \rightarrow \boldsymbol{\beta}$ with respect to $\boldsymbol{E^0}$ using the difference $\triangle \boldsymbol{K}$. Then, the quartet satisfying conditions (1) and (2) is approximately $\boldsymbol{m_1}\cdot \boldsymbol{m_2}\cdot \boldsymbol{p^2}$. Similarly, the $\boldsymbol{m_1}\cdot \boldsymbol{m_2}\cdot \boldsymbol{2^{-n}}\cdot \boldsymbol{p^2}$ quartet satisfies the requirements of (1), (2) and (3) if we obtain $\boldsymbol{I} \oplus \boldsymbol{I'} = \boldsymbol{\gamma}$ under a probability of $\boldsymbol{2^{-n}}$ at all possible values. The related-key differential boomerang characteristic distinguishes cipher E from perfect ciphers if the probability $\boldsymbol{p}\cdot\boldsymbol{q} > \boldsymbol{2^{-n/2}}$, when the supposed number of correct quartets is approximately $\boldsymbol{m_1}\cdot \boldsymbol{m_2}\cdot \boldsymbol{2^{-n}}\cdot \boldsymbol{p^2}\cdot \boldsymbol{q^2}$.

3. MM-128 Block Cipher Description

3.1 Preliminaries

In this section, we notice some notations being used through the whole paper. The cipher $X = (x_1, \ldots, x_n)$ is assigned with x_1 and x_n which are the most significant bit and the least significant bit, respectively.

The related-key amplified boomerang attack is combined with the related differential components of block ciphers, like the input, output, and key of a round function.

- r: round function of a block cipher.
- ΔQ_r, ΔU_r : round key difference values for each round r.
- ΔX_r / ΔY_r : input / output difference values for each round r.
- $e_{i,j}$: binary data bits adjusted for round r, as active bit values i and j; at the i^{th} and j^{th} value are ones, and the others are zeros for each block data (e.g., $e_{2,3}$ = (0, 1, 1, 0, 0,…, 0)).
- $\oplus$: bitwise XOR operation.
- << : cyclic rotation to the left by b bits.

3.2 MM-128 Construction

MM-128 is designed as a DDO-based block cipher mechanism with 128 bits under 256-bit secret keys. The number of rounds is 9. The iterative structure of the ciphers is identical to that the round function $\boldsymbol{Crypt}^{(e)}(\boldsymbol{e} = \boldsymbol{0}: \boldsymbol{encryption}, \boldsymbol{e} = \boldsymbol{1}: \boldsymbol{decryption})$.

The encryption procedure of MM-128 is as follows.

(1) The 128-bit plaintext is divided into two 64-bit sub-blocks A and B:

(2) From the 1^{st} round to the 7^{th}(as r=1 to 7), for each round r, execute an identical operation:

(a) $(A, B) = Crypt^{(e)}(A, B, Q_r, U_r)$

(b) $(A, B) = (B, A)$

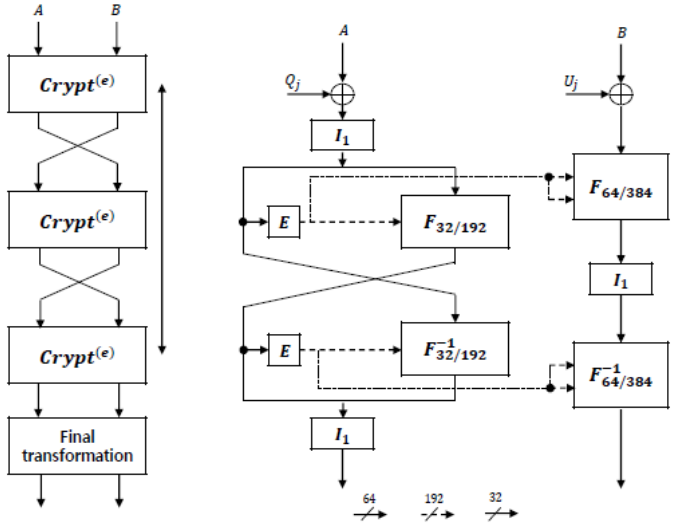
(3) Perform the transformation (A_8, B_8) as follows:

$$(A_8, B_8) = Crypt^{(e)}(A_7, B_7, Q_8, U_8).$$

(4) Perform the final transformation as follows:

$$\left(A', B'\right) = (A_8 \oplus Q_9, B_8 \oplus U_9).$$

The round function $Crypt^{(e)}$ of MM-128 is based on the controlled substitution permutation networks (CSPNs), an extension function E, a permutation I_1 and on DDO-based functions $F_{n/m}^{v/s}$ ($F_{32/192}, F_{64/384}, F_{32/192}^{-1}, F_{64/384}^{-1}$) including the basic controlled function $F_{2/4}$. The round function $Crypt^{(0)}$ is given in Fig. 2.



(a) (b)

Fig. 2. Round function $Crypt^{(e)}$ of MM-128.

$F_{8/48}$ is built based on $F_{2/4}$, as $F_{2/4}$ is defined by $((x_1, x_2), [v_1, v_2, v_3, v_4]/(y_1, y_2))$ in Fig. 3.

Also, as shown in Fig. 4(a) and 4(b), for the $F_{32/192}, F_{32/192}^{-1}$, $F_{64/384}$ *and* $F_{64/384}^{-1}$ operations, there are cascades of four CSPNs $F_{8/48}$, $F_{8/48}^{-1}$, as shown in Fig. 5.

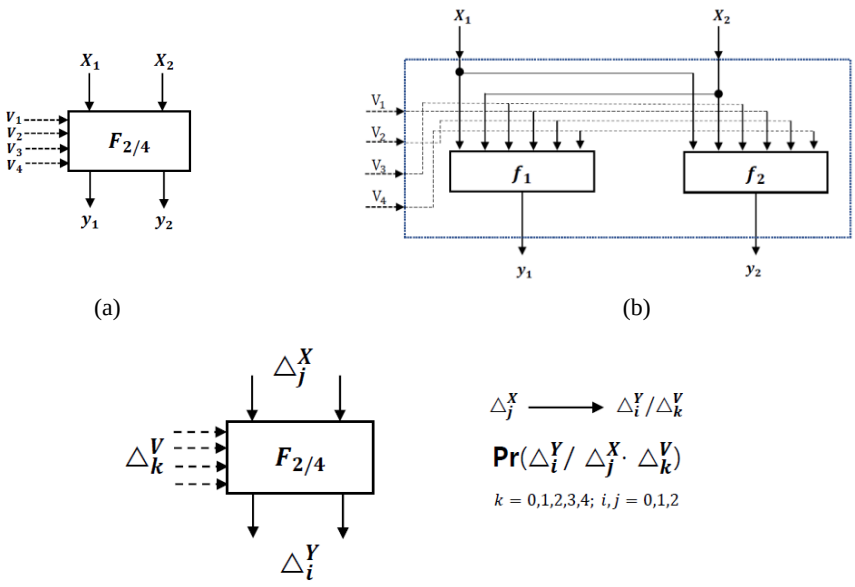


Fig. 3. (a) Controlled elements $F_{2/4}$. (b) Expressed in the form of a pair of Boolean functions. (c) Variants of the differences for CEs $F_{2/4}$.

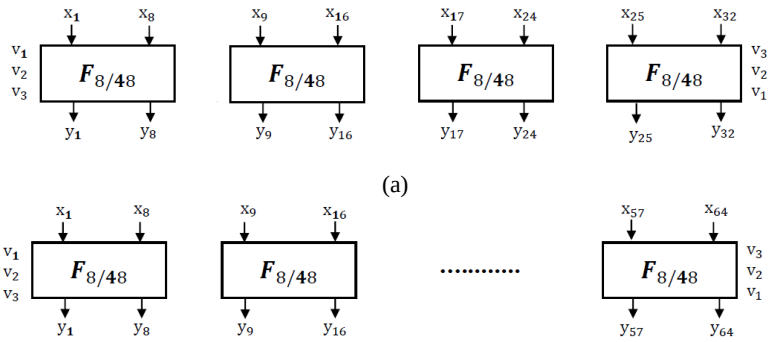


Fig. 4. (a) $F_{32/192}, F_{32/192}^{-1}$ and (b) $F_{64/384}, F_{64/384}^{-1}$.

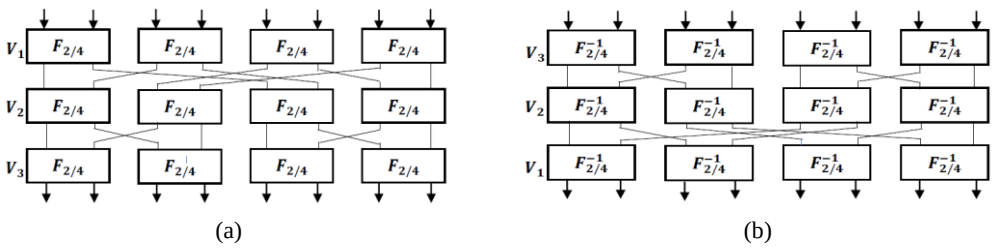


Fig. 5. (a) $F_{8/48}$ and (b) $F_{8/48}^{-1}$.

To analyze the properties of CEs $F_{2/4}$ defined by the $F(i)$ correction set, we describe the first and second output values of $i = 0,1,2,\dots,15$ CEs $F_{2/4}$. The Boolean functions (BFs) f_1 and f_2 can be built easily for a set of 16 ordered pairs of BFs in two variables, each describing one of the 16 modified $F(i)$ cases, where $i = 0,1,2,\dots,15$, which defines several variants of the element $F_{2/4}$. There are 10 different BF pairs in two variables, which describes the basic S-box, which is the involution. Each of the 10 possible BF pairs in the two variables describing the modification of $F(i)$ $(i = 0,1,2,\dots,15)$ can be constructed easily using their schematic representation, as shown in Fig. 6.

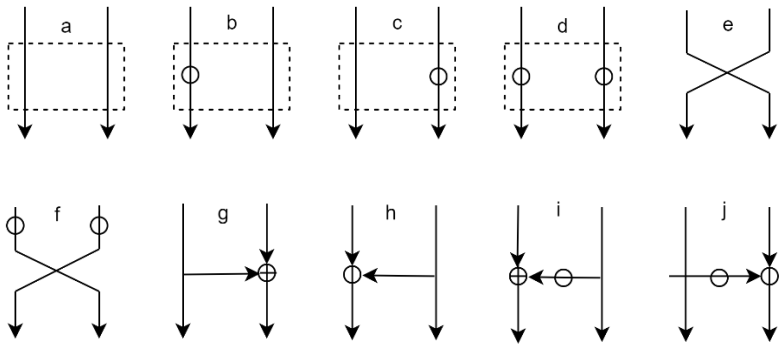


Fig. 6. Schematic representation of the various conventional transformations $(x_1, x_2) \to (y_1, y_2)$ that are the involution.

The concrete format of the two BFs for implementing CEs $F_{2/4}$ can then be obtained from the following two formulae:

$$\begin{aligned} y_1 = {} & (v_1\oplus 1)(v_2\oplus 1)(v_3\oplus 1)(v_4\oplus 1)f_1^1(x_1,x_2)\oplus(v_1\oplus 1)(v_2\oplus 1)(v_3\oplus 1)v_4 f_1^2(x_1,x_2)\oplus \\ & \oplus(v_1\oplus 1)(v_2\oplus 1)v_3(v_4\oplus 1)\, f_1^3(x_1,x_2)\oplus(v_1\oplus 1)(v_2\oplus 1)v_3 v_4 f_1^4(x_1,x_2)\oplus \\ & \oplus(v_1\oplus 1)v_2 v_3(v_4\oplus 1)\, f_1^5(x_1,x_2)\oplus(v_1\oplus 1)v_2(v_3\oplus 1)v_4 f_1^6(x_1,x_2)\oplus \\ & \oplus(v_1\oplus 1)v_2 v_3(v_4\oplus 1)\, f_1^7(x_1,x_2)\oplus(v_1\oplus 1)v_2 v_3 v_4 f_1^8(x_1,x_2)\oplus \\ & \oplus v_1(v_2\oplus 1)(v_3\oplus 1)(v_4\oplus 1)\, f_1^9(x_1,x_2)\oplus v_1(v_2\oplus 1)(v_3\oplus 1)v_4 f_1^{10}(x_1,x_2)\oplus \\ & \oplus v_1(v_2\oplus 1)v_3(v_4\oplus 1)\, f_1^{11}(x_1,x_2)\oplus v_1(v_2\oplus 1)v_3 v_4 f_1^{12}(x_1,x_2)\oplus \\ & \oplus v_1 v_2(v_3\oplus 1)(v_4\oplus 1)\, f_1^{13}(x_1,x_2)\oplus v_1 v_2(v_3\oplus 1)v_4 f_1^{14}(x_1,x_2)\oplus \\ & \oplus v_1 v_2 v_3(v_4\oplus 1)\, f_1^{15}(x_1,x_2)\oplus v_1 v_2 v_3 v_4 f_1^{16}(x_1,x_2) \end{aligned}$$

$$\begin{aligned} y_2 = {} & (v_1\oplus 1)(v_2\oplus 1)(v_3\oplus 1)(v_4\oplus 1)f_2^1(x_1,x_2)\oplus(v_1\oplus 1)(v_2\oplus 1)(v_3\oplus 1)v_4 f_2^2(x_1,x_2)\oplus \\ & \oplus(v_1\oplus 1)(v_2\oplus 1)v_3(v_4\oplus 1)\, f_2^3(x_1,x_2)\oplus(v_1\oplus 1)(v_2\oplus 1)v_3 v_4 f_2^4(x_1,x_2)\oplus \\ & \oplus(v_1\oplus 1)v_2 v_3(v_4\oplus 1)\, f_2^5(x_1,x_2)\oplus(v_1\oplus 1)v_2(v_3\oplus 1)v_4 f_2^6(x_1,x_2)\oplus \\ & \oplus(v_1\oplus 1)v_2 v_3(v_4\oplus 1)\, f_2^7(x_1,x_2)\oplus(v_1\oplus 1)v_2 v_3 v_4 f_2^8(x_1,x_2)\oplus \\ & \oplus v_1(v_2\oplus 1)(v_3\oplus 1)(v_4\oplus 1)\, f_2^9(x_1,x_2)\oplus v_1(v_2\oplus 1)(v_3\oplus 1)v_4 f_2^{10}(x_1,x_2)\oplus \\ & \oplus v_1(v_2\oplus 1)v_3(v_4\oplus 1)\, f_2^{11}(x_1,x_2)\oplus v_1(v_2\oplus 1)v_3 v_4 f_2^{12}(x_1,x_2)\oplus \\ & \oplus v_1 v_2(v_3\oplus 1)(v_4\oplus 1)\, f_2^{13}(x_1,x_2)\oplus v_1 v_2(v_3\oplus 1)v_4 f_2^{14}(x_1,x_2)\oplus \\ & \oplus v_1 v_2 v_3(v_4\oplus 1)\, f_2^{15}(x_1,x_2)\oplus v_1 v_2 v_3 v_4 f_2^{16}(x_1,x_2) \end{aligned}$$

The CEs $F_{2/4}$, related to variant 4 of Table 1, was used to design the block cipher MM-128, which stands for an eight-round repeating block cipher with a block of 128-bit data. Fig. 3(c) shows the variants of all possible differences related to the $F_{2/4}$ type CEs.

The key schedule of MM-128 is constructed in a very simple manner, where the 256-bit secret key K is split into four 64-bit sub-keys; $K = (K_1, K_2, K_3, K_4)$. The key schedule of the algorithm is specified as shown in Table 2.

Table 1. Examples of the sets of $F(i)$ modifications

No.	*The value of the non-inearity of BF* $NL(f_1)$- $NL(f_2)$-$NL(f_3)$	*Set of modifications*
1	22-24-22	$a/b/d/e/f/g/h/i/a/b/c/e/f/g/e/j$
2	22-24-22	$a/b/d/e/f/g/h/j/a/d/e/f/g/h/g/i$
3	24-22-22	$a/b/d/e/f/h/i/j/a/b/c/e/g/h/g/j$
4	22-22-24	$a/b/d/e/g/h/i/j/b/d/e/f/g/h/i/g$

Table 2. Key scheduling in MM-128

	$j=1$	$j=2$	$j=3$	$j=4$	$j=5$	$j=6$	$j=7$	$j=8$	$j=9$
$Q_j^{(e=0)}$	K_1	K_2	K_3	K_4	K_4	K_1	K_3	K_4	K_1
$U_j^{(e=0)}$	K_3	K_4	K_2	K_1	K_2	K_3	K_2	K_3	K_2
$Q_j^{(e=1)}$	K_1	K_3	K_2	K_3	K_2	K_1	K_2	K_4	K_3
$U_j^{(e=1)}$	K_2	K_4	K_3	K_1	K_4	K_4	K_3	K_2	K_1

The extension box E is defined as

$$E(X) = (X, X^{\ll 2}, X^{\ll 4}, X^{\ll 6}, X^{\ll 8}, X^{\ll 10})$$

where $X^{\ll b}$ represents the cyclic rotation of the vector $X = (x_1, \dots, x_{32})$ to the left by b bits.

The permutation involution I_1 is described as follows:

(1)(2,9)((3,17)(4,25)(5,33)(6,41)(7,49)(8,57)(10)(11,18)(12,26)(13,34)(14,42)
(15,50)(16,58)(19)(20,27)(21,35)(22,43)(23,51)(24,59)(28)(29,36)(30,44)(31,52)
(32,60)(37)(38,45)(39,53)(40,61)(46)(47,54)(48,62)(55)(56,63)(64).

4. Related-Key Amplified Boomerang Characteristics of MM-128

This section discusses the way of establishing the related-key differential boomerang characteristics with high probability based on the differential properties of MM-128.

Suppose that the (P, P^*, P', P'^*) plaintexts with the difference $\alpha = P \oplus P^* = P' \oplus P'^* = (e_{64},0)$ are encrypted to obtain the appropriate cipher-text (C, C^*, C', C'^*) using the master key (K, K^*, K', K'^*) that satisfies the key difference $\triangle K = K \oplus K^* = K' \oplus K'^* = (e_{64}, 0,0,0)$.

In this way, the 1^{st} related-key propagation of the differential distinguisher ($\alpha \to \beta$) can be obtained from the 1^{st} round to the 3^{rd} round of MM-128 in order to obtain the output difference $\beta = (0,0)$, with a probability of 1.

Then, the traditional value was assigned as (I, I^*, I', I'^*) with the difference $\gamma = I \oplus I^* = I' \oplus I'^* = e_{64}, e_{64},$). These values are encoded using the master key (K, K^*, K', K'^*), as the key difference is $\triangle K = K \oplus K' = K^* \oplus K'^* = (e_{64}, 0,0,0)$. Finally, we yield the 2^{nd} related-key propagation of the differential distinguisher ($\gamma \to \delta$) from the 4^{th} round to the 7.5^{th} round with a probability of 2^{-5}, to obtain the corresponding output difference $\delta = (e_{64}, 0)$.

5. Key Recovery Attacks on MM-128

This section presents a key recovery attack on MM-128 using a related-key amplified boomerang distinguisher.

5.1 Related-Key Amplified Boomerang Key Recovery Attack

This type of attack exploits a related-key amplified boomerang distinguisher of the 7.5-round MM-128 (Fig. 7). As shown in Table 3, this attack is decomposed into two sub-ciphers: E^0 contains the first three rounds of MM-128, and E^1 contains the remaining 4.5 rounds, where $\triangle K = K \oplus K^* = K' \oplus K'^* = (e_{64}, 0,0,0)$ and $\triangle K' = K \oplus K^* = K' \oplus K'^* = (0,0,0, e_{64})$. The 0.5 round indicates the key-addition layer of the involved round.

Table 3. Two related-key differential characteristics with a probability of approximately $\mathbf{2^{-5}}$ of the 7.5 round MM-128

$\boldsymbol{Round(j)}$	$\triangle \boldsymbol{P^j}$	$\triangle \boldsymbol{Q^{j,(0)}}$,$\triangle \boldsymbol{U^{j,(0)}}$	$\boldsymbol{Probability}$
1	$\alpha = (e_{64}, 0)$	$(e_{64}, 0)$	1
2	$(0, 0)$	$(0, 0)$	1
3	$(0, 0)$	$(0, 0)$	1
Output	$\beta = (0, 0)$		
4	$\gamma = (e_{64}, e_{64})$	$(e_{64}, 0)$	2^{-5}
5	$(e_{64}, 0)$	$(e_{64}, 0)$	1
6	$(0, 0)$	$(0, 0)$	1
7	$(0, 0)$	$(0, 0)$	1
7.5	$\delta = (e_{64}, 0)$	$(e_{64}, 0)$	1
8	$(?, ?)$	-	-
Ft	$(?, ?)$	$(e_{64}, 0)$	-
Output	$(?, ?)$		

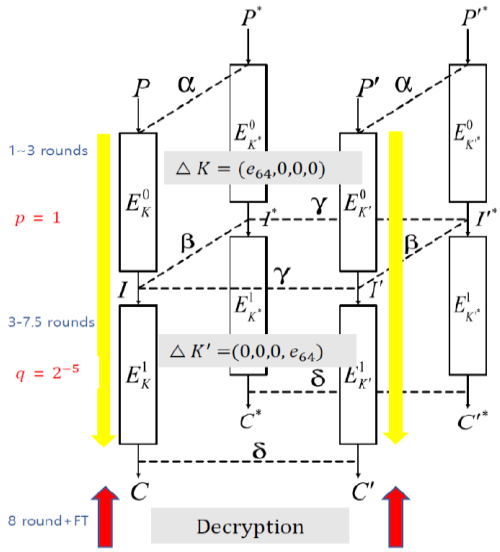


Fig. 7. Related-key amplified boomerang distinguisher of MM-128.

The first related-key differential characteristic for E^0 is $(e_{64},0) \rightarrow (0,0)$ with probability 1 because the input difference to round 1 is canceled by the key difference of the first round, and the zero difference remains up to the output of the second to third rounds. The resultant probability p is 1.

The second related-key differential characteristic for rounds 4–7.5(E^1) is $(e_{64}, e_{64},) \rightarrow (e_{64},0)$ with probability $\left(\frac{36}{64}\right)^6$ ($\approx 2^{-5}$). The details of this result are presented in Figs. 8–10. The difference between the input of the 4^{th} round (e_{64}, e_{64}) and the sub-key difference of the 4^{th} round $(e_{64}, 0)$ is the probability

2^{-5}, and the output difference becomes $(0, e_{64})$. Also, the input difference of round 5 is canceled by the sub-key difference of round 5, and zero difference is maintained until round 7, after which the input difference of the 7.5th round is $(e_{64}, 0)$, and the sub-key difference of the 8^{th} round is $(e_{64}, 0)$. The resulting probability q is also $\approx 2^{-5}$.

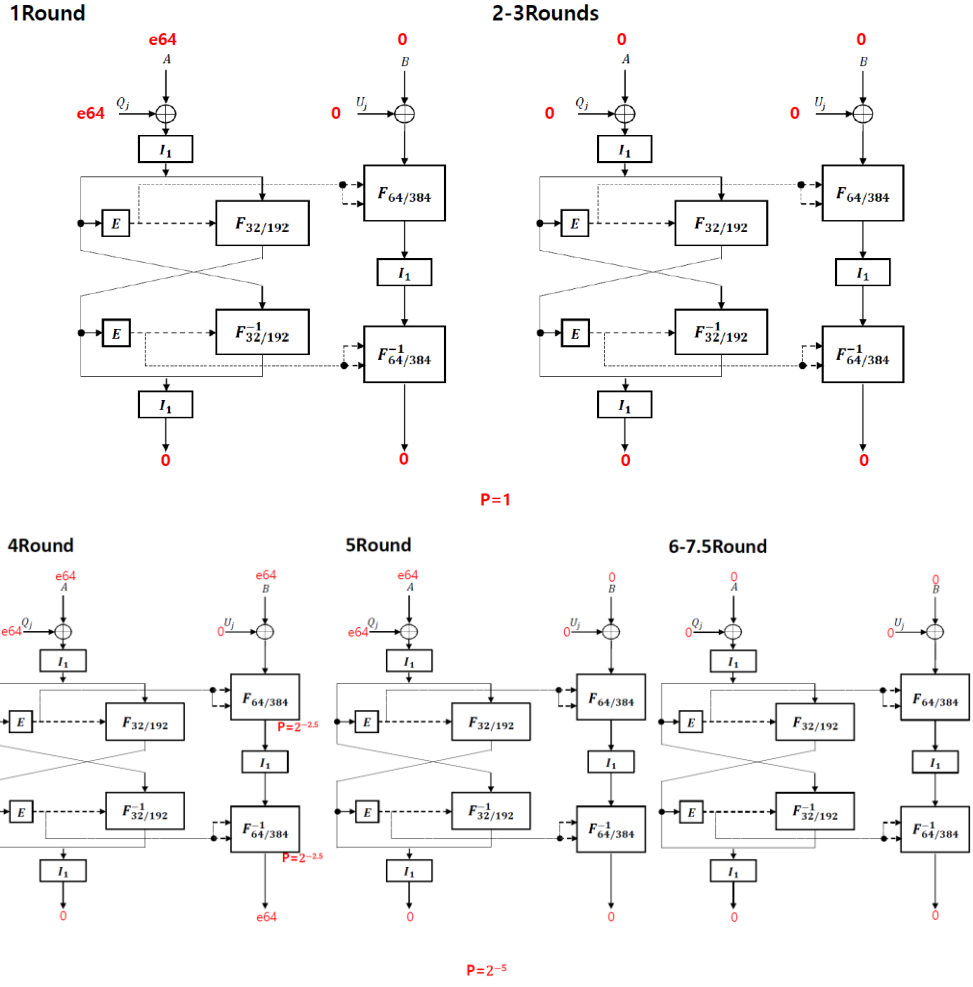


Fig. 8. Propagation in the MM-128 round function in the first round and for the 2^{nd}→7.5^{th} rounds.

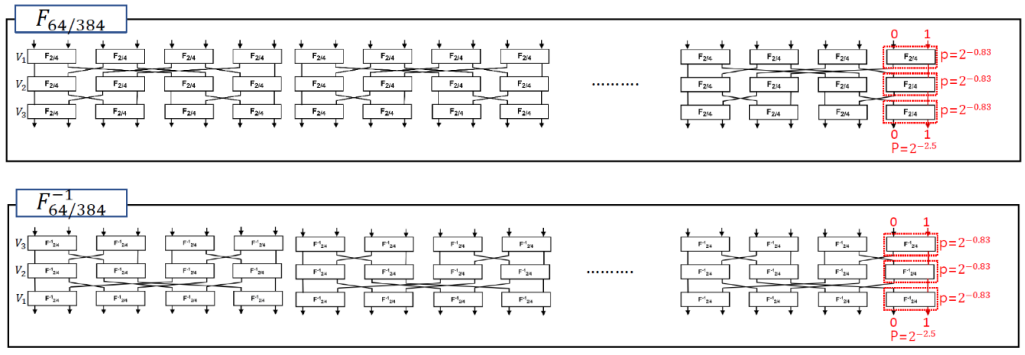


Fig. 9. Possible routes of $F_{64/384}$ and $F^{-1}_{64/384}$ in the fourth round.

		00	01	10	11			00	01	10	11
0000	00	64/64	0/64	0/64	0/64	1000	00	28/64	16/64	8/64	12/64
	01	0/64	36/64	12/64	16/64		01	8/64	20/64	4/64	24/64
	10	0/64	12/64	36/64	16/64		10	8/64	4/64	36/64	16/64
	11	0/64	16/64	16/64	32/64		11	12/64	24/64	24/64	12/64
0001	00	12/64	16/64	16/64	20/64	1001	00	28/64	8/64	8/64	20/64
	01	16/64	20/64	12/64	16/64		01	8/64	28/64	20/64	8/64
	10	16/64	12/64	20/64	16/64		10	8/64	28/64	20/64	8/64
	11	20/64	16/64	16/64	12/64		11	20/64	8/64	8/64	28/64
0010	00	12/64	16/64	16/64	20/64	1010	00	16/64	20/64	12/64	16/64
	01	16/64	12/64	20/64	16/64		01	20/64	16/64	16/64	12/64
	10	16/64	20/64	12/64	16/64		10	12/64	16/64	16/64	20/64
	11	20/64	16/64	16/64	12/64		11	16/64	12/64	20/64	16/64
0011	00	16/64	20/64	20/64	8/64	1011	00	20/64	16/64	24/64	4/64
	01	20/64	32/64	8/64	4/64		01	16/64	36/64	4/64	8/64
	10	20/64	8/64	16/64	20/64		10	24/64	4/64	20/64	16/64
	11	8/64	4/64	20/64	32/64		11	4/64	8/64	16/64	36/64
0100	00	14/64	18/64	14/64	18/64	1100	00	14/64	18/64	14/64	18/64
	01	18/64	14/64	18/64	14/64		01	18/64	14/64	18/64	14/64
	10	14/64	18/64	14/64	18/64		10	14/64	18/64	14/64	18/64
	11	18/64	14/64	18/64	14/64		11	18/64	14/64	18/64	14/64
0101	00	14/64	6/64	26/64	18/64	1101	00	14/64	6/64	26/64	18/64
	01	6/64	14/64	18/64	26/64		01	6/64	14/64	18/64	26/64
	10	26/64	18/64	14/64	6/64		10	26/64	18/64	14/64	6/64
	11	18/64	26/64	6/64	14/64		11	18/64	26/64	6/64	14/64
0110	00	14/64	6/64	26/64	18/64	1110	00	14/64	6/64	26/64	18/64
	01	6/64	14/64	18/64	26/64		01	6/64	14/64	18/64	26/64
	10	26/64	18/64	14/64	6/64		10	26/64	18/64	14/64	6/64
	11	18/64	26/64	6/64	14/64		11	18/64	26/64	6/64	14/64
0111	00	14/64	18/64	14/64	18/64	1111	00	14/64	18/64	14/64	18/64
	01	18/64	14/64	18/64	14/64		01	18/64	14/64	18/64	14/64
	10	14/64	18/64	14/64	18/64		10	14/64	18/64	14/64	18/64
	11	18/64	14/64	18/64	14/64		11	18/64	14/64	18/64	14/64

Fig. 10. Differential distribution table of $F_{2/4}$.

Combining these two characteristics leads to a 7.5-round related-key amplified boomerang distinguisher with probability $\approx 2^{-138}$ ($=2^{-128} \cdot p^2 \cdot q^2$), i.e., for m related-key chosen plaintext pairs (P, P^*) and (P', P'^*) each, $m^2 \cdot 2^{-138}$ right quartets can be expected. Hence, given two pools of $2^{70.5}$ related-key chosen plaintext pairs, eight right amplified boomerang quartets can be expected. The approach to a full-round MM-128 key recovery attack consists in guessing the sub-key of the final transform first, and then decrypting all of the cipher-text, before finally applying the distinguisher to the remaining 7.5 rounds.

The related-key boomerang key recovery attack on the 7.5-round MM-128 is described below.

(1) Choose two pools of $\mathbf{2^{70.5}}$ plaintext pairs $(\boldsymbol{P_i}, \boldsymbol{P_i^*})$ and $(\boldsymbol{P_j'}, \boldsymbol{P_j'^*})$ with difference $(\boldsymbol{e_{64}}, \mathbf{0})(\boldsymbol{i}, \boldsymbol{j} = \mathbf{1}, \mathbf{2}, \ldots, \mathbf{2^{70.5}})$. With the chosen plaintext attack scenario, encrypt the two pools of the collected plaintext pairs $(\boldsymbol{P_i}, \boldsymbol{P_i^*})$ and $(\boldsymbol{P_j'}, \boldsymbol{P_j'^*})$ using the keys, $(\boldsymbol{K}, \boldsymbol{K^*}) = (\boldsymbol{K}, \boldsymbol{K} \oplus (\boldsymbol{e_{64}}, 0,0,0))$ and $(\boldsymbol{K'}, \boldsymbol{K'^*}) = (\boldsymbol{K} \oplus (\mathbf{0}, \mathbf{0}, \mathbf{0}, \boldsymbol{e_{64}}), \boldsymbol{K} \oplus (\boldsymbol{e_{64}}, \mathbf{0}, \mathbf{0}, \boldsymbol{e_{64}}))$, respectively, to obtain the corresponding cipher-text pools $(\boldsymbol{C_i}, \boldsymbol{C_i^*})$ and $(\boldsymbol{C_j'}, \boldsymbol{C_j'^*})$. We keep all of these cipher-texts in a table.

(2) Guess a 64-bit sub-key quartet of the final transformation, $(\boldsymbol{K_1}.\boldsymbol{K_1^*}.\boldsymbol{K_1'}.\boldsymbol{K_1'^*}) = (\boldsymbol{K_1}, \boldsymbol{K_1} \oplus \boldsymbol{e_{64}}, \boldsymbol{K_1}, \boldsymbol{K_1} \oplus \boldsymbol{e_{64}})$, and then complete the following:

(a) Partially decrypt all cipher-texts $\boldsymbol{C_i}, \boldsymbol{C_i^*}, \boldsymbol{C_j'}, \boldsymbol{C_j'^*}$ with the guessed sub-keys $\boldsymbol{K_1}.\boldsymbol{K_1^*}.\boldsymbol{K_1'}.\boldsymbol{K_1'^*}$, respectively, to obtain the intermediate values just before (through the decryption direction) the key addition layer of the last round. These 128-bit values are denoted as $\boldsymbol{U_i}, \boldsymbol{U_i^*}, \boldsymbol{U_j'}, \boldsymbol{U_j'^*}$.

(b) Check that $\boldsymbol{U_i} \oplus \boldsymbol{U_j'} = \boldsymbol{U_i^*} \oplus \boldsymbol{U_j'^*} = (\boldsymbol{e_{64}}, \mathbf{0})$ for all $\boldsymbol{i}, \boldsymbol{j}$. (This step can be performed efficiently by checking a quartet pair after $\boldsymbol{U_i}, \boldsymbol{U_i^*}, \boldsymbol{U_j'}, \boldsymbol{U_j'^*}$ in the table.)

(c) If the number of quartets passing Step 2-(b) is greater than or equal to 6, output the guessed $(\boldsymbol{K_1}.\boldsymbol{K_1^*}.\boldsymbol{K_1'}.\boldsymbol{K_1'^*}) = (\boldsymbol{K_1}, \boldsymbol{K_1} \oplus \boldsymbol{e_{64}}, \boldsymbol{K_1}, \boldsymbol{K_1} \oplus \boldsymbol{e_{64}})$ as the right 64-bit subkey quartet. Otherwise, go to Step 2.

The data complexity of this attack is $2^{72.5}$ related-key chosen plaintexts, and it requires two pools of $2^{70.5}$ plaintext pairs. The required memory for this attack is approximately $2^{76.5}$ ($=2^{72.5} \cdot 16$) memory bytes. The time complexities of Step 1 and Step 2(a) are approximately $2^{72.5}$ full-round MM-128 encryptions and $2^{132.5}$ ($=2^{64} \cdot 2^{72.5} \cdot \frac{1}{2} \cdot \frac{1}{8}$) full-round MM-128 encryptions on average, respectively. Thus, the time complexity of this attack is about $2^{132.5}$ full round MM-128 encryptions—The time complexities of Step 2(b) and Step 2(c) are much lower than that of Step 2(a). If the wrong key is guessed, each decrypted cipher-text quartet is expected to pass Step 2(b) with probability $\approx 2^{-128 \cdot 2} = 2^{-256}$; whereas with probability $\approx$ 1- 2^{-256} , it will not pass Step 2(b). It follows that the probability with which *i* quartets are suggested in Step 2(b) is $\binom{t}{i} \cdot (2^{-256})^i \cdot (1 - (2^{-256}))^{t-i}$, where $t = 2^{143}$ represents the number of all possible cipher-text quartets generated by two pools of $2^{71.5}$ cipher-text pairs. Because this attack outputs a guessed sub-key quartet to cause more than or equal to six quartets to pass Step 2(b) and the total number of wrong key guesses is $2^{64} - 1$, the probability that the output of the above attack algorithm is a wrong sub-key quartet is approximated as follows:

$$
\begin{aligned}
2^{-200} &= \left(\approx \sum_{i=6}^{t} \left(\binom{t}{i} \cdot (2^{-256})^i \cdot \left(1 - (2^{-256})\right)^{t-i}\right) \cdot (2^{64} - 1)\right) \\
&= \left\{\binom{2^{143}}{6} \cdot (2^{-256})^6 \cdot \left(1 - (2^{-256})\right)^{2^{143}-6}\right) + \left(\binom{2^{143}}{7} \cdot (2^{-256})^7 \cdot \left(1 - (2^{-256})\right)^{2^{143}-7}\right) \\
&\quad + \cdots + \left(\binom{2^{143}}{2^{143}} \cdot (2^{-256})^{2^{143}} \cdot \left(1 - (2^{-256})\right)^{2^{143}-2^{143}}\right)\right\} \cdot (2^{64} - 1),
\end{aligned}
$$

where $t = 2^{143}$.

In fact, for some incorrect key guesses (especially those whose differences from the right key are small), decrypted cipher-text quartets do not behave randomly; however, for each such key the probability that a decrypted cipher-text quartet passes Step 2(b) is still much lower than the probability of the proposed 7.5-round related-key amplified boomerang distinguisher; in this study's observation, its probability is less

than or equal to the earlier case due to the differential properties of the DDO-boxes. Thus, the probability that the output of the above attack algorithm is a wrong sub-key quartet is upper bounded by

$$2^{-150} = \left(\approx \sum_{i=6}^{t}\left(\binom{t}{i}\cdot(2^{-192})^{i}\cdot\left(1-(2^{-192})\right)^{t-i}\right)\cdot(2^{64}-1)\right)$$
$$= \left\{\binom{2^{143}}{6}\cdot(2^{-192})^{6}\cdot\left(1-(2^{-192})\right)^{2^{143}-6}) + (\binom{2^{143}}{7}\cdot(2^{-192})^{7}\cdot\left(1-(2^{-192})\right)^{2^{143}-7}\right)$$
$$+\cdots+(\binom{2^{143}}{2^{143}}\cdot(2^{-192})^{2^{143}}\cdot\left(1-(2^{-192})\right)^{2^{143}-2^{143}})\Big\}\cdot(2^{64}-1),$$

where $t = 2^{143}$.

On the other hand, the probability that the number of quartets for the right sub-key is no less than 6 is about

$$0.99 = \left(\approx \sum_{i=6}^{t}\left(\binom{t}{i}\cdot(2^{-128})^{i}\cdot\left(1-(2^{-128})\right)^{t-i}\right)\right)$$
$$= \left\{\binom{2^{143}}{6}\cdot(2^{-128})^{6}\cdot\left(1-(2^{-128})\right)^{2^{143}-6}) + (\binom{2^{143}}{7}\cdot(2^{-128})^{7}\cdot\left(1-(2^{-128})\right)^{2^{143}-7}\right)$$
$$+\cdots+(\binom{2^{143}}{2^{143}}\cdot(2^{-128})^{2^{143}}\cdot\left(1-(2^{-128})\right)^{2^{143}-2^{143}})\Big\},$$

where $t = 2^{143}$, as each decrypted cipher-text quartet for the right key passes Step 2(b) with a probability of $\approx 2^{-128}$ due to the proposed 7.5-round related-key amplified boomerang distinguisher.

Therefore, the success rate of this attack is about 0.99.

6. Conclusion

Previously, the DDO-based cipher MM-128 was designed to realize the rapid implementation of hardware and a high level of security by using a new class of $F_{2/4}$ type CE suitable for FPGA. However, this paper discusses the first cryptanalytic result of the MM-128 cipher, and constructs the differential characteristics of a full 9-round of MM-128 cipher with high probability base on some differential properties combined with a simple key schedule within the MM-128 structure. It then presents a related-key amplified boomerang attack on a full-round MM-128 with $2^{72.5}$ related-key chosen plaintexts, $2^{76.5}$ memory bytes, and time complexity of $2^{132.5}$. Our cryptanalytic result means that the full-round reduced MM-128 can be distinguished from an ideal cipher very efficiently, but remains vulnerable to related-key differential attacks owing to its simple key schedule algorithms and structural weaknesses. Future research could include a better primitive approach to the design of the block ciphers, especially structures based on the DDP, DDO or SDDO functions.

Author's Contributions

Conceptualization, HE, CR. Funding acquisition, CR. Investigation and methodology, HE, CR. Project administration, HE. Resources, HE, BS. Supervision, CR. Writing of the original draft, HE. Writing of the review and editing, HE. Software, HE, BS. Validation, HE, BS. Formal analysis, CR. Data curation, HE, BS. Visualization, HE.

Funding

This research was supported by the Energy Cloud R&D Program (No. 2019M3F2A1073386) through the NRF (National Research Foundation of Korea), both of which are funded by the Ministry of Science and ICT.

Competing Interests

The authors declare that they have no competing interests.

References

[1] A. A. Moldovyan and N. A. Moldovyan, "A cipher based on data-dependent permutations," *Journal of Cryptology*, vol. 15, no. 1, pp. 61-72, 2002.

[2] N. Sklavos, N. A. Moldovyan, and O. Koufopavlou, "High speed networking security: design and implementation of two new DDP-based ciphers," *Mobile Networks and Applications*, vol. 10, no. 1, pp. 219-231, 2005.

[3] N. A. Moldovyan, "On cipher design based on switchable controlled operations," in *Computer Network Security*. Heidelberg, Germany: Springer, 2003, pp. 316-327.

[4] N. A. Iavos, N. A. Moldovyan, and O. Koufopavlou, "A new DDP based cipher CIKS-128h architecture design LSI implementation optimization of CBC encryption hashing over 1Gbps," in *Proceedings of 2003 46th Midwest Symposium on Circuits and Systems*, Cairo, Egypt, 2003, pp. 463-466.

[5] N. H. Minh, D. Bac, and H. Duy, "New SDDO-based block cipher for wireless sensor network security," *International Journal of Computer Science and Network Security*, vol. 10, no. 3, pp. 54-60, 2010.

[6] N. A. Moldovyan and A. A. Moldovyan, *Data-Driven Ciphers for Fast Telecommunication Systems*. Boca Raton, FL: Auerbach Publications, 2008.

[7] P. M. Tuan, B. Do Thi, M. N. Hieu, and N. Do Thanh, "New block ciphers for wireless moblile netwoks," in *Advances in Information and Communication Technology*. Cham, Switzerland: Springer, 2017, pp. 393-402.

[8] N. H. Minh, H. N. Duy, and L. H. Dung, "Design and estimate of a new fast block cipher for wireless communication devices," in *Proceedings of 2008 International Conference on Advanced Technologies for Communications*, Hanoi, Vietnam, 2008, pp. 409-412.

[9] B. D. Thi and M. N. Hieu, "High-speed block cipher algorithm based on hybrid method," in *Ubiquitous Information Technologies and Applications*. Heidelberg, Germany: Springer, 2014, pp. 285-291.

[10] T. S. D. Phuc, Y. H. Shin, and C. Lee, "Recovery-key attacks against TMN-family framework for mobile wireless networks," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 15, no. 6, pp. 2148-2167, 2021.

[11] Y. Ko, C. Lee, S. Hong, J. Sung, and S. Lee, "Related-key attacks on DDP based ciphers: CIKS-128 and CIKS-128H," in *Progress in Cryptology – INCOCRYPT 2004*. Heidelberg, Germany: Springer, 2004, pp. 191-205.

[12] C. Lee, J. Kim, J. Sung, S. Hong, S. Lee, and D. Moon, "Related-key differential attacks on Cobra-H64 and Cobra-H128," in *Cryptography and Coding*. Heidelberg, Germany: Springer, 2005, pp. 201-219.

[13] J. Kang, K. Jeong, C. Lee, and S. Hong, "Distinguishing attack on SDDO-based block cipher BMD-128," in *Ubiquitous Information Technologies and Applications*. Heidelberg, Germany: Springer, 2014, pp. 595-602.

[14] T. S. D. Phuc, N. N. Xiong, and C. Lee, "Cryptanalysis of the XO-64 suitable for wireless systems," *Wireless Personal Communications*, vol. 93, no. 2, pp. 589-600, 2017.

[15] C. Lee, J. Kim, S. Hong, J. Sung, and S. Lee, "Security analysis of the full-round DDO-64 block cipher," *Journal of Systems and Software*, vol. 81, no. 12, pp. 2328-2335, 2008.

[16] J. Kang, K. Jeong, S. S. Yeo, and C. Lee, "Related-key attack on the MD-64 block cipher suitable for pervasive computing environments," in *Proceedings of 2012 26th International Conference on Advanced Information Networking and Applications Workshops*, Fukuoka, Japan, 2012, pp. 726-731.

[17] J. Kelsey, T. Kohno, and B. Schneier, "Amplified boomerang attacks against reduced-round MARS and Serpent," in *Fast Software Encryption*. Heidelberg, Germany: Springer, 2000, pp. 75-93.

[18] M. N. Hieu, D. H. Ngoc, C. H. Ngoc, T. D. Phuong, and M. T. Cong, "New primitives of controlled elements F2/4 for block ciphers," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 5, pp. 5470-5478, 2020.

[19] E. Biham, "New types of cryptanalytic attacks using related keys," *Journal of Cryptology*, vol. 7, no. 4, pp. 229-246, 1994.

[20] D. Wagner, "The boomerang attack," in *Fast Software Encryption*. Heidelberg, Germany: Springer, 1999, pp. 156-170.

[21] E. Biham, O. Dunkelman, and N. Keller, “Related-key boomerang and rectangle attacks,” in *Advances in Cryptology - EUROCRYPT 2005*. Heidelberg, Germany: Springer, 2005, pp. 507-525.

[22]C. Cid, T. Huang, T. Peyrin, Y. Sasaki, L. Song, “Boomerang Connectivity Table: A New Cryptanalysis Tool,” in: J. Nielsen, V. Rijmen (eds), Advances in Cryptology-EUROCRYPT 2018, LNCS 10821, 683-714, 2018.

[23]A. Bar-On, O. Dunkelman, N. Keller, A. Weizman, “DLCT: A new tool for differential-linear cryptanalysis,” in : Y. Ishai, V. Rijmen (Eds): EUROCRYPT 2019, LNCS 11476, pp. 313-342, 2019.