symmetry

MDPI

Article

Cryptanalysis on SDDO-Based BM123-64 Designs Suitable for Various IoT Application Targets

Tran Song Dat Phuc and Changhoon Lee *

Department of Computer Science and Engineering, Seoul National University of Science and Technology, Gongneung-ro, Nowon-gu, Seoul 01811, Korea; datphuc_89@yahoo.com

* Correspondence: chlee@seoultech.ac.kr

Received: 28 June 2018; Accepted: 17 August 2018; Published: 20 August 2018

Abstract: BM123-64 block cipher, which was proposed by Minh, N.H. and Bac, D.T. in 2014, was designed for high speed communication applications factors. It was constructed in hybrid controlled substitution–permutation network (CSPN) models with two types of basic controlled elements (CE) in distinctive designs. This cipher is based on switchable data-dependent operations (SDDO) and covers dependent-operations suitable for efficient primitive approaches for cipher constructions that can generate key schedule in a simple way. The BM123-64 cipher has advantages including high applicability, flexibility, and portability with different algorithm selection for various application targets with internet of things (IoT) as well as secure protection against common types of attacks, for instance, differential attacks and linear attacks. However, in this paper, we propose methods to possibly exploit the BM123-64 structure using related-key attacks. We have constructed a high probability related-key differential characteristics (DCs) on a full eight rounds of BM123-64 cipher. The related-key amplified boomerang attack is then proposed on all three different cases of operation-specific designs with effective results in complexity of data and time consumptions. This study can be considered as the first cryptographic results on BM123-64 cipher.

Keywords: BM123-64; hybrid controlled substitution–permutation network (CSPN); switchable data-dependent operations (SDDOs); cryptanalysis; related-key amplified boomerang attack

1. Introduction

The BM123-64 [1] has a 64-bit block size covering 256-bit secret key size and a total of eight function rounds. This cipher is based on switchable data-dependent operations (SDDO) [2], which is designed to combine data-dependent operations in functions and new feature of hybrid-controlled substitution–permutation network (CSPN) models. By this way, BM123-64 is considered as a solution for a more flexible and suitable approach for appropriate application targets with each specific design. The cipher has advantages including better suitability, applicability with different algorithm designs for specific targets, and high reliability of securing against well-known attacks, for instance, linear attacks and differential attacks.

Although lots of researchers have focused on how to enhance the security of construction designs using different operations and functions, for instance, DDP (Data-Dependent Permutation) -based ciphers (such as DDP-64 [3], Cobra-family [3] and SCO (Switchable Controlled Operation) -family [2]), DDO (Data-Dependent Operation) -based ciphers (such as MD-64 [4], KT-64 [5], CTPO (Controlled Two-Place Operation) [6] and DDO-64 [7]), and SDDO-based ciphers (such as XO-64 [8] or BMD-128 [9]), their weaknesses have been recently explored with common related attacks. A simple key schedule generator for high speed transformation and lightweight targets can lead to an attack possibility for cryptanalysis using common related-key attack methods.

Related-key amplified boomerang attack [10] is an extension of the related-key boomerang attack proposed by Biham et al., 2005 [11] and Wagner, 1999 [12]. The idea of this attack is that it explores two distinctive related-key differentials to construct the related-key boomerang with high probability. Compared to other attacks, the attack was designed as an adaptive chosen plaintext attack that has become a popular and effective method to exploit many types of block ciphers. Previous studies that have applied this attack on various SDDO-based ciphers - such as COCONUT98, IDEA [11], MARS, Serpent [12], DDO-64 [13], MD-64 [14], BMD-128 [15], XO-64 [16], etc.—showed efficiency and high probabilities in cryptanalytic results.

In this paper, we propose attack methods on BM123-64 constructions with related-key approach. By constructing high probability differentials with two related-key boomerangs in distinctive designs, this attack expects to exploit a full eight rounds of BM123-64 with effective cryptanalytic results. The proposed attack requires about 2^{67} data complexity, 2^{70} memory bytes, and time complexity of 2^{67} encryptions with **Case 1** design. For **Case 2** and **Case 3** designs of BM-123-64 constructions, 2^{51} data complexity, 2^{54} memory bytes, and time complexity of 2^{65} are required. This study shows that like lots of other ciphers designed on data-dependent operations, BM123-64 still has weaknesses and is insecure against related-key cryptanalysis. The cipher construction should therefore be based on more secure primitive security approach.

The rest of this paper is organized as follows: The BM123-64 construction is briefly reviewed in Section 2. In Section 3, the proposed attacks on BM123-64 cipher is discussed, including differential characteristics (DCs), analysis methods, and security assessments. Finally, in Section 4, conclusions of the paper are presented.

2. BM123-64 Block Cipher Description

2.1. Preliminaries

This section explains notations used in this paper. With x_1 as the most significant bit and x_n as the least significant bit, a cipher X can be assigned as $X = (x_1, x_2, \ldots, x_n)$.

The DCs applied to the attack methods include descriptions of differential relation of block ciphers, such as input, output, and function round key.

- r denotes each function round of block cipher.
- $\Delta \boldsymbol{X_r}$ denotes input difference value that occurs in each r.
- $\Delta \boldsymbol{Y_r}$ denotes output difference value that occurs in each r.
- $\Delta \boldsymbol{U_r}$, $\Delta \boldsymbol{Q_r}$ denote round key difference values that occur in each r.
- e_i denotes the data bit changing within each round function, with i value considered as an active bit; at the i^{th} position, the bit value is "1", and the remaining bits are "0" in each block data. for instance, $e_{1,3} = (1, 0, 1, 0, \ldots, 0)$).

2.2. BM123-64 Construction

BM123-64 [1] is described as a 64-bit SDDO-based block cipher with 256-bit secret key and eight function rounds in total. Each $\mathbf{Crypt}^{(e)}$ round function in the cipher structure does the same operation from the first round to the final round to generate output ciphertext.

The $\mathbf{Crypt}^{(e)}$ of BM123-64 covers three types of fixed permutation functions (I, I_1, and I_2), an extension box **E**, hybrid-controlled substitution–permutation networks **CSPN**s, and SDDO-based functions $F_{n/m}^{V/e}$ ($F_{16/64}$, $F^{-1}{}_{16/64}$, $F_{16/32}$, $F^{-1}{}_{16/32}$) based on basic controlling element $F_{2/2}$.

The process of BM123-64 encryption is described in the algorithm below.

1. 64-bit input plaintext splits into two 32-bit block A and block B.
2. From rounds r = 1 to 7, they have the same operations for each round:

   $(A, B) = \mathbf{Crypt}^{(0)}(A, B, U_r, Q_r)$

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

3. In the last round, there is final transformation to output ciphertext:

$$(A, B) = \mathbf{Crypt}^{(0)}\ (A, B, U_8, Q_8)$$
$$(A, B) = (L \oplus U_{\mathrm{FT}}, R \oplus Q_{\mathrm{FT}})$$
$$(A, B) = (A, B).$$

Figures 1 and 2 illustrate the **Crypt**$^{(0)}$ round function in detail. Reference [1] contains more description of the BM123-64 construction.

The SDDO-based functions $F_{16/64}$, $F^{-1}{}_{16/64}$ are constructed based on elementary function $F_{2/2}$, since $F_{2/2}$ is described as $((x_1, x_2), [v, z]/(y_1, y_2))$. For better performance on implementation with the target of a specific application and expansion of encryption space, the function $F^{V/e}_{n/m}$ is designed in three different operations with three different description of the basic element $F_{2/2}$.

Case 1:
$$y_1 = vzx_1 \oplus vz \oplus vx_1 \oplus vx_2 \oplus v \oplus z \oplus x_1 \oplus 1$$
$$y_2 = vzx_2 \oplus vz \oplus vx_1 \oplus vx_2 \oplus zx_1 \oplus x_2 \oplus v \oplus z \oplus 1$$
$$y_3 = vzx_1 \oplus vzx_2 \oplus zx_1 \oplus x_1 \oplus x_2.$$

Case 2:
$$y_1 = vzx_1 \oplus vzx_2 \oplus vx_1 \oplus vx_2 \oplus zx_1 \oplus zx_2 \oplus z \oplus v \oplus x_2$$
$$y_2 = vzx_1 \oplus vzx_2 \oplus vz \oplus vx_1 \oplus vx_2 \oplus zx_1 \oplus zx_2 \oplus x_1$$
$$y_3 = vz \oplus v \oplus z \oplus x_1 \oplus x_2.$$

Case 3:
$$y_1 = vx_2 \oplus x_2 \oplus x_1 \oplus v \oplus 1$$
$$y_2 = vx_1 \oplus x_2.$$

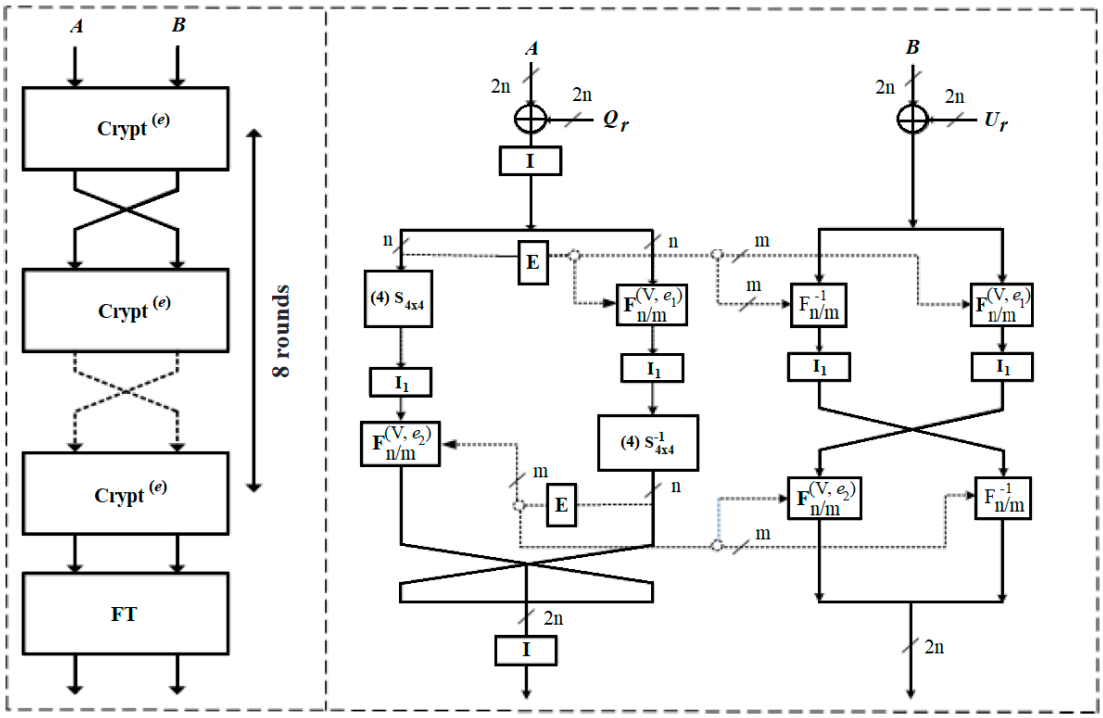


Figure 1. (**a**) The general structure (**left**); and (**b**) round function Crypt$^{(0)}$ (**right**) of BM123-64.

The three fixed permutations I, I_1, and I_2 are denoted as follows:

I_1 = (1) (2,5) (3,9) (4,13) (5,2) (6) (7,10) (8,14) (9,3) (10,7) (11) (12,15) (13,4) (14,8) (15,12) (16).
I_2 = (1) (2,3) (3,2) (4) (5) (6,7) (7,6) (8) (9) (10,11) (11,10) (12) (13) (14,15) (15,14) (16).
I = (1) (2,18) (3) (4,20) (5) (6,22) (7) (8,24) (9) (10,26) (11) (12,28) (13) (14,30) (15) (16,32) (17) (18,2) (19) (20,4) (21) (22,6) (23) (24,8) (25) (26,10) (27) (28,12) (29) (30,14) (31) (32,16).

The expansion function **E** takes a 16-bit input X, since $\mathbf{E}(X) = (X, X^{<<<4}, X^{<<<8}, X^{<<<12})$; it then outputs 64-bit controlled vector $(V, Z) = (V_1, V_2, V_3, V_4, Z_1, Z_2, Z_3, Z_4)$.

The hybrid **CSPN** construction is designed based on the description of permutation function structure covering eight 4 × 4 S-boxes (S_0, S_1, S_2, S_3 and $S^{-1}{}_0$, $S^{-1}{}_1$, $S^{-1}{}_2$, $S^{-1}{}_3$) with SDDO-based function $F^{V/e}_{n/m}$. Figure 3 presents the **CSPN** with its S-boxes in structure.

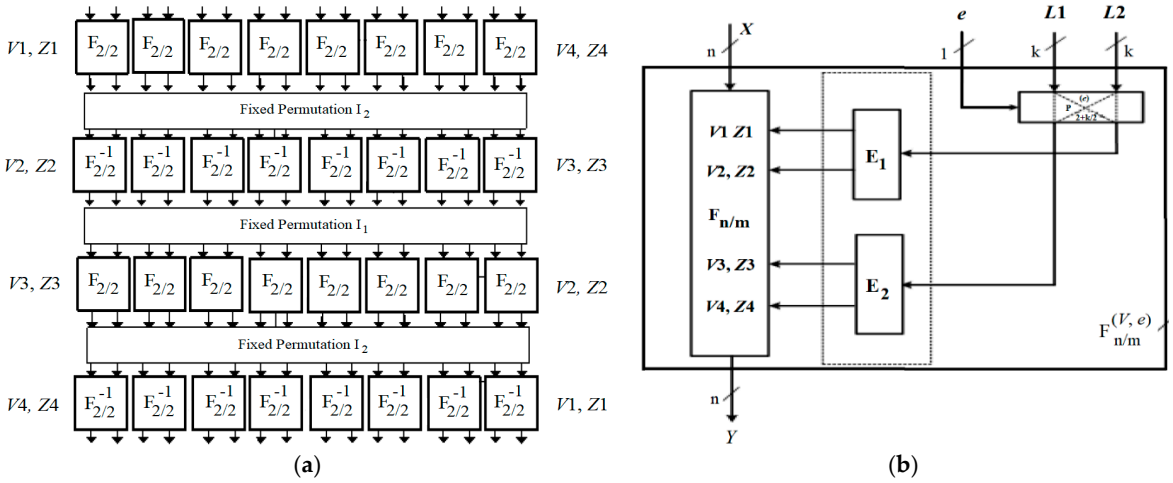
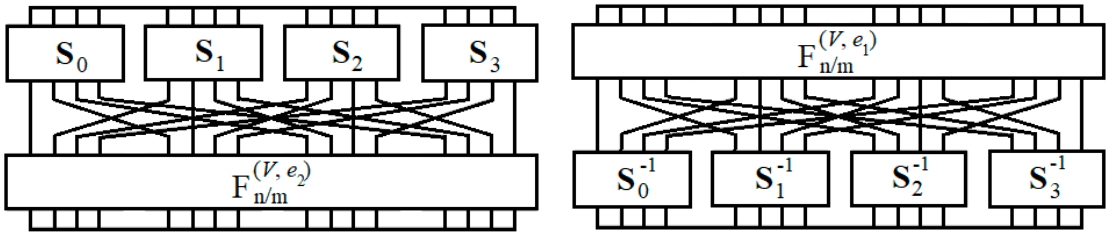


Figure 2. (**a**) Switchable data-dependent operations (SDDO)-based functions $F_{16/64}$, $F^{-1}{}_{16/64}$; and (**b**) $F_{16/32}$, $F^{-1}{}_{16/32}$.



S-box	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
S_1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
S_2	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
S_3	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
S_4	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
S_5	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
S_7	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
S_0^{-1}	14	3	4	8	1	12	10	15	7	13	9	6	11	2	0	5
S_1^{-1}	9	10	5	0	2	15	12	3	6	13	11	14	8	1	7	4
S_2^{-1}	1	8	14	5	13	7	4	11	15	2	0	12	10	9	3	6
S_3^{-1}	12	0	15	5	1	13	10	6	11	14	8	2	4	3	7	9
S_4^{-1}	3	9	13	10	15	12	1	6	14	2	0	15	4	7	11	8
S_5^{-1}	10	4	6	15	13	14	8	3	1	11	12	0	2	7	5	9
S_6^{-1}	12	9	3	14	2	7	8	4	15	6	0	13	5	10	11	1
S_7^{-1}	12	0	15	5	7	9	10	6	3	14	4	11	8	2	13	1

(**c**)

Figure 3. Controlled substitution–permutation network (CSPN) model in (**a**) left and (**b**) right of data sub-block; (**c**) different 4 × 4 S-boxes.

Like other data-dependent ciphers, BM123-64 is constructed with a very simple key schedule for high-speed transformation target. To generate function keys used in each round, 256-bit secret key K is divided into eight 32-bit subkeys $K = (K_1, K_2, \ldots, K_7, K_8)$. The key scheduling is provided with different parameters as shown in Table 1.

Table 1. Key schedule of BM123-64.

Round O_r	O_1	O_2	O_3	O_4	O_5	O_6	O_7	O_8	O_{FT}
U_r	K_3	K_4	K_8	K_6	K_2	K_7	K_5	K_2	K_3
Q_r	K_1	K_2	K_5	K_7	K_3	K_6	K_8	K_4	K_1
e'_1	1	1	1	0	0	1	1	0	-
e'_2	0	1	1	0	1	1	1	1	-
e'_3	0	0	0	1	1	0	0	1	-
e'_4	1	0	0	1	0	0	0	0	-

* O_{FT} performs the final transformation.

3. Proposed Attack Methods on BM123-64 Construction

Differential properties of operations in each round function are fundamental features to build differential characteristics and explore the related-key attack methods. Based on these properties, we can construct high probability DCs on a full eight rounds of BM123-64 with **Crypt$^{(e)}$** function. Furthermore, the related-key amplified boomerang attacks will be addressed with effective complexity results.

3.1. BM123-64 Crypt$^{(e)}$ Function Properties

The **Crypt$^{(e)}$** function in BM123-64 cipher consists of several $F_{n/m}^{V/e}$ functions having appropriate differential properties to construct the high probability DCs.

3.1.1. Differential Properties of $F_{2/2}$ Function

x_1 and x_2 are assumed as input parameters, with a pair (v, z) controlled vector of $F_{2/2}$ function. Therefore, the controlled element $F_{2/2}$ can be described as $F_{2/2}$ $(x_1, x_2, [v, z])$. Based on different distribution applied to different descriptions of $F_{2/2}$ in BM123-64, we have differential properties for each case as the following:

Case 1:
$$y_1 = vzx_1 \oplus vz \oplus vx_1 \oplus vx_2 \oplus v \oplus z \oplus x_1 \oplus 1$$
$$y_2 = vzx_2 \oplus vz \oplus vx_1 \oplus vx_2 \oplus zx_1 \oplus x_2 \oplus v \oplus z \oplus 1$$
$$\Pr\left[F_{2/2}(x_1, x_2, [v, z]) \oplus F_{2/2}(x_1 \oplus 1, x_2, [v, z]) = (1, 0)\right] = 2^{-2}.$$

Case 2:
$$y_1 = vzx_1 \oplus vzx_2 \oplus vx_1 \oplus vx_2 \oplus zx_1 \oplus zx_2 \oplus z \oplus v \oplus x_2$$
$$y_2 = vzx_1 \oplus vzx_2 \oplus vz \oplus vx_1 \oplus vx_2 \oplus zx_1 \oplus zx_2 \oplus x_1$$
$$\Pr\left[F_{2/2}(x_1, x_2, [v, z]) \oplus F_{2/2}(x_1 \oplus 1, x_2, [v, z]) = (1, 0)\right] = 2^{-1}.$$

Case 3:
$$y_1 = vx_2 \oplus x_2 \oplus x_1 \oplus v \oplus 1;$$
$$y_2 = vx_1 \oplus x_2$$
$$\Pr\left[F_{2/2}(x_1, x_2, [v, z]) \oplus F_{2/2}(x_1 \oplus 1, x_2, [v, z]) = (1, 0)\right] = 2^{-1}.$$

For each case of $F_{2/2}$ description, in order to get the (1, 0) output difference with the $(x_1 \oplus 1, 0)$ input difference and the (0, 0) controlled vector difference, the probability will be 2^{-2}, 2^{-1}, and 2^{-1} for **Case 1**, **Case 2,** and **Case 3**, respectively.

3.1.2. Differential Properties of $F_{16/64}$ and $F^{-1}{}_{16/64}$ Functions

In the same way, we can get the properties of SDDO-based functions $F_{16/64}$ and $F^{-1}{}_{16/64}$ using the properties above. Here, X is the input parameters for $F_{16/64}$ and $F^{-1}{}_{16/64}$ and (V, Z) is the controlled vector. Based on the properties of $F_{2/2}$, we can get the following:

Case 1: $\Pr[F_{16/64}(X, V, Z) \oplus F_{16/64}(X \oplus e_{16}, V, Z) = e_{16}] = 2^{-8}$
$\Pr[F^{-1}{}_{16/64}(X, V, Z) \oplus F^{-1}{}_{16/64}(X \oplus e_{16}, V, Z) = e_{16}] = 2^{-8}$

Case 2: $\Pr[F_{16/64}(X, V, Z) \oplus F_{16/64}(X \oplus e_{16}, V, Z) = e_{16}] = 2^{-4}$
$\Pr[F^{-1}{}_{16/64}(X, V, Z) \oplus F^{-1}{}_{16/64}(X \oplus e_{16}, V, Z) = e_{16}] = 2^{-4}$

Case 3: $\Pr[F_{16/64}(X, V, Z) \oplus F_{16/64}(X \oplus e_{16}, V, Z) = e_{16}] = 2^{-4}$
$\Pr[F^{-1}{}_{16/64}(X, V, Z) \oplus F^{-1}{}_{16/64}(X \oplus e_{16}, V, Z) = e_{16}] = 2^{-4}$

With the $F_{16/64}$ and $F^{-1}{}_{16/64}$ function designs, we can see that there is a total of four active layers $F_{2/2}$ within each construction, as shown in Figure 2.

3.2. Related-Key Boomerang of BM123-64

Here, we describe the way to generate related-key differential boomerangs on a full eight rounds of BM123-64 using the obtained properties in Section 3.1 with the key schedule generator.

We construct two related-key differentials as follows:

The first four rounds of related-key differential $\boldsymbol{E^0} = (\alpha \rightarrow \beta)$ holds with chosen input difference $\alpha = (0, 0)$ and key difference $(0, e_{32})$ from the first round to the fourth round with output difference $\beta = (0, 0)$. The key difference, based on the key schedule generator given in Table 1, is to control differential propagation and get high probability. The first related-key differential achieves this with probability $p = 2^{-16}$, 2^{-8}, and 2^{-8} for each case of $F_{2/2}$ description.

The second related-key differential $\boldsymbol{E^1} = (\gamma \rightarrow \delta) = (0, e_{32})$ " $(0, e_{16})$ covering the last four rounds with input difference $\alpha = (0, e_{32})$ and key difference $(0, e_{32})$ from the fifth round gives output difference $\delta = (0, e_{16})$ after the final transformation. The second related-key differential obtains probability $q = 2^{-16}$, 2^{-8}, and 2^{-8}, respectively. In total, the related-key differential characteristics constructed on a full eight rounds of BM123-64 designs give us the probability of 2^{-32} for **Case 1**, 2^{-16} for **Case 2,** and 2^{-16} for **Case 3**. Figure 2 illustrates the DCs propagation of some specific BM123-64 rounds in **Case 2** and **Case 3**.

The differential amplified boomerang can be explored based on the two related-key differentials above.

We can take any chosen plaintexts, namely (P, P^*, P', P'^*) with input difference $\alpha = (0, 0)$ described as $\Delta P = P \oplus P^* = P' \oplus P'^*$, to give respective ciphertexts with output difference $\beta = (0, 0)$ using related-keys (K, K^*, K', K'^*) defined as $\Delta K = K \oplus K^* = K' \oplus K'^* = (0, e_{16}, e_{32}, 0, 0, 0, 0, 0)$. We can hold the first four rounds related-key boomerang with probability of 2^{-16} for **Case 1**, 2^{-8} for **Case 2,** and 2^{-8} for **Case 3**. Furthermore, by pretending an additional round with intermediate differential values (I, I^*, I', I'^*) described as $I \oplus I^* = I' \oplus I'^* = (0, e_{32})$ using another related-key differences $\Delta K' = K \oplus K' = K^* \oplus K'^* = (0, e_{32}, 0, 0, 0, 0, 0, 0)$, we can build the second related-key boomerang on the last four rounds of 2^{-16} probability for **Case 1**, and 2^{-8} for both **Case 2** and **Case 3**.

In Table 2, the detailed DCs of a full eight rounds of BM123-64 with corresponding probabilities is shown. And, Figure 4 illustrates the DCs in $\mathbf{Crypt}^{(e)}$ function of BM123-64 with **Case 2** and **Case 3** at several rounds.

Table 2. Related-key DCs of a full eight rounds of BM123-64 in distinctive designs.

Round (r)	ΔX_r	$(\Delta U_r, \Delta Q_r)$	Probability		
			Case 1	Case 2	Case 3
1	$\alpha = (0, 0)$	$(0, e_{32})$	2^{-16}	2^{-8}	2^{-8}
2	$(e_{16}, 0)$	$(e_{16}, 0)$	1	1	1
3	(0, 0)	(0, 0)	1	1	1
4	(0, 0)	(0, 0)	1	1	1
Output	$\beta = (0, 0)$		2^{-16}	2^{-8}	2^{-8}
5	$(0, e_{32}) = \gamma$	$(0, e_{32})$	1	1	1
6	(0, 0)	(0, 0)	1	1	1
7	(0, 0)	(0, 0)	1	1	1
8	(0, 0)	$(0, e_{16})$	2^{-16}	2^{-8}	2^{-8}
FT	$(0, e_{16})$	(0, 0)	1	1	1
Output (ΔY)	$\delta = (0, e_{16})$				
Total			2^{-32}	2^{-16}	2^{-16}

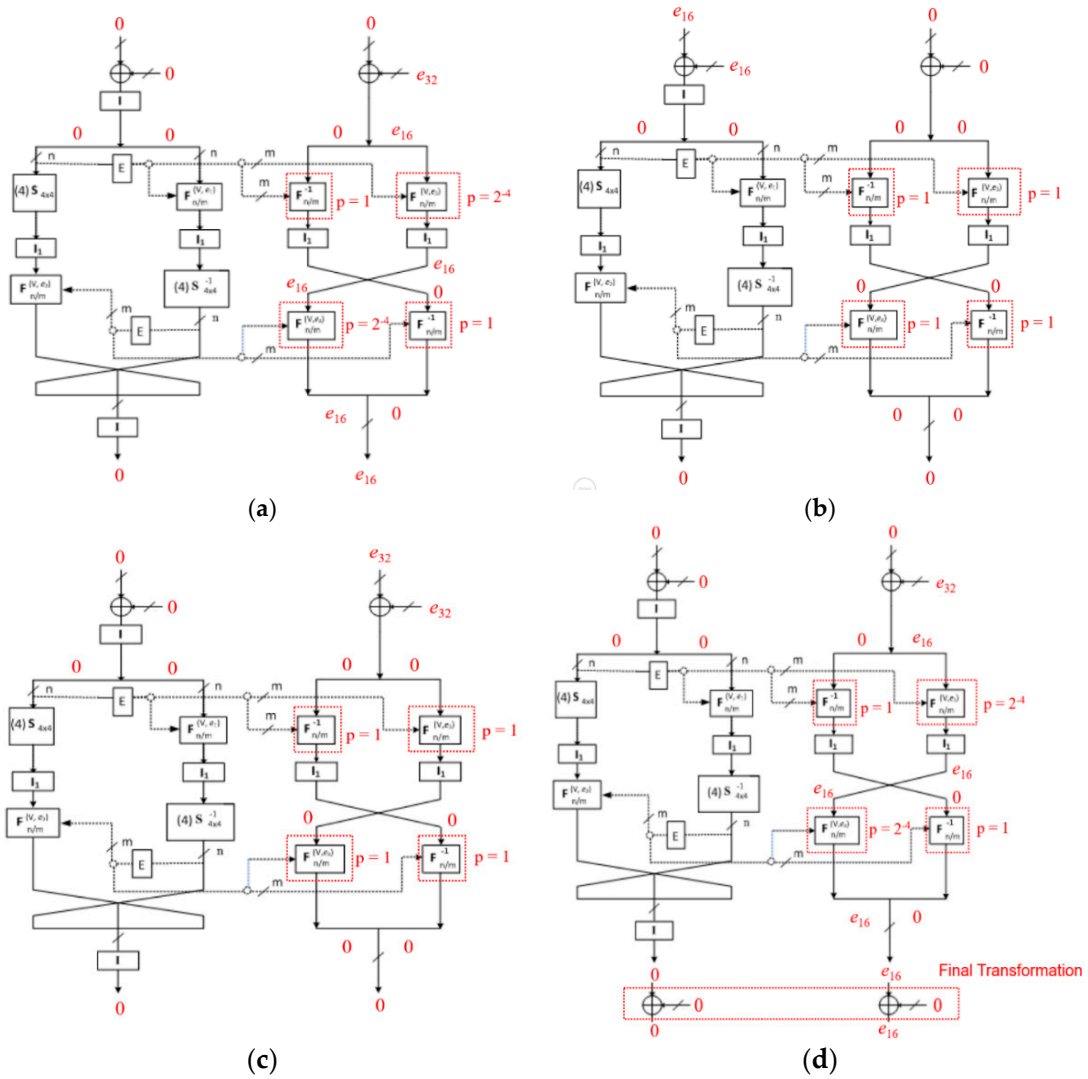


Figure 4. Differential characteristics (DCs) in **Crypt**$^{(e)}$ function at (**a**) the first round; (**b**) the second round; (**c**) the fifth round; and (**d**) the eighth round and final transformation of BM123-64 with **Case 2** and **Case 3**.

See (Appendix A) for more descriptions of DCs with **Case 1**.

3.3. Related-Key Amplified Boomerang Attack on the BM123-64 Designs

With the two obtained differentials, we expect that having $m^2 \cdot 2^{-128}$ of encrypted quartets for **Case 1** is right. For **Case 2** and **Case 3**, the expected number is $m^2 \cdot 2^{-96}$ right quartets. Furthermore, in the case of an ideal cipher, the related-key boomerang differentials applied on a full eight rounds of BM123-64 with probabilities of 2^{-128}, 2^{-96}, and 2^{-96} ($2^{-64} \cdot p^2 \cdot q^2$) for each case, respectively. For the least expected right quartets number of 8, we take a set of 2^{66} pairs of plaintexts ($m^2 \cdot 2^{-128} = 2^3$) for the attack process in **Case 1** and 2^{50} pairs of plaintexts ($m^2 \cdot 2^{-96} = 2^3$) for the attacks in **Case 2** and **Case 3**.

The attacker follows the below steps for a full related-key attack method on BM123-64:

(1) We pick a set of 2^{66} pairs of plaintexts (P_j, P_j *), (j = 1, . . . , 2^{66}), then we expand into another set of 2^{131} quartets of plaintexts, denoted as (P_i, P_i *, P_i ′, P_i ′*), (i = 1, . . . , 2^{131}) in **Case 1**, or 2^{50} pairs of plaintexts (P_j, P_j *), (j = 1, . . . , 2^{50}) and generate 2^{99} quartets of plaintexts (P_i, P_i *, P_i ′, P_i ′*), (i = 1, . . . , 2^{99}) in **Case 2** and **Case 3**, with input difference α = (0, 0). We ask for encryption of all the quartets (P_i, P_i *, P_i ′, P_i ′*) using the related-keys (K, K*, K', K'*) difference, described as two terms of relation: $\Delta K = K \oplus K^* = K' \oplus K'^* = (0, e_{16}, e_{32}, 0, 0, 0, 0, 0)$ and $\Delta K' = K \oplus K' = K^* \oplus K'^* = (0, e_{32}, 0, 0, 0, 0, 0, 0)$ to output respective quartets of ciphertexts (C_i, C_i *, C_i ′, C_i ′*).

(2) We do XOR with all possible values of C_i and C_i′, C_i *, and C_i′* for each i value, then check whether the output result is (0, e_{16}) and store all these difference values to apply in the previous eight rounds.

(3) By this way, at the final transformation, we expect to hold a 64-bit subkey including K_1 and K_3, then get the remaining subkeys (K_1*, K_3*), (K_1′, K_3′), and (K_1′*, K_3′*) of the quartets of subkeys.

   (a) Similarly, at the eighth round, we ask for decryption of all quartets of ciphertexts values obtained from Step 2 with subkey quartets of K_1 and K_3 to hold 64-bit input values (X_j, X_j*, X_j′, X_j′*) at the left side process of round function.

   (b) We do XOR with all possible values of X_j and X_j′, X_j *, and X_j′* for each j value, then check whether the output result is 0.

(4) After passing Step 3, all values of quartets of two subkeys K_1 and K_3 are explored. We can do brute force attacks to obtain the remaining 192-bit subkeys (K_2, K_4, K_5, K_6, K_7, K_8) with all K_1 and K_3.

4. Results and Discussion

With **Case 1**, the proposed attack requires 2^{66} pairs of plaintexts and 2^{67} related-key chosen plaintexts in data complexity, since the related-key DC is 2^{-32}. Furthermore, it needs about 2^{70} (=$2^{67} \times 8$) bytes of memory.

With **Case 2** and **Case 3**, the attack requires 2^{50} pairs of plaintexts and 2^{51} related-key chosen plaintexts in data complexity, while the related-key DCs are 2^{-16}. The attack takes about 2^{54} (=$2^{51} \times 8$) bytes of memory.

At Step 1 of the attack, the complexity of time is a unit of 2^{67} encryptions (**Case 1**), or 2^{51} encryptions (**Case 2** and **Case 3**) of the full eight rounds of BM123-64. Each quartet of ciphertext is planned to achieve Step 2 of the attack with 2^{-64} probability. In addition, we will get 2^{67} (=$2^{131} \times 2^{-64}$) right quartets of ciphertext (**Case 1**) or 2^{35} right quartets of ciphertext (=$2^{99} \times 2^{-64}$) (**Case 2** and **Case 3**) that will achieve Step 2. At Step 3 and Step 4, the complexity of time is a unit of 2^{62} (=$2^{64} \times 4 \times 1/8 \times 1/2$) and 2^{65} (=$2^{64} \times 1 \times 2$) for a full eight rounds of BM123-64 encryptions, respectively. Finally, the results show that all the attacks require total time complexity of 2^{67} ($\approx 2^{67} + 2^{62} + 2^{65}$) (**Case 1**) or 2^{65} ($\approx 2^{51} + 2^{62} + 2^{65}$) (**Case 2** and **Case 3**) for a full eight rounds of BM123-64 encryptions on average. In Table 3, a comparison of cryptanalysis results between the scheme proposed and other data-dependent ciphers in terms of complexity of data and time is given.

At Step 4 of the attack, outputting a wrong quartet of subkey takes 2^{-64} of probability. With our cryptanalysis methods, the results shown with the output possibility in case of a wrong key is lower

than the ideal case. These proposed related-key amplified boomerang attacks can potentially exploit the BM123-64 constructions at all three specific cases.

Table 3. Cryptanalysis results on constructions based on DDP (Data-Dependent Permutation), DDO (Data-Dependent Operation), and SDDO (switchable data-dependent operation).

Block Cipher	Total Rounds	Complexity Data/Time	Key Bits Recovery
DDP-64	10/10	2^{54} RCP/2^{54}	22
		2^{44} RCP/2^{44}	20
CHESS-64	8/8	2^{39} RCP/2^{39}	6
		2^{44} RCP/2^{108}	128
		2^{39} RCP/2^{122}	128
DDO-64V$_1$	8/8	$2^{35.5}$ RCP/$2^{65.5}$	
DDO-64V$_2$	8/8	2^{3} RCP/2^{31}	
MD-64	8/8	$2^{43.1}$ RCP/2^{95}	
BMD-128	7/8	2^{79} RCP/2^{129}	
KT-64	8/8	$2^{45.5}$ RCP/$2^{65.17}$	
XO-64	8/8	2^{44} RCP/2^{65}	
BM123-64 (**Case#1**) (*)	8/8	2^{67} RCP/2^{67}	
BM123-64 (**Case#2**) (*)	8/8	2^{51} RCP/2^{65}	
BM123-64 (**Case#3**) (*)			

(*) our proposed attack results; RCP denotes the Related-key Chosen Plaintext.

5. Conclusions

This paper proposes effective attacks on one of the recent SDDO-based constructions, BM123-64. The methods addressed in the study present main issues in security mechanisms of ciphers based on data-dependent operations that is used in many cipher designs for high speed transformation and lightweight targets. The simple key schedule generator with basic parameters when changed and substituted leads to a possibility of exploiting the structure weaknesses by related-key cryptanalysis. The work presented related-key amplified boomerang attacks on a full eight rounds of BM123-64 in distinctive designs with effective complexity results. This shows that with **Case 1**, it requires 2^{66} related-key chosen plaintexts and 2^{67} encryptions consumptions, and 2^{50} related-key chosen plaintexts and 2^{65} encryptions consumptions are required with **Case 2** and **Case 3**. The results of this study can be applied on many construction designs of these types of ciphers. Along with some new cryptanalysis techniques like Fr Trust or RARE, our research will further enhance performance and is expected to develop novel approaches for a wide range of applications and devices in the IoT environment.

Author Contributions: Conceptualization, T.S.D.P., C.L.; Methodology, T.S.D.P.; Writing-Original Draft Preparation, T.S.D.P.; Writing-Review & Editing, T.S.D.P.; Supervision, C.L.; Funding Acquisition, C.L.

Funding: This work was supported by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) and the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea (Development of Cyber Security Technology for Non-safety Grade Control System (DCS) in Nuclear Power Plants, No. 20161510101810).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Figure A1 illustrates the differential propagation at several rounds of BM123-64 cipher with **Crypt**$^{(e)}$ function in **Case 1**.

We pick a set of 2^{66} pairs of plaintexts (P_j, P_j *) and expand to 2^{131} quartets of plaintexts (P_i, P_i*, P_i', P_i'*). The SDDO-based $F_{n/m}^{V/e}$ function in BM123-64 structure includes $F_{16/64}$ and $F^{-1}{}_{16/64}$, which has four layers with eight $F_{2/2}$ element function in each. Based on the differential properties mentioned in Section 3.1, we can construct two related-key boomerangs on a full eight rounds of BM123-64 in Case 1 with total probability of 2^{-32}. The first four rounds of related-key boomerang holds with the probability $p = 2^{-16}$; the last four rounds of related-key boomerang also obtains with the probability

$q = 2^{-16}$. It requires about 2^{67} chosen plaintexts in complexity of data as input, and the memory required is about 2^{70} (=$2^{67} \times 8$) bytes.

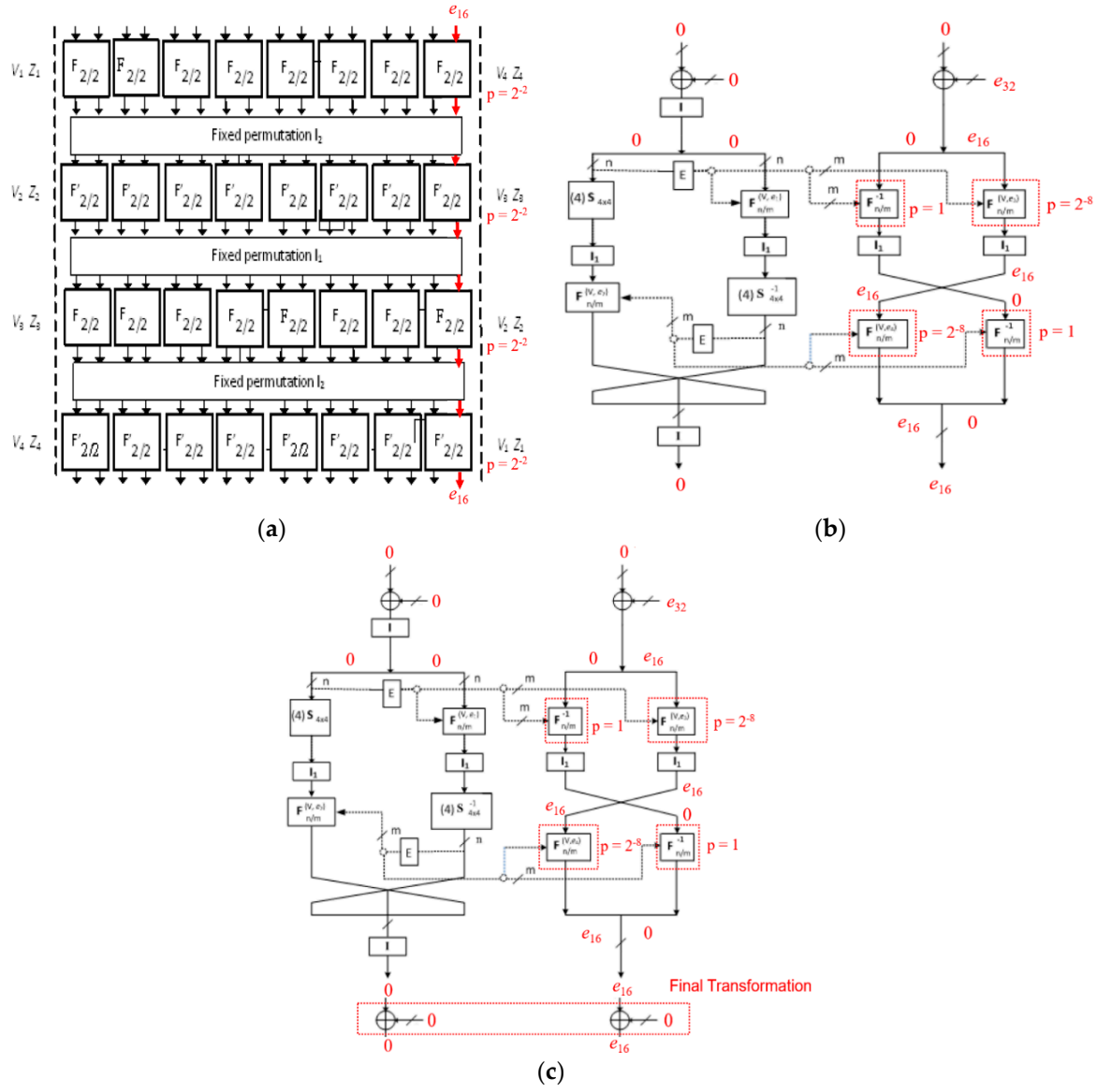


Figure A1. (**a**) The differential propagation of $F_{16/64}$, $F^{-1}{}_{16/64}$ function and the DCs in **Crypt**$^{(e)}$ function at (**b**) the 1st round and (**c**) the eighth round and final transformation of BM123-64 with **Case 1**.

References

1. Bac, D.; Minh, N. High-Speed Block Cipher Algorithm Based on Hybrid Method. In *Ubiquitous Information Technologies Applications*; Lecture Notes in Electrical Engineering; Springer: Berlin/Heidelberg, Germany, 2014; Volume 280, pp. 285–291.
2. Moldovyan, N. On Cipher Design Based on Switchable Controlled Operations. In *MMM-ACNS, LNCS*; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2776, pp. 316–327.
3. Bac, D.; Minh, N.; Duy, H. An Effective and Secure Cipher Based on SDDO. *Int. J. Comput. Netw. Inf. Secur.* **2012**, *4*, 1.
4. Bac, D.; Minh, N.; Duy, H. New SDDO-Based Block Cipher for Wireless Sensor Network Security. *Int. J. Comput. Netw. Inf. Secur.* **2010**, *10*, 54–60.

5. Minh, N.; Luan, N.; Dung, L. KT-64: A New Block Cipher Suitable to Efficient FPGA Implementation. *IJCSNS Int. J. Comput. Netw. Inf. Secur.* **2010**, *19*, 10–18.
6. Minh, N.; Duy, H.; Dung, L. Design and Estimate of a New Fast Block Cipher for Wireless Communication Devices. In Proceedings of the International Conference on Advanced Technologies for Communications, Hanoi, Vietnam, 6–9 October 2008; pp. 409–412.
7. Moldovyan, N.; Moldovyan, A.; Sklavos. Controlled Elements for Designing Ciphers Suitable to Efficient VLSI Implementation. *Telecommun. Syst. J.* **2006**, *32*, 149–163. [CrossRef]
8. Kang, J.; Jeong, K.; Lee, C.; Hong, S. Distinguishing attack on SDDO-based block cipher BMD-128. In *Ubiquitous Information Technologies and Applications*; Springer: Berlin/Heidelberg, Germany, 2014; Volume 280, pp. 595–602.
9. Phuc, T.S.D.; Lee, C.; Xiong, N. Cryptanalysis of the XO-64 Suitable for Wireless Systems. *Wirel. Pers. Commun.* **2017**, *93*, 589–600. [CrossRef]
10. Izotov, B.V.; Moldovyan, N.; Moldovyan, A. Controlled Operations as a Cryptographic Primitive. In *Information Assurance in Computer Networks*; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2052, pp. 230–241.
11. Kang, J.; Jeong, K.; Yeo, S.; Lee, C. Related-key Attack on the MD-64 Block Cipher Suitable for Pervasive Computing Environment. In Proceedings of the International Conference on Advance Information Networking and Application Workshops, Fukuoka, Japan, 26–29 March 2012; pp. 726–731. [CrossRef]
12. Lee, C.; Kim, J.; Sung, J.; Hong, S.; Lee, S. Security analysis of the full-round DDO-64 block cipher. *J. Syst. Softw.* **2008**, *84*, 2328–2335. [CrossRef]
13. Moldovyan, N.; Moldovyan, A. Data-driven Ciphers for Fast Telecommunication Systems. In *Auerbach Publication*; Talor & Francis Group: New York, NY, USA; London, UK, 2008; pp. 77–185, ISBN 1420054112 9781420054118.
14. Biham, E.; Dunkelman, O.; Keller, N. Related-key boomerang and rectangle attacks. In *Advances in Cryptology—EUROCRYPT'05, LNCS*; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3494, pp. 507–525.
15. Kelsey, J.; Kohno, T.; Schneier, B. Amplified Boomerang Attacks against Reduced-Round MARS and Serpent. In *Proceedings of Fast Software Encryption 7*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2000; Volume 1978, pp. 75–93. [CrossRef]
16. Wagner, D. The Boomerang Attack. In *Proceedings of Fast Software Encryption 6*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1636, pp. 156–170. [CrossRef]