A New BISON-like Construction Block Cipher: DBISON

Haixia Zhao[1,3], Yongzhuang Wei[2*], and Zhenghong Liu[1]
[1] Key Laboratory of Cognitive Radio and Information Processing , Ministry of Education,
Guilin University of Electronic Technology, Guilin, 541004, China
[e-mail: guetzhx@163.com, giet.liu@163.com]
[2] Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, 541004, China
[e-mail: walker_wyz@guet.edu.cn]
[3] School of Mathematics and Computing Science, Guilin University of Electronic Technology, Guilin 541004, China
[*]Corresponding author: Yongzhuang Wei

Received April 25, 2021; revised January 26, 2022; accepted May 11, 2022; published May 31, 2022

Abstract

At EUROCRYPT 2019, a new block cipher algorithm called BISON was proposed by Canteaut et al. which uses a novel structure named as Whitened Swap−Or−Not (WSN). Unlike the traditional wide trail strategy, the differential and linear properties of this algorithm can be easily determined. However, the encryption speed of the BISON algorithm is quite low due to a large number of iterative rounds needed to ensure certain security margins. Commonly, denoting by n is the data block length, this design requires $3n$ encryption rounds. Moreover, the block size n of BISON is always odd, which is not convenient for operations performed on a byte level. In order to overcome these issues, we propose a new block cipher, named DBISON, which more efficiently employs the ideas of double layers typical to the BISON-like construction. More precisely, DBISON divides the input into two parts of size $n/2$ bits and performs the round computations in parallel, which leads to an increased encryption speed. In particular, the data block length n of DBISON can be even, which gives certain additional implementation benefits over BISON. Furthermore, the resistance of DBISON against differential and linear attacks is also investigated. It is shown the maximal differential probability (MDP) is $1/2^{n-1}$ for n encryption rounds and that the maximal linear probability (MLP) is strictly less than $1/2^{n-1}$ when $(n/2+3)$ iterative encryption rounds are used. These estimates are very close to the ideal values when n is close to 256.

Keywords: BISON block cipher, DBISON block cipher, Differential cryptanalysis, Linear cryptanalysis, WSN construction.

This research was supported by the Natural Science Foundation of China (61872103, 62162016, 62062026), the Guangxi Natural Science Foundation(2019GXNSFGA245004, 2020GXNSFAA159076), the Foundation of Key Laboratory of Cognitive Radio and Information Processing , Ministry of Education（CRKL180107）

http://doi.org/10.3837/tiis.2022.05.011 **ISSN : 1976-7277**

1. Introduction

Block ciphers play an important role in the area of data storage and secure transmission in an open internet environment. During the past three decades, block ciphers have received a lot of attention from academic and industrial community.

Generally, security and implementation efficiency can be considered as the most crucial aspects in the design of block ciphers. To achieve sufficient security margins, block ciphers commonly employ multiple encryption rounds for the purpose of achieving a satisfactory level of diffusion and confusion [1]. On the other hand, the internal structure of a block cipher is also importance since it directly affects the implementation cost and performance in both hardware and software. Currently, the most prominent block ciphers employ diverse structures such as Feistel [2, 3], SPN [4], MISTY [5] and Lai-Massey [6], among others. A very common approach is to implement a block cipher as a substitution permutation network (SPN), which was extensively used in many prominent block ciphers, including AES [4, 7] whose design additionally embeds the concept of wide trail strategy[8]. One important issue with this design rationale regards the problem of determining the differential or linear properties of a given cipher, which is considered to be quite a difficult task. More specifically, in order to ensure good resistance against differential and linear cryptanalysis, the so-called branch number of diffusion (linear) layer and the cryptographic properties of the S-boxes (used in the substitution layer) have to be taken into account [9, 10]. Due to the iterative structure of block ciphers and an exponential growth of possible differential/linear patterns, the exact security estimates are not easy to specify. An alternative design rationale of constructing block ciphers that achieve an optimal security level (under the ideal model assumption) was introduced in [11]. This method uses the so-called Whitened Swap-Or-Not (WSN) construction, which itself is based on the Swap-or-Not method introduced in [12] and applicable in the settings when the internal functions are kept secret. Furthermore, instead of the need for a set of random Boolean functions for the Swap-or-Not method, the WSN approach [11] requires only two public random n-variable Boolean functions to achieve full security. Actually, there are very few known instances of WSN and an encryption algorithm based on this approach was specified in [12] but later broken by Vaudenay [13]. Another example of using the WSN method is the BISON block cipher, which was proposed by Canteaut et al. at EUROCRYPT 2019 [14]. The design of BISON implements XOR-ing of the round keys by using a quadratic bent function. Additionally, BISON seems to be resistant against differential cryptanalysis [15], linear cryptanalysis [16], and algebraic cryptanalysis [17] provided that the number of rounds is approximately $3n$, where n is the data block length and n is odd. In particular, the MDP value of BISON can be easily evaluated without the exact details about its components, which is completely different to the wide trail strategy.

Consequently, the encryption speed of BISON is quite low due to a large number of rounds used and a large n-bit input size. For instance, assuming that n=127 implies that there are 381 rounds and additionally one needs to implement a large 126-bit nonlinear function which is quite demanding. To overcome these issues, we propose a new block cipher that borrows the design ideas from BISON, named DBISON. More specifically, the length of data block of DBISON is even and therefore the input x can be divided into two halves x_L and x_R which are then processed in parallel using a similar structure as in Feistel networks. The details of round operations are given in **Fig. 1** and, additionally, the used parameters are

described in Definition 4. Notice that, to complete the round operation, the left and right branch are swapped but in the final round the swap operation is not performed.

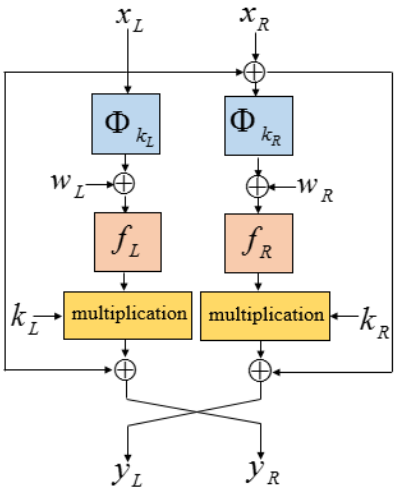


Fig. 1. The round function of DBISON

It will be shown that DBISON is resistant against both differential and linear cryptanalysis when the number of rounds r reaches n. More specifically, we show that the MDP value equals $1/2^{n-1}$ when n encryption rounds are used, whereas the MLP is strictly less than $1/2^{n-1}$ if at least (n/2+3) encryption rounds are applied. It is worth mentioning that the MDP can almost reach the ideal value $1/2^n$ if the size of data block n is close to 256. A comparison between BISON and DBISON is given in **Table 1**. However, to ensure that the algebraic degree of DBISON attains its maximal value n, the number of rounds is approximately 3n. DBISON offers a significant advantage over BISON in terms of encryption/decryption speed since the input size is divided into two halves (each having n/2 bits) which are processed in parallel.

The rest of this paper are organized as follows. In Section 2, the DBISON block cipher is fully described. In Section 3, the differential cryptanalysis against DBISON is examined and the estimates of its MDP are provided. In Section 4, the resistance of DBISON against linear cryptanalysis is analyzed and the bounds on its MLP are derived. In Section 5, certain specific instances of DBISON are specified. Some concluding remarks can be found in Section 6.

Table 1. Comparison of BISON and DBISON

Algorithm	Nonlinear function	MDP	MLP	Source
BISON	n-bit input size	$2^{-(n-1)}$ (n-round)	$2^{-(n-1)}$ (n-round)	[14]
DBISON	Two n/2-bit input halves processed in parallel	$\le 2^{-(n-1)}$ (n-round)	$< 2^{-(n-1)}$ ((n/2+3)-round)	New

2. Preliminaries

Definition 1 [18] Let F be a function from F_2^n into F_2^n. For any $u,\ v \in F_2^n$, define $W_F(u,v) = \sum_{x \in F_2^n} (-1)^{u \bullet x \oplus v \bullet F(x)}$, where $\bullet$ denotes the inner product in F_2^n, that is $u \bullet x = u_1 x_1 \oplus u_2 x_2 \oplus \ldots \oplus u_n x_n$. The multiset $\{W_F(u,v) \mid u,\ v \in F_2^n\}$ is called the Walsh

spectrum of F.

Definition 2 [19] The r-round differential characteristic of an iterative block cipher is denoted as $\Omega=(\delta_0,\delta_1,...,\delta_r)$. Assuming that the round keys $k_1,k_2,...,k_r$ are independent and uniform, the differential characteristic probability $\mathrm{DP}(\Omega)$ is defined as $\mathrm{DP}(\Omega)=\prod_{i=1}^{r}\mathrm{DP}(\delta_{i-1},\delta_i)$, i.e. it is the probability that the difference between input pair is δ_0 and the difference between intermediate state (y_i,y_i^*) is δ_i, $1\le i\le r$.

Definition 3 [19] The r-round linear characteristic of an iterative block cipher is denoted as $\theta=(\theta_0,\theta_1,...,\theta_r)$. Assuming that the round keys $k_1,k_2,...,k_r$ are independent and uniform, the linear characteristic probability $\mathrm{LP}(\theta)$ is defined by $\mathrm{LP}(\theta)=\prod_{i=1}^{r}\mathrm{LP}(\theta_{i-1},\theta_i)$, i.e. the probability that the input mask is θ_0 and the mask of an intermediate state y_i is θ_i, $1\le i\le r$.

For the input and output difference (α,β), it is a difficult task to compute the MDP of (α,β), even for a small number of rounds. However, computing the MDP of an r-round differential characteristic $\Omega=(\delta_0,\delta_1,...,\delta_r)$ is an easier task, and the MDP of Ω also reflects the ability of the cipher to resist differential cryptanalysis. A similar reasoning applies when the MLP values is considered, thus having an initial mask (a,b) and an r-round linear trail $\theta=(\theta_0,\theta_1,...,\theta_r)$. We will investigate in detail the properties of DBISON in this context, hence its resistance against differential and linear cryptanalysis by providing the estimates on MDP and MLP using Ω and θ, respectively.

Definition 4 Let the data block length of DBISON be $n=4m+2$, where m is a positive integer. The input x of any encryption round is divided into the left half and right half, i.e. $x=(x_L,x_R)$. The i-th round function $F_{k_i,w_i}(x)$: $F_2^n\to F_2^n$ is defined as

$$F_{k_i,w_i}(x)=\left(x_L\oplus x_R\oplus f_{iR}\left(w_{iR}\oplus\Phi_{k_{iR}}(x_L\oplus x_R)\right)k_{iR},\ x_L\oplus f_{iL}\left(w_{iL}\oplus\Phi_{k_{iL}}(x_L)\right)k_{iL}\right),\tag{1}$$

where $k_i=(k_{iL},k_{iR})$, $w_i=(w_{iL},w_{iR})$ are round keys (w_i is the whitened key), and f_{iL} and f_{iR} are bent functions with $n/2-1$ variables. Moreover, $\Phi_{k_{iL}}$, $\Phi_{k_{iR}}$: $F_2^{n/2}\to F_2^{n/2-1}$ are linear functions and $\ker\Phi_{k_{iL}}=\{0,\ k_{iL}\}$, $\ker\Phi_{k_{iR}}=\{0,\ k_{iR}\}$, where k_{iL} and k_{iR} are generated by two LFSRs so that $k_{iL}\ne 0$ and $k_{iR}\ne 0$, respectively.

Remark 1 The analysis in this work follows two basic assumptions of symmetric cryptanalysis, i.e. the whitened keys are linearly independent, and the round keys satisfy the so-called random equivalence hypothesis.

3. Differential cryptanalysis of DBISON block cipher

The derivative of a function f in direction α is defined as $D_\alpha f(x)=f(x)\oplus f(x\oplus\alpha)$. A successful application of differential cryptanalysis against block ciphers heavily relies on the differential properties of its substitution layer. The round function F of a block cipher with n-bit input and output can be viewed as a vectorial Boolean function $F:F_2^n\to F_2^n$. The behavior of the derivatives of F are described by the Differential Distribution Table (DDT) of F, whose entries are

$$\mathrm{DDT}_F[\alpha,\beta]=\left|\left\{x\in F_2^n \mid F(x)\oplus F(x\oplus\alpha)=\beta\right\}\right|,$$

where $\alpha\in F_2^n$ is referred to as the input difference and $\beta\in F_2^n$ as the output difference.

In this context, we are primarily interested in the DDT of the round function $F_{k_i,w_i}(x)$, which can be calculated explicitly using Theorem 1 below.

Theorem 1 Using (1), the round function of DBISON can be rewritten as

$$F(x)=\left(x_L\oplus x_R\oplus f_R\left(w_R\oplus\Phi_{k_R}(x_L\oplus x_R)\right)k_R,\ x_L\oplus f_L\left(w_L\oplus\Phi_{k_L}(x_L)\right)k_L\right). \tag{2}$$

Then $\mathrm{DDT}_F[\alpha,\beta]$ can be specified as follows:

1) $\mathrm{DDT}_F[\alpha,\beta]=2^n$ if $\beta=(\alpha_L\oplus\alpha_R,\alpha_L)$ and $\alpha\in\{\mathbf{0},\ (\mathbf{0},k_R),\ (k_L,k_L),\ (k_L,k_L\oplus k_R)\}$.
2) $\mathrm{DDT}_F[\alpha,\beta]=2^{n-1}$ if $\beta=(\alpha_L\oplus\alpha_R,\alpha_L)$ and $(\alpha_L\oplus\alpha_R,\ \alpha_L)\in\{(\mathbf{0},\alpha_L),\ (k_R,\alpha_L),$ $(\alpha_L\oplus\alpha_R,\mathbf{0}),\ (\alpha_L\oplus\alpha_R,k_L)\mid \alpha_L\notin\{\mathbf{0},k_L\},\alpha_L\oplus\alpha_R\notin\{\mathbf{0},k_R\}\}$, or $\beta=(\alpha_L\oplus\alpha_R,\alpha_L)\oplus(\mathbf{0},k_L)$, $\alpha_L\oplus\alpha_R\in\{\mathbf{0},k_R\}$ and $\alpha_L\notin\{\mathbf{0},k_L\}$, or $\beta=(\alpha_L\oplus\alpha_R,\alpha_L)\oplus(k_R,\mathbf{0})$, $\alpha_L\oplus\alpha_R\notin\{\mathbf{0},k_R\}$ and $\alpha_L\in\{\mathbf{0},k_L\}$.
3) $\mathrm{DDT}_F[\alpha,\beta]=2^{n-2}$ if $\beta=(\alpha_L\oplus\alpha_R,\alpha_L)\oplus\gamma$, $\gamma\in\{\mathbf{0},\ (\mathbf{0},k_L),\ (k_R,\mathbf{0}),\ (k_R,k_L)\}$ and $\alpha_L\oplus\alpha_R\notin\{\mathbf{0},k_R\}$, $\alpha_L\notin\{\mathbf{0},k_L\}$.
4) Otherwise, $\mathrm{DDT}_F[\alpha,\beta]=0$.

Proof Using the definitions of DDT and $F(x)$, $\mathrm{DDT}_F[\alpha,\beta]$ can be deduced as:

$$\mathrm{DDT}_F[\alpha,\beta]$$
$$=\left|\left\{x\in F_2^n\middle|\left(D_{\Phi_{k_R}(\alpha_L\oplus\alpha_R)}f_R\left(w_R\oplus\Phi_{k_R}(x_L\oplus x_R)\right)k_R,\ D_{\Phi_{k_L}(\alpha_L)}f_L\left(w_L\oplus\Phi_{k_L}(x_L)\right)k_L\right)=(\alpha_L\oplus\alpha_R,\alpha_L)\oplus\beta\right\}\right|. \tag{3}$$

Clearly, $\mathrm{DDT}_F[\alpha,\beta]=0$ if $(\alpha_L\oplus\alpha_R,\alpha_L)\oplus\beta\notin\{\mathbf{0},\ (\mathbf{0},k_L),\ (k_R,\mathbf{0}),\ (k_R,k_L)\}:=K^*$.

In the following, we split our analysis of $(\alpha_L\oplus\alpha_R,\alpha_L)\oplus\beta$ into four cases.

Case 1. $\beta=(\alpha_L\oplus\alpha_R,\alpha_L)$.

By (3) and $k_L\neq\mathbf{0}$, $k_R\neq\mathbf{0}$, it can be deduced that

$$\mathrm{DDT}_F[\alpha,\beta]=\left|\left\{x\in F_2^n\middle|D_{\Phi_{k_R}(\alpha_L\oplus\alpha_R)}f_R\left(w_R\oplus\Phi_{k_R}(x_L\oplus x_R)\right)=0\ \text{ and }\ D_{\Phi_{k_L}(\alpha_L)}f_L\left(w_L\oplus\Phi_{k_L}(x_L)\right)=0\right\}\right|.$$

① $\Phi_{k_R}(\alpha_L\oplus\alpha_R)\neq\mathbf{0}$ and $\Phi_{k_L}(\alpha_L)\neq\mathbf{0}$. Denote $w_L\oplus\Phi_{k_L}(x_L)$ by x_L'.

Since f_L is a bent function, thus $\left|\left\{x_L'\in F_2^{n/2-1}\middle|D_{\Phi_{k_L}(\alpha_L)}f_L(x_L')=0\right\}\right|=2^{n/2-2}$. Furthermore, Φ_{k_L} is a linear function from $F_2^{n/2}$ to $F_2^{n/2-1}$ and $\ker\Phi_{k_L}=\{\mathbf{0},\ k_L\}$, and therefore $|A_L|:=\left|\left\{x_L\in F_2^{n/2}\middle|\ D_{\Phi_{k_L}(\alpha_L)}f_L\left(w_L\oplus\Phi_{k_L}(x_L)\right)=0\right\}\right|=2^{n/2-1}$. For any $a_i\in A_L$, $i=1,2,\ldots,2^{n/2-1}$, $\left|\left\{x_R\in F_2^{n/2}\middle|D_{\Phi_{k_R}(\alpha_L\oplus\alpha_R)}f_R\left(w_R\oplus\Phi_{k_R}(a_i\oplus x_R)\right)=0\ \right\}\right|=2^{n/2-1}$ since $\Phi_{k_R}(\alpha_L\oplus\alpha_R)\neq\mathbf{0}$ and f_R is a bent function. Therefore, $\mathrm{DDT}_F[\alpha,\beta]=2^{n/2-1}\times2^{n/2-1}=2^{n-2}$.

② $\Phi_{k_R}(\alpha_L\oplus\alpha_R)\neq\mathbf{0}$ and $\Phi_{k_L}(\alpha_L)=\mathbf{0}$. $\mathrm{DDT}_F[\alpha,\beta]=2^{n/2}\times2^{n/2-1}=2^{n-1}$.

③ $\Phi_{k_R}(\alpha_L\oplus\alpha_R)=\mathbf{0}$ and $\Phi_{k_L}(\alpha_L)\neq\mathbf{0}$. $\mathrm{DDT}_F[\alpha,\beta]=2^{n/2-1}\times2^{n/2}=2^{n-1}$.

④ $\Phi_{k_R}(\alpha_L \oplus \alpha_R) = \mathbf{0}$ and $\Phi_{k_L}(\alpha_L) = \mathbf{0}$. $\mathrm{DDT}_F[\alpha,\beta] = 2^{n/2} \times 2^{n/2} = 2^n$.

To summarize, when $\beta = (\alpha_L \oplus \alpha_R, \alpha_L)$ is satisfied then $\mathrm{DDT}_F[\alpha,\beta]$ can be computed as follows:

$$\mathrm{DDT}_F[\alpha,\beta] = \begin{cases} 2^n, & \text{if } \alpha \in \{\mathbf{0},\ (\mathbf{0},k_R),\ (k_L,k_L),\ (k_L,k_L \oplus k_R)\}, \\ 2^{n-1}, & \text{if } (\alpha_L \notin \{\mathbf{0},k_L\} \text{ and } \alpha_L \oplus \alpha_R \in \{\mathbf{0},k_R\}) \ or\ (\alpha_L \in \{\mathbf{0},k_L\} \text{ and } \alpha_L \oplus \alpha_R \notin \{\mathbf{0},k_R\}), \\ 2^{n-2}, & \text{if } \alpha_L \notin \{\mathbf{0},k_L\} \text{ and } \alpha_L \oplus \alpha_R \notin \{\mathbf{0},k_R\}. \end{cases} \tag{4}$$

The same method can be used to address the remaining cases, and the following results are then obtained.

Case 2. $\beta = (\alpha_L \oplus \alpha_R, \alpha_L) \oplus (\mathbf{0}, k_L)$.

$$\mathrm{DDT}_F[\alpha,\beta] = \begin{cases} 2^{n-1}, & \text{if } \alpha_L \notin \{\mathbf{0},k_L\} \text{ and } \alpha_L \oplus \alpha_R \in \{\mathbf{0},k_R\}, \\ 2^{n-2}, & \text{if } \alpha_L \notin \{\mathbf{0},k_L\} \text{ and } \alpha_L \oplus \alpha_R \notin \{\mathbf{0},k_R\}, \\ 0, & \text{if } \alpha_L \in \{\mathbf{0},k_L\}. \end{cases} \tag{5}$$

Case 3. $\beta = (\alpha_L \oplus \alpha_R, \alpha_L) \oplus (k_R, \mathbf{0})$

$$\mathrm{DDT}_F[\alpha,\beta] = \begin{cases} 2^{n-1}, & \text{if } \alpha_L \in \{\mathbf{0},k_L\} \text{ and } \alpha_L \oplus \alpha_R \notin \{\mathbf{0},k_R\}, \\ 2^{n-2}, & \text{if } \alpha_L \notin \{\mathbf{0},k_L\} \text{ and } \alpha_L \oplus \alpha_R \notin \{\mathbf{0},k_R\}, \\ 0, & \text{if } \alpha_L \oplus \alpha_R \in \{\mathbf{0},k_R\}. \end{cases} \tag{6}$$

Case 4. $\beta = (\alpha_L \oplus \alpha_R, \alpha_L) \oplus (k_R, k_L)$

$$\mathrm{DDT}_F[\alpha,\beta] = \begin{cases} 2^{n-2}, & \text{if } \alpha_L \notin \{\mathbf{0},k_L\} \text{ and } \alpha_L \oplus \alpha_R \notin \{\mathbf{0},k_R\}, \\ 0, & \text{if } \alpha_L \in \{\mathbf{0},k_L\} \text{ or } \alpha_L \oplus \alpha_R \in \{\mathbf{0},k_R\}. \end{cases} \tag{7}$$

By (4), (5), (6), and (7), the DDT of $F(x)$ can be obtained.#

Moreover, we consider the differential properties when the round function is applied iteratively. It is well-known that the probability of a differential characteristic of Markov cipher [20] can be easily calculated. In what follows, we first prove that DBISON is a Markov cipher.

Lemma 1 The round function $F_{k,w}(x)$ of DBISON has the following property

$$\Pr_w\left[F_{k,w}(x) \oplus F_{k,w}(x \oplus \alpha) = \beta\right] = \Pr_x\left[F_{k,w}(x) \oplus F_{k,w}(x \oplus \alpha) = \beta\right]. \tag{8}$$

Proof Let $A_w := \left\{w \in F_2^{n-2} \middle| F_{k,w}(x) \oplus F_{k,w}(x \oplus \alpha) = \beta\right\}$, $A_x := \left\{x \in F_2^{n} \middle| F_{k,w}(x) \oplus F_{k,w}(x \oplus \alpha) = \beta\right\}$.

More specifically,

$$A_w = \left\{w \in F_2^{n-2} \middle| \left(D_{\Phi_{k_R}(\alpha_L \oplus \alpha_R)} f_R\left(w_R \oplus \Phi_{k_R}(x_L \oplus x_R)\right)k_R,\ D_{\Phi_{k_L}(\alpha_L)} f_L\left(w_L \oplus \Phi_{k_L}(x_L)\right)k_L\right) = (\alpha_L \oplus \alpha_R, \alpha_L) \oplus \beta\right\}.$$

$$A_x = \left\{x \in F_2^{n} \middle| \left(D_{\Phi_{k_R}(\alpha_L \oplus \alpha_R)} f_R\left(w_R \oplus \Phi_{k_R}(x_L \oplus x_R)\right)k_R,\ D_{\Phi_{k_L}(\alpha_L)} f_L\left(w_L \oplus \Phi_{k_L}(x_L)\right)k_L\right) = (\alpha_L \oplus \alpha_R, \alpha_L) \oplus \beta\right\}.$$

If $(\alpha_L \oplus \alpha_R, \alpha_L) \oplus \beta \notin K^*$, then $|A_w| = |A_x| = 0$, and (8) holds. If $(\alpha_L \oplus \alpha_R, \alpha_L) \oplus \beta \in K^*$, then $|A_w|$ and $|A_x|$ are calculated as below.

Case 1. $\beta = (\alpha_L \oplus \alpha_R, \alpha_L)$.

$$A_w = \left\{w_L \in F_2^{n/2-1} \middle| D_{\Phi_{k_L}(\alpha_L)} f_L\left(w_L \oplus \Phi_{k_L}(x_L)\right) = 0\right\} \times \left\{w_R \in F_2^{n/2-1} \middle| D_{\Phi_{k_R}(\alpha_L \oplus \alpha_R)} f_R\left(w_R \oplus \Phi_{k_R}(x_L \oplus x_R)\right) = 0\right\}.$$

Denote $w_L \oplus \Phi_{k_L}(x_L) = u$ and $w_R \oplus \Phi_{k_R}(x_L \oplus x_R) = v$, then

$$A_w=\left\{u\oplus\Phi_{k_L}\left(x_L\right)\in F_2^{n/2-1}\middle|D_{\Phi_{k_L}(\alpha_L)}f_L\left(u\right)=0\right\}\times\left\{v\oplus\Phi_{k_R}\left(x_L\oplus x_R\right)\in F_2^{n/2-1}\middle|D_{\Phi_{k_R}(\alpha_L\oplus\alpha_R)}f_R\left(v\right)=0\right\}$$

$$=\left[\Phi_{k_L}\left(x_L\right)\oplus\left(F_2^{n/2-1}-\mathrm{supp}\left(D_{\Phi_{k_L}(\alpha_L)}f_L\right)\right)\right]\times\left[\Phi_{k_R}\left(x_L\oplus x_R\right)\oplus\left(F_2^{n/2-1}-\mathrm{supp}\left(D_{\Phi_{k_R}(\alpha_L\oplus\alpha_R)}f_R\right)\right)\right].$$

Thus,

$$\Pr_w\left[F_{k,w}\left(x\right)\oplus F_{k,w}\left(x\oplus\alpha\right)=\beta\right]=\frac{\left|A_w\right|}{\left|F_2^{n-2}\right|}=\frac{\left(2^{n/2-1}-\left|\mathrm{supp}\left(D_{\Phi_{k_L}(\alpha_L)}f_L\right)\right|\right)\left(2^{n/2-1}-\left|\mathrm{supp}\left(D_{\Phi_{k_R}(\alpha_L\oplus\alpha_R)}f_R\right)\right|\right)}{2^{n-2}}.$$

On the other hand, $\left|A_x\right|$ can be calculated as follows.

$$A_x=\left\{\left(x_L,x_R\right)\in F_2^n\ \middle|\ D_{\Phi_{k_R}(\alpha_L\oplus\alpha_R)}f_R\left(w_R\oplus\Phi_{k_R}\left(x_L\oplus x_R\right)\right)=0\text{ and }D_{\Phi_{k_L}(\alpha_L)}f_L\left(w_L\oplus\Phi_{k_L}\left(x_L\right)\right)=0\right\}.$$

If $\Phi_{k_L}\left(\alpha_L\right)=\mathbf{0}$, then $\left|\mathrm{supp}\left(D_{\Phi_{k_L}(\alpha_L)}f_L\right)\right|=0$ and $\left|A_L\right|=2^{n/2}$. If $\Phi_{k_L}\left(\alpha_L\right)\neq\mathbf{0}$, it can be deduced that $\left|\mathrm{supp}\left(D_{\Phi_{k_L}(\alpha_L)}f_L\right)\right|=2^{n/2-2}$ since f_L is a bent function, and $\left|A_L\right|=2^{n/2-1}$ (see Theorem 1). In both cases, $\left|A_L\right|=2^{n/2}-2\left|\mathrm{supp}\left(D_{\Phi_{k_L}(\alpha_L)}f_L\right)\right|$.

For any $a_i\in A_L$, $i=1,2,...,2^{n/2-1}$, if $\Phi_{k_R}\left(\alpha_L\oplus\alpha_R\right)=\mathbf{0}$, then $\left|\mathrm{supp}\left(D_{\Phi_{k_R}(\alpha_L\oplus\alpha_R)}f_R\right)\right|=0$ and $\left|\left\{x_R\in F_2^{n/2}\middle|D_{\Phi_{k_R}(\alpha_L\oplus\alpha_R)}f_R\left(w_R\oplus\Phi_{k_R}\left(a_i\oplus x_R\right)\right)=0\right\}\right|=2^{n/2}$. If $\Phi_{k_R}\left(\alpha_L\oplus\alpha_R\right)\neq\mathbf{0}$, it can be deduced that $\left|\mathrm{supp}\left(D_{\Phi_{k_R}(\alpha_L\oplus\alpha_R)}f_R\right)\right|=2^{n/2-2}$, and $\left|\left\{x_R\in F_2^{n/2}\middle|D_{\Phi_{k_R}(\alpha_L\oplus\alpha_R)}f_R\left(w_R\oplus\Phi_{k_R}\left(a_i\oplus x_R\right)\right)=0\right\}\right|=2^{n/2-1}$. In both cases, $\left|\left\{x_R\in F_2^{n/2}\middle|D_{\Phi_{k_R}(\alpha_L\oplus\alpha_R)}f_R\left(w_R\oplus\Phi_{k_R}\left(a_i\oplus x_R\right)\right)=0\right\}\right|=2^{n/2}-2\left|\mathrm{supp}\left(D_{\Phi_{k_R}(\alpha_L\oplus\alpha_R)}f_R\right)\right|$.

To summarize, $\left|A_x\right|=\left(2^{n/2}-2\left|\mathrm{supp}\left(D_{\Phi_{k_L}(\alpha_L)}f_L\right)\right|\right)\left(2^{n/2}-2\left|\mathrm{supp}\left(D_{\Phi_{k_R}(\alpha_L\oplus\alpha_R)}f_R\right)\right|\right)$, thus (8) holds. The similar results are easily verified for the remaining cases.#

Corollary 1 Let $E_{k,w}^r$ denote the *r*-round encryption of DBISON, where its *i*-th round function is $F_{k_i,w_i}\left(x\right)$ and using the round keys $k_1,k_2,...,k_r$. Then, we have

$$\Pr_{w,x}\left[E_{k,w}^r\left(x\right)\oplus E_{k,w}^r\left(x\oplus\delta_0\right)=\delta_r\right]=\prod_{i=1}^{r}\Pr_{w,x}\left[F_{k_i,w_i}\left(x\right)\oplus F_{k_i,w_i}\left(x\oplus\delta_{i-1}\right)=\delta_i\right].$$

To describe the necessary conditions under which $\Omega=\left(\delta_0,\delta_1,...,\delta_r\right)$ is a valid differential characteristic and to compute the MDP of DBISON, we need to introduce a new operation.

Definition 5 Let $\lambda_L,\lambda_R\in\left\{0,1\right\}$, $\left(k_L,k_R\right)\in F_2^n$, $k_L\in F_2^{n/2},k_R\in F_2^{n/2}$. We define a "product'' between $\left(\lambda_L,\lambda_R\right)$ and $\left(k_L,k_R\right)$ as $\left(\lambda_L,\lambda_R\right)*\left(k_L,k_R\right)=\left(\lambda_L k_L,\lambda_R k_R\right)$.

By Corollary 1, the probability of having the differential characteristic $\Omega=\left(\delta_0,\delta_1,...,\delta_r\right)$ after *r* rounds is $\mathrm{DP}\left(\Omega\right)=\prod_{i=1}^{r}\mathrm{DP}\left[\delta_{i-1},\delta_i\right]$. In particular, $\mathrm{DP}\left(\Omega\right)=0$ if and only if there is $0\le j\le r$, such that $\mathrm{DP}\left[\delta_{j-1},\delta_j\right]=0$. By Theorem 1, $\mathrm{DDT}_F\left[\delta_{i-1},\delta_i\right]=0$ if

$$\delta_i\notin\left\{\left(\delta_{(i-1)L}+\delta_{(i-1)R},\delta_{(i-1)L}\right)\oplus\gamma\ \middle|\ \gamma\in\left\{\mathbf{0},\ \left(\mathbf{0},k_{iL}\right),\ \left(k_{iR},\mathbf{0}\right),\ \left(k_{iR},k_{iL}\right)\right\}\right\},$$

which means $\mathrm{DP}\left[\delta_{i-1},\delta_i\right]=0$. Moreover, a valid differential characteristic $\Omega=\left(\delta_0,\delta_1,...,\delta_r\right)$ should have the following form.

$$\Omega=(\delta_0,\delta_1,...,\delta_r),\ \delta_i=\left(\delta_{(i-1)L}\oplus\delta_{(i-1)R},\delta_{(i-1)L}\right)\oplus(\lambda_{iL},\lambda_{iR})*(k_{iR},k_{iL}),\tag{9}$$

where $\lambda_{iL},\lambda_{iR}\in\{0,1\}$, and $k_i=(k_{iL},k_{iR})$ is the round key.

Theorem 2 For *n*-round DBISON, if the round keys satisfy $k_{iR}\notin\left\{k_{(i-1)L},k_{(i+1)L}\right\}$, then there is no nontrivial differential characteristic whose probability equals 1.

Proof Assume $\Omega=(\delta_0,\delta_1,...,\delta_n)$ is a nontrivial differential characteristic in (9) and $DP[\Omega]=1$, thus $\mathrm{DP}(\delta_{i-1},\delta_i)=1$, $i=1,2,...,n$. Especially, $\mathrm{DP}(\delta_0,\delta_1)=\mathrm{DP}(\delta_1,\delta_2)=1$. By Theorem 1, $\mathrm{DP}[\delta_0,\delta_1]=1$ if and only if $\delta_1=(\delta_{0L}\oplus\delta_{0R},\delta_{0L})$ and $\delta_0\in\left\{\mathbf{0},(\mathbf{0},k_{1R}),(k_{1L},k_{1L}),(k_{1L},\ k_{1L}\oplus k_{1R})\right\}$.

If $\delta_0=0$, by Theorem 1, it can be deduced that $\delta_1=\delta_2=...=\delta_n=0$, thus Ω is a trivial differential characteristic that holds with probability 1, which contradicts the assumption.

If $\delta_0=(\mathbf{0},k_{1R})$, then $\delta_1=(\mathbf{0}\oplus k_{1R},\mathbf{0})$. Using $\mathrm{DP}(\delta_1,\delta_2)=1$ and Theorem 1, we have

$$(k_{1R},\mathbf{0})=\delta_1\in\left\{\mathbf{0},(\mathbf{0},k_{2R}),(k_{2L},k_{2L}),(k_{2L},k_{2L}\oplus k_{2R})\right\}.$$

This contradicts the conditions that $k_{1R}\neq\mathbf{0}$ and $k_{1R}\neq k_{2L}$.

If $\delta_0=(k_{1L},k_{1L})$, then $\delta_1=(k_{1L}\oplus k_{1L},k_{1L})=(\mathbf{0},k_{1L})$. From $\mathrm{DP}(\delta_1,\delta_2)=1$ and Theorem 1, it can be deduced that

$$(\mathbf{0},k_{1L})=\delta_1\in\left\{\mathbf{0},(\mathbf{0},k_{2R}),(k_{2L},k_{2L}),(k_{2L},k_{2L}\oplus k_{2R})\right\}.$$

This contradicts the conditions that $k_{iL}\neq\mathbf{0}$ and $k_{2R}\neq k_{1L}$.

If $\delta_0=(k_{1L},k_{1L}\oplus k_{1R})$, then $\delta_1=(k_{1L}\oplus k_{1R}\oplus k_{1L},k_{1L})=(k_{1R},k_{1L})$. Using $\mathrm{DP}(\delta_1,\delta_2)=1$ and Theorem 1, it can be deduced that

$$(k_{1R},k_{1L})=\delta_1\in\left\{\mathbf{0},(\mathbf{0},k_{2R}),(k_{2L},k_{2L}),(k_{2L},k_{2L}\oplus k_{2R})\right\}.$$

Again, this violates the conditions that $k_{1R}\neq\mathbf{0}$ and $k_{1R}\neq k_{2L}$.

From the above cases, it can be concluded that there is no nontrivial differential characteristic with probability 1.#

To prove that DBISON is resistant against differential cryptanalysis, we need to analyze its MDP.

Theorem 3 For the differential characteristic Ω given by (9), we have:

1) If there is $\delta_j=\mathbf{0}$ and $\delta_{j+1}\neq\mathbf{0}$, then $\mathrm{DP}[\Omega]=0$.
2) If there is $\delta_j=\mathbf{0}$ and $\delta_{j-1}\neq\mathbf{0}$, then $\mathrm{DP}[\Omega]=0$.

Proof

1) By (9), using $\delta_j=\mathbf{0}$ and $\delta_{j+1}\neq\mathbf{0}$, it can be deduced that

$$\delta_{j+1}=(\lambda_{jL},\lambda_{jR})*(k_{jR},k_{jL})\in\left\{(k_{jR},\mathbf{0}),(\mathbf{0},k_{jL}),(k_{jR},k_{jL})\right\}.$$

If $\delta_{j+1}=(k_{jR},\mathbf{0})$, then $\mathrm{DDT}\left[\delta_j,\delta_{j+1}\right]\neq 2^n$ since $\delta_{j+1}\neq(\delta_{jL}\oplus\delta_{jR},\delta_{jL})$. Also, $\mathrm{DDT}\left[\delta_j,\delta_{j+1}\right]\neq 2^{n-2}$, since we can represent $\delta_{j+1}=(\delta_{jL}\oplus\delta_{jR},\delta_{jL})\oplus(k_{jR},\mathbf{0})$ and the assumption $\delta_{jL}=\mathbf{0}$ contradicts Thereom 1. Moreover, $\mathrm{DDT}\left[\delta_j,\delta_{j+1}\right]\neq 2^{n-1}$, since $\delta_{j+1}\neq(\delta_{jL}\oplus\delta_{jR},\delta_{jL}),\delta_{j+1}\neq(\delta_{jL}\oplus\delta_{jR},\delta_{jL})\oplus(\mathbf{0},k_{jL})$, and representing $\delta_{j+1}=(\delta_{jL}\oplus\delta_{jR},\delta_{jL})\oplus(k_{jR},\mathbf{0})$ along with $\delta_{jL}\oplus\delta_{jR}=\mathbf{0}$ implies that $\mathrm{DDT}\left[\delta_j,\delta_{j+1}\right]\neq 2^{n-1}$.

If $\delta_{j+1}=(\mathbf{0},k_{jL})$, then $\mathrm{DDT}\left[\delta_j,\delta_{j+1}\right]\neq 2^n$ since $\delta_{j+1}\neq(\delta_{jL}\oplus\delta_{jR},\delta_{jL})$. Similarly,

$\mathrm{DDT}\left[\delta_j,\delta_{j+1}\right]\neq 2^{n-2}$ since $\delta_{j+1}=\left(\delta_{jL}\oplus\delta_{jR},\delta_{jL}\right)\oplus\left(\mathbf{0},k_{jL}\right)$ and $\delta_{jL}=\mathbf{0}$. Also, $\mathrm{DDT}\left[\delta_j,\delta_{j+1}\right]\neq 2^{n-1}$ since $\delta_{j+1}\neq\left(\delta_{jL}\oplus\delta_{jR},\delta_{jL}\right)$, $\delta_{j+1}\neq\left(\delta_{jL}\oplus\delta_{jR},\delta_{jL}\right)\oplus\left(k_{jR},\mathbf{0}\right)$ and expressing $\delta_{j+1}=\left(\delta_{jL}\oplus\delta_{jR},\delta_{jL}\right)\oplus\left(\mathbf{0},k_{jL}\right)$ along with the assumption $\delta_{jL}=\mathbf{0}$ proves the claim.

If $\delta_{j+1}=\left(k_{jR},k_{jL}\right)$, then $\mathrm{DDT}\left[\delta_j,\delta_{j+1}\right]\neq 2^{n}$ since $\delta_{j+1}\neq\left(\delta_{jL}\oplus\delta_{jR},\delta_{jL}\right)$. Also, $\mathrm{DDT}\left[\delta_j,\delta_{j+1}\right]\neq 2^{n-2}$ since $\delta_{j+1}=\left(\delta_{jL}\oplus\delta_{jR},\delta_{jL}\right)\oplus\left(k_{jR},k_{jL}\right)$ but $\delta_{jL}=\mathbf{0}$. Finally, $\mathrm{DDT}\left[\delta_j,\delta_{j+1}\right]\neq 2^{n-1}$ since $\delta_{j+1}\neq\left(\delta_{jL}\oplus\delta_{jR},\delta_{jL}\right)$, $\delta_{j+1}\neq\left(\delta_{jL}\oplus\delta_{jR},\delta_{jL}\right)\oplus\left(\mathbf{0},k_{jL}\right)$ and $\delta_{j+1}\neq\left(\delta_{jL}\oplus\delta_{jR},\delta_{jL}\right)\oplus\left(k_{jR},\mathbf{0}\right)$.

Therefore, $\mathrm{DP}\left[\delta_j,\delta_{j+1}\right]=0$, and moreover $\mathrm{DP}\left[\Omega\right]=0$.

The proof of 2) is similar to the proof of 1). #

Actually, from the result of Theorem 3, we only need to consider Ω in (9) when $\delta_i\neq\mathbf{0}, i=1,2,...,n$.

Theorem 4 For *n*-round DBISON, let Ω be the *n*-round differential characteristics given by (9) with $\delta_i\neq\mathbf{0},\ i=1,2,...,n$. Let also the round keys satisfy $k_{iR}\notin\left\{k_{(i-1)L},k_{iL},k_{(i+1)L},k_{iL}\oplus k_{(i-1)L}\right\}$. If there is δ_{j-1} such that $\mathrm{DP}\left[\delta_{j-1},\delta_j\right]=1$, then $\mathrm{DP}\left[\delta_{j-2},\delta_{j-1}\right]\neq 1$ and $\mathrm{DP}\left[\delta_j,\delta_{j+1}\right]\neq 1$.

Proof By Theorem 1 and using $\delta_i\neq\mathbf{0},\ i=1,2,...,n$, it is clear that $\mathrm{DP}\left[\delta_{j-1},\delta_j\right]=1$ if and only if $\delta_j=\left(\delta_{(j-1)L}\oplus\delta_{(j-1)R},\delta_{(j-1)L}\right)$ and $\delta_{j-1}\in\left\{\left(\mathbf{0},k_{jR}\right),\left(k_{jL},k_{jL}\right),\left(k_{jL},k_{jL}\oplus k_{jR}\right)\right\}$. $\mathrm{DP}\left[\delta_j,\delta_{j+1}\right]\neq 1$ can be proved using reduction to the absurd, the proof of $\mathrm{DP}\left[\delta_{j-2},\delta_{j-1}\right]\neq 1$ is similar, thus it is omitted here.

Now, assuming that $\mathrm{DP}\left[\delta_j,\delta_{j+1}\right]=1$, by Theorem 1, $\mathrm{DP}\left[\delta_j,\delta_{j+1}\right]=1$ if and only if $\delta_{j+1}=\left(\delta_{jL}\oplus\delta_{jR},\delta_{jL}\right)$ and $\delta_j\in A_{\delta_j}:=\left\{\left(\mathbf{0},k_{(j+1)R}\right),\left(k_{(j+1)L},k_{(j+1)L}\right),\left(k_{(j+1)L},k_{(j+1)L}\oplus k_{(j+1)R}\right)\right\}$.

If $\delta_{j-1}=\left(\mathbf{0},k_{jR}\right)$, using that $\mathrm{DP}\left[\delta_{j-1},\delta_j\right]=1$, we get $\delta_j=\left(\mathbf{0}\oplus k_{jR},\mathbf{0}\right)=\left(k_{jR},\mathbf{0}\right)$. Combining this with $\mathrm{DP}\left[\delta_j,\delta_{j+1}\right]=1$, we have $\left(k_{jR},\mathbf{0}\right)=\delta_j\in A_{\delta_j}$ which contradicts the condition that $k_{iR}\neq k_{(i+1)L}$.

If $\delta_{j-1}=\left(k_{jL},k_{jL}\right)$, using that $\mathrm{DP}\left[\delta_{j-1},\delta_j\right]=1$, we get $\delta_j=\left(k_{jL}\oplus k_{jL},k_{jL}\right)=\left(\mathbf{0},k_{jL}\right)$. Combining this with $\mathrm{DP}\left[\delta_j,\delta_{j+1}\right]=1$, we have $\left(\mathbf{0},k_{jL}\right)=\delta_j\in A_{\delta_j}$ which contradicts the condition that $k_{iR}\neq k_{(i-1)L}$.

If $\delta_{j-1}=\left(k_{jL},k_{jL}\oplus k_{jR}\right)$, using that $\mathrm{DP}\left[\delta_{j-1},\delta_j\right]=1$, we get

$$\delta_j=\left(k_{jL}\oplus k_{jR}\oplus k_{jL},k_{jL}\right)=\left(k_{jR},k_{jL}\right).$$

Again, combining this with $\mathrm{DP}\left[\delta_j,\delta_{j+1}\right]=1$, we have $\left(k_{jR},k_{jL}\right)=\delta_j\in A_{\delta_j}$ which contradicts the condition that $k_{iR}\neq k_{(i+1)L}$.

Therefore, the assumption that $\mathrm{DP}\left[\delta_j,\delta_{j+1}\right]=1$ does not hold, thus $\mathrm{DP}\left[\delta_j,\delta_{j+1}\right]\neq 1$. #

By Theorem 4, we know that any two consecutive factors of $\mathrm{DP}\left[\Omega\right]=\prod_{i=1}^{n}\mathrm{DP}\left[\delta_{i-1},\delta_i\right]$

cannot be 1 simultaneously, hence there are at most $n/2$ multiplicative factors that are equal 1. Moreover, because $\mathrm{DP}[\delta_{i-1},\delta_i]\in\{0,\ 1/2^2,\ 1/2,\ 1\}$, it is clear that $\mathrm{DP}[\Omega]\le 2^{-n/2}$.

Theorem 5 For *n*-round DBISON, let Ω be the *n*-round differential characteristic given by (9), with $\delta_i\ne\mathbf{0},\ i=1,2,...,n$. Let the round keys satisfy:

$$k_{iR}\notin\{k_{(i-1)L},k_{iL},k_{(i+1)L},k_{(i-1)L}\oplus k_{iL},k_{(i-2)R}\}\ \text{and}\ k_{iL}\ne k_{(i+1)L}.$$

If $\mathrm{DP}[\delta_{i-2},\delta_{i-1}]=\mathrm{DP}[\delta_i,\delta_{i+1}]=1$, then $\mathrm{DP}[\delta_{i-1},\delta_i]\ne 1/2$.

Proof Assume $\mathrm{DP}[\delta_{i-1},\delta_i]=1/2$. By Theorem 1, $\mathrm{DP}[\delta_{i-1},\delta_i]=1/2$ if and only if one of the following cases occurs.

Case 1.

$$\delta_i=(\delta_{(i-1)L}\oplus\delta_{(i-1)R},\delta_{(i-1)L})\in\{(\mathbf{0},\delta_{(i-1)L}),(k_{iR},\delta_{(i-1)L}),(\delta_{(i-1)L}\oplus\delta_{(i-1)R},\mathbf{0}),(\delta_{(i-1)L}\oplus\delta_{(i-1)R},k_{iL})$$
$$|\delta_{(i-1)L}\notin\{\mathbf{0},k_{iL}\},\delta_{(i-1)L}\oplus\delta_{(i-1)R}\notin\{\mathbf{0},k_{iR}\}\}:=A_1.$$

Using $\mathrm{DP}[\delta_i,\delta_{i+1}]=1$, we get $\delta_i\in A_{\delta_i}:=\{(\mathbf{0},k_{(i+1)R}),(k_{(i+1)L},k_{(i+1)L}),(k_{(i+1)L},k_{(i+1)L}\oplus k_{(i+1)R})\}$. Due to the conditions that the round keys satisfy, $A_1\cap A_{\delta_i}\ne\varnothing$ if and only if $\delta_{(i-1)L}=k_{(i+1)R}$. However, using $\mathrm{DP}[\delta_{i-2},\delta_{i-1}]=1$, we get $\delta_{(i-1)L}=\delta_{(i-2)L}\oplus\delta_{(i-2)R}\in\{k_{(i-1)R},\mathbf{0}\}$ which means $k_{(i+1)R}=k_{(i-1)R}$, a contradiction.

Case 2. $\delta_i=(\delta_{(i-1)L}\oplus\delta_{(i-1)R},\delta_{(i-1)L})\oplus(\mathbf{0},k_{iL})$, $\delta_{(i-1)L}\oplus\delta_{(i-1)R}\in\{\mathbf{0},k_{iR}\}$ and $\delta_{(i-1)L}\notin\{\mathbf{0},k_{iL}\}$.

In this case, $\delta_i\in\{(\mathbf{0},\delta_{(i-1)L}\oplus k_{iL}),(k_{iR},\delta_{(i-1)L}\oplus k_{iL})|\delta_{(i-1)L}\notin\{\mathbf{0},k_{iL}\}\}:=A_2$. Using $\mathrm{DP}[\delta_i,\delta_{i+1}]=1$, we get $\delta_i\in A_{\delta_i}$. $A_1\cap A_{\delta_i}\ne\varnothing$ if and only if $\delta_{(i-1)L}\oplus k_{iL}=k_{(i+1)R}$. However, since $\mathrm{DP}[\delta_{i-2},\delta_{i-1}]=1$, then $\delta_{(i-1)L}=\delta_{(i-2)L}\oplus\delta_{(i-2)R}\in\{k_{(i-1)R},\mathbf{0}\}$ which implies that $k_{iL}=k_{(i+1)R}\oplus k_{(i-1)R}$ or $k_{(i+1)R}$, a contradiction.

Case 3. $\delta_i=(\delta_{(i-1)L}\oplus\delta_{(i-1)R},\delta_{(i-1)L})\oplus(k_{iR},\mathbf{0})$, $\delta_{(i-1)L}\oplus\delta_{(i-1)R}\notin\{\mathbf{0},k_{iR}\}$ and $\delta_{(i-1)L}\in\{\mathbf{0},k_{iL}\}$.

In this case, $\delta_i\in\{(\delta_{(i-1)L}\oplus\delta_{(i-1)R}\oplus k_{iR},\mathbf{0}),(\delta_{(i-1)L}\oplus\delta_{(i-1)R}\oplus k_{iR},k_{iL})|\delta_{(i-1)L}\oplus\delta_{(i-1)R}\notin\{\mathbf{0},k_{iR}\}\}$ $:=A_3$. By $\mathrm{DP}[\delta_i,\delta_{i+1}]=1$, we have $\delta_i\in A_{\delta_i}$. Then, the conditions imposed on the round keys imply that $A_3\cap A_{\delta_i}=\varnothing$.

To summarize, the assumption $\mathrm{DP}[\delta_{i-1},\delta_i]=1/2$ cannot hold. #

Remark 2 For *n*-round DBISON, let Ω be the *n*-round differential characteristic given by (9) with $\delta_i\ne\mathbf{0},\ i=1,2,...,n$. Assuming that the round keys satisfy the conditions of Theorem 5, we cannot possibly have the case $DP[\Omega]=1\times(1/2)\times1\times(1/2)\times1...$.

Theorem 6 For *n*-round DBISON, let Ω be the *n*-round differential characteristic given by (9) with $\delta_i\ne\mathbf{0},i=1,2,...,n$. Assume that the round keys satisfy

1) $k_{iR}\notin\{k_{(i-1)L},k_{iL},k_{(i+2)L},k_{(i-2)L}\oplus k_{(i-1)L},k_{(i-1)L}\oplus k_{iL},k_{iL}\oplus k_{(i+2)L},k_{(i-1)R}\}$.
2) $k_{iL}\notin\{k_{(i-2)L},k_{(i-1)L},k_{iR}\oplus k_{(i+1)R},k_{(i+1)R}\oplus k_{(i+2)R}\}$.
3) $k_{(i-1)L}\oplus k_{iL}\ne k_{iR}\oplus k_{(i+1)R}$.

If $\mathrm{DP}[\delta_{i-2},\delta_{i-1}]=\mathrm{DP}[\delta_i,\delta_{i+1}]=1$, then $\mathrm{DP}[\delta_{i-1},\delta_i]\ne 1/2^2$.

Proof Assume $\mathrm{DP}\left[\delta_{i-1},\delta_i\right]=1/2^2$. By Theorem 1, $\mathrm{DP}\left[\delta_{i-1},\delta_i\right]=1/2^2$ if and only if one of the following cases occurs.

Case 1. $\delta_i=\left(\delta_{(i-1)L}\oplus\delta_{(i-1)R},\delta_{(i-1)L}\right)$, $\delta_{(i-1)L}\notin\{\mathbf{0},k_{iL}\}$ and $\delta_{(i-1)L}\oplus\delta_{(i-1)R}\notin\{\mathbf{0},k_{iR}\}$

Using $\mathrm{DP}\left[\delta_{i-2},\delta_{i-1}\right]=\mathrm{DP}\left[\delta_i,\delta_{i+1}\right]=1$, one can deduce:

$$\delta_{i+1}=\left(\delta_{iL}\oplus\delta_{iR},\delta_{iL}\right)=\left(\delta_{(i-1)R},\ \delta_{(i-1)L}\oplus\delta_{(i-1)R}\right)=\left(\delta_{(i-2)L},\delta_{(i-2)R}\right),$$

where $\delta_{iL}\in\left\{\mathbf{0},k_{(i+1)L}\right\}:=B_1$, and $\delta_{(i-2)R}\in\left\{k_{(i-1)R},k_{(i-1)L},k_{(i-1)L}\oplus k_{(i-1)R}\right\}:=B_2$. The conditions on the round keys imply that $B_1\cap B_2=\varnothing$, which contradicts the fact that $\delta_{iL}=\delta_{(i-2)R}$.

Case 2. $\delta_i=\left(\delta_{(i-1)L}\oplus\delta_{(i-1)R},\delta_{(i-1)L}\right)\oplus\left(\mathbf{0},k_{iL}\right)$, $\delta_{(i-1)L}\notin\{\mathbf{0},k_{iL}\}$ and $\delta_{(i-1)L}\oplus\delta_{(i-1)R}\notin\{\mathbf{0},k_{iR}\}$

Using $\mathrm{DP}\left[\delta_{i-2},\delta_{i-1}\right]=\mathrm{DP}\left[\delta_i,\delta_{i+1}\right]=1$, we get the following equation

$$\delta_{i+1}=\left(\delta_{iL}\oplus\delta_{iR},\delta_{iL}\right)=\left(\delta_{(i-1)R}\oplus\ k_{iL},\delta_{(i-1)L}\oplus\delta_{(i-1)R}\right)=\left(\delta_{(i-2)L}\oplus k_{iL},\delta_{(i-2)R}\right),$$

where $\delta_{iL}\oplus\delta_{iR}\in\left\{\mathbf{0},k_{(i+1)R}\right\}:=B_3$, and $\delta_{(i-2)L}\oplus k_{iL}\in\left\{k_{iL},k_{(i-1)L}\oplus k_{iL}\right\}:=B_4$. The conditions on the round keys give that $B_3\cap B_4=\varnothing$, which contradicts the fact that $\delta_{iL}\oplus\delta_{iR}=\delta_{(i-2)L}\oplus k_{iL}$.

Case 3. $\delta_i=\left(\delta_{(i-1)L}\oplus\delta_{(i-1)R},\delta_{(i-1)L}\right)\oplus\left(k_{iR},\mathbf{0}\right)$, $\delta_{(i-1)L}\notin\{\mathbf{0},k_{iL}\}$ and $\delta_{(i-1)L}\oplus\delta_{(i-1)R}\notin\{\mathbf{0},k_{iR}\}$

Using $\mathrm{DP}\left[\delta_{i-2},\delta_{i-1}\right]=\mathrm{DP}\left[\delta_i,\delta_{i+1}\right]=1$, we have

$$\delta_{i+1}=\left(\delta_{iL}\oplus\delta_{iR},\delta_{iL}\right)=\left(\delta_{(i-1)R}\oplus\ k_{iR},\delta_{(i-1)L}\oplus\delta_{(i-1)R}\oplus k_{iR}\right)=\left(\delta_{(i-2)L}\oplus k_{iR},\delta_{(i-2)R}\oplus k_{iR}\right),$$

where $\delta_{iL}\oplus\delta_{iR}\in B_3$, and $\delta_{(i-2)L}\oplus k_{iR}\in\left\{k_{iR},k_{(i-1)L}\oplus k_{iR}\right\}:=B_5$. The assumptions on the round keys give that $B_3\cap B_5=\varnothing$, which contradicts $\delta_{iL}\oplus\delta_{iR}=\delta_{(i-2)L}\oplus k_{iR}$.

Case 4. $\delta_i=\left(\delta_{(i-1)L}\oplus\delta_{(i-1)R},\delta_{(i-1)L}\right)\oplus\left(k_{iR},k_{iL}\right)$, $\delta_{(i-1)L}\notin\{\mathbf{0},k_{iL}\}$ and $\delta_{(i-1)L}\oplus\delta_{(i-1)R}\notin\{\mathbf{0},k_{iR}\}$

Again, using $\mathrm{DP}\left[\delta_{i-2},\delta_{i-1}\right]=\mathrm{DP}\left[\delta_i,\delta_{i+1}\right]=1$, we obtain

$$\delta_{i+1}=\left(\delta_{iL}\oplus\delta_{iR},\delta_{iL}\right)=\left(\delta_{(i-1)R}\oplus\ k_{iR}\oplus k_{iL},\delta_{(i-1)L}\oplus\delta_{(i-1)R}\oplus k_{iR}\right)=\left(\delta_{(i-2)L}\oplus k_{iR}\oplus k_{iL},\delta_{(i-2)R}\oplus k_{iR}\right),$$

where $\delta_{iL}\oplus\delta_{iR}\in B_3$, $\delta_{(i-2)L}\oplus k_{iR}\oplus k_{iL}\in\left\{k_{iR}\oplus k_{iL},k_{iR}\oplus k_{(i-1)L}\oplus k_{iL}\right\}:=B_6$. Similarly as above, we get $B_3\cap B_6=\varnothing$ which contradicts $\delta_{iL}\oplus\delta_{iR}=\delta_{(i-2)L}\oplus k_{iR}\oplus k_{iL}$.

Therefore, the assumption that $\mathrm{DP}\left[\delta_{i-1},\delta_i\right]=1/2^2$ cannot hold. #

Remark 3 For *n*-round DBISON, let Ω denote the *n*-round differential characteristic given by (9) with $\delta_i\neq\mathbf{0},\ i=1,2,...,n$. Assuming that the round keys satisfy conditions in Theorem 6, it is impossible to have $DP[\Omega]=1\times\left(1/2^2\right)\times1\times\left(1/2^2\right)\times1...$.

Theorem 7 For *n*-round DBISON, let Ω be the *n*-round differential characteristic given by (9), with $\delta_i\neq\mathbf{0},\ i=1,2,...,n$. Assume that the round keys satisfy $k_{iR}\notin\left\{k_{(i+1)R},k_{iL},k_{(i+1)L}\right\}$ and $k_{iL}\notin\left\{k_{(i+1)R},k_{iR}\oplus k_{(i+1)R}\right\}$. If $\mathrm{DP}\left[\delta_{i-1},\delta_i\right]=\mathrm{DP}\left[\delta_{i+2},\delta_{i+3}\right]=1$, then the following equalities cannot hold: $\mathrm{DP}\left[\delta_i,\delta_{i+1}\right]=\mathrm{DP}\left[\delta_{i+1},\delta_{i+2}\right]=1/2$.

Proof By Theorem 1, the conditions on the round keys, and $\mathrm{DP}\left[\delta_{i-1},\delta_i\right]=1$, one can deduce that $\mathrm{DP}\left[\delta_i,\delta_{i+1}\right]=1/2$ if and only if $\delta_{i-1}=\left(k_{iL},k_{iL}\right)$, $\delta_i=\left(\mathbf{0},k_{iL}\right)$, and $\delta_{i+1}=\left(k_{iL}\oplus k_{(i+1)R},\mathbf{0}\right)$. Furthermore, $\mathrm{DP}\left[\delta_{i+1},\delta_{i+2}\right]=1/2$ holds if and only if $\delta_{i+2}=\left(k_{iL}\oplus k_{(i+1)R}\oplus k_{(i+2)R},k_{iL}\oplus k_{(i+1)R}\right)$ or

$\delta_{i+2} = \left(k_{iL} \oplus k_{(i+1)R}, k_{iL} \oplus k_{(i+2)L} \oplus k_{(i+1)R}\right)$.

If $\delta_{i+2} = \left(k_{iL} \oplus k_{(i+1)R} \oplus k_{(i+2)R}, k_{iL} \oplus k_{(i+1)R}\right)$, then from Theorem 1 and $\mathrm{DP}\left[\delta_{i+2}, \delta_{i+3}\right] = 1$, it can be easily verified that

$\delta_{i+3} = \left(\delta_{(i+2)L} \oplus \delta_{(i+2)R}, \delta_{(i+2)L}\right)$ and $\delta_{i+2} \in \left\{\left(\mathbf{0}, k_{(i+3)R}\right), \left(k_{(i+3)L}, k_{(i+3)L}\right), \left(k_{(i+3)L}, k_{(i+3)R} \oplus k_{(i+3)L}\right)\right\}$.

This means that

$$\left(k_{iL} \oplus k_{(i+1)R} \oplus k_{(i+2)R}, k_{iL} \oplus k_{(i+1)R}\right) \in \left\{\left(\mathbf{0}, k_{(i+3)R}\right), \left(k_{(i+3)L}, k_{(i+3)L}\right), \left(k_{(i+3)L}, k_{(i+3)R} \oplus k_{(i+3)L}\right)\right\},$$

which contradicts the assumptions on the round keys. If $\delta_{i+2} = \left(k_{iL} \oplus k_{(i+1)R}, k_{iL} \oplus k_{(i+2)L} \oplus k_{(i+1)R}\right)$, a similar conclusion is valid. #

Generalizing the conclusions given in Theorem 7, we observe the following.

Remark 4 For *n*-round DBISON, let Ω be the *n*-round differential characteristic given by (9) with $\delta_i \neq \mathbf{0}$, $i = 1, 2, \ldots, n$. Assuming that the round keys $k_i = \left(k_{iL}, k_{iR}\right)$ satisfy the conditions that k_{iR} is linearly independent from $k_{iL}, k_{(i+1)L}, \ldots, k_{(i+l-2)L}$ and k_{iL} is linearly independent from $k_{iR}, k_{(i+1)R}, \ldots, k_{(i+l-2)R}$, then $\mathrm{DP}\left[\delta_i, \delta_{i+1}\right] = \mathrm{DP}\left[\delta_{i+1}, \delta_{i+2}\right] = \ldots = \mathrm{DP}\left[\delta_{i+l-2}, \delta_{i+l-1}\right] = \frac{1}{2}$ and $\mathrm{DP}\left[\delta_{i-1}, \delta_i\right] = \mathrm{DP}\left[\delta_{i+l-1}, \delta_{i+l}\right] = 1$ cannot hold.

By Remarks 2, 3, 4, for *n*-round DBISON (whose round keys satisfy certain conditions) and Ω described by (9) with $\delta_i \neq \mathbf{0}$, $i = 1, 2, \ldots, n$, if there exists a differential characteristic of the form

$$\mathrm{DP}[\Omega] = \prod_{i=1}^{n} \mathrm{DP}\left[\delta_{i-1}, \delta_i\right] = 1 \times (1/2) \times \left(1/2^2\right) \times 1 \times (1/2) \times \left(1/2^2\right) \times 1 \ldots,$$

then the probability of this differential characteristic is maximal. Then,

$$\prod_{i=1}^{n} \mathrm{DP}\left[\delta_{i-1}, \delta_i\right] = 1 \times (1/2) \times \left(1/2^2\right) \times 1 \times (1/2) \times \left(1/2^2\right) \times 1 \ldots = 1^{\lceil n/3 \rceil} (1/2)^{\lceil (n-1)/3 \rceil} \left(1/2^2\right)^{\lceil (n-2)/3 \rceil} := h(n).$$

Table 2 gives some values of $h(n)$ for different *n*. Most notably, $h(n) = 1/2^n$ if *n* is divisible by 6, otherwise, $h(n) = 1/2^{n-1}$.

Remark 5 For *n*-round DBISON, we have $\mathrm{MDP} \leq 1/2^{n-1}$ when the round keys satisfy the conditions given in the previous theorems. Therefore, we conclude that *n*-round DBISON is resistant against differential cryptanalysis.

Table 2. Values of h(*n*)

n	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62	66
h(*n*)	2^{-6}	2^{-9}	2^{-13}	2^{-18}	2^{-21}	2^{-25}	2^{-30}	2^{-33}	2^{-37}	2^{-42}	2^{-45}	2^{-49}	2^{-54}	2^{-57}	2^{-61}	2^{-66}
n	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126	130
h(*n*)	2^{-69}	2^{-73}	2^{-78}	2^{-81}	2^{-85}	2^{-90}	2^{-93}	2^{-97}	2^{-102}	2^{-105}	2^{-109}	2^{-114}	2^{-117}	2^{-121}	2^{-126}	2^{-129}
n	134	138	142	146	150	154	158	162	166	170	174	178	182	186	190	194
h(*n*)	2^{-133}	2^{-138}	2^{-141}	2^{-145}	2^{-150}	2^{-153}	2^{-157}	2^{-162}	2^{-165}	2^{-169}	2^{-174}	2^{-177}	2^{-181}	2^{-186}	2^{-189}	2^{-193}
n	198	202	206	210	214	218	222	226	230	234	238	242	246	250	254	258
h(*n*)	2^{-198}	2^{-201}	2^{-205}	2^{-210}	2^{-213}	2^{-217}	2^{-222}	2^{-225}	2^{-229}	2^{-234}	2^{-237}	2^{-241}	2^{-246}	2^{-249}	2^{-253}	2^{-258}

4. Linear cryptanalysis of the DBISON block cipher

To evaluate the resistance of DBISON against linear cryptanalysis, we need to specify the linear approximation table (LAT) of the round function $F_{k,w}(x)$. Recall that $F_{k,w}(x)$ was defined in (1), where the linear functions $\Phi_{k_{iL}}$ and $\Phi_{k_{iR}}$ are given by:

$$\begin{aligned}\Phi_{k_L}(x_L) &= \left(x_{L_{i(k_L)}} k_L \oplus x_L\right)\left[1,\ldots,i(k_L)-1,i(k_L)+1,\ldots,n/2\right] \\ \Phi_{k_R}(x_R) &= \left(x_{R_{i(k_R)}} k_R \oplus x_R\right)\left[1,\ldots,i(k_R)-1,i(k_R)+1,\ldots,n/2\right]\end{aligned}, \tag{10}$$

where $i(k_L)$ and $i(k_R)$ denote the indices of the lowest bit which is set to 1 in k_L, k_R, respectively. Moreover, it is easy to deduce that Φ_{k_L} and Φ_{k_R} are both linear functions, $\operatorname{Ker}\Phi_{k_L} = \{\mathbf{0}, k_L\}$, and $\operatorname{Ker}\Phi_{k_R} = \{\mathbf{0}, k_R\}$. In particular, the notation

$$\left(x_{i(k_L)} k_L \oplus x_L\right)\left[1,\ldots,i(k_L)-1,i(k_L)+1,\ldots,n/2\right]$$

refers to an $(n/2-1)$-bit vector, which consists of the bits of $x_{i(k_L)} k_L \oplus x_L$ except for the $i(k_L)_{th}$ bit.

Theorem 8 For the round function $F_{k,w}(x)$ of DBISON, which is defined by (2) and (10), the entries of LAT of $F_{k,w}(x)$ are determined as:

1) $\mathrm{LAT}_{F_{k,w}}[a,b] = 2^{n-1}$, if $b_L \bullet k_R = b_R \bullet k_L = 0$, $a_R = b_L$ and $a_L \oplus b_L \oplus b_R = \mathbf{0}$.
2) $\mathrm{LAT}_{F_{k,w}}[a,b] = \pm 2^{(3n/2-1)/2}$, if $b_L \bullet k_R = 0$, $b_R \bullet k_L = 1$, $a_R = b_L$ and $a_L \oplus b_L \oplus b_R = \mathbf{0}$.
3) $\mathrm{LAT}_{F_{k,w}}[a,b] \in \left(-2^{(3n/2-1)/2}, 2^{(3n/2-1)/2}\right)$, if $b_L \bullet k_R = 1$ and $(a_L \oplus b_L) \bullet k_R = 0$.
4) Otherwise, $\mathrm{LAT}_{F_{k,w}}[a,b] = 0$.

Proof By Definition 1, it is clear that

$$\mathrm{LAT}_{F_{k,w}}[a,b] := \left|\left\{x \in F_2^n \,\middle|\, a \bullet x \oplus b \bullet F_{k,w}(x) = 0\right\}\right| - 2^{n-1} = \frac{1}{2} W_{F_{k,w}}(a,b).$$

$$\begin{aligned}W_{F_{k,w}}(a,b) &:= \sum_{x \in F_2^n} (-1)^{a \bullet x \oplus b \bullet F_{k,w}(x)} \\ &= \sum_{x \in F_2^n} (-1)^{a_L \bullet x_L \oplus a_R \bullet x_R \oplus b_L \bullet \left(x_L \oplus x_R \oplus f_R\left(w_R \oplus \Phi_{k_R}(x_L \oplus x_R)\right) k_R\right) \oplus b_R \bullet \left(x_L \oplus f_L\left(w_L \oplus \Phi_{k_L}(x_L)\right) k_L\right)} \\ &= \sum_{x_L \in F_2^{n/2}} (-1)^{(a_L \oplus b_L \oplus b_R) \bullet x_L \oplus f_L\left(w_L \oplus \Phi_{k_L}(x_L)\right) b_R \bullet k_L} \sum_{x_R \in F_2^{n/2}} (-1)^{(a_R \oplus b_L) \bullet x_R \oplus f_R\left(w_R \oplus \Phi_{k_R}(x_L) \oplus \Phi_{k_R}(x_R)\right) b_L \bullet k_R}.\end{aligned}$$

According to the value of $b_L \bullet k_R$, $W_{F_{k,w}}(a,b)$ can be calculated in the following cases.

Case 1. $b_L \bullet k_R = 0$.

In this case, $W_{F_{k,w}}(a,b) = \sum_{x_L \in F_2^{n/2}} (-1)^{(a_L \oplus b_L \oplus b_R) \bullet x_L \oplus f_L\left(w_L \oplus \Phi_{k_L}(x_L)\right) b_R \bullet k_L} \sum_{x_R \in F_2^{n/2}} (-1)^{(a_R \oplus b_L) \bullet x_R} := W_1$.

If $a_R \neq b_L$, then $\sum_{x_R \in F_2^{n/2}} (-1)^{(a_R \oplus b_L) \bullet x_R} = 0$, thus $W_1 = 0$.

If $a_R = b_L$, then $W_1 = 2^{n/2} \sum_{x_L \in F_2^{n/2}} (-1)^{(a_L \oplus b_L \oplus b_R) \bullet x_L \oplus f_L\left(w_L \oplus \Phi_{k_L}(x_L)\right) b_R \bullet k_L}$. On the one hand, if $b_R \bullet k_L = 0$, then $W_1 = 2^{n/2} \sum_{x_L \in F_2^{n/2}} (-1)^{(a_L \oplus b_L \oplus b_R) \bullet x_L} = \begin{cases} 0, & \text{if } a_L \oplus b_L \oplus b_R \neq \mathbf{0}, \\ 2^n, & \text{if } a_L \oplus b_L \oplus b_R = \mathbf{0}. \end{cases}$ On the other hand, if

$b_R \bullet k_L = 1$, then $W_1 = 2^{n/2} \sum_{x_L \in F_2^{n/2}} (-1)^{(a_L \oplus b_L \oplus b_R)\bullet x_L \oplus f_L(w_L \oplus \Phi_{k_L}(x_L))}$. Assuming that $\Phi_{k_L}(x_L) = y_L$, using that Φ_{k_L} is linear and $\mathrm{Ker}\Phi_{k_L} = \{\mathbf{0}, k_L\}$, we obtain

$$\sum_{x_L \in F_2^{n/2}} (-1)^{(a_L \oplus b_L \oplus b_R)\bullet x_L \oplus f_L(w_L \oplus \Phi_{k_L}(x_L))} = \sum_{y_L \in F_2^{n/2-1}} (-1)^{(a_L \oplus b_L \oplus b_R)\bullet y_L' \oplus f_L(w_L \oplus y_L)} + \sum_{y_L \in F_2^{n/2-1}} (-1)^{(a_L \oplus b_L \oplus b_R)\bullet (y_L' \oplus k_L) \oplus f_L(w_L \oplus y_L)}$$

$$= \left[1 + (-1)^{(a_L \oplus b_L \oplus b_R)\bullet k_L}\right] \sum_{y_L \in F_2^{n/2-1}} (-1)^{(a_L \oplus b_L \oplus b_R)\bullet y_L' \oplus f_L(w_L \oplus y_L)},$$

where y_L' is the same as y with an additional bit set to zero at position $i(k_L)$. Furthermore, if $(a_L \oplus b_L \oplus b_R)\bullet k_L = 1$, then $W_1 = 2^{n/2} \times 0 = 0$. If $(a_L \oplus b_L \oplus b_R)\bullet k_L = 0$, then

$$W_1 = 2^{n/2+1} \sum_{y_L \in F_2^{n/2-1}} (-1)^{(a_L \oplus b_L \oplus b_R)\bullet y_L' \oplus f_L(w_L \oplus y_L)}$$

Let $w_L \oplus y_L = u_L$, and accordingly $W_1 = 2^{n/2+1}(-1)^{(a_L'' \oplus b_L'' \oplus b_R'')\bullet w_L} \sum_{u_L \in F_2^{n/2-1}} (-1)^{(a_L'' \oplus b_L'' \oplus b_R'')\bullet u_L \oplus f_L(u_L)}$, where a_L'' is an $(n/2-1)$-dimensional vector obtained by removing the bit in position $i(k_L)$ of a_L. Since f_L is a bent function, then $W_1 = 2^{n/2+1}(-1)^{(a_L'' \oplus b_L'' \oplus b_R'')\bullet w_L}\left(\pm 2^{(n/2-1)/2}\right) = \pm 2^{(3n/2+1)/2}$.

Case 2. $b_L \bullet k_R = 1$.

$$W_{F_{k,w}}(a,b) = \sum_{x_L \in F_2^{n/2}} (-1)^{(a_L \oplus b_L \oplus b_R)\bullet x_L \oplus f_L(w_L \oplus \Phi_{k_L}(x_L))b_R \bullet k_L} \sum_{x_R \in F_2^{n/2}} (-1)^{(a_R \oplus b_L)\bullet x_R \oplus f_R(w_R \oplus \Phi_{k_R}(x_L) \oplus \Phi_{k_R}(x_R))}.$$

For any fixed $x_L \in F_2^{n/2}$, it can be calculated that

$$\sum_{x_R \in F_2^{n/2}} (-1)^{(a_R \oplus b_L)\bullet x_R \oplus f_R(w_R \oplus \Phi_{k_R}(x_L) \oplus \Phi_{k_R}(x_R))} = \begin{cases} 0, & if\ (a_R \oplus b_L)\bullet k_R = 1, \\ \pm(-1)^{(a_R'' \oplus b_L'')\bullet(w_R \oplus \Phi_{k_R}(x_L))}\, 2^{(n/2+1)/2}, & if\ (a_R \oplus b_L)\bullet k_R = 0. \end{cases}$$

Thus, if $(a_R \oplus b_L)\bullet k_R = 1$, then $W_{F_{k,w}}(a,b) = 2^{n/2} \times 0 = 0$. If $(a_R \oplus b_L)\bullet k_R = 0$, then

$$W_{F_{k,w}}(a,b) = \pm 2^{(n/2+1)/2} \sum_{x_L \in F_2^{n/2}} (-1)^{(a_L \oplus b_L \oplus b_R)\bullet x_L \oplus f_L(w_L \oplus \Phi_{k_L}(x_L))b_R \bullet k_L \oplus (a_R'' \oplus b_L'')\bullet(w_R \oplus \Phi_{k_R}(x_L))}.$$

Thus, $-2^{(3n/2+1)/2} \le W_{F_{k,w}}(a,b) \le 2^{(3n/2+1)/2}$, where the equalities hold if and only if for all $x_L \in F_2^{n/2}$, we have

$$(a_R'' \oplus b_L'')\bullet(w_R \oplus \Phi_{k_R}(x_L)) \oplus (a_L \oplus b_L \oplus b_R)\bullet x_L \oplus f_L(w_L \oplus \Phi_{k_L}(x_L))b_R \bullet k_L = 0 \text{ or } 1.$$

The probability that these extreme cases occurring is very small, thus we can suppose $-2^{(3n/2+1)/2} < W_{F_{k,w}}(a,b) < 2^{(3n/2+1)/2}$. #

Theorem 9 For DBISON cipher, let its round function $F_{k,w}(x)$ be given by (2) and (10). If the number of rounds is $r = n/2+3$, then we have $\mathrm{MLP} < 2^{-(n-1)}$ for $n > 4$.

Proof Assume that there exists a nontrivial linear characteristic $\theta = (\theta_0, \theta_1, ..., \theta_{n/2+3})$. In particular, let the linear characteristic $\theta^* = (\theta_0, \theta_1, ..., \theta_{n/2})$ be such that $\mathrm{LP}(\theta_{i-1}, \theta_i) = 1$, $i = 1, 2, ..., n/2$. By Theorem 8, we have $\mathrm{LP}(\theta_{i-1}, \theta_i) = 1$ if and only if $\theta_{iL} \bullet k_{iR} = \theta_{iR} \bullet k_{iL} = 0$, $\theta_{iL} = \theta_{(i-1)R}$ and $\theta_{iR} = \theta_{(i-1)L} \oplus \theta_{(i-1)R}$. Note that there are two constraints (two-bit constraint conditions) for each round subkey, i.e. $\theta_{iL} \bullet k_{iR} = \theta_{iR} \bullet k_{iL} = 0$. In this case, considering $n/2$ rounds, the cardinality of a weak subkey set (satisfying the constraint conditions) should be

only $2^n \times 2^{-2\times(n/2)} = 1$ on average. On the other hand, if there are $n/2+3-n/2=3$ rounds, then the linear characteristic $\theta^* = (\theta_{n/2}, \theta_{n/2+1}, \theta_{n/2+2}, \theta_{n/2+3})$ exists with probability $\left[2^{-(n/2-1)}\right]^3 = 2^{-(3n/2-3)}$. Therefore, $\mathrm{MLP} < 2^{-(n-1)}$ for $n > 4$.

Remark 6. To resist algebraic attacks, the default round number should be at least *3n*.

5. DBISON instances and implementation results

In this section, we discuss our implementation of DBISON encryption algorithm with input block size of 10 bits, where the generations of round keys, whitened keys and round constants are also specified. Similarly to the standard BISON encryption algorithm, the bent function used in this instance of DBISON is the quadratic function $f(X_1, X_2) = X_1 \bullet X_2$, where $X_i \in F_2^5$. The differential uniformity and nonlinearity for round-reduced versions of DBISON consisting of 30 rounds (alternatively 10 or 20 rounds) and for different instances (specifying different secret keys via LFSRs) are given. The truth table of one particular instance and the intermediate values for 30 encryption rounds are given in Appendix A and B, respectively.

Assume that the input bit string for DBISON is $x = (x_{10}, x_9, ..., x_1)$, which is divided into two parts, i.e. $x_L = (x_{10}, x_9, ..., x_6)$ and $x_R = (x_5, x_4, ..., x_1)$. The first encryption round is described below.

- The encryption operation for the left branch includes the following five steps.

1) The left key k_L is derived from the state of an LFSR, where the primitive polynomial used is $x^5 + x^2 + 1$, and the initial state belongs to $F_2^5 \setminus \{\mathbf{0}\}$.
2) $\Phi_{k_L}(x_L) = \left(x_{L_{i(k_L)}} k_L \oplus x_L\right)\left[1, ..., i(k_L)-1, i(k_L)+1, ..., 5\right]$.
3) The left whitened key w_L is derived from the state of another LFSR, where the primitive polynomial used is $x^4 + x^3 + 1$, and the initial state is fixed by (1, 0, 0, 0). The round constant C_L is derived from the state of the same LFSR, and the initial state is given by (0, 0, 0, 1).
4) $\Phi_{k_L}(x_L) \oplus w_L \oplus C_L = (y_4, y_3, y_2, y_1)$, $f(y_4, y_3, y_2, y_1) = y_4 y_2 \oplus y_3 y_1 \oplus b_L$, and $b_L = 0$ for the first *r*/2 rounds, and $b_L = 1$ for the remaining *r*/2 rounds, where *r* is the number of rounds.
5) The value of $x_L \oplus f(y_4, y_3, y_2, y_1) k_L$ is calculated.

- The encryption operation for the right branch contains the five portions below. In particular, the input string for the right branch is $x_L \oplus x_R$, denote it as x'_R.

1) The right-hand part of the key k_R is derived from the state of an LFSR, where the primitive polynomial used is given by $x^5 + x^3 + 1$, and the initial state belongs to $F_2^5 \setminus \{\mathbf{0}\}$.
2) $\Phi_{k_R}(x'_R) = \left(x'_{R_{i(k_R)}} k_R \oplus x'_R\right)\left[1, ..., i(k_R)-1, i(k_R)+1, ..., 5\right]$.
3) The right-hand part of the whitened key w_R is derived from the state of another LFSR, the primitive polynomial used is given by $x^4 + x + 1$, and the initial state is fixed by (1, 0, 0, 1). The round constant C_R is derived from the state of the same LFSR, and the initial state is fixed by (0, 0, 0, 1).
4) $\Phi_{k_R}(x'_R) \oplus w_R \oplus C_R = (y'_4, y'_3, y'_2, y'_1)$, $f(y'_4, y'_3, y'_2, y'_1) = y'_4 y'_2 \oplus y'_3 y'_1 \oplus b_R$, and $b_R = 0$ for the

first $r/2$ rounds and $b_R = 1$ for the remaining $r/2$ rounds, where r is the number of rounds.

5) The value of $x'_R \oplus f(y'_4, y'_3, y'_2, y'_1)k_R$ is calculated.

Finally, the output value of the first round is $\left(x'_R \oplus f(y'_4, y'_3, y'_2, y'_1)k_R, x_L \oplus f(y_4, y_3, y_2, y_1)k_L\right)$. Similarly, in the second round, k, w and C are also derived from the states of the corresponding LFSRs in the next clock, and so on. More specifically, the initial state of the LFSR for deriving k_L in the first encryption round is fixed to any value in $F_2^5 \setminus \{\mathbf{0}\}$. On the other hand, the initial state of the LFSR for deriving k_R in the first round, selects another value k_L in $F_2^5 \setminus \{\mathbf{0}\}$. This gives in total 930 instances (different keys) of DBISON which we have checked. The differential uniformities and nonlinearities of these instances for DBISON that implements 10, 20 and 30 encryption rounds are verified, respectively. These results are described in **Fig. 2** and **Fig. 3**. In particular, the horizontal axis represents the value of the differential uniformity (nonlinearity), whereas the vertical axis is the number of instances whose differential uniformity (nonlinearity) is fixed.

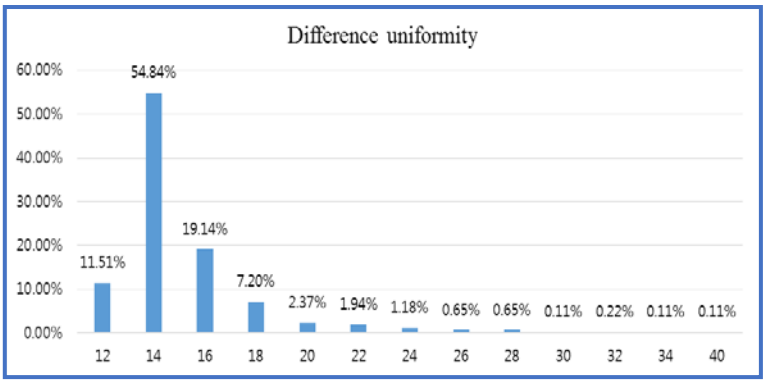


Fig. 2(a). The differential uniformities of 10-round DBISON

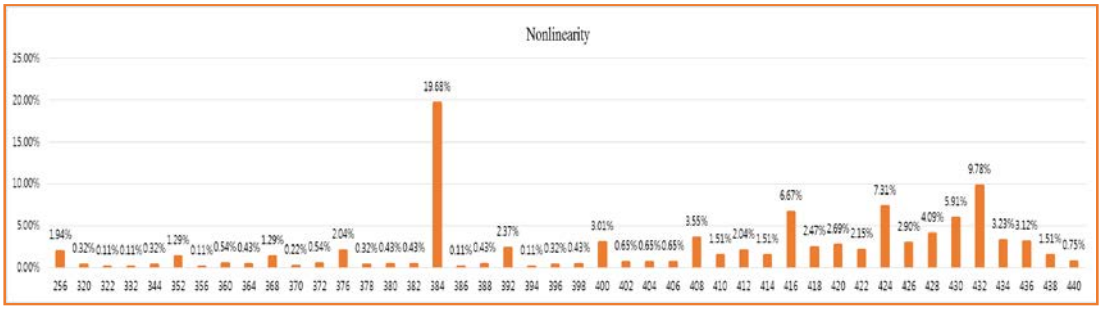


Fig. 2(b). The nonlinearities of 10-round DBISON

In **Fig. 2**, for DBISON consisting of 10 encryption rounds, the differential uniformity is mainly distributed among the values 12, 14, 16 and 18. Actually, these values have a percentage of approximately 92.26%. On the other hand, the maximal nonlinearity that has been achieved in the simulations is 440. Also, the nonlinearity in the range between 384 and 440 stands for the percentage of approximately 95.91%. In fact, it means that these functions achieve relatively high nonlinearity. (note that the nonlinearity of bent functions is 496, and the nonlinearity of almost optimal functions is 480 when n=10.) Moreover, the best differential uniformity of these instances is 14, and the nonlinearity is 440, which is quite

close to the almost optimal functions. This illustrates that most of these DBISON instances have quite good differential uniformity and nonlinearity, though only 10 encryption rounds are considered.

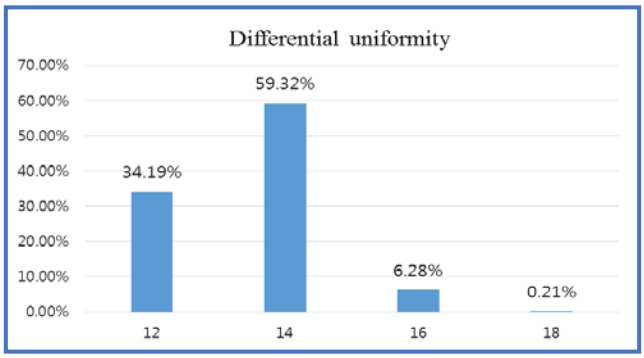


Fig. 3(a). The differential uniformities of 30-round DBISON

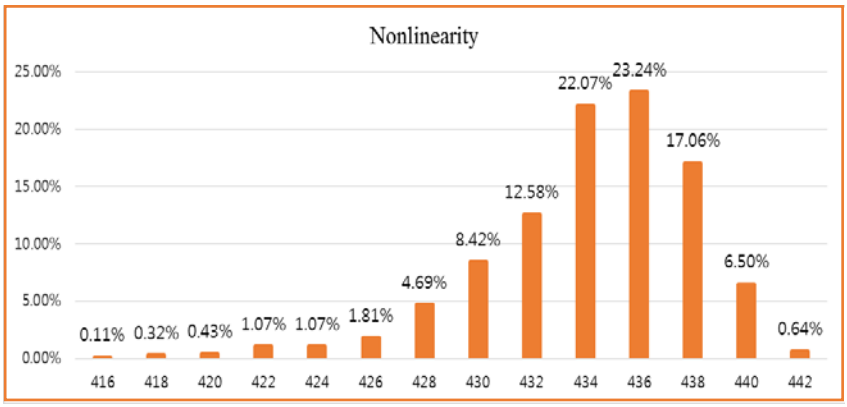


Fig. 3(b). The nonlinearities of 30-round DBISON

Fig. 3(a) illustrates that the differential uniformity takes values 12 and 14 with the percentage of approximately 93.51%, when the number of rounds is 30. The nonlinearity distribution is given in **Fig. 3(b)** and the nonlinearities between 428 and 442 occur with the percentage of approximately 95.2%. There exist many DBISON instances, using 30 rounds, whose differential uniformity equals 12 and having nonlinearity 442. The truth table of one of these instances is given in Appendix A, whereas the test vectors for each round are provided in Appendix B.

In addition, the differential uniformities and nonlinearities of DBISON instances using 20 rounds can be found in Appendix C. Comparing the 20-round and 30-round results, it is clear that their performances are quite close (of course 30-round DBISON is somewhat better). Of course, all DBISON instances are balanced bijections. Therefore, DBISON has quite good cryptographic performance.

Similarly to the encryption operation, the decryptions of left branch and right branch are also performed in parallel. More precisely, let $\tau_L(x_L) = x_L \oplus f_L(w_L \oplus \Phi_{k_L}(x_L))k_L$, $\tau_R(x_R) = x_R \oplus f_R(w_R \oplus \Phi_{k_R}(x_R))k_R$, x_L, $x_R \in F_2^{n/2}$. Then, τ_L and τ_R can be derived as below. For any $x_L \in F_2^{n/2}$,

$$\tau_L \circ \tau_L(x_L) = \tau_L\left(x_L \oplus f_L\left(w_L \oplus \Phi_{k_L}(x_L)\right)k_L\right)$$
$$= x_L \oplus f_L\left(w_L \oplus \Phi_{k_L}(x_L)\right)k_L \oplus f_L\left(w_L \oplus \Phi_{k_L}\left(x_L \oplus f_L\left(w_L \oplus \Phi_{k_L}(x_L)\right)k_L\right)\right)k_L .$$

If $f_L\left(w_L \oplus \Phi_{k_L}(x_L)\right) = 0$, it is clear that $\tau_L \circ \tau_L(x_L) = x_L$. If $f_L\left(w_L \oplus \Phi_{k_L}(x_L)\right) = 1$, then we have

$$\tau_L \circ \tau_L(x_L) = x_L \oplus k_L \oplus f_L\left(w_L \oplus \Phi_{k_L}(x_L \oplus k_L)\right)k_L = x_L \oplus k_L \oplus f_L\left(w_L \oplus \Phi_{k_L}(x_L)\right)k_L = x_L ,$$

because $\mathrm{Ker}\Phi_{k_L} = \{\mathbf{0}, k_L\}$. Thus, τ_L is involutory, and this also holds for τ_R.

Note that the round function $F(x)$ of DBISON can be represented as $F(x) = \left(\tau_R(x_L \oplus x_R), \tau_L(x_L)\right)$. Then, the output of the left branch is $y_L = \tau_R(x_L \oplus x_R)$, and the output of the right branch is $y_R = \tau_L(x_L)$. Since both τ_L and τ_R are involutory, we have $x_L = \tau_L(y_R)$, $x_L \oplus x_R = \tau_R(y_L)$, that is, $x_R = \tau_R(y_L) \oplus \tau_L(y_R)$. The round decryption function is $F^{-1}(y) = \left(\tau_L(y_R),\ \tau_R(y_L) \oplus \tau_L(y_R)\right)$, see **Fig. 4**. Therefore, the decryption process actually uses the reversed encryption round keys.

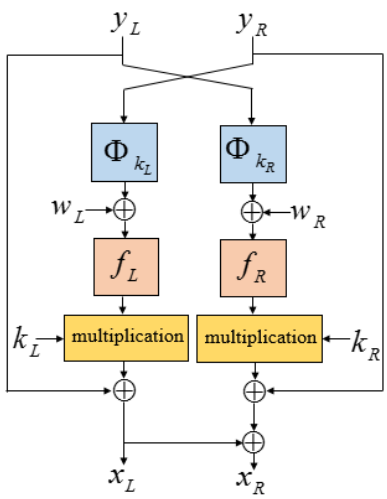


Fig. 4. The decryption round function $F^{-1}(y)$ of DBISON

6. Conclusion

In this paper, a new block cipher DBISON has been proposed, which employs double layers of a BISON-like construction. Compared to the original BISON cipher, DBISON divides the input into two halves and the nonlinear round function is computed in parallel, which results in a better performance in both software and hardware. Moreover, DBISON consisting of 3*n* rounds is provably resistant against differential and linear attacks. More precisely, it is shown the MDP is $1/2^{n-1}$ for *n* encryption rounds, and the MLP is strictly less than $1/2^{n-1}$ when (*n*/2 + 3) encryption rounds are used. Actually, if we select the data block size *n* = 258, then both MDP and MLP of DBISON are very close to the ideal value.

Appendix

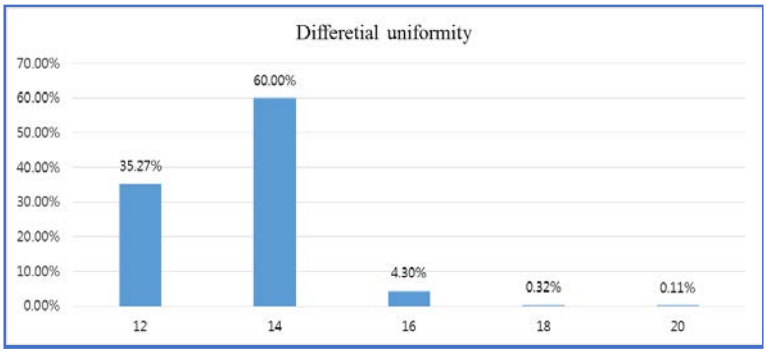
A. The truth table of a permutation F on F_2^{10} of one DBISON instance given in hexadecimal format (r = 30, differential uniformity is 12, nonlinearity is 442）

0E7	35A	324	2E8	11B	08A	29A	025	3AB	3BA	3CE	2C1	1A9	143	0F4	155
07D	10A	228	15C	177	2FB	081	2D4	28D	0A8	010	088	35C	152	142	1FA
326	056	2CB	1B7	310	1A4	0AD	0FD	11D	218	29C	186	175	1C8	257	0BB
2C2	2BE	377	208	0A6	115	189	057	092	291	1C5	238	1C1	104	3E8	0BD
11C	114	27B	293	067	06D	052	132	331	0AB	27E	16E	3D0	194	26F	122
1A0	12A	109	1BD	262	1B2	068	229	342	0D9	255	0AF	3CF	184	369	1F3
1C9	3D6	0E1	27D	2D7	290	36F	01E	384	312	11F	049	2A9	07A	007	35E
3AF	0B2	36A	008	0FF	063	034	01C	102	32B	009	268	3D3	261	08E	210
0DF	339	3E6	026	17F	19F	371	0C1	20E	1CB	2A2	2AE	045	069	370	287
289	080	11E	380	0BC	18B	0CE	2C7	2AC	265	241	121	3E1	03A	1F8	3A5
329	2A4	252	0EE	070	0D0	0E6	10C	0B3	3EB	14C	3A2	316	38D	118	1FF
292	382	3F7	03C	27C	06B	23D	283	22D	375	2DF	34A	079	062	353	3BC
0EB	0F2	16B	318	181	0E2	3ED	120	090	37D	0FC	13E	1AB	385	3B4	3B5
01F	134	21C	279	3E5	39A	191	38B	093	29D	0E4	386	311	2ED	31D	376
006	248	065	2BF	072	105	110	18D	359	1A1	270	0EC	395	0DA	2FC	0B6
13F	2CD	187	0D2	319	307	39C	3E7	3B8	32C	076	1A2	389	3FF	226	1B0
2D9	2F8	18F	12B	309	28F	15D	17A	251	3BD	2DC	3A8	123	213	05F	2B9
0D1	31A	39D	22F	18E	1A5	38C	3F4	235	346	373	0C5	335	089	1D8	1EB
3C1	1B8	39F	10B	0BF	024	29E	394	095	09E	2AB	0C3	03E	1DA	042	02A
3CA	12E	05C	02B	247	0CB	023	0A9	1FD	222	204	00A	11A	100	016	298
083	34B	349	002	305	071	0F1	148	1AC	269	328	1E2	224	0C7	084	3F9
0E0	15A	32A	21A	099	2BA	07C	147	16A	219	1AF	0F8	3DB	2B2	321	091
356	202	1FE	1F1	3A9	0FB	237	392	25E	2C6	0A7	05B	207	2F6	2F7	157
308	200	1ED	1A6	3A7	39E	139	112	3AD	1F4	3DA	1C6	350	23B	035	256
314	23A	018	01A	085	01D	30C	348	097	178	1CD	399	2FA	039	2F5	16F
337	267	1F2	201	1D2	096	37E	18C	215	2D2	0ED	082	203	153	15B	0C2

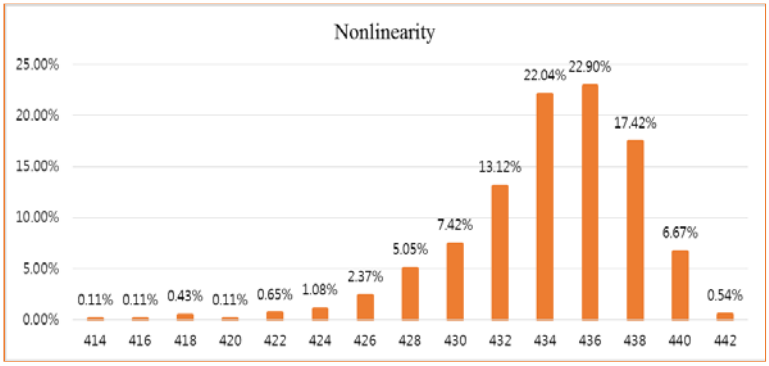
B. Test vectors with intermediate results for the DBISON instance in Appendix A. The input value is 1000011001

i	x_{L_i}	k_{L_i}	w_{L_i}	C_{L_i}	x_{R_i}	k_{R_i}	w_{R_i}	C_{R_i}	$x_{L_{i+1}}$	$x_{R_{i+1}}$
0	10000	10110	0100	1000	11001	00110	0100	1000	01001	00110
1	01001	01011	0010	0100	00110	10011	0010	1100	0111	01001
2	01111	00101	1001	0010	01001	11001	0001	1110	00110	01010
3	00110	10010	1100	1001	01010	11100	1000	1111	10000	00110
4	10000	01001	0110	1100	00110	11110	1100	0111	10110	10000
5	10110	00100	1011	0110	10000	11111	1110	1011	00110	10010
6	00110	00010	0101	1011	10010	01111	1111	0101	10100	00110
7	10100	00001	1010	0101	00110	00111	0111	1010	10101	10101
8	10101	10000	1101	1010	10101	00011	1011	1101	00000	10101
9	00000	01000	1110	1101	10101	10001	0101	0110	00100	00000
10	00100	10100	1111	1110	00000	11000	1010	0011	11100	10000
11	11100	01010	0111	1111	10000	01100	1101	1001	01100	11100
12	01100	10101	0011	0111	11100	10110	0110	0100	10000	01100
13	10000	11010	0001	0011	01100	11011	0011	0010	11100	10000
14	11100	11101	1000	0001	10000	11101	1001	0001	01100	11100
15	01100	01110	0100	1000	11100	01110	0100	1000	11110	01100
16	11110	10111	0010	0100	01100	10111	0010	1100	10010	01001
17	10010	11011	1001	0010	01001	01011	0001	1110	11011	01001
18	11011	01101	1100	1001	01001	10101	1000	1111	00111	11011
19	00111	00110	0110	1100	11011	01010	1100	0111	11100	00111
20	11100	00011	1011	0110	00111	00101	1110	1011	11011	11111
21	11011	10001	0101	1011	11111	00010	1111	0101	00110	01010
22	00110	11000	1010	0101	01010	00001	0111	1010	01100	11110
23	01100	11100	1101	1010	11110	10000	1011	1101	00010	01100
24	00010	11110	1110	1101	01100	01000	0101	0110	01110	11100
25	01110	11111	1111	1110	11100	00100	1010	0011	10110	10001
26	10110	01111	0111	1111	10001	10010	1101	1001	10101	11001
27	10101	00111	0011	0111	11001	01001	0110	0100	01100	10101
28	01100	10011	0001	0011	10101	10100	0011	0010	01101	01101
29	01101	11001	1000	0001	01101	11010	1001	0001	10100	11011

C. Distribution of the differential uniformity and nonlinearity for 20-round DBISON



(a) Distribution of the differential uniformity for 20-round DBISON



(b) Distribution of the nonlinearity for 20-round DBISON

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949. Article (CrossRef Link)

[2] M. Kanda, "Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function," in *Proc. of SAC 2000: Selected Areas in Cryptography-SAC 2000*, Ontario, Canada, pp. 324-338, 2000. Article (CrossRef Link)

[3] J. Zhang and W. L. Wu, "Authenticated encryption based on SM4 round function," *Acta Electronica Sinica*, vol. 46, no.6, pp. 1294-1299, 2018. Article (CrossRef Link)

[4] J. Daemen and V. Rijmen, *The Design of Rijndael: AES – The Advanced Encryption Standard*, Berlin, Germany: Springer, 2002. Article (CrossRef Link)

[5] M. Matsui, "New block encryption algorithm MISTY," in *Proc. of FSE 1997: Fast Software Encryption-FSE'97*, Haifa, Israel, pp. 54-68, 1997. Article (CrossRef Link)

[6] S. Vaudenay, "On the Lai-Massey scheme," in *Proc. of Advances in Cryptology-ASIACRYPT'99*, Singapore, pp. 8-19, 1999. Article (CrossRef Link)

[7] A. Hamza, D. Shehzad, M. S. Sarfraz, et al., "Novel secure hybrid image steganography technique based on pattern matching," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 3, pp. 1051-1077, 2021. Article (CrossRef Link)

[8] J. Daemen and V. Rijmen, "Security of a wide trail design," in *Proc. of Cryptology-INDOCRYPT 2002*, Hyderabad, India, pp. 1-11, 2002. Article (CrossRef Link)

[9] L. Grassi, C. Rechberger, and S. Rønjom, "Subspace trail cryptanalysis and its applications to AES," *IACR Trans. Symm.Cryptol*, vol. 2016, no. 2, pp. 192-225, 2017. Article (CrossRef Link)
[10] L. Grassi, C. Rechberger, and S. Rønjom, "A new structural-differential property of 5-round AES," in *Proc. of EUROCRYPT 2017*, Paris, France, pp. 289-317, 2017. Article (CrossRef Link)
[11] S. Tessaro, "Optimally secure block ciphers from ideal primitives," in *Proc. of ASIACRYPT 2015*, Auckland, New Zealand, pp. 437-462, 2015. Article (CrossRef Link)
[12] V. T. Hoang, B. Morris and P. Rogaway, "An enciphering scheme based on a card shuffle," in *Proc. of CRYPTO 2012*, California, USA, pp. 1-13, 2012. Article (CrossRef Link)
[13] S. Vaudenay, "The end of encryption based on card shuffling," in *Proc. of CRYPTO 2012 Rump Session*, California, USA, 2012. Article (CrossRef Link)
[14] A. Canteaut, V. Lallemand, G. Leander, et al., "BISON instantiating the Whitened Swap-Or-Not construction," in *Proc. of EUROCRYPT 2019*, Darmstadt, Germany, pp. 585-616, 2019. Article (CrossRef Link)
[15] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, pp. 3-72, 1991. Article (CrossRef Link)
[16] T. Kranz, G. Leander and F. Wiemer, "Linear cryptanalysis: key schedules and tweakable block ciphers," *IACR Trans. Symmetric Cryptol*, vol. 2017, no. 1, pp. 474-505, 2017. Article (CrossRef Link)
[17] N. T. Courtois and G. V. Bard, "Algebraic cryptanalysis of the Data Encryption Standard," in *Proc. of Cryptography and Coding 2007*, Cirencester, UK, pp. 152-169, 2007. Article (CrossRef Link)
[18] A. Canteaut and J. Roué, "On the behaviors of affine equivalent S-boxes regarding differential and linear attacks," in *Proc. of EUROCRYPT 2015*, Sofia, Bulgaria, pp. 45-74, 2015. Article (CrossRef Link)
[19] C. Li, B Sun, R. Li, et al., *Attack Methods and Instances Analysis for Block Ciphers*, Beijing, China: Science Press, 2010.
[20] X. Lai, J. L. Massey and S. Murphy, "Markov ciphers and differential cryptanalysis," in *Proc. of EUROCRYPT 1991*, Brighton, UK, pp. 17-38, 1991. Article (CrossRef Link)

Haixia Zhao is a PhD student in information security at Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education, Guilin University of Electronic Technology, Guilin, China. She has received an MS degree from Southwest University, Chongqing, China, in 2007. Her research interests include cryptographic functions and cryptanalysis of block ciphers.

Yongzhuang Wei is a professor at Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, China. He received an MS degree and PhD degree from Xidian University, Xian, China, in 2004 and 2009, respectively. His research interests include the design and analysis of symmetric encryption algorithms.

Zhenghong Liu is an associate professor at Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education, Guilin University of Electronic Technology, Guilin, China. He has received an MS degree from Guilin University of Electronic Technology, Guilin, China, in 2009. His research interests include wideband signal processing, intelligence information process, and FPGA hardware design.